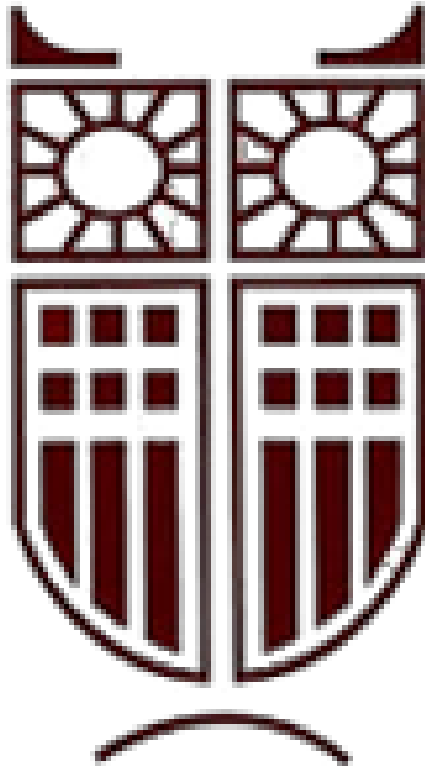


ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ



ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ, ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ο Ρόλος της Αντικατασκοπίας στην Εθνική Ασφάλεια

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΑΝΤΟΥΝΙΔΗΣ ΕΛΕΥΘΕΡΙΟΣ (Α. Μ. 1213Δ008)

ΑΘΗΝΑ, 2019

Τριμελής Επιτροπή:

Παπασωτηρίου Χαράλαμπος, Τακτικός Καθηγητής Παντείου Πανεπιστημίου
Κολιόπουλος Κωνσταντίνος, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου
Λιαρόπουλος Ανδρέας, Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς

Copyright © Αντουνίδης Ελευθέριος, 2019

All rights reserved. Με επιφύλαξη παντός δικαιώματος

Η παρούσα διατριβή αποτελεί συνιδιοκτησία του συγγραφέα και του Παντείου Πανεπιστημίου Κοινωνικών και Πολιτικών Επιστημών, ο καθένας από τους οποίους έχει δικαίωμα ανεξάρτητης χρήσης και αναπαραγωγή της (στο σύνολο ή τμηματικά) για διδακτικούς ή ερευνητικούς σκοπούς, αναφέροντας σε κάθε περίπτωση τον τίτλο, τον συγγραφέα και το ίδρυμα όπου εκπονήθηκε

***Ο Ρόλος της Αντικατασκοπίας στην Εθνική
Ασφάλεια***

Αντουνίδης Ελευθέριος

ΠΡΟΛΟΓΟΣ

Η παρούσα μελέτη εκπονήθηκε υπό τη φιλοδοξία καταγραφής του ρόλου της πληροφόρησης και ειδικότερα της αντιπληροφόρησης / αντικατασκοπίας και των σχετικών Υπηρεσιών στην προσπάθεια δόμησης ενός ικανού μηχανισμού εθνικής ασφαλείας και προώθησης κρατικών συμφερόντων.

Για ορισμένους αυτός ο ρόλος είναι αυταπόδεικτος, αλλά το αυτονόητο για κάποιους δεν είναι αυτονόητο για όλους. Περαιτέρω, δεν αρκεί να λέγεται κάτι αλλά πρέπει, επίσης, να εγγράφεται ...*scripta manent*. Ωστόσο, η ελληνική εργογραφία έχει καθυστερήσει. Πολύ λίγα έχουν κατατεθεί για την έννοια της πληροφόρησης και τις υπηρεσίες Πληροφοριών / Αντιπληροφοριών τόσο σε ευρύ εκδοτικό / εμπορικό επίπεδο όσο σε επίπεδο ακαδημαϊκής ερεύνης / συγγραφής με την τελευταία να χωλαίνει σε ακόμα πιο αξιοσημείωτο βαθμό για διαφόρους λόγους.¹

Επί τη βάσει των άνω επισημάνσεων ελπίζουμε όπως συμβάλουμε έστω κατ' ελάχιστον: α) στην κατά το δυνατό αποκρυπτογράφηση της έννοιας «πληροφόρηση», β) στη συστηματική ανάδειξη του έργου των αντιπληροφοριακών οργανισμών υπέρ εθνικών αναγκαιοτήτων, γ) στην περιεκτική αποτύπωση περιορισμών και προκλήσεων του 21^{ου} αιώνα ως προς το εξεταζόμενο ήτοι, τη σύνδεση πληροφοριών και εθνικής ασφαλείας, δ) στη συζήτηση, εντός του τελευταίου κεφαλαίου, περί του καυτού θέματος 'Ελλάς και Πληροφόρηση'. Ουσιαστικά επιθυμούμε να 'συμμαζέψουμε' αλλά και να 'ζυμώσουμε' τη διάσπαρτη δεδομένη (διεθνή) γνώση δομώντας ένα αρχικό, μεν, στέρεο, δε, θεωρητικό υπόβαθρο περί την έννοια της «πληροφόρησης» και ειδικότερα της «αντιπληροφόρησης»² αποδίδοντας την ίδια στιγμή στο κοινό και στην ελληνική εργογραφία ένα εύληπτο πρωτότυπο κείμενο / πρόταση πολιτικής εθνικής ασφαλείας, ένα κείμενο που ίσως βοηθήσει στο κτίσιμο ενός νέου τομέα σπουδών στον ελληνικό χώρο, του τομέα «Σπουδές στην Πληροφόρηση».

Δύο από τα πρόσωπα στα οποία οφείλω ευχαριστίες είναι ο τακτικός καθηγητής Διεθνών Σχέσεων Χαράλαμπος Παπασωτηρίου και ο επίκουρος καθηγητής Διεθνών Σχέσεων Ιωάννης Κωνσταντόπουλος. Ο πρώτος αποδέχτηκε την επίβλεψη της μελέτης, ο, δε, δεύτερος με εισήγαγε από ετών στο πεδίο εφοδιάζοντάς με παράλληλα με ένα πράγματι 'συνολικό' υλικό. Από κει και πέρα θεωρώ υποχρέωσή μου να αναφερθώ στον υποψήφιο διδάκτορα, φίλο και παλαιό συμφοιτητή μου Φίλιππο Κοντιζά που κριτικάρε εποικοδομητικά ορισμένα τμήματα αυτής της εργασίας. Επισημαίνω περαιτέρω τη βοήθεια κάποιων ατόμων στη διασαφήνιση κυρίως τεχνικών όρων / θεμάτων που για την ώρα επιθυμούν να παραμείνουν στην ανωνυμία -το τελευταίο δεν αφορά στον ξάδερφό μου Θεόφιλο Παπαδόπουλο, ειδικό σε ζητήματα υπολογιστικών / πληροφοριακών συστημάτων.

Τέλος, έχω χρέος να ζητήσω προκαταβολικά συγγνώμη για τα όποια στριφνά σημεία, παραλήψεις, αβλεψίες ακόμα και λάθη. Σε κάθε περίπτωση οι όποιες αστοχίες βαρύνουν αποκλειστικά τον γράφοντα.

Αντουνίδης Ελευθέριος
Αθήνα, Δεκέμβριος 2018

¹ Είναι χαρακτηριστικό πως σε επίπεδο ακαδημαϊκής ερεύνης και συγγραφής στον ελληνικό χώρο απολύτως τίποτα δεν έχει γραφεί περί την έννοια και σημασία της αντιπληροφόρησης στην προσπάθεια επίρρωσης αισθήματος εθνικής ασφαλείας

² Οφείλει να γίνει κατανοητό πως πληροφόρηση και αντιπληροφόρηση δεν αποτελούν παρά τις δύο όψεις του αυτού νομίσματος

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος	1
Περιεχόμενα.....	2
Εισαγωγή	3
1. Η θεωρία της Πληροφόρησης	
1. Περί της μελέτης της πληροφορίας / πληροφόρησης... ..	11
2. Περί της φύσεως της πληροφόρησης <i>per se</i>	27
3. Περί της θεωρίας της πληροφόρησης	47
2. Η πράξη της Αντιπληροφόρησης	
4. Περί των υπηρεσιών εθνικής Αντικατασκοπίας (Counterintelligence -CI).....	55
5. Περί της στρατιωτικής αντικατασκοπίας	84
6. Αντικατασκοπία και οικονομία.....	115
7. Αντικατασκοπία και τρομοκρατία	130
8. Αντικατασκοπία και κυβερνοχώρος	152
9. Η κλήση του 21 ^{ου} αιώνα. CI, Homeland Security, Law Enforcement	177
3. Οι περιορισμοί και το μέλλον της Πληροφόρησης και των Υπηρεσιών	
10. Τα όρια της πληροφόρησης / αντιπληροφόρησης εντός της προσπάθειας επίρρωσης περιβάλλοντος εθνικής ασφαλείας, επίτευξης κρατικών σχεδιασμών και πλήρωσης ανάλογων συμφερόντων.....	194
11. Το μέλλον της πληροφόρησης, της αντιπληροφόρησης και των Υπηρεσιών ως προς την επίρρωση περιβάλλοντος εθνικής ασφαλείας, επίτευξης κρατικών σχεδιασμών και πλήρωσης ανάλογων συμφερόντων	209
4. Πληροφόρηση και Ελλάδα	
12. Πληροφόρηση και Ελλάδα	234
Επίλογος.....	282
Αρκτικόλεξο.....	284
Βιβλιογραφία	290

ΕΙΣΑΓΩΓΗ

Οι σπουδές στην Πληροφόρηση. Το επιστημονικό υπόβαθρο

Η ανά χείρας μελέτη εντάσσεται στη χορεία αυτών που ασχολούνται με το πεδίο των Πληροφοριών και των (κρατικών) Υπηρεσιών που τις συλλέγουν / αναλύουν. Υπό ευρύτερης οπτικής σχετίζεται με τις Στρατηγικές Σπουδές τη στιγμή που οι τελευταίες αποτελούν παρακλάδι των σπουδών των Διεθνών Σχέσεων και κατ' επέκταση των σπουδών στις Πολιτικές Επιστήμες. Πάρα τούτα συζήτηση υπάρχει περί του εάν η μελέτη της Πληροφόρησης πρέπει να αυτονομηθεί ή όχι. Αίσθησή μας είναι ότι προς το παρόν αφομοιώνεται ικανοποιητικά εντός του κύκλου των Στρατηγικών Σπουδών. Τρεις κυρίως λόγοι οδηγούν σ' αυτή τη θέση, ειδικότερα: α) η σπουδή της Πληροφόρησης έχει να κάνει με σπουδή θεμάτων εθνικής / διεθνούς Ασφαλείας, άρα, στρατηγικής / μακροστρατηγικής, β) η εν λόγω σπουδή έχει σχετιστεί με την εξέταση της στρατιωτικοποιημένης όψης της εθνικής και διεθνούς πολιτικής (αν και μετά το 1990 εμφανίζεται και επισήμως δίπλα στο στρατιωτικό το οικονομικό στοιχείο) και γ) η μελέτη για την οποία κάνουμε λόγο χαρακτηρίζεται, αν όχι από έλλειψη, από καθυστέρηση παραγωγής εργογραφίας σε σχέση, τουλάχιστον, με την εργογραφία του τομέα των Διεθνών Σχέσεων και Πολιτικών Επιστημών, συνεπώς, καλώς, θεωρούμε, εγγράφεται εντός αυτού / αυτών.

Πληροφόρηση και Θεωρία Διεθνών Σχέσεων. Το θεωρητικό πλαίσιο

Η πληροφόρηση ως κατασκοπική δράση συνδέεται, όσον αφορά στη θεωρία των διεθνών σχέσεων, με τον *πολιτικό ρεαλισμό*. Το *γιατί* αναλύεται άριστα από τους Κωνσταντίνο Κολιόπουλο και Ιωάννη Κωνσταντόπουλο στα έργα *Στρατηγικός Αιφνιδιασμός. Υπηρεσίες Πληροφοριών και Αιφνιδιαστικές Επιθέσεις* του πρώτου και *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη* του δεύτερου -κατά συνέπεια δεν χρήζει περαιτέρω συλλογισμών. Αυτό στο οποίο στεκόμαστε είναι ότι η αξία της πληροφόρησης δεν αμφισβητείται από την άλλη μεγάλη θεώρηση ήτοι, τη θεώρηση του *φιλελευθερισμού*. Η διαφορά έγκειται στο ότι ο φιλελευθερισμός ως συνεργατική προσέγγιση δεν αποδέχεται (επισήμως) τη δράση των μυστικών υπηρεσιών. Οι όποιες πληροφορίες διαμεμβώνονται ελεύθερα μεταξύ κρατών στα διεθνή fora, μέσω ανοικτών πηγών, διαχειρίζονται, δε, από εθνικούς και υπερεθνικούς φορείς. Κάτι τέτοιο ασφαλώς δεν μπορεί να καλύψει κάθε ανάγκη, επιπλέον, υπάρχουν πληροφορίες που ουδέποτε ένα κράτος θα απεκάλυπτε σε κάποιο άλλο κράτος, κατά τη διάρκεια κάποιου forum ή σε κάποιον διεθνή οργανισμό.

Περί μεταθετικιστικών / μεταμοντέρνων προσεγγίσεων, επουδενί γίνεται λόγος. Ο Ralf Lillbacka αποδομεί κάθε δυνατότητα σύνδεσης της πληροφόρησης με αυτές.¹ Από τη μεριά τους οι Jill Steans και Lloyd Pettiford σημειώνουν πως υπάρχουν κριτικές οι οποίες δεν δέχονται καν την ένταξη του μεταμοντερνισμού στον κλάδο των διεθνών σχέσεων.²

Σε κάθε περίπτωση η έρευνά μας, ενώ αποδέχεται την αναμφίβολη σημασία του open sources intelligence, ερείδεται στην παραδοχή της ιδιαίτερης αξίας της γνώσης της κρυφής λεπτομέρειας και της σημαντικότητας των μυστικών υπηρεσιών ως προς την εκμείωση / ανάδειξη αυτής. Μυστική πληροφόρηση και υπηρεσίες

¹ Lillbacka R., "Realism, Constructivism, and Intelligence Analysis" στο *International Journal of Intelligence and CounterIntelligence*, Volume 26, Issue 2, 2013, σ. 305-306

² Steans Jill, Pettiford Lloyd, κ. α., *Εισαγωγή στη Θεωρία των Διεθνών Σχέσεων*, μτφρ. Μορφόπουλος Άγγελος, Τουρίκης, Αθήνα, χ. χ., σ. 229-230

Πληροφοριών στηρίζουν την εθνική πολιτική ασφαλείας. Μυστική πληροφόρηση και Υπηρεσίες δεν μπορεί παρά να σχετιστούν με τη ρεαλιστική θεώρηση.³

Κατάταξη, μεθοδολογία / μέθοδος, πηγές

Ο Stephen van Evera κατατάσσει τις διατριβές των Πολιτικών Επιστημών σε επτά κατηγορίες ήτοι, της *πρότασης θεωρίας*, του *ελέγχου θεωρίας*, της *αποτίμησης βιβλιογραφίας*, της *αποτίμησης πολιτικής ή πρότασης πολιτικής*, της *ιστορικής ερμηνείας*, της *ιστορικής αποτίμησης* και, τέλος, της *πρόβλεψης* με σκοπό την εξαγωγή συμπερασμάτων για το μέλλον μέσα από σύγχρονα γεγονότα ή θεωρούμενες ως δεδομένες μελλοντικές εξελίξεις. Περαιτέρω, αποδέχεται ένα ημιεπίσημο όγδοο πεδίο, το πεδίο της *περιγραφικής διατριβής* με την υπόσχεση ότι αυτή συνδυάζεται με τη δημιουργία, τον έλεγχο ή την εφαρμογή θεωρίας αν και φαινόμενα που δεν έχουν κατανοηθεί σε βάθος δεν δύναται, ως ο ίδιος παραδέχεται, να ερμηνευθούν / αξιολογηθούν⁴, άρα, η περιγραφή προηγείται, ίσως μάλιστα, επιτακτικά. Υπό την προϋπόθεση ότι η παρούσα μελέτη ανήκει διασταλτικά σ' αυτές της Πολιτικής Επιστήμης, πού κατατάσσεται; Θεωρούμε πως από τη στιγμή που: α) δεν προτείνουμε / ελέγχουμε μια θεωρία, β) δεν προβαίνουμε σε πολιτική / ιστορική αποτίμηση ή ιστορική ερμηνεία, γ) δεν 'προβλέπουμε', τότε, κατατάσσεται, έστω εμμέσως, στην κατηγορία μελετών πρότασης πολιτικής υπό την έννοια μιας πρότασης, ασφαλώς μεταξύ άλλων αξιόπιστων, που οφείλει / δύναται να εργαλειοποιηθεί από μια κυβέρνηση προκειμένου η τελευταία να προασπίσει την εθνική ασφάλεια / εθνικό συμφέρον της χώρας και των πολιτών που υπηρετεί. Οποσδήποτε η περιγραφή / καταγραφή είναι κάτι που χαρακτηρίζει το κείμενό μας. Αν και υπάρχουν πολιτικοί επιστήμονες που δεν την εκτιμούν ως συγγραφικό εργαλείο, στην περίπτωσή μας είναι απαραίτητη μόνο και μόνο διότι έννοιες όπως «πληροφόρηση» και «αντιπληροφόρηση» ελάχιστα έως καθόλου έχουν αποδοθεί / οριστεί από εντοπίους συγγραφείς, το ίδιο ισχύει για τη σπουδή της δράσης των Υπηρεσιών. Επιπλέον, λόγω της εξαντλητικής χρήσης και ανάλυσης δευτερευουσών πηγών το συγκεκριμένο πόνημα δύναται να καταταχθεί μεθοδολογικά στα πονήματα βιβλιογραφικής επισκόπησης / αποτίμησης του πεδίου των πληροφοριών.

Ο van Evera στο περί μεθοδολογίας έργο του εντυφά στην *ποιοτική μέθοδο έρευνας* των πολιτικών επιστημών αποδεχόμενος την καταλληλότητά της ως προς τη διαλεύκανση πολιτικών και κοινωνικών φαινομένων. Στο ίδιο μοτίβο, η έρευνά μας κατατάσσεται στις μεθοδολογικά *ποιοτικές*. Το συγκεκριμένο μοντέλο προσφέρεται ως πλέον συμβατό καθώς μια *ποσοτική, στατιστική ή content analysis* που αποδίδει το όποιο συμπέρασμα μέσω ποσοτικοποιημένων ή αριθμητικών δεδομένων δεν προσεγγίζει ικανοποιητικά το αντικείμενο *πληροφόρηση* καθώς η *υφή* του, η *μυστικότητα* που το περιβάλλει (και ο παράγοντας *ανθρώπινη φύση*) δεν πριμοδοτούν μια 'ποσοτική οδό'. Κατά τον τρόπο τούτο προβαίνουμε σε *ποιοτική ανάλυση ανοικτού τύπου* ή, αλλιώς, σε μια οιονεί *στρατηγική ανάλυση τύπου SWOT*. Μια τέτοια ανάλυση (Strengths, Weaknesses, Opportunities, Threats -SWOT), παρά το ότι χρησιμοποιείται κυρίως προς διερεύνηση οικονομικών ή επιχειρηματικών ζητημάτων,

³ Αν το θεωρητικό πλαίσιο της μελέτης δένει με τον πολιτικό ρεαλισμό, το εννοιολογικό εκκινεί από την πληροφορία: πρόκειται για έννοια εκ της οποίας απορρέουν / παράγονται άλλες όπως αυτή της πληροφόρησης και της αντιπληροφόρησης. Το ίδιο κρίσιμη, ωστόσο, είναι η έννοια της ασφαλείας. Η τελευταία αποτελεί σύνολο συνιστωσών όπως η πολιτικοστρατιωτική ασφάλεια, η οικονομική ασφάλεια, η ασφάλεια έναντι απειλών ασύμμετρου τύπου κ. λ.

⁴ van Evera, Stephen, *Εισαγωγή στη Μεθοδολογία της Πολιτικής Επιστήμης*, μτφρ. Συλογίδου Έλλη, Ποιότητα, Αθήνα, 2009⁴, σ. 147-156

δεν απάδει του εγχειρήματός μας· πρόθεσή μας καθίσταται η ανάδειξη των πλεονεκτημάτων και δυνατοτήτων μιας ικανής (αντι)πληροφόρησης (Strengths, Opportunities) χωρίς να παραλείπουμε την καταγραφή αδυναμιών (Weaknesses, Threats) που οφείλουν να τονιστούν προς αποφυγή εξελίξεων με αρνητικό αντίκτυπο σε υποθέσεις εθνικής στρατηγικής.

Η συζήτηση περί μεθοδολογίας δύναται να επεκταθεί. Θα μπορούσαμε να μιλήσουμε για μία μεικτή προσέγγιση με την ανάλυση, σύγκριση αλλά και σύνθεση στοιχείων, την αναφορά παραδειγμάτων και την αφήγηση να τίθενται στην υπηρεσία του επιχειρήματός μας με απώτερο σκοπό την οργάνωση τής περί την πληροφόρηση / αντιπληροφόρηση γνώσεως. Επίσης δεχόμενοι ότι αποδεικνύουμε τη σημαντικότητα της αντιπληροφόρησης στο κτίσιμο ενός αισθήματος εθνικής ασφαλείας μέσα από διαδρομές και σχέσεις επιμέρους συνιστωσών [πολιτική, στρατιωτική, οικονομική κ. ο. κ. αντιπληροφόρηση → πολιτική, στρατιωτική, οικονομική κ. ο. κ. (συνολική) ασφάλεια] μπορούμε να μιλήσουμε για μια μελέτη επαγωγικού τύπου ή, εκτατικά, για μία μελέτη που ακολουθεί το βασικό μεθοδολογικό δρόμο (από τα μερικά στο ολικό) μελετών *θεμελιωμένης θεωρίας* (*grounded theory*).

Αν θελήσουμε να ακολουθήσουμε μια οιονεί μεθοδολογία ή μέθοδο *χρονικού προσανατολισμού*, τότε, μπορούμε να χωρίσουμε τη μελέτη μας: α) στην μέχρι το 1990 περίοδο. Πρόκειται για περίοδο κατά την οποία κυριαρχούσαν πολιτικοστρατιωτικές έγνοιες, προκλήσεις, απειλές, β) στην περίοδο από το 1990 μέχρι το 2001. Πρόκειται για περίοδο εντός της οποίας προσετέθησαν απειλές οικονομικού τύπου, γ) στην περίοδο από το 2001 και πέρα. Πρόκειται για περίοδο εντός της οποίας στις ανωτέρω προκλήσεις ‘επισυνάφθηκαν’ προκλήσεις που σχετίζονται με την έξαρση της διεθνούς τρομοκρατίας αλλά και με το φαινόμενο της γέννησης ενός νέου τομέα ισχύος, του τομέα της κυβερνοσφαίρας.

Τονίζουμε πως διά της προσεγγίσεως αυτής θέτουμε ως χρονική αρχή μελέτης τον Β΄ Π. Π. καθώς αυτός αποτελεί σημείο εκ του οποίου εκκίνησε (ή λίγο αργότερα) η νεώτερη αναλυτική έρευνα περί την έννοια «πληροφόρηση» με πρωτοπόρο τον Αμερικανό Sherman Kent.

Αν θελήσουμε να ακολουθήσουμε μια οιονεί μεθοδολογία ή μέθοδο *ποιότητας απειλών*, τότε, μπορούμε να χωρίσουμε τη μελέτη μας: α) στο κομμάτι των σύμμετρων απειλών. Ως σύμμετρες απειλές ορίζουμε λίγο έως πολύ τις απειλές που εκπορεύονται από κρατικούς δρώντες. Αυτές αφορούν σε πολιτικοστρατιωτικά και οικονομικά ζητήματα, οφείλουν, δε, να αντιμετωπιστούν, ως απειλές εθνικής ασφαλείας, και από τις υπηρεσίες Αντιπληροφοριών, β) στο κομμάτι των ασύμμετρων απειλών. Ως ασύμμετρες απειλές ορίζουμε λίγο έως πολύ είτε τις απειλές που εκπορεύονται από μη κρατικούς δρώντες, είτε τις απειλές που «τρέχουν» στο κυβερνοδιάστημα. Αυτές αφορούν κυρίως σε τρομοκρατία ή σε έκνομες δράσεις στο «πέμπτο πεδίο ισχύος». Εναλλακτικά, αλλά πάντα σε σχέση με τρομοκρατία και κυβερνοχώρο, ασύμμετρες απειλές δύναται να θεωρηθούν αυτές που δεν αφήνουν ιδιαίτερη δυνατότητα ταυτοποίησης ή σύλληψης του δράστη, αυτές που δεν αναμένονται, αυτές που αναγκάζουν τα κράτη να κηρύξουν έναν ‘πόλεμο χωρίς εχθρό’. Οι συγκεκριμένες προκλήσεις, ως προκλήσεις εθνικής ασφαλείας, οφείλουν να αντιμετωπιστούν και από τις υπηρεσίες Αντιπληροφοριών.⁵

⁵ Περί ασύμμετρων απειλών βλέπε Ντόκος Θάνος, «Ασύμμετρες απειλές και διεθνής ασφάλεια» στο *Διεθνείς Σχέσεις. Σύγχρονη Θεματολογία και Προσεγγίσεις*, επιμ. Τριανταφύλλου Δ., Υφαντής Κ. κ. α., Παπαζήσης, Αθήνα, 2008, σ. 311-319, επίσης, Γρίβας Κωνσταντίνος, «Οι ασύμμετρες απειλές ως γεωπολιτικό φαινόμενο και ο ρόλος των Υπηρεσιών Πληροφοριών στην αντιμετώπισή τους» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας,

Ακολουθώντας αυτήν την προσέγγιση οφείλουμε να απαντήσουμε στο εξής: «Εντός των ασύμμετρων απειλών εντάσσονται μόνο απειλές εκ της τρομοκρατίας και του κυβερνοδιαστήματος;». Η απάντηση είναι *όχι*. Ασύμμετρη απειλή δύναται να θεωρηθεί η εκδήλωση μιας διεθνούς επισιτιστικής κρίσης, μια μείζων φυσική / περιβαλλοντική καταστροφή που αφορά στον πλανήτη, μια παγκόσμια επιδημία, ένα φυλετικό ή θρησκευτικό πογκρόμ «κάπου μακριά» που μεταξύ άλλων ίσως πυροδοτήσει ανεξέλεγκτη μετακίνηση πληθυσμών. Ωστόσο αυτές έχουν να κάνουν, ως προς την πρόβλεψη και αντιμετώπισή τους, περισσότερο με την ικανότητα / ετοιμότητα διαφόρων άλλων ‘πιο διαφανών’ κρατικών υποδομών (διπλωματικών, υγειονομικών, κοινωνικών, προνοίας, μεταναστευτικών κ. λ.), με ερευνητικούς επιστημονικούς σταθμούς και με διεθνείς πολιτικούς, ανθρωπιστικούς και λοιπούς οργανισμούς και οργανώσεις παρά, υποτίθεται, με μυστικές υπηρεσίες. Επιπλέον δεν θεωρούνται ‘στρατιωτικοποιημένες’ ήτοι, απειλές που ενδέχεται να απαιτήσουν, ως προς την αποσόβησή τους και σε πρώτο χρόνο, την άμεση εμπλοκή του στρατιωτικού στοιχείου ήγουν, του στοιχείου της βίας και της επιβολής.⁶

Διευκρινίζουμε ότι στην ερώτηση «είναι η οικονομική απειλή μια στρατιωτικοποιημένη απειλή;» απαντάμε πως η κλοπή, ειδικότερα, τεχνολογικών μυστικών δύναται να συντελέσει κατά τον έναν ή άλλο τρόπο στην εξέλιξη της μάχης

Αθήνα, 2009, σ. 89-95. Κάποια σημεία ωστόσο που ωφελεί να μείνουν στο μυαλό έστω και σε αδρές γραμμές είναι τα κάτωθι:

α) Κατά το αμερικανικό DoD ένας πόλεμος ορίζεται ως ασύμμετρος όταν ...οι αντίπαλοι είναι πιθανόν να προσπαθήσουν να παρακάμψουν ή να υπονομεύσουν την ισχύ των ΗΠΑ επιχειρώντας παράλληλα να εκμεταλλευτούν τις αδυναμίες τους [των ΗΠΑ] χρησιμοποιώντας μεθόδους που διαφέρουν σημαντικά από τις αμερικανικές ανάλογες. Οι ασύμμετρες προσεγγίσεις γενικά σκοπούν σε μείζον ψυχολογικό πλήγμα που θα επηρεάσει την ελευθερία κινήσεων ή τη βούληση του αντιπάλου. Κατά τις αμερικανικές Ένοπλες Δυνάμεις ...ο ασύμμετρος πόλεμος συνίσταται σε απρόβλεπτες ή μη παραδοσιακές προσεγγίσεις προκειμένου να παρακαμφθούν / υπονομευθούν οι δυνατότητες ισχύος του αντιπάλου επιχειρώντας παράλληλα την εκμετάλλευση των αδυναμιών του μέσω μη αναμενόμενων τεχνολογιών ή καινοτόμων μέσων / μεθόδων -για μια άποψη βλέπε Ντόκος Θάνος, «Ασύμμετρες απειλές και διεθνής ασφάλεια», ό. π., σ. 314.

β) Σύμφωνα με τους Steven Lambakis, James Kiras και Kristin Kolet το τι αποτελεί «ασύμμετρο» μεταβάλλεται συνεχώς. Η ασάφεια του όρου δεικνύοντας αντικείμενο συζήτησης και κριτικής έχει ωθήσει ακόμα και το DoD στη σκέψη κατάργησής του παρά, μάλιστα, τη συμβολή του σ’ αυτόν -για μια εικόνα βλέπε Lambakis S., Kiras J., Kolet K., *Understanding “Asymmetric” Threats to the United States*, National Institute for Public Policy, USA, 2002, σ. vi, 1, επίσης, M^cKenzie, Kenneth F., Jr., “The Revenge of the Melians: Asymmetric Threats and the Next QDR”, *McNair Paper*, 62, Carlisle Barracks / Pennsylvania, Νοέμβριος 2000, σ. 15, 55.

γ) Ο Κωνσταντίνος Γρίβας σημειώνει ότι ορισμός περί ασύμμετρων απειλών είναι πολύ δύσκολο έως αδύνατον να δοθεί αφού πρώτα επισημαίνει κάποιες νατοϊκές ακροβασίες στο θέμα. Κατά τον μελετητή η Βορειοατλαντική Συμμαχία συντηρεί μια στάση που τροφοδοτείται από πολιτικούς, επιχειρησιακούς και νοητικούς συμβιβασμούς και αντίστοιχες κατασκευές υπό την έποψη μιας ανάγκης δημιουργίας ενός κοινού πλαισίου (συν)εργασίας -πρόκειται για πλαίσιο / συνθήκη εντός του οποίου (συν)εργάζονται άτομα προερχόμενα από διαφορετικές χώρες και οργανισμούς κομίζοντας διαφορετικές κουλτούρες και παραστάσεις. Η συγκεκριμένη συνεργατική (συμβιβαστική, συμπληρώνουμε) απαίτηση εξυπηρετείται πολύ περισσότερο σε σχέση με μια ανάλογη απαίτηση ξεκάθαρης κατανόησης εννοιών γύρω από τη δυναμική των νέων «ασυμμετροτήτων» -περί τούτων βλέπε Γρίβας Κωνσταντίνος, «Οι ασύμμετρες απειλές ως γεωπολιτικό φαινόμενο και ο ρόλος των Υπηρεσιών Πληροφοριών στην αντιμετώπισή τους», ό. π., σ. 89, 92

⁶ ...και αφού δεν θεωρούνται στρατιωτικοποιημένες ή στρατιωτικές είναι δύσκολο να ‘συγκινήσουν’ την κοινή γνώμη. Άλλωστε μέχρι το 1990 δεν αποτελούσαν καν δευτερεύον αντικείμενο των παραδοσιακών ανησυχιών εθνικής, και όχι μόνο, ασφαλείας. Είναι γεγονός πως μέχρι πρόσφατα χαρακτηρίζονταν (ή και χαρακτηρίζονται) ως *Φαινόμενα Γκρίζας Περιοχής*, ευρίσκονταν (ή βρίσκονται) κάπου μεταξύ απειλής και μη απειλής -περί τούτων βλέπε Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, Παπαζήσης, Αθήνα, 2005, σ. 24, 32

της στρατιωτικής πρωτοπορίας, άρα, η οικονομική απειλή αυτής της μορφής είναι δυνητικά μια στρατιωτικοποιημένη απειλή. Επίσης οφείλουμε να εντοπίσουμε το σημείο όπου συναντώνται κατά κάποιο τρόπο «η συμμετρία και η ασυμμετρία των απειλών», πρόκειται για περιπτώσεις κρατικών δρώντων που προβαίνουν σε χρήση επίβουλων ασύμμετρων τακτικών.

Η έρευνά μας βασίζεται σε δυτικές αγγλόφωνες εξωτερικές πηγές τόσο πρωτογενείς που έχουν απελευθερωθεί ή ανέκαθεν κυκλοφορούσαν χωρίς περιορισμούς [αρχεία / εκδόσεις του αμερικανικού Department of Defense, του αμερικανικού στρατού, των διακλαδικών αμερικανικών δυνάμεων, αγγλοσαξονικών Υπηρεσιών και οργανισμών (CIA, The Stationery Office κ. λ.)] όσο και, κυρίως, δευτερογενείς (άρθρα, βιβλία, κείμενα επιστημονικών περιοδικών του πεδίου, σχετικές διατριβές κ. λ.)· το γεγονός αυτό ενδεχομένως καθίσταται περιοριστικό, ωστόσο, ελπίζουμε, όχι καθοριστικό. Περαιτέρω επιθυμούμε να επισημάνουμε τη συμβολή του διαδικτυακού εργαλείου και των λεγόμενων open sources ως προς την αναζήτηση δεδομένων. Τέλος, ως έχει ήδη αναφερθεί στον πρόλογο, ανεπίσημη αλλά ικανή συμμετοχή στην απάντηση ερωτημάτων έπαιξαν συζητήσεις με πρόσωπα του ακαδημαϊκού και όχι μόνο χώρου.

Τι σημαίνει «εθνική ασφάλεια»;

Πώς ορίζεται η «εθνική ασφάλεια»; Ο John Baylis υποστηρίζει ότι οι περισσότεροι μελετητές θεωρούν πως η έννοια της *ασφάλειας* δεν ορίζεται επακριβώς αν και είναι πασιφανές πως υποδηλώνει προστασία από απειλές κατά θεμελιωδών ατομικών και κοινωνικών αξιών.⁷ Ενδεικτικά αναφέρεται στους Arnold Wolfers και Barry Buzan: ο πρώτος τονίζει πως ...*ασφάλεια ως αντικειμενική ιδέα σημαίνει έλλειψη απειλών κατά επίκτητων αξιών τη στιγμή που ως υποκειμενική έννοια σημαίνει έλλειψη φόβου περί προσβολής αυτών*. Ο δεύτερος σημειώνει ότι ...*στην περίπτωση της ασφάλειας, η συζήτηση αφορά στην αναζήτηση της απαλλαγής από απειλές. Όταν η συζήτηση κινείται στο πλαίσιο του διεθνούς συστήματος η ασφάλεια αφορά την ικανότητα των κρατών και των κοινωνιών να διατηρήσουν την αυτόνομη ταυτότητα και τη λειτουργική ακεραιότητά τους*.⁸ Ο Walter Lippmann βεβαιώνει ότι ...*ένα έθνος είναι ασφαλές στο βαθμό που δεν είναι αναγκασμένο να θυσιάσει τις βασικές αξίες του προκειμένου να αποφύγει τον πόλεμο και στο βαθμό που είναι ικανό, αν το προκαλέσουν, να διατηρήσει αυτές τις αξίες μέσω νίκης σε έναν τέτοιο πόλεμο*.⁹ Ο Lippman ουσιαστικά λέει ότι ένα έθνος είναι ασφαλές όταν: α) δεν φοβάται περίπτωση υποταγής ή πολεμικής ήττας, β) δεν κινδυνεύει από κατάρρευση σε περίπτωση πολέμου και γ) είναι ικανό να αποκρούσει / κατανικήσει τον όποιο επιθετικό εις βάρος του παίκτη. Από τη μεριά τους οι Θάνος Ντόκος και Παναγιώτης Τσάκωνας επισημαίνουν πολύ εύστοχα πως έχουμε πλέον εισέλθει σε μια εποχή κατά την οποία η ασφάλεια δεν αποτελεί καθαρά και μόνο στρατιωτικό ζήτημα¹⁰ και με την έννοια της «ανθρώπινης ασφάλειας» να συζητείται ευρέως.¹¹

⁷ Baylis John, «Διεθνής και παγκόσμια ασφάλεια στην μεταψυχροπολεμική εποχή» στο *Η παγκοσμιοποίηση της διεθνούς πολιτικής*, επιμ. Baylis J., Smith St., Owens P. (επιμ. ελληνικής έκδοσης Υφαντής Κ.), Επίκεντρο, Αθήνα, 2007, σ. 391

⁸ Baylis J., ό. π., σ. 391

⁹ Booth Ken, «War, security and strategy: toward a doctrine for stable peace» στο *New Thinking About Strategy and International Security*, επιμ. Booth Ken, Harper Collins Academic, UK, 1991, σ. 344-345

¹⁰ Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, Παπαζήσης, ό. π., σ. 20-48, 188. Μάλιστα, σε πολλές περιπτώσεις, συνεχίζουν οι δύο μελετητές, η διαφορά μεταξύ εσωτερικών και εξωτερικών απειλών εθνικής ασφαλείας καθίσταται δυσδιάκριτη. Προκειμένου επίτευξης εθνικής ασφαλείας απαιτείται από τούδε και στο εξής

Αλλά σε τι αναφέρονται οι αξίες και η αυτόνομη ταυτότητα / λειτουργική ακεραιότητα ενός φιλελεύθερου κράτους; Σύμφωνα με τη (δική μας) μεθοδολογία ‘ποιότητας απειλών’ αναφέρονται στο εθνικό πολιτικό, στρατιωτικό, οικονομικό, κατ’ επέκταση κοινωνικό, status υπό την προϋπόθεση πως αυτό δεν αντιμετωπίζει απειλή όπως αυτή δύναται να περιγραφεί / εισπραχθεί. Επίσης αναφέρονται στη διατήρηση του αισθήματος ασφαλείας έναντι ασύμμετρων απειλών όπως αυτές έχουν ήδη οριστεί παραπάνω.¹²

Εντούτοις πώς δύναται, π. χ., να μορφοποιηθεί / εμφανιστεί μια πολιτική απειλή; Ως απάντηση κομίζουμε τη σειρά γεγονότων στην Ουκρανία από το 2004 και έπειτα. Τα γεγονότα αυτά διασάλευσαν την πολιτική ισορροπία στη χώρα, πυροδότησαν κάποια στιγμή εμπλοκή εξωγενών παραγόντων με κύριο αυτόν της Ρωσικής Ομοσπονδίας, μετακύλισαν εαυτόν από πολιτικά σε στρατιωτικά, προκάλεσαν την αποκοπή τμήματος της εθνικής επικρατείας (Κριμαία). Άλλο παράδειγμα δεικνύει η έκρυθμη κατάσταση στη περιοχή των Σκοπίων, ουσιαστικά από το 1990 μέχρι σήμερα. Πρόκειται για κατάσταση που απειλεί το πολιτικό μέλλον του κρατιδίου, εμπλέκει, δε, εσωγενή και εξωγενή στοιχεία. Άλλο παράδειγμα πολιτικής απειλής εκφράστηκε, μάλιστα σε real time απόδοση / μετάδοση, μέσω του στρατιωτικού πραξικοπήματος στην Τουρκία τη 15^η Ιουλίου 2016. Αν θελήσουμε να αναφερθούμε σε κράτη που δεν φημίζονται για τη δημοκρατική παράδοση, π. χ., των εκλογών, τότε, φέρουμε αμέσως στο νου τη Συρία. Η εν λόγω χώρα σπαράσσεται από το 2011 εξ αιτίας ενός πολιτικού, στρατιωτικού, ταυτόχρονα οικονομικού και κοινωνικού, εφιάλτη με δρώντες καθεστωτικές και αντάρτικες ή τρομοκρατικές ομάδες, ημεδαπούς και αλλοδαπούς μαχητές επισήμως κληθέντες ή όχι.

Αν η συζήτηση έρθει στις ασύμμετρες απειλές, τότε, η τρομοκρατία αποτελεί τη νούμερο ένα πρόκληση συμβάλλοντας και αυτή στην επανάσταση των υποθέσεων ασφαλείας (*revolution in security affairs* -RSA). Το φαινόμενο βρίσκεται σε έξαρση από το 2001, εσχάτως, δε, κάνει αισθητή την παρουσία του στην Ευρώπη συνδεδεμένο με μη κρατικούς σχηματισμούς και οντότητες που δρουν στη Μέση Ανατολή. Από τη μεριά του το κυβερνοδιάστημα, αν και δεν κάνει μέχρι στιγμής ορατό στο ευρύ κοινό το χαρακτήρα του ως πολλαπλασιαστή ευκαιρίας για δράση κατά του εθνικού συμφέροντος / ασφαλείας, αποτελεί προνομιακό χώρο επιχειρήσεων τόσο κρατικών οργανισμών όσο εξτρεμιστικών και εγκληματικών συσσωματώσεων ή μεμονωμένων κυβερνοπειρατών.

Διευκρινήσεις

- Η επιλογή του τίτλου, *Ο Ρόλος της Αντικατασκοπίας / Αντιπληροφόρησης στην Εθνική Ασφάλεια*, καταδεικνύει πως στόχο εργασίας αποτελεί η συνολική κατά το δυνατό αποτύπωση των θεωριών και των δράσεων της σύγχρονης αντικατασκοπίας / αντιπληροφόρησης (χωρίς να παραλείπεται το ευρύτερο πεδίο της πληροφόρησης) προς τη συγκεκριμένη κατεύθυνση. Επιλέξαμε αυτή την οδό

συντονισμός και συνεργασία υπουργείων (Αμύνης, Εξωτερικών), υπηρεσιών law enforcement / Ασφαλείας καθώς και πληροφοριακών οργανισμών

¹¹ ...η οποία συνδέει την ασφάλεια με τις κοινωνικές συνθήκες διαβίωσης ήτοι, τροφή, στέγη, εργασία, ιατρική περίθαλψη, δημόσια ευταξία κ. λ. -για μια άποψη βλέπε Cambone Stephen, *A New Structural for National Security Policy Planning*, CSIS, Washington, D.C., 1998, σ. 134-135

¹² Ο Arnold Wolfers σημειώνει πως οι βασικές αξίες μιας δυτικής κοινωνίας αφορούν: α) στην προστασία των πολιτών και της εδαφικής επικράτειας της χώρας, β) στη διασφάλιση της πολιτικής ανεξαρτησίας και αυτονομίας του κράτους, γ) στην επίτευξη εθνικής οικονομικής ευμάρειας και ανάπτυξης -για μια ευρύτερη εικόνα βλέπε Wolfers Arnold, “National Security as an Ambiguous Symbol” στο *Discord and Collaboration*, Johns Hopkins, Baltimore, 1962, σ. 147-165

διότι εάν δεν έχει καταγραφεί μια τέτοια μελέτη στον ελληνικό, και όχι μόνο, ακαδημαϊκό και εκδοτικό χώρο, τότε, μια επιμέρους μελέτη (στρατιωτική αντικατασκοπία, οικονομική αντικατασκοπία, αντικατασκοπία και τρομοκρατία κ. λ.) μπορεί να περιμένει.¹³ Οποσδήποτε γίνεται κατανοητό πως η προσπάθειά μας θα έβριθε ρίσκων εάν επιχειρούσε μια καθολική στο χρόνο συζήτηση περί την πληροφόρηση / αντιπληροφόρηση ήδη εμπεριέχει αρκετά από τη στιγμή που ασχολείται με το αντικείμενο στη θεωρητική του κατά το δυνατό ολότητα. Κατά την έννοια τούτη δεν εντρυνούμε στην αρχαία, στη μεσαιωνική ή στη νεώτερη πληροφόρηση / αντιπληροφόρηση αλλά στη σύγχρονη ήτοι, αυτή του 20^{ου} και 21^{ου} αιώνα αν και η φύση ή, αλλιώς, το DNA της πληροφοριακής και αντιπληροφοριακής πρακτικής δεν έχει αλλάξει ουσιαστικά στο διάβα των ετών, αυτό που αλλάζει είναι το είδος της πρόκλησης και τα μέσα διευθέτησής της.

- Ήγουν, η μελέτη κύριο σκοπό έχει να αναδείξει τη θεωρητική και πρακτική εμπλοκή της (σύγχρονης) αντικατασκοπίας στην (σύγχρονη) προάσπιση της εθνικής ασφαλείας και του εθνικού συμφέροντος.¹⁴
- Στην παρούσα το δίπολο ‘αντικατασκοπία / ασφάλεια’ γίνεται κατανοητό με τρόπο διασταλτικό. Δεν σημαίνονται μόνο αμυντικές δράσεις. Σημαίνονται επίσης προωθημένες / επιθετικές, άλλωστε, *η καλύτερη άμυνα είναι η επίθεση*. Εξάλλου μελετητές όπως ο George P. Morse, ο Mark Reagan, ο Robert P. Hanssen, ο Christopher Felix, ο Angelo Codevilla, ο A. C. Wasemiller, η Michelle van Cleave κ. α. αφήνουν να εννοηθεί πως η αντικατασκοπία συνδέεται ή πρέπει να συνδέεται κυρίως, αν όχι αποκλειστικά, με την ‘επίθεση’, ότι έχει ή οφείλει να έχει την τελευταία ως απώτερο στόχο -σ’ αυτήν την περίπτωση ο όρος counterintelligence μεταβάλλεται στον όρο counterespionage.
- Κάθε έρευνα περί πληροφοριών και Υπηρεσιών κατατρύχεται από το εμπόδιο της μυστικότητας που φυσιολογικά διακρίνει τον χώρο. Η συγκεκριμένη τροχοπέδη δεν δύναται να αποφευχθεί παρά για ελάχιστους, μάλλον, ερευνητές.
- Όπου Υπηρεσίες με Υ κεφαλαίο νοούνται οι μυστικές υπηρεσίες / πληροφοριακοί οργανισμοί. Εναλλαγή λέξεων όπως πληροφορία - πληροφόρηση, θεωρία - θεώρηση, πληροφόρηση - intelligence, αντικατασκοπία - αντιπληροφόρηση - counterintelligence, κυβερνοχώρος - κυβερνοδιάστημα ή σημείων στίξεως όπως «» - ‘’ κ. λ. παρατηρείται μόνον προς αποφυγήν λεκτικών επαναλήψεων ή επαναλήψεων αναγνωστικών συμβόλων.
- Η προσπάθειά μας δεν δύναται φυσικά να καλύψει όλες τις επιχειρησιακές όψεις του πεδίου *αντικατασκοπία*. Κινείται στη λογική της ανάλυσης των κατά τεκμήριο σημαντικότερων ή, αλλιώς, αυτών που κυριαρχούν στο ενδιαφέρον της διεθνούς βιβλιογραφίας.
- Το κυρίως κείμενο αποτελείται από τέσσερα μέρη. Το πρώτο (κεφ. 1 - 3) ασχολείται με τη μελέτη, τη φύση και εν γένει τη θεωρία της πληροφόρησης, το δεύτερο (κεφ. 4 - 9) με την πράξη της αντικατασκοπίας, το τρίτο (κεφ. 10 - 11)

¹³ Στην ηλεκτρονική διεύθυνση <http://ethos.bl.uk/Home.do> βρίσκονται ανηρτημένοι χιλιάδες τίτλοι διατριβών, πολλές εκ των οποίων διατίθενται σε μορφή PDF, εκπονημένων στη Βρετανία και σε διάφορες περιόδους. Έρευνα στην οποία προβήκαμε το Μάιο του 2015 κατέδειξε περί τις εβδομήντα πέντε (75) μελέτες σχετικές, αμέσως ή εμμέσως, με την πολιτικοστρατιωτική κατασκοπία. Εντύπωση προκαλεί το γεγονός της παρουσίας μόνο πέντε εργασιών αφιερωμένων στην αντικατασκοπία εκ των οποίων οι τρεις τη συνδέουν, μάλλον, με τον έτερο πληροφοριακό κλάδο -ουσιαστικά μόνο δύο αναφέρονται αμιγώς στο counterintelligence

¹⁴ Πολλές φορές διά λόγους πολιτικής ορθότητας το εθνικό συμφέρον ταυτίζεται με την επίτευξη εθνικής ασφαλείας ήτοι, με αμυντικούς σχεδιασμούς. Δεν είναι αρκετό. Το εθνικό συμφέρον ενδέχεται να απαιτήσει επίσης την εκτέλεση επιθετικών, μυστικών ή και ‘κατακριτέων’ τακτικισμών

με τα όρια του πληροφοριακού τομέα όπως και τις προκλήσεις που αυτός καλείται να αντιμετωπίσει στον 21^ο αιώνα, το, δε, τέταρτο (κεφ. 12) δεικνύει κατάθεση στο ερώτημα περί του ελληνικού πληροφοριακού συστήματος και των τρόπων βελτιστοποίησής του. Στο τέλος των κεφαλαίων παρατίθενται απόψεις, συμπεράσματα ή προτάσεις.

Τονίζουμε ότι εντός της έννοιας *εθνική πληροφόρηση / αντιπληροφόρηση* δύναται να εμπεριέχεται κάθε είδους πολιτική, στρατιωτική, οικονομική ή άλλη πληροφόρηση. Ουσιαστικά κάθε ‘σημαντική’ πληροφορία είναι πληροφορία εθνικής ενδεχομένως σημασίας ασχέτως πολιτικού, στρατιωτικού κ. λ. προσανατολισμού, άλλωστε, πολιτικό, στρατιωτικό και οικονομικό πεδίο διαπλέκονται. Μένοντας στο ζήτημα καταγράφουμε τις τρεις, κατά τον Νίκο Κυριαζή, πληροφοριακές ενότητες ήτοι, α) την πληροφόρηση επί θεμάτων αμύνης ή, κατά Edward Waltz, εθνική πληροφόρηση, β) την πληροφόρηση επί θεμάτων στρατιωτικού ενδιαφέροντος και γ) την στρατιωτική πληροφόρηση. Η πρώτη, και ευρύτερη, αφορά σε ζητήματα πολιτικής και διπλωματίας, η τρίτη σε καθαρά στρατιωτικά θέματα τακτικού επιπέδου, ενώ η δεύτερη αποτελεί το μέσο χώρο μεταξύ πρώτης και τρίτης.¹⁵ Σημειώνουμε ότι το πολιτικό σύστημα κάθε χώρας εξαρτά το που θα δοθεί η ‘πληροφοριακή πρωτοκαθεδρία’ ήτοι, αν θα δοθεί στις πολιτικές ή στις στρατιωτικές κρατικές Υπηρεσίες.

¹⁵ Κυριαζής Νίκος, Σπανός Στέλιος, *Το Πρόσωπο του Πολέμου στον 21^ο Αιώνα*, Εστία, Αθήνα, 2000, σ. 135

ΚΕΦΑΛΑΙΟ 1

Περί της μελέτης της πληροφορίας / πληροφόρησης

I am confident that the history of World War II will eventually be rewritten, integrating analysis of the impacts of ULTRA, the Double Cross system, special operations, and the rest, for many documents are open. Together with official histories, they provide a basis for cross-questioning the testimony in autobiographies and trial records. Eventually, the new details will be pieced together with the old, altering the panorama

Ernst R. May¹

Περί της διεθνούς μελέτης της πληροφορίας. Οι αρχικοί πρωταγωνιστές

Οι ερευνητές Martin Alexander και Huw Dulan σε άρθρο τους, το 2013, στο *Intelligence and National Security* τονίζουν την αποδοχή και στήριξη της μελέτης της πληροφορίας εκ μέρους της κοινότητας των Ιστορικών Σπουδών. Μέσω αυτής κατανοείται βαθύτερα το παρελθόν καθώς μεταφερόμαστε «στην άλλη πλευρά του λόφου» με ό,τι αυτό ενδέχεται να σημαίνει. Κατά την έννοια τούτη το ιστορικό μάθημα ζυμώνεται με έναν καινοφανή όσο και παραγνωρισμένο παράγοντα που δρα καταλυτικά ως προς την αποκρυπτογράφηση της αλήθειας.

Όμως αν όλοι, λίγο ή πολύ, αντιλαμβανόμαστε την έννοια της πληροφορίας στα καθ' ημάς, πώς αυτή νοείται σε επίπεδο διεθνών διαμοιβών; Οι λεγόμενες *Σπουδές στην Πληροφόρηση* απαντούν, με θεμιτή τη σύνδεσή τους με τον τομέα της Ιστορίας² και των Διεθνών Σχέσεων.³

Οι σπουδές για τις οποίες κάνουμε λόγο φέρουν στο τραπέζι τέσσερις ομάδες: αυτή των ιστορικών επιστημόνων, των πολιτικών επιστημόνων, των ερευνητών με επιχειρησιακή πείρα (π. χ. πρώην παραγόντων της πληροφοριακής κοινότητας) και, τέλος, διαφόρων ανεξαρτήτων μελετητών, συγγραφέων, δημοσιογράφων κ. λ. Η κυριαρχία των πρώτων μέσω μορφών όπως ο Donald Watt, ο Christopher Andrew, ο Wesley Wark, ο John Gaddis κ. λ. είναι πρόδηλη.⁴ Ακριβώς αυτοί είναι που θέτουν μια πρώτη βάση ανάγνωσης και ενσωμάτωσης της πληροφορίας εντός του πλαισίου

¹ May E., "The importance of interchange. Studying and Teaching Intelligence" στο *Studies in Intelligence*, Volume 38, Number 5, 1995

² Κατά τον Adam Svendsen οι σπουδές στην πληροφόρηση ξεπήδησαν από τους τομείς της Διεθνούς Ιστορίας, των Στρατηγικών Σπουδών, του Δικαίου και της Κοινωνιολογίας -για περισσότερα βλέπε Svendsen Ad., "Connecting Intelligence and Theory: Intelligence Liaison and International Relations" στο *Intelligence and National Security*, Volume 24, Number 5, 2009, σ. 705

³ Οι Michael Fry και Miles Hochstein αναφέρουν πως ο καθηγητής John Gaddis εξέφρασε, παλαιότερα, έναν προβληματισμό αλλά και μια ελπίδα. Ο πρώτος σχετίζεται με μια μάλλον πενιχρή παρουσία και αποδοχή των πληροφοριακών αναφορών εντός και από το πεδίο των Διεθνών Σχέσεων. Από την άλλη, το ενθαρρυντικό στοιχείο έχει να κάνει με μια αναβαθμισμένη εμφάνιση, από τα μέσα της δεκαετίας του 1980, σχετικών μελετών σε επίπεδο πανεπιστημιακών / ερευνητικών συγγραμμάτων -για μια καλύτερη άποψη βλέπε Fry M., Hochstein M., "Epistemic communities: Intelligence studies and international relations" στο *Intelligence and National Security*, Volume 8, Number 3, 1993, σ. 14, επίσης, Alexander Martin, Dulan Huw, "A Century of Intelligence (1909-2009): International Perspectives" στο *Intelligence and National Security*, Volume 28, Number 3, 2013, σ. 297-298

⁴ Fry M., Hochstein M., "Epistemic communities: Intelligence studies and international relations", ό. π., σ. 14. Οι Fry και Hochstein σημειώνουν από τη μία την κυρίαρχη παρουσία των ιστορικών και από την άλλη την ελλιπή αντίστοιχη των πολιτικών επιστημόνων εντός των ομάδων που ασχολούνται με την μελέτη της πληροφορίας· η παραγνώριση της αξίας της τελευταίας εντός του ευρύτερου χώρου της Πολιτικής Επιστήμης και των Διεθνών Σχέσεων γίνεται φανερή τουλάχιστον μέχρι ενός χρονικού σημείου

των θεωρητικών επιστημών ⁵ αφήνοντας πίσω τα όποια ηθικά διλήμματα που παρεμπόδιζαν την ακαδημαϊκή ενασχόληση μ' αυτήν.⁶

Κάτι τέτοιο καθόλου δεν σημαίνει πως η αποστολή είναι εύκολη. Η πρόσβαση σε στοιχεία, και δη και αξιόπιστα, δεν είναι ό,τι πιο απρόσκοπτο. Η σύμπραξη, επίσης, των επιστημονικών ειδικοτήτων δεικνύει ένα ερώτημα. Πέρα των ιστορικών, εντός του χώρου ανακαλύπτουμε αξιομνημόνευτα πρόσωπα των Πολιτικών Επιστημών: Richard Betts, Loch Johnson, Michael Handel, Roy Godson, Len Scott, Peter Jackson κ. α. Ασφαλώς δεν πρέπει να ξεχνάμε τη συνεισφορά των κλασικών των Διεθνών Σχέσεων όπως του Raymond Garthoff, του Alexander George ή του Robert Jervis -γίνεται αντιληπτό πως η επίτευξη 'συμφωνίας' μεταξύ όλων δεν είναι κάτι που προκύπτει αυτομάτως παρά την κοινή μήτρα από την οποία προέρχονται. Τέλος, ενώ από τα μέσα / τέλη της δεκαετίας του 1970 οι σπουδές περί ζητημάτων ασφαλείας γνώρισαν άνθηση (με κορύφωση του debate την περίοδο 1989-1991), οι εξελίξεις δεν συμπαρέσυραν σε αντίστοιχο ρυθμό τη σπουδή της πληροφορίας χωρίς αυτό να σημαίνει πως δεν παρουσιάστηκε μια εγρήγορση.⁷

Σταθμοί στη διεθνή πληροφοριακή μελέτη

Μέχρι τα τέλη της δεκαετίας του 1980 ένα πέπλο κρυψίνοιας επί πληροφοριακών ζητημάτων στο δυτικό ευρωπαϊκό, και όχι μόνο, κόσμο καθιστά ολοφάνερη την ύπαρξή του με κάποιες συζητήσεις ή συγγραφικές απόπειρες να λαμβάνουν χώρα αραιά και που. Υπό αυτών των συνθηκών, η ακαδημαϊκή κοινότητα αρνούμενη να ασχοληθεί με το θέμα δεν αποτελεί εξαίρεση με ελάχιστους τολμηρούς να επιχειρούν κατά περιόδους κάποια ανοίγματα. Μετά την πτώση των κομμουνιστικών καθεστώτων η διάθεση σταδιακά αλλάζει με αρχειακό υλικό να δίδεται εκ μέρους των Υπηρεσιών όλο και πιο συχνά στη δημοσιότητα.⁸ Από το 2001 ο αγγλοσαξονικός κόσμος φαίνεται να ακολουθεί ένα γοργότερο τέμπο με έναν αριθμό Πανεπιστημίων να ιδρύουν και να διατηρούν τμήματα σπουδών στην πληροφόρηση αξιοποιώντας τις νέες συνθήκες και απαιτήσεις που γεννιούνται⁹ όσο και αν μελετητές σαν τη Jennifer Sims παρουσιάζονται φειδωλοί, επιφυλακτικοί ή απαιτητικότεροι ως προς τους ζητούμενους ρυθμούς ανάπτυξης του πεδίου. Η έννοια της *ασφάλειας* και οι ανάγκες που προκύπτουν μελετώνται όλο και περισσότερο από το ακαδημαϊκό και πολιτικό επιτελείο. Ο καθηγητής Christopher Andrew βεβαιώνει πως οι Osama bin Laden και

⁵ Ο Donald Watt αναφέρεται στη δημιουργία μιας πρώτης ξεχωριστής αγγλικής σχολής περί τη σπουδή της πληροφόρησης γύρω στα μέσα της δεκαετίας του 1980. Πρόκειται για σχολή που δομείται υπό δύο κλάδων, τον κλάδο της *Στρατιωτικής Ιστορίας* και τον αντίστοιχο της *Ιστορίας των Διεθνών Σχέσεων* -για περισσότερες λεπτομέρειες βλέπε Watt Donald, "Intelligence Studies: The Emergence of the British School" στο *Intelligence and National Security*, Volume 3, Number 2, 1988, σ. 338. Ο Michael Herman μας προτρέπει να αντιληφθούμε τις σπουδές στην πληροφόρηση ως ...*μείξη της ιστορικής μελέτης με τη μελέτη και πράξη των πληροφοριακών οργανισμών, και [συνεχίζει] μην ανησυχείτε περαιτέρω γύρω από (περι)ορισμούς*

⁶ Fry M., Hochstein M., "Epistemic communities: Intelligence studies and international relations", ό. π., σ. 14-15

⁷ ό. π., σ. 15-17

⁸ Άλλωστε και όσον αφορά στις βρετανικές αρχές ήταν μόλις το 1992 που παραδέχτηκαν επίσημα την ύπαρξη εξωτερικής υπηρεσίας Πληροφοριών στη διάθεση της κυβέρνησης. Μέχρι τότε ούτε ένα έγγραφο δεν είχε απελευθερωθεί από την Joint Intelligence Committee -JIC, την υπεύθυνη αρχή που κατευθύνει τις δράσεις των πληροφοριακών οργανισμών στη Βρετανία -για περισσότερα βλέπε Andrew C., "Intelligence, International Relations and 'Under-Theorization'" στο *Intelligence and National Security*, Volume 19, Number 2, 2004, σ. 172

⁹ Scott L., "Sources and Methods in the Study of Intelligence: A British View" στο *Intelligence and National Security*, Volume 22, Number 2, 2007, σ. 185

Saddam Hussein κατάφεραν να μεταλλάξουν τη συνήθη βρετανική πολιτική μη λογοδοσίας και σιωπής όταν τα ερωτήματα έφταναν να αγγίζουν και τον άγνωστο κόσμο των Υπηρεσιών. Αποτέλεσμα τούτου υπήρξε η έκθεση τμήματος της διαμοιβής των μυστικοσυμβουλίων μεταξύ πολιτικών αρχών και παραγόντων εθνικής ασφαλείας στην κοινή γνώμη και στη δημόσια κριτική -κάπως έτσι καταλήξαμε στο σάλο που ξέσπασε μόλις ένα μήνα μετά τον Μάρτιο του 2003 με την, κατά πολλούς, χαλκευμένη κατηγορία ύπαρξης όπλων μαζικής καταστροφής στο ιρακινό στρατόπεδο να πλανάται.¹⁰

Αν εξετάσουμε λεπτομερέστερα το ζήτημα θα διαπιστώσουμε πως ο διάλογος περί την πληροφορία ενέσκηψε πρώτα στην Αμερική (γύρω στις αρχές της δεκαετίας του 1950) και μετά την παρουσίαση του έργου του Sherman Kent *Strategic Intelligence for American World Policy* (1949).¹¹ Στα μέσα της δεκαετίας του 1970 το *The Double-Cross System in the War of 1939 - 1945* του J.C. Masterman και το *The Ultra Secret* του F.C. Winterbotham έπαιξαν αντίστοιχο ρόλο στη Βρετανία.¹² Πρέπει να περιμένουμε το 1984 προκειμένου δύο εξέχουσες καθηγητικές προσωπικότητες να επικαλεστούν τον σερ Alexander Cadogan περί την χαμένη διάσταση της πληροφόρησης στη μελέτη των διακρατικών υποθέσεων¹³ -αναφερόμαστε στους Christopher Andrew και David Dilks και στο, υπό την επιμέλειά τους, έργο *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*. Από κείνη τη στιγμή η ανάπτυξη των πληροφοριακών σπουδών ως υποπεδίο των Διεθνών Σχέσεων παίρνει, κατά πολλούς, αργά αλλά σταθερά το δρόμο της.¹⁴

¹⁰ Scott L., Jackson P., "The Study of Intelligence in Theory and Practice" στο *Intelligence and National Security*, Volume 19, Number 2, 2004, σ. 139-140

¹¹ ό. π., σ. 140

¹² Goodman M., "Studying and Teaching About Intelligence: The Approach in the United Kingdom" στο *Studies in Intelligence*, Volume 50, Number 2, 2006, σ. 57. Περαιτέρω, η ανάμειξη της CIA στο πραξικόπημα κατά του Αλιέντε στη Χιλή και το σκάνδαλο Watergate πιέζει την αμερικανική κοινωνία και τους θεσμούς προς επιζήτηση μεθόδων ελέγχου των Υπηρεσιών. Μέχρι το τέλος της δεκαετίας συστήνεται ένα πλήθος εξεταστικών επιτροπών στην αμερικανική Βουλή, εμφανίζεται ένα κύμα θεωριών συνωμοσίας, ξεσπά η ιρανική επανάσταση, ακόμα και ένας αριθμός φιλμ της μεγάλης οθόνης τροφοδοτεί τη λαϊκή φαντασία. Εντός αυτού του κλίματος κάτι ξεκινά να κινείται στον ακαδημαϊκό περίγυρο των ΗΠΑ έστω και υπό μίας χαώδους μορφής. Στη Βρετανία το πρώτο περί την πληροφορία ακαδημαϊκό πρόγραμμα εγκαινιάζεται από τον σερ Francis Hinsley το 1969 στο Κέμπριτζ για να τον ακολουθήσει πολύ αργότερα (δεκαετία του 1990) στον ίδιο χώρο ο Christopher Andrew. Τη δεκαετία του 1980 δραστηριοποιείται ο καναδικός CASIS (Canadian Association for Security and Intelligence Studies) ενώ ο αμερικανικός ISA (International Studies Association) ιδρύει το Intelligence Studies Section. Την ίδια περίοδο πρωτοεκδίδονται το *Intelligence and National Security* (Βρετανία 1986, υπό τους Christopher Andrew και Michael Handel) και το *International Journal of Intelligence and CounterIntelligence* (ΗΠΑ 1987, υπό τον Reese Brown) -για όλα αυτά βλέπε Rudner M., "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand" στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 1, 2009, σ. 111-112. Συμπληρώνουμε ότι έχουν προηγηθεί έντυπα όπως το *Studies in Intelligence* (1955, υπό την αιγίδα της CIA) ή το *American Intelligence Journal* (1982, υπό την U.S National Military Intelligence Association)

¹³ ...και ειδικότερα των πολιτικών, διπλωματικών και στρατιωτικών επεισοδίων -για περισσότερα βλέπε Evans G., Newnham J., *The Penguin Dictionary of International Relations*, Penguin Books, 1998, σ. 256. Σ' αυτό ακριβώς το σημείο ανακαλείται στη μνήμη η πρόσκληση / πρόκληση, μάλιστα εν έτει 1960, του Peter Dorando προς την αμερικανική ακαδημαϊκή κοινότητα περί δημιουργίας ...ενός βασικού προγράμματος σπουδής της πληροφόρησης, της σημαντικότητάς της στην εκπόνηση πολιτικών και επιχειρησιακών πλάνων, του τρόπου εμπλοκής της στα πεπραγμένα, των αρχών και των διαδικασιών μέσω των οποίων παράγεται και μοιράζεται. Ένα τέτοιο πρόγραμμα οφείλει να αναπτύξει αρχές ικανές να εφαρμοστούν σε κάθε πεδίο -για μια ιδέα ανέτρεξε στο Dorando P., "For College Courses in Intelligence" στο *Studies in Intelligence*, Volume 4, Number 3, 1960, A15-A19

¹⁴ Scott L., Jackson P., "The Study of Intelligence in Theory and Practice", ό. π., σ. 140

Στο πρώτο, εν έτει 1986, τεύχος του *Intelligence and National Security* αναφέρεται πως κάποιες περιοχές της μοντέρνας Ιστορίας και των Πολιτικών Επιστημών παραμένουν στο ερευνητικό λυκόφως -πρόκειται για περιοχές των οποίων η μελέτη απαιτεί γνώση σχετικά με τη δράση των Υπηρεσιών όπως και την επίδραση της πληροφόρησης στην υψηλή πολιτική / στρατηγική.¹⁵ Κάτι τέτοιο, επιμένει το περιοδικό, δεν μπορεί να συνεχιστεί υπονοώντας πως τίποτα δεν καθιστά το πεδίο των πληροφοριών ακατάλληλο προς ακαδημαϊκή διερεύνηση τη στιγμή που ο σύγχρονος σχεδιασμός εξωτερικής πολιτικής και πολιτικής ασφαλείας υποχρεούνται να εστιάζει στο κάθε τι που μια επεξεργασμένη πληροφορία ενδέχεται να κομίσει.¹⁶ Ελάχιστα χρόνια αργότερα, η κατάρρευση του σοβιετικού καθεστώτος ήρθε να απλοποιήσει τα πράγματα. Η προηγούμενη μυστικοπάθεια και αδιαφάνεια αποτελούσε όλο και πιο διαχειρίσιμο, ως έναν βαθμό, εμπόδιο. Η δεκαετία του 1990 έπεισε πολλούς πως οι χώρες μπορούσαν να απεμπλακούν από παλιές διπολικές έγνοιες¹⁷ -ακόμα και αν ίσχυε κάτι τέτοιο ο Σεπτέμβριος του 2001 φρόντισε να

¹⁵ Ο καθηγητής Martin Rudner γράφει πως το όλο πρόβλημα περιστρέφεται γύρω από τρεις πυλώνες. Πρόκειται γι' αυτόν της μυστικότητας που χαρακτηρίζει το χώρο των Υπηρεσιών, γι' αυτόν της διστακτικότητας των ακαδημαϊκών να εμπλακούν με ένα αμφιλεγόμενο αντικείμενο και, τρίτον, γι' αυτόν που αφορά σε φοβίες διαφόρων προσώπων περί υπονόμησης και αργότερα εξάρτησης του επιστημονικού τους έργου από την Πληροφοριακή Κοινότητα -για περισσότερα βλέπε Rudner M., "CANADA: Intelligence studies in higher education" στο *University World News* και στην ιστοσελίδα <http://www.universityworldnews.com/article.php?story=2009011717424810> από όπου αντλήσαμε στοιχεία τη 13^η Δεκεμβρίου 2013. Πέραν τούτου η Jennifer Sims καταθέτει την άποψη κορυφαίου, όπως τονίζει χωρίς όμως να κατονομάζει, καθηγητή των Διεθνών Σχέσεων σύμφωνα με την οποία η πληροφορία δεν μπορεί (ή δεν αξίζει) να μελετηθεί. Η ίδια αναφέρεται στο γεγονός της έλλειψης διδακτορικών διατριβών στο αντικείμενο (τουλάχιστον κατά την περίοδο 2001-2006 και εντός του αμερικανικού χώρου) όπως και στην έλλειψη σχετικών άρθρων εντός περιοδικών και εκδόσεων (κατά την πρώτη δεκαετία του 21^{ου} αιώνα) που ασχολούνται με τις διεθνείς σχέσεις -για περισσότερα βλέπε Sims J., "Defending adaptive realism. Intelligence theory comes of age" στο *Intelligence Theory. Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, UK, 2009, σ. 151

¹⁶ Βλέπε στο editorial του *Intelligence and National Security*, Volume 1, Number 1, 1986, σ. 3

¹⁷ ...σε τέτοιο βαθμό, ωστόσο, που εμφανίστηκε μια μερική αδιαφορία / οπισθοδρόμηση ως προς τις συγκεκριμένες σπουδές παρά τις θετικές προοπτικές έρευνας που τις περιέβαλαν -περί τούτου βλέπε Campbell St., "A Survey of the U. S. Market for Intelligence Education" στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 2, 2011, σ. 308. Μάλιστα το 1991 δεν συμπεριλήφθηκαν στην εκπαιδευτική ατζέντα του National Security Education Act των ΗΠΑ -για περισσότερα στοιχεία βλέπε στο <http://www.intelligence.senate.gov/davidlborennationalsecurityact.pdf> στον οποίο ανατρέξαμε την 23^η Νοεμβρίου 2013. Βέβαια η CIA μέσω του Center for the Study of Intelligence φρόντιζε να καλλιεργεί την επαφή μεταξύ των practitioners και των academics προκειμένου να ενταχθεί η πληροφορία σε τμήματα / σχολές των Διεθνών Σχέσεων. Μέχρι το τέλος του 20^{ου} αιώνα υπολογίζεται πως 200 με 300 ανάλογα προγράμματα είχαν παρουσιαστεί ή παρουσιάζονταν στα αμερικανικά κολλέγια και πανεπιστήμια με έναν αριθμό αντίστοιχων βρετανικών, καναδικών, ευρωπαϊκών και ισραηλινών ιδρυμάτων να ακολουθεί έστω από μακριά. Το 2001 εμφανίζεται στην ηπειρωτική Ευρώπη το *Journal of Intelligence History* υπό την αιγίδα του International Intelligence History Association (Γερμανία), το 2007 ακολουθεί το *European Journal of Intelligence Studies*, παράγωγο ολλανδοβελγικής συνεργασίας, τη στιγμή που περιοδικά όπως το *Foreign Policy*, το *Foreign Affairs*, το *International Security*, το *Survival* ή το *Political Science Quarterly* φιλοξενούν όλο και πιο συχνά στις σελίδες τους άρθρα που σχετίζονται στον έναν ή άλλο βαθμό με την πληροφόρηση -περί τούτων βλέπε Rudner M., "CANADA: Intelligence studies in higher education", *University World News*, ό. π., Rudner M., "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand", ό. π., σ. 112-113, Varouhakis M., "What is Being Published in Intelligence? A Study of Two Scholarly Journals" στο *International Journal of Intelligence and CounterIntelligence*, Volume 26, Issue 1, 2013, σ. 176 και Κωνσταντόπουλος Ι., Δόγα Αλεξάνδρα, "The (R)evolution of Intelligence as an Academic Discipline: Challenges and Constraints" στο *Journal of Mediterranean and Balkan Intelligence*, Volume 5, Number 1, 2015, σ. 5-7

ανανεώσει ή να αντικαταστήσει / επανακαθορίσει τους φόβους τους.¹⁸ Κατ' αυτή την έννοια η σπουδή της πληροφορίας μετατρέπεται σε ανάγκη που σχετίζεται με την αγωνία των κυβερνήσεων για ακριβή ενημέρωση επί καινοφανών και όχι μόνο απειλών αλλά και με τη φιλοδοξία τμήματος του ακαδημαϊκού τομέα για άνοιγμα του πεδίου και της αντίστοιχης γνώσης. Ο Michael Goodman υποστηρίζει πως τα συμβάντα της πρώτης δεκαετίας της νέας χιλιετηρίδας έχουν καταστήσει την πληροφορία ακρογωνιαίο λίθο πολιτικής ανάλυσης / σχεδιασμού και δράσης είτε αυτή αφορά σε αμυντικούς είτε σε επιθετικούς σκοπούς -ως αποτέλεσμα απαιτείται μια περαιτέρω εντρύφηση στο αντικείμενο.¹⁹

Μεθοδολογίες και προγράμματα μελέτης. Προσκόμματα και προοπτικές

Κατά τον Donald Watt η σπουδή της πληροφορίας χωρίζεται σ' αυτήν της εν καιρώ πολέμου και σ' αυτήν της εν καιρώ ειρήνης. Τα δύο είδη υποδιαιρούνται σε τρία τμήματα ήτοι, στο τμήμα της σπουδής της συλλογής, της ανάλυσης και, τέλος, της αξιοποίησης ή, αλλιώς, της εμπλοκής της πληροφόρησης στην υψηλή στρατηγική.²⁰ Ο ερευνητής Adam Svendsen αντιλαμβάνεται τα πράγματα υπό μίας ευρύτερης οπτικής. Ορμώμενος από την έκφραση «only connect» που χρησιμοποιεί ο Βρετανός μυθιστοριογράφος E. M. Forster εντός της νουβέλας με τίτλο *Howards End*, δηλώνει πως ένα είδος «συνδεσιμότητας» πρέπει να συνέχει τις δραστηριότητες των Υπηρεσιών με τη θεωρητική μελέτη. Όσον αφορά στην τελευταία, δεν καλείται να σχετιστεί μόνο με τα υποπεδία της πληροφόρησης (συλλογή, ανάλυση κ. λ.) αλλά και με τα πεδία των διεθνολογικών, διπλωματικών, πολιτικών, οικονομικών σπουδών -κάτι τέτοιο, μας λέει, δεν υιοθετείται ακόμα στον πρόπονα βαθμό. Ο Michael Goodman συμφωνεί αναζητώντας την εξήγηση στο ότι η σπουδή της πληροφορίας: α) δεικνύει σχετικά πρόσφατο αντικείμενο και β) αυτοπεριορίζεται σε ό,τι ενδιαφέρει τις ΗΠΑ σε επίπεδο πολιτικών απαντήσεων συρρικνώνοντας τον ορίζοντά της -ο Svendsen προτείνει ως λύση μια ενεργητικότερη διασύνδεση του πεδίου με τον τομέα των Διεθνών Σχέσεων και των σχετικών θεωριών.²¹

Ο Thomas Stafford υιοθετεί μια άποψη βάσει της οποίας η μελέτη κάθε ζητήματος που αφορά στο χώρο πρέπει να απαντά σε τρεις ερωτήσεις, ήτοι: α) γνωρίζουμε τα πάντα γύρω από αυτό το ζήτημα; β) αν δεν γνωρίζουμε τα πάντα, τότε, τι είναι αυτό που γνωρίζουμε; γ) ποιες οι πηγές μας; Περαιτέρω, υποθέτοντας πως κάποια στοιχεία περιέπεσαν στα χέρια μας, απαιτείται: α) μια ικανότητα συμπύκνωσης (ή και απομείωσης) του όγκου δεδομένων, β) μια διαβεβαίωση ενός ελαχίστου στάνταρ αντικειμενικότητας αυτών, γ) μια γνώση περί της βαρύτητάς τους τόσο σε επίπεδο εσωτερικής όσο και εξωτερικής πολιτικής, δ) μια δυνατότητα «τυποποίησης» ή

¹⁸ ...κάτι που κατά τον Michael Herman είχε περαιτέρω αντίκτυπο στην αποδοχή (και, άρα, σπουδή) της πληροφορίας -για μια άποψη βλέπε Herman Michael, *Intelligence Services in the Information Age*, Frank Cass Publishers, Λονδίνο, 2001, σ. 228

¹⁹ Goodman M., "Studying and Teaching About Intelligence: The Approach in the United Kingdom", ό. π., σ. 57. Ωστόσο δεν πρέπει να παραβλέψουμε το γεγονός της σταδιακά όλο και πιο αυστηρής νέας αμερικανικής νομοθεσίας γύρω από προϋποθέσεις απελευθέρωσης εγγράφων και πληροφοριών σχετικών με κρατικές δραστηριότητες. Η κυβέρνηση Bush, Jr θεώρησε πως κατ' αυτόν τον τρόπο διαφυλάσσεται η εθνική ασφάλεια σε μια περίοδο που ο πόλεμος κατά της τρομοκρατίας είχε φουντώσει -για το θέμα βλέπε Diaz-Matey, G., *Intelligence studies at the dawn of the 21st century: New possibilities and resources for recent topic in international relations*, Research Unit on International Security and Cooperation (UNISCI), Madrid, 2005, σ. 12-13

²⁰ Watt D., "Intelligence Studies: The Emergence of the British School", ό. π., σ. 339

²¹ Svendsen Ad., "Connecting Intelligence and Theory: Intelligence Liaison and International Relations", ό. π., σ. 704

«κατηγοριοποίησης» εντός ενός εκ των τεσσάρων πεδίων της εξηγητικής του διαδικασίας. Τα μοντέλα / προσεγγίσεις του στη μελέτη του πεδίου καταδεικνύουν τη συστηματικότητά του -αναφερόμαστε σ' αυτά της ιστορικής / βιογραφικής, της λειτουργικής, της δομικής και της πολιτικής προσέγγισης.²²

Ο Καναδός Wesley Wark επεκτείνει τη σκέψη του Thomas Stafford χτίζοντας στις κατευθύνσεις του Αμερικανού. Εφευρίσκει οκτώ μεθοδολογικές παραμέτρους (methodologies / projects) σπουδής του αντικειμένου, ειδικότερα: α) την *ερευνητική μεθοδολογία* (research project) αξιοποιώντας πρωτογενείς πηγές και αρχειακό υλικό, β) την *ιστορική μεθοδολογία* (historical project) με σκοπό την *περιπτωσιολογική μελέτη*, γ) την *προσδιοριστική μεθοδολογία* (definitional project) με φιλοδοξία τον ορισμό της πληροφορίας, δ) την *προσδιοριστική μεθοδολογία* σε συνδυασμό με την *περιπτωσιολογική μελέτη* (fourth perspective) προκειμένου να ελεγχθεί η θεωρία στην πράξη, ε) τη μεθοδολογία *χρήσης απομνημονευμάτων και αυτοβιογραφιών* (memoirs methodology). Οι υπόλοιπες τρεις μεθοδολογίες αφορούν στον έλεγχο της συμβατότητας της δράσης των Υπηρεσιών σε σχέση / αντιδιαστολή με τις αστικές ελευθερίες (civil liberties project), στη δημοσιογραφική έρευνα (investigative journalism) και, τέλος, στην καταγραφή δημοφιλών μυθοπλασιών όπως μυθιστορήματα, κινηματογραφικές παραγωγές κ. λ. και στον τρόπο που αυτές επιδρούν στην λαϊκή κουλτούρα (popular culture project).²³

Οι Len Scott και Peter Jackson καταθέτουν πως, γενικά, υιοθετούνται τρεις οδοί / κατευθύνσεις. Η πρώτη, ιδιαίτερα δημοφιλής στην κοινότητα των ιστορικών, εκλαμβάνει την πληροφόρηση ως καίρια προσλαμβάνουσα προκειμένου να εξηγηθούν αποφάσεις της πολιτικής ηγεσίας. Η δεύτερη ερευνά τους λόγους επιτυχιών και αποτυχιών των Υπηρεσιών δίδοντας βαρύτητα στην πληροφοριακή διαδικασία και κυρίως στη διαδρομή από την ανάλυση μέχρι τη λήψη απόφασης. Ασχολείται με τη σημασία των προκαταλήψεων, των εσφαλμένων αντιλήψεων, της *πολιτικοποίησης* (politicization) κ. λ. με την ελπίδα εύρεσης τρόπων αποκάθαρσης / βελτίωσης του τελικού προϊόντος. Η τρίτη κατεύθυνση ελέγχει την πληροφορία όχι ως καταλύτη δράσεων υπέρ της εθνικής ασφαλείας ή των σχεδιασμών της εξωτερικής πολιτικής ενός κράτους αλλά ως μοχλό εσωτερικής πίεσης εκ μέρους του τελευταίου επί της κοινωνίας με στόχευση στον έλεγχό της.²⁴

Ο Martin Rudner προτείνει τρία κύρια προγράμματα (core, cognate και optional) ανωτάτου επιπέδου βασισμένα στη διεπιστημονική (interdisciplinary / multidisciplinary) μεθοδολογία καταδεικνύοντας τη σύνδεση της σπουδής της πληροφορίας με μια γκάμα άλλων σπουδών επί θεμάτων ασφαλείας, πολιτικής,

²² Stafford Th., "Assessing current intelligence studies" στο *International Journal of Intelligence and CounterIntelligence*, Volume 2, Issue 2, 1988, σ. 217-239, επίσης, Svendsen Ad., "Connecting Intelligence and Theory: Intelligence Liaison and International Relations", ό. π., σ. 720, Goodman M., "Studying and Teaching About Intelligence: The Approach in the United Kingdom", ό. π., σ. 57, Rudner M., "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand", ό. π., σ. 113, Campbell St., "A Survey of the U. S. Market for Intelligence Education", ό. π., σ. 326- 328, Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, Polity Press, USA, 2012², σ. 1-6

²³ Goodman M., "Studying and Teaching About Intelligence: The Approach in the United Kingdom", ό. π., σ. 59, Wark Wesley, "Introduction: The Study of Espionage: Past, Present, Future?" στο *Espionage: Past, Present, Future?*, επιμ. Wark K. Wesley, Frank Cass & Co. Ltd., Great Britain, 1994, σ. 1-9

²⁴ Scott L., Jackson P., "The Study of Intelligence in Theory and Practice", ό. π., σ. 143-144, Tiberiu Tanase, "The study of Intelligence in the Euro-Atlantic area" στη διαδικτυακή τοποθεσία http://www.upm.ro/facultati_departamente/stiinte_litere/conferinte/situl_integrare_europeana/Lucrari3/istorie/98_Tanase_TIberiu.pdf (σ. 980-981) εις την οποία ανατρέξαμε την 21^η Ιουλίου 2016

οικονομίας κ. λ.²⁵ Οι Γάλλοι Eric Denécé και Gáld Arboit αναφέρονται σε τρία patterns μελέτης: της καταγραφής της επιχειρησιακής δράσης, της διαδρομής της πληροφορίας από τη συλλογή μέχρι την απόδοσή της και, τέλος, της σχέσης κράτους και Υπηρεσιών με τις τελευταίες να υπηρετούν το πρώτο. Ο επίσης Γάλλος ναύαρχος Lacoste υιοθετεί έντεκα θεματικές ξεκινώντας από την ιστορική αποτύπωση και τεκμηρίωση (*documentation*) φτάνοντας μέχρι το πρόβλημα των αστικών ελευθεριών ή της ηθικής και της δεοντολογίας που αναπτύσσεται γύρω από την Κοινότητα της Πληροφόρησης.²⁶ Όσον αφορά στη Γερμανία επισημαίνουμε πως οι σπουδές σε θέματα εσωτερικής και διεθνούς Ασφαλείας, στρατιωτικής Ιστορίας και πληροφοριών ελάχιστη πρόοδο παρουσιάζουν τουλάχιστον μέχρι τα μέσα της πρώτης δεκαετίας του 21^{ου} αιώνα. Ως αιτία φέρεται η δράση της χώρας κατά το πρώτο μισό του 20^{ου} αιώνα, μια δράση και αποτέλεσμα που προκάλεσαν απέχθεια έναντι οιοδήποτε στρατικοποιημένου αντικειμένου. Αν και μετά την κομμουνιστική κατάρρευση οι σπουδές περίξ της ασφαλείας απογειώθηκαν διεθνώς, κανείς Γερμανός ακαδημαϊκός δεν θέτει εαυτόν εντός της λίστας των ειδικών του *intelligence*. Περαιτέρω, πολύ λίγα έχουν γίνει γνωστά για τον πόλεμο μεταξύ της δυτικογερμανικής BND και της ανατολικογερμανικής Stasi ενώ, κατά τον Krieger Wolfgang, γεγονός αποτελεί ότι η Γερμανία δεν έτρεφε, γενικά, ιδιαίτερη εκτίμηση στην αξία των Υπηρεσιών.²⁷

Εκ των ανωτέρω γίνεται κατανοητό πως η σπουδή του αντικειμένου δύναται να ακολουθήσει τον έναν ή τον άλλο δρόμο. Επίσης κατανοείται πως κάποιες τάσεις ομοιάζουν ή επικαλύπτονται, πως κάποιες άλλες ίσως εμφανιστούν στο τοπίο. Αν θελήσουμε, ωστόσο, να καταγράψουμε την πορεία της μελέτης στις ΗΠΑ και στη Βρετανία, τότε, δεν μπορούμε παρά να την τοποθετήσουμε, σε γενικές γραμμές, εντός της πολιτικής και της ιστορικής, αντιστοίχως, προσέγγισης.²⁸ Βέβαια, είναι αμφίβολο αν και κατά πόσο απασχολεί η σπαζοκεφαλιά της ταξινόμησης σε σχέση με την υπαρκτή ακόμα απροθυμία των κοινωνικών επιστημών να την αποδεχτούν -είναι χαρακτηριστικό πως ένας από τους πατριάρχες του χώρου, ο Christopher Andrew, δηλώνει ότι ...*η ρίζα του προβλήματος έχει να κάνει με μια «γνωστική δυσαρμονία» (cognitive dissonance). Πρόκειται για τη δυσκολία των παραδοσιακών σχολών των*

²⁵ Rudner M., "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand", ό. π., σ. 119-122. Περί διεπιστημονικότητας του πεδίου βλέπε και στο Κωνσταντόπουλος Ι., Δόγα Αλεξάνδρα, "The (R)evolution of Intelligence as an Academic Discipline: Challenges and Constraints", ό. π., σ. 6. Στο ίδιο και στις σελίδες 9-13 καταγράφεται η γεωγραφική διάσταση της μελέτης σύμφωνα με την οποία: α) οι δυτικές φιλελεύθερες δημοκρατίες βρίσκονται στην πρωτοκαθεδρία της σπουδής των πληροφοριών, β) οι «νέες δημοκρατίες» έπονται αντιμετωπίζοντας / προσπαθώντας να λύσουν συστημικά / δομικά προβλήματα (αποδοχή, χρηματοδότηση, έλλειψη ερευνητικού υλικού -βλέπε παράδειγμα Ρουμανίας) που καθιστούν την ανάπτυξη του τομέα ανεμική και γ) οι «άλλες χώρες / καθεστώτα», εκτιμώντας ιδιαίτερος την έννοια της μυστικότητας, δεν αφήνουν περιθώριο εξέλιξης εκτός ενός αυστηρά θεσμοθετημένου «επαγγελματικού, κυβερνητικού / υπηρεσιακού» πλαισίου

²⁶ Denécé E., Arboit G., "Intelligence Studies in France" στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 4, 2010, σ. 743-744

²⁷ Krieger Wolfgang, "German Intelligence History: A Field in Search of Scholars" στο *Intelligence and National Security*, Volume 19, Number 2, 2004, σ. 185-198

²⁸ Goodman M., "Studying and Teaching About Intelligence: The Approach in the United Kingdom", ό. π., σ. 59, επίσης, Scott L., "Sources and Methods in the Study of Intelligence: A British View", ό. π., σ. 199-200, Marrin St., "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful" στο *Intelligence and National Security*, Volume 27, Number 3, 2012, σ. 414-416 και "Improving Intelligence Studies as an Academic Discipline" του ίδιου στο *Intelligence and National Security* στη δικτυακή τοποθεσία <http://www.tandfonline.com/doi/pdf/10.1080/02684527.2014.952932> όπου καταφύγαμε τη 14^η Ιανουαρίου 2015

*Διεθνών Σχέσεων και των Ιστορικών / Πολιτικών Σπουδών να λάβουν υπόψη τη διαθέσιμη, πλέον, πληροφορία σχετικά με το ρόλο των Υπηρεσιών.*²⁹

Αλήθεια είναι λοιπόν πως αν και από τα μέσα της δεκαετίας του 1980 η πληροφορία εξελίσσεται ως υποπεδίο των Διεθνών Σχέσεων δεν έχει ακόμα κατακτήσει μια ευρέως καθιερωμένη θέση. Ίσως ορισμένοι υποστηρίζουν το τυχαίο της κατηγοριοποίησής της εντός του συγκεκριμένου χώρου από τη στιγμή που θα μπορούσε να σχετιστεί με την Ιστορική ή την ευρύτερη Πολιτική Επιστήμη, ίσως ορισμένοι διακηρύζουν πως μ' αυτούς τους τομείς μπορεί να συνδεθεί αρτιότερα. Όπως και να έχει, σχεδόν δέκα χρόνια αργότερα, οι Michael Fry και Miles Hochstein επιμένουν πως ...*μια φανερή αποτυχία των σπουδών των Διεθνών Σχέσεων να ενσωματώσουν την πληροφόρηση εξακολουθεί να λαμβάνει χώρα*³⁰ με τον Christopher Andrew να επαναλαμβάνει στα μέσα της πρώτης δεκαετίας του νέου μιλένιουμ την προ εικοσαετίας ένστασή του. Υπό αυτών των συνθηκών δεν είναι απορίας άξιο το γεγονός της απουσίας της από τις εργασίες των περισσότερων θεωρητικών των Διεθνών Σχέσεων, είτε αυτοί πρόσκεινται στο θετικισμό, είτε όχι -μάλιστα, υπάρχουν παραδείγματα αμφισβήτησής της ακόμα και εντός του ρεαλιστικού μοντέλου.

Το πρόβλημα της υπο-θεωρητικοποίησης / υπο-εκπροσώπησης της πληροφορίας στη μελέτη της Ιστορίας και των Διεθνών Σχέσεων

Μέχρι πρόσφατα ο ρόλος της πληροφόρησης στις παγκόσμιες υποθέσεις παρέμενε στη σκιά των παραδοσιακών ερευνών περί τις διεθνείς σχέσεις. Είναι κρίμα ότι χρειάστηκαν γεγονότα όπως αυτό στο Περλ Χάρμπορ το 1941, οι αποκαλύψεις των Operation Chaos και COINTELPRO το 1974, οι τρομοκρατικές επιθέσεις της 11^{ης} Σεπτεμβρίου και τα λάθη περί την ύπαρξη όπλων μαζικής καταστροφής στο Ιράκ το 2002 προκειμένου να αποκαλυφθεί η σημαντικότητά της. Τουλάχιστον το κοινό (και ίσως κάποιοι θεωρητικοί των Διεθνών Σχέσεων) φαίνεται έτοιμο να αναγνωρίσει την ανάγκη της κατανόησης της 'κρυφής πλευράς των κυβερνήσεων'.³¹

Παράδειγμα Α

Ο Ρίχαρντ Ζόρχε γεννήθηκε στο Μπακού του Αζερμπαϊτζάν από Γερμανίδα μητέρα και Ρώσο πατέρα. Μεγάλωσε στη Γερμανία συμμετέχοντας με το γερμανικό στρατό στον Α' Π. Π. Το 1919 προσχωρεί στην Κομιντέρ η οποία πέρα από συντονιστικό όργανο του διεθνούς κομμουνιστικού κινήματος λειτουργεί ως δεξαμενή στρατολόγησης υπέρ των σοβιετικών μυστικών υπηρεσιών. Το 1924 μεταβαίνει στη Μόσχα και εκπαιδεύεται ως πράκτορας. Το

²⁹ Andrew C., "Intelligence, International Relations and 'Under-Theorization'", ό. π., σ. 174, Haines G., "An Emerging New Field of Study: US Intelligence" στο *Diplomatic History*, Volume 28, Number 3, 2004, σ. 442. Τόσο ο Andrew όσο και οι James Der Derian, Len Scott και Peter Jackson έχουν αναφερθεί στην υποεκπροσώπηση της πληροφορίας στο χώρο των σπουδών γύρω από τον ψυχρό πόλεμο (την Ιστορία γενικότερα) και τις Διεθνείς Σχέσεις. Οι δύο τελευταίοι επισημαίνουν πως τα μόνα πρόσωπα που δείχνουν ενδιαφέρον είναι αυτά που ασχολούνται με θεωρίες λήψης αποφάσεων τη στιγμή που οι scholars των διαφόρων διεθνολογικών τμημάτων δεν φαίνεται να τη λαμβάνουν ιδιαιτέρως υπόψη -για περισσότερες λεπτομέρειες βλέπε Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, Ποιότητα, Αθήνα, 2010, σ. 34-35. Ο Derian παρατηρεί ότι η πληροφορία δεικνύει το πλέον παραμελημένο συστατικό στη σπουδή των Διεθνών Σχέσεων ...*intelligence is the least understood and most undertheorized area of international relations*, γράφει -για περισσότερα βλέπε Scott L., Jackson P., "The Study of Intelligence in Theory and Practice", ό. π., σ. 141

³⁰ Fry M., Hochstein M., "Epistemic communities: Intelligence studies and international relations", ό. π., σ. 14

³¹ Loch Johnson στο *Toward a Theory of Intelligence. Workshop Report*, επιμ. Treverton Gregory, Jones Seth, Boraz Steven, Lipsy Phillip, RAND, Santa Monica, 2006, σ. 12

1929 εντάσσεται στο προσωπικό των σοβιετικών Υπηρεσιών ενώ το 1933 δέχεται την αποστολή στην Ιαπωνία με σκοπό τη δημιουργία ενός πληροφοριακού δικτύου υπέρ του Κρεμλίνου. Τον Ιούνιο του 1941 ξεσπά πόλεμος μεταξύ Γερμανίας και ΕΣΣΔ. Οι γερμανικές δυνάμεις πλησιάζουν στη Μόσχα με τον Στάλιν να μη γνωρίζει τις προθέσεις των Ιαπώνων. Χιλιάδες στρατιώτες και πλήθος τεθωρακισμένων μεραρχιών βρίσκονται στην Άπω Ανατολή με σκοπό την απόκρουση μιας ιαπωνικής εισβολής. Το Κρεμλίνο επικοινωνεί με τον Ζόργκε ζητώντας να μάθει περί των σχεδιασμών του Τόκιο. Ο Ζόργκε τα καταφέρνει απολύτως καλά αποστέλλοντας το ακόλουθο μήνυμα: «Η Ιαπωνία δεν πρόκειται να κηρύξει πόλεμο στη Σοβιετική Ένωση». Η τελευταία, βάσει αυτής ακριβώς της διαβεβαίωσης, αποσύρει δυνάμεις από τα ανατολικά της χώρας ενισχύοντας το ευρωπαϊκό μέτωπο, καταφέροντας να αναστρέψει την εικόνα των επιχειρήσεων. Ο Ζόργκε συλλαμβάνεται σχεδόν αμέσως από την ιαπωνική αντικατασκοπία και καταδικάζεται σε θάνατο. Απαγχονίζεται την 7^η Νοεμβρίου 1944.³²

Παράδειγμα Β

Από το Φεβρουάριο του 1945 και μετά τη Β' Σύνοδο Κορυφής στη Γιάλτα της Ουκρανίας όλοι γνωρίζουν πως το τέλος του Β' Π. Π. αποτελεί ζήτημα χρόνου. Σε όλες τις φωτογραφίες της Συνόδου οι Τσώρτσιλ, Ρούζβελτ και Στάλιν απεικονίζονται καθιστοί και αυτό διότι ο Αμερικανός πρόεδρος βρίσκεται καθηλωμένος σε αναπηρικό αμαξίδιο. Ελάχιστοι, είναι αλήθεια, περίμεναν ότι ο Ρούζβελτ θα έφτανε μέχρι τη Γιάλτα. Πράγματι λίγο μετά, τη 12^η Απριλίου 1945, αποβιώνει. Από τα μέσα του 1944 και με την υγεία του να επιδεινώνεται μέρα με τη μέρα, οι στενοί του συνεργάτες θορυβούνται. Βάσει του Συντάγματος των ΗΠΑ, σε περίπτωση θανάτου του Προέδρου αναλαμβάνει ο αντιπρόεδρος της κυβέρνησης. Τη συγκεκριμένη θέση κατέχει ο Χένρι Ουάλας, εκπρόσωπος της αριστερής πτέρυγας του κόμματος και φιλοσοβιετικός. Ο Ουάλας υποστηρίζει μια αμερικανοσοβιετική μεταπολεμική συμφωνία θεωρώντας πως η Αμερική έχει πολλά περισσότερα κοινά με τη Ρωσία παρά με παρηκμασμένες αποικιοκρατικές δυνάμεις όπως η Γαλλία και η Αγγλία. Παράλληλα, προετοιμαζόμενος για τον επικείμενο θάνατο του Ρούζβελτ, συντάσσει την επόμενη κυβέρνηση με σκοπό την τοποθέτηση ανθρώπων του σε καίριες θέσεις. Μεταξύ αυτών βρίσκονται οι Λόρενς Ντάγκαν και Χάρι Ντέξτερ Γουάιτ, προαλειφόμενοι για τις θέσεις των επικεφαλής στα υπουργεία Εξωτερικών και Οικονομίας αντιστοίχως. Ωστόσο, τον Ιούλιο του 1944 οι εσωκομματικοί αντίπαλοι του Ουάλας κατά τη διάρκεια του πανεθνικού συνεδρίου των Δημοκρατικών ηγούνται ενός πραξικοπήματος. Ο Ουάλας καθαιρείται με συνοπτικές διαδικασίες, στη θέση του τοποθετείται ο Χάρι Τρούμαν. Ο τελευταίος, εκπροσωπώντας τη συντηρητική πλευρά του κόμματος, θεωρείται καταλληλότερος για την ανάληψη της προεδρίας των ΗΠΑ. Η αντικατάσταση του Ουάλας δεν είναι παρά μια από τις συγκλονιστικότερες ενδοκομματικές ανατροπές έως σήμερα με παγκόσμιες, μάλιστα, προεκτάσεις. Κατά τον τρόπο τούτο στον προεδρικό θώκο των ΗΠΑ ανεβαίνει ο αντικομμουνιστής Τρούμαν συντελώντας στην έναρξη του ψυχρού πολέμου. Αν ο Ρούζβελτ είχε αποβιώσει κάποιους μήνες ενωρίτερα, τότε, πρόεδρος των Ηνωμένων Πολιτειών θα γινόταν ο Ουάλας. Τι θα σήμαινε αυτό; Ίσως μια φιλοσοβιετική εξωτερική πολιτική από την Ουάσιγκτον, ίσως κάτι περισσότερο. Όλα αυτά τα γνωρίζουμε σήμερα βάσει αδιάσειστων ντοκουμέντων σύμφωνα με τα οποία τόσο ο Λόρενς Ντάγκαν όσο και ο Χάρι Ντέξτερ Γουάιτ ήταν πράκτορες των Σοβιετικών με κωδικά ονόματα Frank, ο πρώτος, Jurist, ο δεύτερος. Ως απόδειξη κομίζεται η αποκρυπτογράφηση τριών χιλιάδων σοβιετικών τηλεγραφημάτων στο πλαίσιο υποκλοπών του προγράμματος Venona που δημοσίευσε το πανεπιστήμιο Γέιλ το 2000. Τα συμβάντα επιβεβαιώνονται, επίσης, από έρευνα του καθηγητή Christopher Andrew, έρευνα βασισμένη σε αρχεία της KGB που βρέθηκαν στα χέρια του μέσω των βρετανικών μυστικών υπηρεσιών και, κυρίως, μέσω του πρώην αρχειοθέτη της σοβιετικής Υπηρεσίας

³² Deakin F., Storry G., "The Journalist: Richard Sorge, the Spy Who Tricked Hitler", *Famous Soviet Spies: The Kremlin's Secret Weapon*, επιμ. Newman J., US News & World Report, Ουάσιγκτον, 1973, σ. 24-61 και Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, Ποταμός, Αθήνα, 2015, σ. 46-48

Βασίλι Μιτρόκιν. Ο Γουάιτ πεθαίνει το 1948 εξ αιτίας καρδιακού επεισοδίου, ο Ντάγκαν αυτοκτονεί το ίδιο έτος. Και οι δύο βρίσκονταν λίγο πριν την παραπομπή σε δίκη με την κατηγορία της κατασκοπίας.³³

Τα δύο παραδείγματα είναι χαρακτηριστικά της αξίας και της συμβολής των μυστικών υπηρεσιών και των πληροφοριών στη διαμόρφωση και στην κατανόηση των ιστορικών δρώμενων. Στην πρώτη περίπτωση, μια πληροφορία άλλαξε, ίσως, τη ροή του Β' Π. Π. Στη δεύτερη, η σοβιετική προσπάθεια δεν καρποφόρησε, ωστόσο, καταδεικνύεται μια λεπτομέρεια της οποίας η μελέτη προσδίδει άλλες διαστάσεις στην αντίληψη των πραγμάτων. Ο ρόλος των πληροφοριών και των οργανισμών που ασχολούνται μ' αυτές είναι πολύ συχνά σημαντικός, ενίοτε, δε, καταλυτικός επί γεγονότων και εξελίξεων που σφραγίζουν την Ιστορία. Πάρα ταύτα, σπάνια ερευνάται / μεταφέρεται εντός ιστοριογραφίας, πολιτικών μελετών και αναλύσεων -πρόκειται για το φαινόμενο της υπο-θεωρητικοποίησης ή υπο-εκπροσώπησης της πληροφορίας στη μελέτη της Ιστορίας και των Διεθνών Σχέσεων. Κατ' αυτόν τον τρόπο: α) καίριες λεπτομέρειες ενός πεπραγμένου παραμένουν στο ημίφως ή στο σκοτάδι, β) στρεβλώνεται καθοριστικά η ερευνητική πορεία / μελέτη σημαντικών περιστατικών. Αν αυτό δεικνύει τη μια πλευρά του προβλήματος, την ακαδημαϊκή, μια άλλη είναι, κατά τη γνώμη μας, ιδιαιτέρως βαρύνουσα: η μη απόδοση των οφειλομένων στην πληροφόρηση δεν επιτρέπει την ανάπτυξη κρατικής κουλτούρας πληροφοριών. Ομιλούμε για μια κουλτούρα / αντίληψη που το πολιτικό, κυρίως, προσωπικό οφείλει να αποκτήσει αν θέλει να συμπληρώσει τις προϋποθέσεις που οδηγούν ορθώς τη διαδικασία λήψεως αποφάσεων.

Άλλο κύριο εμπόδιο ανάπτυξης των σπουδών στο χώρο συνιστά, κατά τον Diaz-Matey, η έλλειψη πρωτογενών πηγών και αρχείων. Σχεδόν το σύνολο των Υπηρεσιών παγκοσμίως αρνείται να αποχαρακτηρίσει φακέλους που θεωρεί καυτούς ή αν κάνει κάτι τέτοιο το κάνει με ιδιαίτερη επιφυλακτικότητα. Προσοχή πρέπει να δοθεί επιπλέον στην ποιότητα των παραγόμενων εργασιών και της νέας εργογραφίας καθώς το μυστήριο που περιβάλλει τα σχετικά ζητήματα ενδέχεται να οδηγήσει σε υπερβολές.³⁴ Οι Fry και Hochstein όπως και ο Ιωάννης Κωνσταντόπουλος παρουσιάζονται πιο αναλυτικοί υποστηρίζοντας πως τα προβλήματα που αντιμετωπίζει η μελέτη συνοψίζονται ή συνοψίζονταν, κυρίως, στα κάτωθι: α) στην επικέντρωση των πληροφοριακών σπουδών στην προ του 1945 περίοδο τη στιγμή που η κοινότητα των Διεθνών Σχέσεων μελετά την αμέσως επόμενη, β) στον εγκλωβισμό εντός των διπόλων ΗΠΑ-ΕΣΣΔ και CIA-KGB, γ) στη μη διάθεση πραγματικής εμβάθυνσης ακόμα και από θεωρητικούς της ρεαλιστικής αποτίμησης, δ) στην άρνηση, σε ικανό βαθμό ακόμα, της κοινότητας των Διεθνών Σχέσεων να εμπλακεί με ένα αντικείμενο μη ιδιαίτερου θεωρητικού υποβάθρου. Η τελευταία υποστηρίζει πως τίποτα δεν εντάσσει την πληροφορία εντός των υπαρχουσών διεθνολογικών μεθοδολογιών, απορρίπτει, δε, την ανάγκη δημιουργίας νέου πλαισίου αντίληψης προκειμένου να την ενσωματώσει.³⁵

³³ Andrew C., Mitrokhin V., *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, Basic Books, New York, 2000, σ. 109, Klehr H., *VENONA: Decoding Soviet Espionage in America*, Yale University Press, USA, 2000, σ. 141-142, 201-204, Bostdorf D., *Proclaiming the Truman Doctrine: The Cold War Call to Arms*, Texas A&M University Press, USA, 2008, σ. 31-37 και Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 13-17

³⁴ Diaz-Matey, G., *Intelligence studies at the dawn of the 21st century: New possibilities and resources for recent topic in international relations*, ό. π., σ. 14

³⁵ Fry M., Hochstein M., "Epistemic communities: Intelligence studies and international relations", ό. π., σ. 17-18 και Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 200-201

Όσο διεξοδικοί εμφανίζονται οι ανωτέρω τόσο συνοπτικοί είναι οι Graham Evans και Jeffrey Newnham. Πολύ απλά, λένε, η φύση του εγχειρήματος και οι περιορισμοί κάτω από τους οποίους λειτουργούν οι Υπηρεσίες δεν επιτρέπουν την απρόσκοπτη εξέλιξη της μελέτης.³⁶ Μαζί τους συναινεί η Amy B. Zegart καταθέτοντας, περαιτέρω, μια επιπλέον άποψη: η έλλειψη θεωρητικής βάσης ή, αλλιώς, θεωρίας πληροφόρησης απομειώνει τη θέληση για ενασχόληση με το αντικείμενο διά λόγους που σχετίζονται αρνητικά με την όποια δυνατότητα επαγγελματικής αποκατάστασης και ακαδημαϊκής καριέρας.³⁷

Αν από την άλλη μεριά αναζητήσουμε πλεονεκτήματα δεν μπορούμε παρά να κάνουμε μνεία στη δυναμική που παρουσιάζει ο χώρος ή στο γεγονός της συμπλοκής του με έναν αριθμό πεδίων γνώσης. Δεύτερον, πρέπει να έχουμε κατά νου πως οι εμπλεκόμενοι στη διαδικασία λήψης αποφάσεων όλο και περισσότερο αποτιμούν θετικά αυτό που προσφέρει η πληροφόρηση. Τρίτον, τεχνολογία και ανοικτές πηγές (open sources) λύνουν σε κάποιο, μικρό ή μεγάλο, βαθμό τα χέρια των μελετητών που δεν επαφίονται πλέον αποκλειστικά στις διαθέσιμες κρατών, κυβερνήσεων και Υπηρεσιών προκειμένου να καλύψουν τις ερευνητικές τους ανάγκες (πρωτογενή πληροφορία διαφόρων μορφών, αρχειακή υποστήριξη κ. λ.). Σημειώνουμε ακόμα την παραγωγή και διάθεση αυτοβιογραφιών προσώπων που γνωρίζουν τις καταστάσεις από μέσα, τη βοήθεια που παρέχει ο τύπος και η δημοσιογραφική έρευνα, τις κοινοβουλευτικές απαιτήσεις διαφάνειας³⁸ -όλα αυτά τροφοδοτούν φιλοδοξίες που φτάνουν μέχρι την αυτονόμηση του πεδίου από το πλαίσιο των σπουδών των Διεθνών Σχέσεων.

Κλείνουμε το συγκεκριμένο τμήμα με το εξής ερώτημα: *τι πρέπει να προσεχθεί ώστε η σπουδή της πληροφορίας να χαράξει ένα γόνιμο μονοπάτι;* Ο Matthew Crosston ευελπιστεί: α) στην αποφυγή εγκλωβισμού του πεδίου αποκλειστικά εντός του αγγλοσαξονικού μοντέλου, β) στη δημιουργία μιας θεωρίας πληροφόρησης, γ) στην αποφυγή θέσεων που χαρακτηρίζονται από προκατάληψη, δ) σε μια ισορροπία μεταξύ των «θεωρητικών» (*those who think*) και των «πρακτικών» (*those that do*) που θα κληθούν να αναπτύξουν θέσεις³⁹.

Οι σκοποί των Σπουδών Πληροφόρησης

Αλλά ποιοι οι λόγοι / σκοποί των σπουδών στην πληροφόρηση εξαιρώντας την ανάγκη διαμόρφωσης / εντρύφησης εντός τεχνικών / επιχειρησιακών μεθόδων (*intelligence tradecraft*), μια ανάγκη που επαφίεται μάλλον αποκλειστικά στην πληροφοριακή κοινότητα; Κατά τον Rudner αυτοί πρέπει να στοχεύουν: α) στη δημόσια παρουσίαση των Υπηρεσιών ως μονάδων του συνόλου των κρατικών οργανισμών ασφαλείας (= αναγνωρισιμότητα), β) στην ανάδειξη της αξίας αυτών των μονάδων όσον αφορά στη λειτουργία και στις επιδιώξεις ενός κράτους (= αποδαιμονοποίηση / συμμετοχικότητα), γ) στη θεωρητική προετοιμασία όσων σκοπεύουν να εμπλακούν επαγγελματικά (συλλογή, ανάλυση πληροφορίας κ. λ.) με το αντικείμενο, δ) στην προπαίδεια όσων επιθυμούν να ακολουθήσουν ακαδημαϊκή ή ερευνητική καριέρα στον τομέα, ε) στην προαπαιτούμενη επιμόρφωση ατόμων που

³⁶ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 33-34

³⁷ Zegart B. Amy, "Cloaks, Daggers, And Ivory Towers" στο *Strategic Intelligence*, Volume 1, επιμ. Johnson K. Loch, Praeger Security International, 2007, σ. 23-31

³⁸ Diaz-Matey, G., *Intelligence studies at the dawn of the 21st century: New possibilities and resources for recent topic in international relations*, ό. π., σ. 13-15

³⁹ Crosston M., "Occam's Follies: Real and Imagined Biases Facing Intelligence Studies" στο *Journal of Strategic Security*, Volume 6, Number 3, 2013, σ. 40-53

θα κληθούν να επανδρώσουν / χειριστούν ευαίσθητους μηχανισμούς ασφαλείας ή να υπηρετήσουν σε ειδικές θέσεις ευθύνης εντός ή εκτός χώρας, στ) στην εξυπηρέτηση, γενικότερα, της ιστορικής αλήθειας, στην απομυθοποίηση των Υπηρεσιών, στην, κατά το δυνατό, ενημέρωση και εξοικείωση της κοινής γνώμης γύρω από και με θέματα ασφαλείας, αμύνης και εξωτερικής πολιτικής υπό μιας άλλης οπτικής και παρουσίασης⁴⁰ και βέβαια, κατά τη γνώμη μας και ειδικότερα, στην εμβάθυνση της έρευνας και ερμηνείας χρονικών περιόδων και στιγμών, γεγονότων, κρίσεων ή αποφάσεων που αποτελούν προνομιακό τομέα μελέτης της Πολιτικής Επιστήμης και της Ιστορίας, των Διεθνών Σχέσεων και των Στρατηγικών Μελετών.

Από τη μεριά του ο Stephen Martin υπογραμμίζει ότι το στοιχείο της πληροφόρησης δύναται να ενταχθεί / ελεγχθεί εντός πλειάδας πεδίων όπως αυτών της ανθρωπολογίας, της κοινωνιολογίας, των ΜΜΕ ακόμα και της φιλομορφίας ή της λογοτεχνίας. Αν αυτά κάπου εντυπωσιάζουν, σίγουρα οι βασικοί άξονες είναι δεδομένοι. Κατά την έννοια τούτη ο συγγραφέας υποστηρίζει ότι η σπουδή για την οποία ομιλούμε: α) εξηγεί τη δομή της αμερικανικής πολιτείας υπό την έποψη της πληροφοριακής λειτουργίας ως τμήμα του κυβερνητικού μηχανισμού και, κυρίως, της εξωτερικής πολιτικής και της πολιτικής εθνικής ασφαλείας, β) συνεισφέρει στη συγκριτική κατανόηση κρατικών πολιτικών. Τί, π. χ., σημαίνει πληροφόρηση για ένα δημοκρατικό, κομμουνιστικό ή απολυταρχικό καθεστώς; γ) συντείνει στην πληρέστερη τυπολογία της απειλής (περιγραφή, αίτια, εκτίμηση, πρόβλεψη), δ) αποδίδει πιστότερα την πραγματικότητα της αμερικανικής και της παγκόσμιας ιστορίας.⁴¹

Σχετικά με το απαραίτητο των συγκεκριμένων σπουδών εντός στρατιωτικών σχολών, όσον αφορά τουλάχιστον στις Ηνωμένες πολιτείες, οι Roger Z. George και Robert D. Kline τονίζουν την ανάγκη επιμόρφωσης τόσο των δυνητικών παραγωγών όσο και ληπτών πληροφόρησης που φοιτούν σ' αυτές. Στους τελευταίους πρέπει, μεταξύ άλλων, να διασαφηνιστεί: α) ο ρόλος της πληροφόρησης ως εργαλείο διαμόρφωσης πολιτικής απόφασης / δράσης, ως καταλύτης στρατηγικής, ως ασπίδα ασφαλείας, β) η λειτουργία του πληροφοριακού κύκλου και ο ρόλος / ευθύνη της πολιτικής και στρατιωτικής ηγεσίας ως προς την επίδοση κατευθύνσεων / προτεραιοτήτων στις Υπηρεσίες, γ) ο γραφειοκρατικός και δομικός χάρτης των πληροφοριακών οργανισμών, η πολλαπλότητα των αποστολών, η υπηρεσιακή κουλτούρα κ. λ., δ) ο τρόπος ή οι τρόποι παραγωγής / απόδοσης της μέγιστης πληροφοριακής υποστήριξης στο πλήθος των κατά τον νόμο ενδιαφερομένων.⁴²

Το 2012 ο Loch Johnson και η Allison Shelton διεξήγαγαν μια έρευνα -επρόκειτο επί της ουσίας περί ενός ερωτηματολογίου πάνω στη σπουδή της πληροφόρησης διανεμημένο σε ειδικούς του χώρου. Ένα από τα θέματα που εθίχθησαν αφορούσε στις προκλήσεις που αντιμετωπίζει το πεδίο σήμερα. Ο Lowenthal επανέλαβε ότι η κυριότερη σχετίζεται με την (μη) αποδοχή του από τον ακαδημαϊκό περίγυρο. Η όποια δυσκολία εντοπίζεται, κατά την Rose McDermott, στην αντίδραση των φιλελεύθερων πανεπιστημιακών οργάνων που το συνδέουν με τον πολιτικό συντηρητισμό. Αν όμως μια σχετική σπουδή, τονίζουν οι Johnson και Shelton, αναφέρεται, πέρα των κλασικών ζητημάτων, και σε ανάλογα αστικών ελευθεριών,

⁴⁰ Rudner M., "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand", ό. π., σ. 116-119

⁴¹ Marin St., "Guide to the Study of Intelligence: Why Teach About Intelligence" στο *The Intelligence Journal of U.S. Intelligence Studies*, Volume 20, Number 1, 2013, σ. 67-68.

⁴² George Z. Roger, Kline D. Robert, "Introduction: Teaching Intelligence" στο *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, επιμ. George Z. Roger, Kline D. Robert, Rowman & Littlefield Publishers, Inc., USA, 2006, σ. xvii-xx

προστασίας της ιδιωτικής ζωής, λογοδοσίας των Υπηρεσιών κ. λ., τότε, κάτι τέτοιο δεν ισχύει. Από την άλλη μεριά ο William Nolte συμπαρατάσσεται με αυτούς που πιστεύουν ότι έχουν γίνει ικανοποιητικά βήματα τονίζοντας την ανταπόκριση της φοιτητικής κοινότητας στα προγράμματα που περιστρέφονται γύρω από το intelligence. Ο Jervis σημειώνει ότι ο χώρος έχει δυνατότητα να επιλέξει μεταξύ μιας εσωστρεφούς ή εξωστρεφούς ερευνητικής τάσης⁴³ ενώ ο Betts προβληματίζεται από το γεγονός της δέσμευσης σημαντικών στοιχείων από τις Υπηρεσίες.⁴⁴ Στο ίδιο paper καταγράφονται απόψεις σχετικά με τις πιθανότητες εξέλιξης της σπουδής σε mainstream topic της Πολιτικής Επιστήμης, των Διεθνών Σχέσεων και της Ιστορίας -ο Jervis δεν πιθανολογεί κάτι τέτοιο για λόγους μεθοδολογίας / έρευνας⁴⁵ τη στιγμή που ο σερ David Omand τηρεί διαφορετική στάση αν και θεωρεί πως πάντα αυτή θα εντάσσεται στο πλαίσιο των International Relations (IR). Οι Nolte και Kislenko συμφωνούν με τον Omand τουλάχιστον ως προς τη δεύτερη τοποθέτηση (πληροφόρηση και IR) ο, δε, Phythian εντοπίζει / καταγράφει μια πιο ανεξάρτητη πορεία.⁴⁶ Η μελέτη κλείνει με την παρουσίαση ορισμένων, διστάμενων είναι αλήθεια, απόψεων σχετικά με το ατέρμονο debate περί χρήσης ή μη ποσοτικών μοντέλων ως ερευνητική οδό στις κοινωνικές επιστήμες και στη μελέτη του intelligence. Ο Lowenthal είναι ξεκάθαρος διακηρύσσοντας πως δεν μπορεί να αντιληφθεί πώς κάτι τέτοιο θα αποδώσει. Επιπλέον θεωρεί ότι η εξάρτηση / στήριξη του πεδίου από και σε μεθόδους ποσοτικοποίησης και συσσώρευσης δεδομένων αντιβαίνει έναν κύριο κανόνα του οποίου βάση συνθέτει η γνώση ως εγκεφαλική διαδικασία και φιλοδοξία και όχι η «αριθμολαγνεία». Συμφωνώντας μαζί του ο Nolte δηλώνει ότι η ποσοτικοποίηση στην έρευνα έχει οδηγήσει την πολιτική επιστήμη μακριά από το εμπράγματο αντικείμενό της του οποίου κύριο στοιχείο δεικνύει η υποκειμενικότητα και η προσωπική άποψη. Ο Phythian συμπαρατάσσεται όχι τόσο λόγω καθαρής απόρριψης αλλά λόγω ποσοτικής έλλειψης δεδομένων εξ αιτίας της μυστικότητας που κυριαρχεί στο χώρο. Από τη μεριά του ο Jervis συνηγορεί υπέρ μιας ποσοτικής μεθόδου συμφωνώντας, ωστόσο, με τον Phythian περί μιας ένδειας στοιχείων που θα μπορούσαν να τη στηρίξουν. Οι Scott, McDermott και Treverton στον έναν ή άλλο βαθμό διαφωνούν με τους Lowenthal και Nolte ενώ, τέλος, ο Omand εφιστά την προσοχή σε όσους πιστεύουν πως κάποιοι νόμοι της οικονομικής επιστήμης και της στατιστικής μπορούν να λειτουργήσουν ως θεραπεινίδες των σπουδών στην πληροφόρηση.⁴⁷

⁴³ Ο Jervis αναφέρεται στις σχέσεις του πεδίου της πληροφορίας με άλλα ανάλογα όπως αυτό της ιστορίας, της κοινωνιολογίας κ. λ.

⁴⁴ Περαιτέρω, ο Gregory Treverton θέτει ζήτημα ορισμού της πληροφορίας, ο Arne Kislenko της σύνδεσης θεωρίας και πράξης, ο Walter Dorn της επέκτασης της σπουδής πέρα από τον αμερικανικό χώρο, ο Anthony Gleeves του είδους και του τρόπου συνεργασίας των ειδικών κ. λ. -για όλα αυτά βλέπε Johnson L., Shelton A., "Thoughts on the State of Intelligence Studies: A Survey Report" στο *Intelligence and National Security*, Volume 28, Number 1, 2013, σ. 116-117

⁴⁵ Ο Jervis γράφει ότι η Πολιτική Επιστήμη κυριαρχείται από στατιστικά και οικονομικά ερευνητικά μοντέλα -κάτι τέτοιο, δηλώνει, δεν μπορεί να ισχύσει στο πεδίο της Πληροφορίας λόγω έλλειψης στοιχείων ικανών να τροφοδοτήσουν αυτά τα μοντέλα

⁴⁶ Johnson L., Shelton A., "Thoughts on the State of Intelligence Studies: A Survey Report" στο *Intelligence and National Security*, ό. π., σ. 118

⁴⁷ ό. π., σ. 118-119

Συμπεράσματα

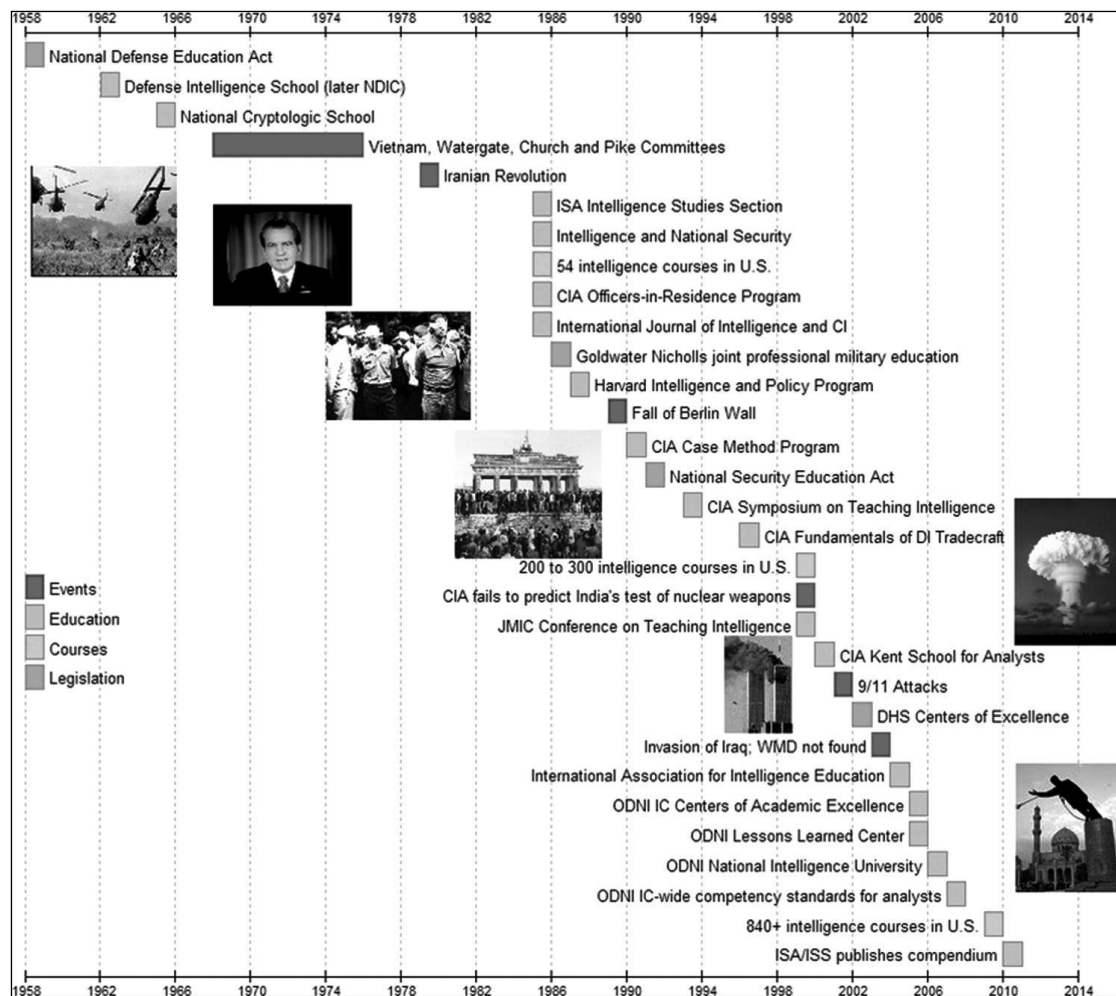
Συμπερασματικά υποστηρίζουμε πως: α) αν και η μελέτη των πληροφοριών κατά βάσει θεωρείται υποπεδίο των Διεθνών Σχέσεων και ακόμα στενότερα των Στρατηγικών Σπουδών, συμπλέκεται με το ευρύτερο πεδίο των Πολιτικών και Ιστορικών Επιστημών με τις τελευταίες να έχουν πρωτοστατήσει στην παραδοχή του, β) η σπουδή της πληροφορίας σε επίπεδο πρακτικών εφαρμογών δύναται να αφορά στην πληροφοριακή διαδικασία, σε ζητήματα *intelligence machinery* και *covert action*, εσωτερικής και διεθνούς ασφαλείας, αντιμετώπισης τρομοκρατίας, ασύμμετρων απειλών κ. λ., γ) οι ερευνητικές προσεγγίσεις που ακολουθούνται χαρακτηρίζονται από ποικιλία, επαφίενται των ανησυχιών του έκαστου μελετητή ενώ αφίστανται μιας δεδομένης μεθοδολογίας. Το ερώτημα περί του αν η μελέτη της πληροφορίας αποτελεί υποπεδίο των Διεθνών Σχέσεων και, ειδικότερα, αν δικαιώνεται εντός του ρεαλιστικού υποδείγματος τίθεται από ορισμένους, έστω, λίγους, δ) η ιστορική και η πολιτική προσέγγιση δεικνύουν αυτή τη στιγμή τα δύο κύρια μονοπάτια ανάγνωσης του αντικειμένου. Σκοπό της πρώτης αποτελεί η πληρέστερη κατανόηση παλαιότερων σελίδων του χρόνου αποκαλύπτοντας την αξία της γνώσης της κρυφής λεπτομέρειας. Σκοπός της δεύτερης είναι η αποτύπωση της εργαλειακής χρείας των Υπηρεσιών σε ζητήματα πολιτικής, σχεδιασμών ασφαλείας και στρατηγικής. Η πολιτική προσέγγιση μεταξύ άλλων περιγράφει το πλέγμα διαμοιβής ανάμεσα στους practitioners και στους policymakers αποκαλύπτοντας δομικές και θεσμικές δυσλειτουργίες, εξηγώντας ενέργειες διεθνών δρώντων που καταγράφονται ως λανθασμένες και, αρχικά τουλάχιστον, ως ανεξήγητες, ε) η μελέτη της πληροφορίας συνθέτει εργαλείο που σκοπό έχει, πέραν της ακαδημαϊκής χρηστικότητας, να εξυπηρετήσει την κρατική οντότητα. Ερωτήματα ασφαλείας και πλάνα στρατηγικής απαντώνται και οργανώνονται αρτιότερα όταν η πολιτεία διαθέτει ικανές Υπηρεσίες και εκπαιδευμένο πολιτικό προσωπικό. Οι πρώτες μέσα από τη σπουδή του αντικειμένου ωφελούνται ποικιλοτρόπως (ποιοτικότερη επάνδρωση, θεσμική καταξίωση, νέες προσεγγίσεις δράσης / αντιμετώπισης καταστάσεων, ευρύτερη αντίληψη των τελευταίων, πλουραλιστική αποκωδικοποίηση γεγονότων κ. λ.). Όσον αφορά στο δεύτερο, δεν διανοείται να μην αποδέχεται την αξία, να μην επιζητά τη ραφιναρισμένη πληροφορία ως παράγοντα που φέρει τον κάτοχό της ένα βήμα μπροστά από τον όποιο αντίπαλο, στ) η διεθνής σπουδή του αντικειμένου παρουσιάζοντας κατά τις δύο πρώτες δεκαετίες του 21^{ου} αιώνα ενθαρρυντικούς, μάλλον, ρυθμούς ανάπτυξης παρά την όποια διάσταση απόψεων, παρά τα όποια εσωτερικά και εξωτερικά προβλήματα και συγκεντρώνοντας το ενδιαφέρον, πλην των παλαιότερων, μιας νέας γενιάς ακαδημαϊκών και επιχειρησιακών αναμένεται να παράξει αποτελέσματα στη θεωρία και πράξη. Τέλος, η αποπεριθωριοποίηση του θέματος, ουσιαστικά η απόρριψη προκαταλήψεων που ακόμα ταλαιπωρούν, θα διευκολύνει την έρευνα συγκεντρώνοντας γύρω από αυτήν τόσο το απαραίτητο ανθρώπινο / πνευματικό κεφάλαιο όσο και τους ανάλογους χρηματοδοτικούς πόρους.

Οι Κωνσταντόπουλος, Δόγα αποδεχόμενοι λίγο έως πολύ τις άνω καταθέσεις και ανατρέχοντας σε μελετητές όπως ο Robert Dover, ο Michael Goodman, ο Christopher Andrew, η Claudia Hillebrand ή η Amy Zegart γράφουν πως αν και οι σπουδές στην πληροφόρηση επαναστατικοποιούν τον τρόπο με τον οποίο αναγιγνώσκουμε τις παγκόσμιες πολιτικές / στρατηγικές ή τις διεθνείς σχέσεις, αρκετά απομένουν να γίνουν. Κατ' αυτήν την έννοια επιτακτική παρουσιάζεται μια ανάγκη: α) «απεθνοκεντροποίησης» της μελέτης υπό την προοπτική μιας έρευνας που θα απλώνεται πέραν του αγγλοσαξονικού τόξου, β) αποσαφήνισης των περί την πληροφόρηση ορισμών, γ) ικανοποίησης θεωρητικών και μεθοδολογικών

προκλήσεων (όπως η δημιουργία μιας θεωρίας πληροφόρησης) με σκοπό τη σύνδεση του πεδίου με τη θεωρία των Διεθνών Σχέσεων, δ) επικέντρωσης στη συγκριτική μελέτη της πληροφορίας όσον αφορά, π. χ., στις διαφορετικές σχετικές κρατικές κουλτούρες, ε) ανάπτυξης ερευνών ποσοτικών προσεγγίσεων, στ) επικέντρωσης στις «χαμένες διαστάσεις» της πληροφόρησης καθ'αυτή ήτοι, της οικονομικής κατασκοπίας (ιδιαίτερα μεταξύ συμμάχων), της συνεργασίας μεταξύ κρατών / Υπηρεσιών, του κυβερνοπολέμου, της κεκαλυμμένης δράσης, της σχέσεως μεταξύ πληροφόρησης / Υπηρεσιών και law enforcement, πληροφόρησης / Υπηρεσιών και διεθνούς δικαίου, τεχνολογίας, διαχείρισης κρίσεων [(λαθρο)μετανάστευσης, περιβαλλοντικών, επισιτιστικών ή άλλων κρίσεων κ. λ.]. Επιπλέον και προκειμένου οι ερευνητές να εκπληρώσουν την ακαδημαϊκή τους αποστολή πρέπει: α) να περιοριστεί η μυστικότητα που χαρακτηρίζει το αντικείμενο, β) να περιοριστεί η τάση διαβάθμισης αρχείων εκ μέρους των Υπηρεσιών και γ) να ξεπεραστούν τα αντικίνητρα που κατευθύνουν τους μελετητές σε συγκεκριμένες περιοχές ερεύνης αγνοώντας άλλες ή, τέλος, συρρικνώνουν το θεωρητικό τους ενδιαφέρον.⁴⁸

⁴⁸ Κωνσταντόπουλος Ι., Δόγα Αλεξάνδρα, “The (R)evolution of Intelligence as an Academic Discipline: Challenges and Constraints”, ό. π., σ. 13-14. Επιπλέον, οι δύο συγγραφείς καταγράφουν τη ρήση του Len Scott κατά την οποία «η σπουδή της πληροφόρησης στα πρώτα χρόνια του 21^{ου} αιώνα συμβαδίζει με καιρούς που κάθε άλλο παρά δείχνουν σημάδια κόπωσης. Ο ρόλος της μυστικής πληροφόρησης στη διεθνή ασφάλεια και παγκόσμια πολιτική καθίσταται σημαντικότερος από ποτέ. Σε καμία περίπτωση η κατανόηση της πληροφοριακής διαδικασίας και της σπουδαιότητάς της στην επίτευξη εθνικής και διεθνούς ασφάλειας δεν παρουσιάζοταν ποτέ επιτακτικότερη από σήμερα» -περί τούτου βλέπε ειδικότερα Scott L., “Sources and Methods in the Study of Intelligence: A British View”, ό. π., σ. 185-186

Η εξέλιξη της μελέτης της Πληροφορία στις ΗΠΑ



Εικόνα 1: Η εικόνα έχει αντιγραφεί από το Campbell St., “A Survey of the U. S. Market for Intelligence Education” στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 2, 2011, σ. 307

ΚΕΦΑΛΑΙΟ 2

Περί της φύσεως της πληροφόρησης *per se*

Τι σημαίνει πληροφόρηση / intelligence;

Ο Roy Godson γράφει πως απάντηση στην ερώτηση «τι σημαίνει intelligence;» δεν είναι εύκολο να δοθεί. Η ημι-επιστημονική (semi-scholarly) βιβλιογραφία βρίθει προσδιορισμών -«το δεύτερο αρχαιότερο επάγγελμα», «ένα απαραίτητο κακό», «εργαλείο τυράννων» κ. λ. Η επιστημονική, συνεχίζει ο Godson, «τα πάει καλύτερα αλλά όχι αρκετά καλύτερα». ¹ Ο συγγραφέας καταλήγει στο συμπέρασμα ότι intelligence δεν είναι άλλο από κρατική / κυβερνητική (ενδεχομένως και ιδιωτική) προσπάθεια αφιερωμένη: α) στη συλλογή, ανάλυση, διασπορά και αξιοποίηση πληροφορίας που σχετίζεται / εξυπηρετεί οικεία συμφέροντα, που αναφέρεται σε άλλες κυβερνήσεις, πολιτικές ομάδες, ένοπλες δυνάμεις, πρόσωπα κ. λ., β) στην προστασία του έθνους έναντι πληροφοριακών δραστηριοτήτων εκ μέρους ξένων κυβερνήσεων, πολιτικών ομάδων, ενόπλων σωμάτων κ. λ., γ) στην εκτέλεση μυστικών δράσεων με σκοπό τη χειραγώγηση κυβερνήσεων, πολιτικών ομάδων, ενόπλων δυνάμεων, προσώπων κ. λ. -εξ αυτών συνάγονται τα τέσσερα διακριτά μέρη της ήτοι, α) συλλογή, β) ανάλυση, γ) αντιπληροφόρηση / αντικατασκοπία, δ) κεκαλυμμένη δράση.²

Το πώς θα ληφθεί / εργαλειοποιηθεί η πληροφόρηση εξαρτάται από πέντε κύριους παράγοντες, ειδικότερα: α) τον τύπο διακυβέρνησης. Οι μη αστικές δημοκρατίες συνήθως χρησιμοποιούν τις Υπηρεσίες προς έλεγχο του τοπικού πληθυσμού μη διαχωρίζοντας μεταξύ εχθρών εντός και εκτός χώρας. Σ' αυτήν την περίπτωση οι πληροφοριακοί οργανισμοί προσομοιάζουν με τις κλασικές υπηρεσίες εσωτερικής Ασφαλείας. Πιστεύεται, π. χ., πως επί Σοβιετικής Ένωσης η KGB απασχολούσε περίπου το 90% του δυναμικού της σε υποθέσεις εγχωρίου ενδιαφέροντος σε αντίθεση με τις αμερικανικές και βρετανικές Υπηρεσίες που απασχολούσαν περί το 95% του προσωπικού τους σε υποθέσεις εξωτερικής υφής³, β) τις πολιτικές συνθήκες και αντιλήψεις. Πώς, δηλαδή, γίνεται αντιληπτή η έννοια του κινδύνου της πολεμικής σύρραξης, της αμυντικής ή επιθετικής πληροφόρησης, των όποιων ειδικών ή έκτακτων απειλών⁴ κ. λ., γ) τις γραφειοκρατικές πραγματικότητες⁵, δ) τις σχέσεις μεταξύ κυβέρνησης-ρνήσεων και Υπηρεσιών⁶, ε) την τεχνολογική καινοτομία.⁷

¹ Godson R., "Intelligence: an American View" στο *British and American Approaches to Intelligence*, επιμ. Robertson G. K., Royal United Services Institute, USA, 1987, σ. 3

² ό. π., σ. 4, 17-27. Ο Godson σημειώνει πως «είναι δύσκολο να φανταστούμε ένα αποτελεσματικό σύστημα συλλογής πληροφοριών [σύστημα πληροφόρησης] χωρίς την ανάλυση ή χωρίς διευκρινήσεις / εντολές προς τους συλλέκτες. Η αντιπληροφόρηση καθίσταται απαραίτητη για την προστασία των τελευταίων από τις ξένες μυστικές υπηρεσίες. Παρομοίως, η κεκαλυμμένη δράση βασίζεται στη συλλογή, ανάλυση και αντικατασκοπία. Αυτά καταδεικνύουν πως τα μέρη της πληροφόρησης ουσιαστικά συνθέτουν ένα ενιαίο σύστημα του οποίου η επιτυχία εξαρτάται από τη συνεργασία ακριβώς αυτών των μερών» -για μια καλύτερη εικόνα βλέπε Godson R., "Intelligence and Policy: An Introduction" στο *Intelligence Requirements for the 1980s: Intelligence and Policy*, επιμ. Godson R., Lexington Books, Lexington / Massachusetts, 1986, σ. 2, επίσης, Johnson J., "Bricks and Mortar for a theory of Intelligence" στο *Comparative Strategy*, Volume 22, Issue 1, 2003, σ. 1-28

³ Godson R., "Intelligence: an American View", ό. π., σ. 5-8

⁴ ό. π., σ. 8-11

⁵ ό. π., σ. 11-14

⁶ ό. π., σ. 14-15

⁷ ό. π., σ. 15-16

Σύμφωνα με τον Fred Schreier ο όρος «intelligence» υποδηλώνει: α) είδος γνώσεως / 'προ-γνώσεως' με σκοπό τη διασφάλιση κρατικών / εθνικών συμφερόντων, β) τις Υπηρεσίες (εσωτερικών πληροφοριών, εξωτερικών πληροφοριών, στρατιωτικών πληροφοριών, law enforcement / criminal intelligence), γ) τις επιχειρησιακές δραστηριότητες των Υπηρεσιών (συλλογή, ανάλυση, counterintelligence, κεκαλυμμένη δράση), δ) τον πληροφοριακό κύκλο, ε) το παραγόμενο προϊόν των Υπηρεσιών.⁸

Ο Loch Johnson πρακτικά δεν διαφοροποιείται από τον Schreier. Κατ' αυτόν το intelligence (national security intelligence όπως γράφει) σχετίζεται είτε με: α) τις Υπηρεσίες (intelligence as organizations), β) τη διαδικασία παραγωγής πληροφοριακού προϊόντος ή, αλλιώς, τον πληροφοριακό κύκλο (intelligence as process), γ) το τελικό προϊόν / αναφορά (intelligence as information), δ) τις πληροφοριακές αποστολές ήτοι, συλλογή, ανάλυση, αντιπληροφόρηση και κεκαλυμμένη δράση (intelligence as a set of missions).⁹

Ο Mark Lowenthal συγγράφει πως ...intelligence σημαίνει: α) διαδικασία μέσω της οποίας συγκεκριμένες πληροφορίες σημαντικές για την εθνική ασφάλεια, αφού απαιτηθούν και συλλεχθούν, αναλύονται και αποδίδονται στους πολιτικούς ηγέτες, β) το προϊόν αυτής της διαδικασίας, γ) μέθοδο προστασίας / ασφάλειας ευαίσθητων δεδομένων μέσω πρακτικών counterintelligence, δ) εκτέλεση απαιτητών επιχειρήσεων για λογαριασμό των έννομων αρχών.¹⁰ Στο *Introduction to Intelligence Studies* (2013) διαβάζουμε ότι αν και αποστολή του intelligence είναι η απόδοση γνωστικού πλεονεκτήματος στους decisionmakers, αποδεκτός κοινός ορισμός δεν υπάρχει. Η έννοια προσλαμβάνεται ποικιλοτρόπως κατά την κάθε Υπηρεσία εξ αιτίας της διαφορετικότητας των όποιων επιχειρησιακών πλάνων. Ο Michael Warner στηριγμένος στη σελίδα 26 της Commission on Organization of the Executive Branch of the Government [the Hoover Commission], *Intelligence Activities*, του 1955 συμφωνεί σημειώνοντας επιπλέον ότι ...ασχολείται [το intelligence] με πράγματα που οφείλουν να γίνονται γνωστά πριν την έναρξη μιας πορείας ενεργειών.¹¹

Ο Vernon Walters, πρώην αναπληρωτής διευθυντής της CIA, στο έργο του *Silent Missions* γράφει ότι ...[πληροφόρηση / intelligence] είναι πληροφορία, όχι πάντα διαθέσιμη στο κοινό, σχετική με πόρους, δυνατότητες, προθέσεις, οπωσδήποτε την ισχύ μιας ξένης χώρας που δύναται να επηρεάσει τη διαβίωση και την ασφάλεια του [αμερικανικού] πληθυσμού.¹² Ένας άλλος υψηλόβαθμος αξιωματούχος της «the Company», ο Lyman Kirkpatrick, συνεισφέρει ως ακολούθως: «intelligence σημαίνει γνώση, ιδεατά πρόγνωση, ζητούμενη από έθνη προς αντιμετώπιση εξωτερικών απειλών και προστασία ζωτικών συμφερόντων της κοινωνίας τους».¹³ Ο Director of National Intelligence (DNI) James R. Clapper, Jr (HPIA) δηλώνει ότι «πληροφόρηση

⁸ Schreier Fred, *Transforming Intelligence Services. Making Them Smarter, More Agile, More Effective and More Efficient*, National Defence Academy, Austrian Ministry of Defence and Sports, Geneva Centre for the Democratic Control and Armed Forces, Βιέννη, 2010, σ. 22-23, 25-27

⁹ Johnson Loch, "National Security Intelligence" στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson Loch, Oxford University Press, New York, 2010, σ. 7-27

¹⁰ Lowenthal M., *Intelligence: From Secrets to Policy*, CQPress, Washington, D.C., HPIA, 2008⁴, σ. 8

¹¹ Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA, 2013, σ. 2-3. Επίσης βλέπε Commission on Organization of the Executive Branch of the Government [the Hoover Commission], *Intelligence Activities*, Ιούνιος 1955, σ. 26, διαθέσιμο και στο <https://babel.hathitrust.org/cgi/pt?id=mdp.39015012152321;view=1up;seq=6> όπου ανατρέξαμε την 21^η Απριλίου 2015

¹² Walters Vernon, *Silent Missions*, Doubleday, Garden City / N.Y., 1978, σ. 621

¹³ Kirkpatrick Lyman, Jr., "Intelligence" στο *Encyclopedia of US Foreign Relations*, Volume 2, επιμ. Jentelson Bruce, Paterson Thomas, Oxford University Press, New York, 1997, σ. 365

σημαίνει στοιχείο του οποίου σκοπός είναι ένας και μόνος: η εξάλειψη ή, έστω, απομείωση της αβεβαιότητας προς εξυπηρέτηση των decisionmakers».¹⁴ Ο George Allen αφού αποδώσει στην πληροφόρηση την έννοια της γνώσης γράφει πως αυτή οφείλει: α) να εξυπηρετεί τα πολυποίκιλα κρατικά ενδιαφέροντα, πλάνα, συμφέροντα, β) να ασχολείται πρωτίστως με εξωτερικές προκλήσεις που ενδεχομένως αντιβαίνουν στο εθνικό συμφέρον και γ) να χαρακτηρίζεται από εμπιστευτικότητα.¹⁵

Οι Peter Gill και Mark Phythian σημειώνουν πως η έννοια intelligence: α) σημαίνει κάτι περισσότερο από συλλεγμένη πληροφορία, β) καλύπτει ένα εύρος συνδεδεμένων δραστηριοτήτων, γ) συνδέεται με την έννοια της ασφάλειας, δ) σχετίζεται με την έγκαιρη προειδοποίηση, ε) σχετίζεται με την κεκαλυμμένη δράση, στ) σχετίζεται με την έννοια της μυστικότητας, ζ) αφορά στο ανταγωνιστικό διεθνές περιβάλλον.¹⁶

Ο John Bruce Lockhart, εκπροσωπώντας κυρίως τη βρετανική προσέγγιση, ορίζει την πληροφόρηση ως έννοια-ομπρέλα που καλύπτει μια ευρεία γκάμα καθηκόντων και δεξιοτήτων. Οι παραδεκτές κύριες περιοχές αναφέρονται: α) στην απόδοση πληροφοριακών απαιτήσεων εκ μέρους του κυβερνητικού επιτελείου, β) στη συλλογή πληροφοριών μέσω ανοικτών πηγών, μυστικών μεθόδων και τεχνολογικών assets, γ) στην αντιπληροφόρηση / αντικατασκοπία και στην (εσωτερική) ασφάλεια, δ) στην ανάλυση / αξιολόγηση όλων των συλλεχθέντων στοιχείων. Επιπλέον ο ερευνητής υποστηρίζει πως η παραστρατιωτική δράση δεν πρέπει να θεωρείται κομμάτι των υποχρεώσεων των μυστικών υπηρεσιών. Δεν δύναται, συνεχίζει ο Lockhart, μια παραστρατιωτική επιχείρηση να περάσει απαρατήρητη· πρόκειται για αλήθεια που κατέστη αδιαμφισβήτητη μετά την επιχείρηση-φιάσκο της CIA με την κωδική ονομασία *Bay of Pigs* (1961).¹⁷ Ο Lockhart ασχολείται κατά κύριο λόγο με τις επιχειρησιακές όψεις της πληροφόρησης και των σχετικών οργανισμών βγάζοντας έξω από τα καθήκοντα τους τόσο το κομμάτι των παραστρατιωτικών εγχειρημάτων όσο και αυτό των κεκαλυμμένων δράσεων ήτοι, το «μακρύ χέρι» της κυβερνητικής πολιτικής που δρα μέσω μυστικών / κρυφών και μη αποδοτέων δράσεων (secret and non-attributable means).

Ο Ιωάννης Κωνσταντόπουλος σε άρθρο του γράφει για τη σχέση πληροφόρησης και υψηλής στρατηγικής. Η συμβολή της πρώτης στην επιτυχία της δεύτερης έχει να κάνει με: α) τη μείωση της αβεβαιότητας στη διεθνή πολιτική σκηνή, την αναγνώριση απειλών / ευκαιριών κ. λ., β) το κτίσιμο εσωτερικής / εξωτερικής νομιμοποίησης στρατηγικών δράσεων όπως και την αντίστοιχη απονομιμοποίηση του αντιπάλου μέσω εργαλείων κεκαλυμμένης δράσης (προπαγάνδα, influence agents κ. λ.), γ) την επίτευξη στόχων εξωτερικού ενδιαφέροντος επίσης μέσω εργαλείων κεκαλυμμένης δράσης (κρυφή πολιτική ή οικονομική βοήθεια, παραστρατιωτικές επιχειρήσεις κ. λ.), δ) την προστασία στρατηγικών σχεδιασμών μέσω της αντικατασκοπίας, ε) τη διαπίστωση της επιτυχίας ή όχι μιας υψηλής στρατηγικής, τις εναλλακτικές προτάσεις εφόσον κριθεί απαραίτητη μια αλλαγή πλάνων και τη γνώση της αντίδρασης τού απέναντι στρατοπέδου.¹⁸

¹⁴ Clapper R. J. "Luncheon Remarks, Association, of Former Intelligence Officers" στο *The Intelligence*, AFIO newsletter, McLean, Virginia, 1995, σ. 3

¹⁵ Allen George, "Professionalization of Intelligence" στο *Ethics of Spying. A Reader for the Intelligence Professional*, Volume 2, επιμ. Goldman Jan, The Scarecrow Press, Inc., UK, 2010, σ. 6

¹⁶ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, Polity Press, USA, 2012², σ. 18

¹⁷ Lockhart B. J., "Intelligence: a British View" στο *British and American Approaches to Intelligence*, επιμ. Robertson G. K., Royal United Services Institute, USA, 1987, σ. 37-51

¹⁸ Κωνσταντόπουλος Ιωάννης, «Πληροφόρηση (Intelligence) και Υψηλή Στρατηγική: Η περίπτωση της Ελλάδας», 2 Ιουνίου 2016, στο ηλεκτρονικό *Liberal* (<http://www.liberal.gr/arthro/54589/amyna-->

Από τη μεριά της η National Security Act του 1947 κάνει λόγο για τη λεγόμενη *εξωτερική πληροφόρηση (foreign intelligence)*: η συγκεκριμένη αποκαλύπτει δυνατότητες, προθέσεις και δράσεις αλλοδαπών οργανισμών / χωρών ή ατόμων. Η ίδια Πράξη δεν παραλείπει να σημειώσει πως εντός της έννοιας «intelligence» περιλαμβάνεται και η αντιπληροφόρηση.¹⁹ Κατά την Brown-Aspin Committee μια χρηστική όσο και απλή προσέγγιση είναι η εξής ...[intelligence] σημαίνει πληροφόρηση σχετική με ξένες οντότητες, πρόσωπα, καταστάσεις, τοποθεσίες, γεγονότα κ. λ. απαιτούμενη από το κυβερνητικό επιτελείο προς εκτέλεση συγκεκριμένων σχεδιασμών.²⁰ Το FBI υποστηρίζει ότι ...[intelligence] σημαίνει πληροφορία που έχει αναλυθεί με σκοπό τη χρήση της στη διαδικασία λήψεως αποφάσεων, ειδικότερα, αποφάσεων επί ζητημάτων που αφορούν στην εθνική ασφάλεια των ΗΠΑ. Κατά το Bureau και άλλους οργανισμούς που συνθέτουν την αμερικανική πληροφοριακή κοινότητα, η πληροφόρηση, αναλόγως προσέγγισης, δεικνύει: α) διαδικασία, β) προϊόν, γ) αναφορά.²¹ Η CIA τονίζει πως με τους απλούστερους όρους ...πληροφόρηση δεν σημαίνει άλλο από (προ)γνώση γύρω από τον κόσμο ή, αλλιώς, προαπαιτούμενο για μια ορθή διαδικασία λήψης αποφάσεων και ανάληψης δράσεων [actionable intelligence] εκ μέρους των policymakers των ΗΠΑ.²² Μελέτη για λογαριασμό του Council of Foreign Relations υποστηρίζει πως ...[intelligence] είναι μη ανοικτή πληροφορία / πληροφόρηση ή ανάλυση στηριγμένη, τουλάχιστον εν μέρει, σε μη ανοικτές πηγές που αποδίδεται στους διαμορφωτές πολιτικής ή άλλους παράγοντες εντός της κυβέρνησης.²³ Η Joint Publication (JP) 2-0, *Joint Intelligence*, αναφέρει μεταξύ άλλων ότι intelligence σημαίνει έργο που παράγεται μέσω συλλογής, εκτίμησης, ανάλυσης και αποκωδικοποίησης διαθέσιμων πληροφοριών σχετικών με ξένα έθνη, εχθρικών ή δυνητικά εχθρικών στοιχείων ή δυνάμεων, δυνητικών περιοχών επιχειρήσεων ή περιοχών που ήδη εμπλέκονται.²⁴ Το *Dictionary of Military and Associated Terms* (JP 1-02) του Νοεμβρίου του 2010 (as amended through 15 February 2015) αποκρυπτογραφεί το λήμμα «intelligence» ως: α) προϊόν διαδικασίας συλλογής, εκτίμησης, ανάλυσης, αποκωδικοποίησης πρωτογενών στοιχείων σχετικών με αλλοδαπά έθνη, εχθρικές ή δυνητικά εχθρικές οντότητες, περιοχές εντός των οποίων εκτελούνται ή δύναται να εκτελεστούν [διαφόρων ειδών] δράσεις, β) δραστηριότητες που απαιτούνται για την παραγωγή πληροφόρησης (συλλογή,

diplomatia/2016/pliroforisi-Intelligence-kai-ypsili-stratigiki-i-periptosi-tis-elladas.html) εις το οποίο καταφύγαμε τη 18^η Ιουνίου 2016

¹⁹ 50 USC 401a στο <http://openjurist.org/title-50/us-code/section-401-a/definitions> όπου ανατρέξαμε την 21^η Απριλίου 2015 και *National Security Act of 1947* [(chapter 343; 61 Stat. 496; approved July 26, 1947) As Amended Through P.L. 110-53, Enacted August 3, 2007], σ. 6, διαθέσιμο και στην ιστοσελίδα <https://www.ncsc.gov/training/resources/nsaact1947.pdf> με ημερομηνία καταφυγής επίσης την 21^η Απριλίου 2015

²⁰ Commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the 21st Century: An Appraisal of US Intelligence [the "Brown-Aspin Report"], Government Printing Office, Washington, D.C., 1996, σ. 5, διαθέσιμο και στον δικτυακό χώρο <https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2011/08/Aspin-Brown-Report-on-the-Intelligence-Community-1996.pdf> όπου ανατρέξαμε τη 23^η Απριλίου 2016

²¹ Για περισσότερα βλέπε Federal Bureau of Investigation, "Intelligence Defined" στη δικτυακή σελίδα <https://www.fbi.gov/about-us/intelligence/defined> όπου καταφύγαμε την 27^η Ιουλίου 2015

²² Central Intelligence Agency, Office of Public Affairs, *A Consumer's Guide to Intelligence. Gaining Knowledge and Foreknowledge of the World around Us*, Washington, D.C., 1999, σ. vii

²³ *Making Intelligence Smarter: Report of an Independent Task Force*, Council on Foreign Relations, New York, 1996, σ. 8

²⁴ Joint Publication (JP) 2-0, *Joint Intelligence*, Οκτώβριος 2013, σ. GL-8

ανάλυση κ. λ.) και γ) οργανισμούς που εμπλέκονται στις μόλις αναφερόμενες δραστηριότητες.²⁵

Το *National Intelligence. A Consumer's Guide* (ODNI, 2009) αναφέρεται στη σπουδαιότητα της πληροφορίας καταγράφοντας τη συνεισφοράς της στους τομείς: α) της παραγωγής πολιτικής απόφασης, β) της ενημέρωσης γύρω από δυνητικές απειλές, γ) της αποκρυπτογράφησης καταστάσεων, δ) της αποκρυπτογράφησης άμεσων καταστάσεων (situational awareness) και αντιμετώπισής τους, ε) της μακροπρόθεσμης στρατηγικής εκτίμησης, στ) της προετοιμασίας συναντήσεων / συσκέψεων εθνικού ενδιαφέροντος, συμφερόντων, ή ασφαλείας, ζ) της ενημέρωσης περίξ ειδικών ζητημάτων, η) της ενημέρωσης περίξ προσώπων ειδικού ενδιαφέροντος.²⁶

Επίσης στην ίδια έκδοση γίνεται λόγος περί του τι δεν μπορεί να πράξει η πληροφόρηση, ειδικότερα: α) δεν μπορεί να προκαταβάλει το μέλλον και β) δεν μπορεί (δεν πρέπει) να παραβιάσει ως οργανισμός / γραφειοκρατία την (αμερικανική) συνταγματική αρχή και νομιμότητα.²⁷

Τέλος η FM 2-0, *Intelligence*, του 2004 αναφέρει ότι στρατιωτική πληροφόρηση ίσον παροχή πληροφοριών: α) περίξ του εχθρού, β) περίξ του πεδίου επιχειρήσεων, γ) προς επίτευξη προστασίας φίλων δυνάμεων. Οι συγκεκριμένες δράσεις λειτουργώντας καταλυτικά ως προς την κατανόηση, εκ μέρους της στρατιωτικής ηγεσίας, των εχθρικών δυνατοτήτων / σχεδιασμών και του επιχειρησιακού περιβάλλοντος συμβάλουν αποφασιστικά στην κατάρτιση των οικείων πλάνων, στην επίτευξη μιας βέλτιστης διαδικασίας λήψεως αποφάσεων και σε μια οιονεί πρόβλεψη των μελλοντικών εχθρικών κινήσεων.²⁸

Ο Michael Warner καταγράφοντας πλήθος τοποθετήσεων υποστηρίζει πως το κλειδί ενός πετυχημένου ορισμού περί την πληροφόρηση βρίσκεται στην παραδοχή της αξίας της μυστικότητας στο όποιο εγχείρημα (συλλογή, κεκαλυμμένη δράση) -χωρίς μυστικότητα δεν νοείται 'πληροφόρηση'. Ο μελετητής κλείνει προς την άποψη του R. A. Random κατά την οποία ...*intelligence is the official, secret collection and processing of information on foreign countries to aid in formulating and implementing foreign policy, and the conduct of covert activities abroad to facilitate the implementation of foreign policy.*²⁹ Ό,τι ορίζει ο Warner ως intelligence: α) στηρίζεται σε εμπιστευτικές πηγές και μεθόδους, β) 'εκτελείται' από κρατικούς αξιωματούχους προς επίτευξη εθνικών σκοπών, γ) επικεντρώνει / στοχεύει σε ξένες οντότητες, συνηθέστατα κρατικές αλλά όχι μόνο, δ) σχετίζεται με παραγωγή και διασπορά πληροφόρησης, ε) εμπλέκεται στην προσπάθεια επιρροής επί αλλοδαπών κυβερνήσεων χρησιμοποιώντας και μη αποδοτέα (unattributable) μέσα.³⁰ Ο συγγραφέας θεωρεί ότι η θέση του Random ενσωματώνει σε ικανό βαθμό τα πέντε αναφερόμενα σημεία, συμπυκνώνει, δε, σημειώνοντας πως «πληροφόρηση σημαίνει

²⁵ JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 15 February 2015), σ. 120

²⁶ *National Intelligence. A Consumer's Guide*, ODNI, 2009, σ. 10-11

²⁷ ό. π., σ. 11

²⁸ Field Manual 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., Μάιος 2014, σ. 1-1 – 1-2

²⁹ Warner M., "Wanted: A Definition of 'Intelligence'" στο *Studies in Intelligence*, Volume 46, Number 3, 2002, σ. 19, επίσης βλέπε Random R., "Intelligence as a Science" στο *Studies in Intelligence*, Volume 2, Number 2 διαθέσιμο στο δικτυακό τόπο https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no2/html/v02i2a09p_0001.htm εις τον οποίο ανατρέξαμε την 22^α Απριλίου 2016

³⁰ Warner M., "Wanted: A Definition of 'Intelligence'", ό. π., σ. 21

μυστική, κρατική δράση με σκοπό την κατανόηση ή τη χειραγώγηση ξένων δρώντων». ^{31, 32}

Τα επίπεδα της πληροφόρησης

Στο *Intelligence and Counterintelligence. Spy Agencies, Intelligence Operations, and the People Behind Them* διαβάζουμε ότι οι πληροφοριακές επιχειρήσεις κατηγοριοποιούνται σε τρία επίπεδα. Το στρατηγικό, το επιχειρησιακό / τακτικό και το αντιπληροφοριακό. Το πρώτο αναφέρεται σε δυνατότητες και προθέσεις ξένων δυνάμεων. Το δεύτερο σχετίζεται συνηθέστατα με τα πεδία μαχών (combat intelligence). Σημειώνουμε ότι λόγω της καταστροφικής δύναμης των σύγχρονων όπλων η ηγεσία λαμβάνει σοβαρά υπόψη την πληροφόρηση που προέρχεται από αυτά προκειμένου να καταλήξει σε μια απόφαση, άρα, η διαχωριστική γραμμή μεταξύ στρατηγικής και επιχειρησιακής / τακτικής πληροφόρησης συχνά ξεθωριάζει. Το τρίτο επίπεδο αφορά στην αντικατασκοπία με σκοπό την αποτροπή διείσδυσης επίβουλων προσώπων εντός κυβερνητικών, στρατιωτικών, πληροφοριακών οργανισμών. Το αντικατασκοπευτικό έργο μετά τη δεκαετία του 1990 έχει επωμισθεί καθήκοντα που σχετίζονται και με αποτροπή τρομοκρατικών κτυπημάτων όπως και με την πάταξη του οργανωμένου εγκλήματος. Η αντιπληροφόρηση συχνά μετατρέπεται σε πληροφόρηση κομίζοντας στοιχεία περίξ, π. χ., πληροφοριακών εργαλείων και ανάλογων τεχνικών / τακτικών ξένων χωρών ή του είδους δεδομένων που οι τελευταίες επιθυμούν να υποκλέψουν. Τονίζουμε πως μια υπηρεσία CI θα επιχειρήσει, δοθέντων ευκαιριών, παραπληροφόρηση / χειραγώγηση εις βάρος αντιπάλων οργανισμών. ³³

Στη JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (2010), διαβάζουμε ότι «στρατηγική πληροφόρηση καλείται η πληροφόρηση που απαιτείται προς διαμόρφωση πολιτικών και στρατιωτικών πλάνων εθνικής και διεθνούς προοπτικής». ³⁴ Στην ίδια JP και σχετικά με την επιχειρησιακή και τακτική πληροφόρηση αναφέρεται ότι «επιχειρησιακή καλείται η απαιτούμενη προς σχεδιασμό / εκτέλεση ευρέων εγχειρημάτων πληροφόρηση και με σκοπό την επίτευξη στόχων που αναφέρονται στο θέατρο δράσεων» ³⁵ τη στιγμή που «τακτική καλείται η πληροφόρηση που επιβοηθά στο σχεδιασμό / εκτέλεση ‘τακτικών επιχειρήσεων’» ³⁶ ήτοι, στο σχεδιασμό / εκτέλεση των κατά τόπους κινήσεων. Σύμφωνα με τον Lock Johnson στρατηγική πληροφόρηση σημαίνει ακριβώς εκείνη που θα οδηγήσει τους ηγέτες ενός έθνους στην ορθή επί καίριων ζητημάτων απόφαση. Προφανώς δεν πρόκειται για πληροφορία τοπικού ενδιαφέροντος αλλά για ...*knowledge and foreknowledge of the world around us, the prelude to presidential decision and*

³¹ Warner M., “Wanted: A Definition of ‘Intelligence’”, ό. π., σ. 21

³² Για μια ευρεία γκάμα ορισμών περί την πληροφόρηση βλέπε Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, CRC Press, Florida, 2014, κεφάλαιο 3, επίσης, Høffding Simon, Rønn Kira, “The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence” στο *Intelligence and National Security*, Volume 28, Number 5, 2013, σ. 694-716

³³ *Intelligence and Counterintelligence. Spy Agencies, Intelligence Operations, and the People Behind Them*, επιμ. Curley Rob, Britannica Educational Publishing, Rosen Educational Services, New York, 2013, chapter 1

³⁴ JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, DoD, November 2010 (as amended through February 2016), σ. 226

³⁵ ό. π., σ. 176

³⁶ ό. π., σ. 234, επίσης βλέπε Joint Test Publication 2-0, *Doctrine for Intelligence Support to Joint Operations*, The Joint Staff, Washington, D.C., June 1991, σ. IV-1 – IV-2 και JP 2-0, *Joint Intelligence*, Joint Chiefs of Staff, Οκτώβριος 2013, σ. I-23 – I-25

action.³⁷ Από τη μεριά του ο John Heidenrich σημειώνει πως «στρατηγική πληροφόρηση είναι αυτή που απαιτείται προκειμένου να σχεδιαστεί και να εφαρμοστεί μια υψηλή στρατηγική ή, όπως την αποκαλούν οι αξιωματούχοι, μια στρατηγική εθνικού επιπέδου».³⁸

Οι Carl Jensen, David McElreath και Melissa Graves γράφουν ότι η στρατηγική πληροφόρηση βλέπει σε βάθος χρόνου αφορώντας σε πολιτικά, οικονομικά, στρατιωτικά ζητήματα υψηλής σημαντικότητας / προτεραιότητας. Δεν διαφοροποιούνται με την JP 1-02 του 2010 σχετικά με τα καθήκοντα της επιχειρησιακής και τακτικής εξωτερικής (foreign) και εσωτερικής (domestic) πληροφόρησης. Περί της πρώτης ανατρέχουν στο *Title 50, United States Code 401a* της *National Security Act* του 1947 αποδίδοντας σ' αυτήν κατασκοπευτική δράση προς όφελος των policymakers. Επίσης προς όφελος των ιδίων (των policymakers), συνεχίζουν, λειτουργεί η εσωτερική πληροφόρηση με σκοπό αυτή τη φορά την εκ μέρους τους αρτιότερη άσκηση πολιτικής στο εσωτερικό περιβάλλον.³⁹

Τέλος, ο Antony Antoniou γράφει πως: α) η στρατηγική πληροφόρηση απευθύνεται σε ανώτατους πολιτικούς και στρατιωτικούς ηγέτες, ανώτατους κρατικούς υπαλλήλους, εκτελεστικούς διευθυντές μεγάλων consortium κ. λ. Σκοπό αποτελεί η επιβοήθεια στην ανάπτυξη στρατηγικών πλάνων κρατικού αλλά και ιδιωτικού ενδιαφέροντος, η επίβλεψη του διεθνούς περιβάλλοντος προς ενημέρωση κρατικών και ιδιωτικών φορέων, η επιβοήθεια στην ανάπτυξη στρατιωτικών και επιχειρηματικών πλάνων και η επιβοήθεια στην εκτέλεση στρατηγικών σχεδιασμών κρατικής και ιδιωτικής σπουδαιότητας, β) η επιχειρησιακή πληροφόρηση απευθύνεται σε ανώτερους στρατιωτικούς διοικητές, αξιωματούχους, μάνατζερ κ. λ. Σκοπό έχει την αποκάλυψη των στρατιωτικών δυνατοτήτων και προθέσεων του εχθρού (δημόσιος τομέας) όπως και την αποκάλυψη των εταιρικών δυνατοτήτων και προθέσεων του ανταγωνιστή (ιδιωτικός τομέας), την επίβλεψη των όποιων επιχειρησιακών θεάτρων, περιβαλλόντων κ. λ., την επιβοήθεια στο σχεδιασμό και στην εκτέλεση των όποιων επιχειρησιακών πλάνων κρατικού ή ιδιωτικού συμφέροντος και την αναγνώριση του κέντρου βάρους των ανταγωνιστών είτε αυτοί αποτελούν κρατικούς είτε ιδιωτικούς φορείς, γ) η τακτική πληροφόρηση αποτελείται σε στρατιωτικούς διοικητές και οικονομικούς μάνατζερ με σκοπό την επιβοήθεια στον σχεδιασμό και στη διεξαγωγή της μάχης όπως και την επιβοήθεια στον σχεδιασμό και στη διεξαγωγή της μάχης στον οικονομικό στίβο και την απόδοση πληροφόρησης πέραν άμεσων απειλών στρατιωτικής / επιχειρηματικής υφής.⁴⁰

Οι τύποι της πληροφόρησης

Οι τύποι πληροφόρησης που μια χώρα επιζητεί είναι ποικίλοι. Ενδέχεται να υπάρξει ενδιαφέρον για πολιτική, στρατιωτική, επιστημονική, οικονομική / βιομηχανική ή άλλη ενημέρωση. Εντύπωση ίσως προκαλεί το γεγονός της κατάταξης της πολιτικής πληροφόρησης στο τελευταίο επίπεδο αξιοπιστίας. Αν και πλέον ζητούμενη, δύσκολα αξιολογείται ξεκομμένη από άλλες συνιστώσες προκειμένου πρόβλεψης πολιτικών

³⁷ Johnson L., *Secret Agencies U.S. Intelligence in a hostile world*, Yale University Press, ΗΠΑ, 1996, σ. 2

³⁸ Heidenrich John, "The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence" στο *Studies in Intelligence*, Volume 51, Number 2, 2007, σ. 16

³⁹ ό. π., σ. 7-8. Οι μελετητές ουσιαστικά δηλώνουν ότι domestic intelligence ίσον ομπρέλα κάτω από την οποία βρίσκουν θέση οι υπηρεσίες ασφαλείας / law enforcement και αντιπληροφόρησης

⁴⁰ Antoniou Antony, *Open Source Information. The Future of Intelligence*, European Intelligence Academy, E-Book, Number 1, Μάιος 2013, σ. 40

ενδεχομένων επί των οποίων, έτσι ή αλλιώς, δρουν εσωτερικές / εξωτερικές δυνάμεις, ανορθολογικές επιρροές, απρόβλεπτοι παράγοντες, η τυχειότητα / τύχη κ. λ.⁴¹

Ο Edward Waltz κάνει λόγο για: α) *εθνική πληροφόρηση (national intelligence)* με σκοπό την κατανόηση του διεθνούς περιβάλλοντος και της συμπεριφοράς των διεθνών δρώντων, β) *στρατιωτική πληροφόρηση (military intelligence / MI)* με σκοπό την κατανόηση / εκτίμηση στρατιωτικών απειλών, την καταγραφή υπόπτων ενδείξεων και την προειδοποίηση (indication & warning / I & W), τη στοχοποίηση οπλικών συστημάτων (weapons targeting) και την εκτίμηση της ζημίας που υπέστη ο αντίπαλος εξ αιτίας πλήγματος εν καιρώ πολέμου, γ) *επιχειρηματική πληροφόρηση (business intelligence / BI)* με σκοπό τη συλλογή / ανάλυση στοιχείων που σχετίζονται με εσωτερικούς και εξωτερικούς οικονομικούς παράγοντες και δ) *πληροφόρηση περί του ανταγωνιστού (competitor intelligence / CI)* με σκοπό την αποκάλυψη των προθέσεων του αντιπάλου entrepreneur.⁴²

Ο Hank Prunckun αναφέρεται στην εθνική πληροφόρηση χρησιμοποιώντας τον όρο *πληροφόρηση εθνικής ασφαλείας (national security intelligence)* αλλά και *πληροφόρηση εξωτερικής πολιτικής (foreign policy intelligence)* με σκοπό την αποκρυπτογράφηση κάθε στοιχείου ικανού να επηρεάσει τις εξωτερικές αλλά και εσωτερικές εξελίξεις. Πρόκειται για τον ευρύτερο τύπο πληροφόρησης· ουσιαστικά ομιλούμε για σύνθετη πληροφόρηση (ή για σύνθεση πληροφοριών) στην άγρα της οποίας βρίσκονται πολιτικοί και στρατιωτικοί μηχανισμοί. Πέραν της στρατιωτικής και επιχειρηματικής πληροφόρησης ο Prunckun γράφει για *πληροφόρηση επιβολής νόμου (law enforcement intelligence)* και, τέλος, για *ιδιωτική πληροφόρηση (private intelligence)*. Στην πράξη το law enforcement intelligence⁴³ είναι ίσως ευρύτερο από αυτό που η ελληνική μετάφραση αποδίδει. Έχει να κάνει με πληροφόρηση χρήσιμη σε κάθε είδους αστυνομικό οργανισμό ή οργανισμό ασφαλείας, αντιτρομοκρατίας, οικονομικών υπηρεσιών, υπηρεσιών μετανάστευσης, τελωνείων, υπηρεσιών πάταξης λαθρεμπορίου, διακίνησης επικίνδυνων υλικών, οργανωμένου εγκλήματος κ. λ. Τέλος το private intelligence σχετίζεται με ένα πολλαπλό δίκτυο παροχών που προσφέρεται από ιδιώτες σε ιδιώτες με σκοπό την παρακολούθηση στόχων, την ανάλυση πληροφοριών, την εταιρική αντικατασκοπία, την προστασία προσώπων κ. λ.⁴⁴

Ο David M. Keithy κάνει λόγο για τους εξής τρεις τύπους: α) *βασική πληροφόρηση (basic intelligence)*, β) *τρέχουσα πληροφόρηση (current intelligence)* και γ) *πληροφοριακή εκτίμηση (intelligence estimate)*. Η πρώτη έχει να κάνει με παρελθοντικά γεγονότα, είναι, δε, σχετικά αδιαφοροποίητη. Η δεύτερη αφορά σε τρέχουσες καταστάσεις. Η τρίτη προσπαθεί να αποκρυπτογραφήσει το παρόν όπως επίσης να εκτιμήσει το μέλλον.⁴⁵

Στην FM 2-0, *Intelligence*, του 2004 διαβάζουμε για έξι τύπους πληροφόρησης ήτοι, α) *της καταγραφής υπόπτων ενδείξεων και προειδοποίησης (indication &*

⁴¹ *Intelligence and Counterintelligence. Spy Agencies, Intelligence Operations, and the People Behind Them*, επιμ. Curley Rob, ό. π., chapter 1

⁴² Waltz Edward, *Knowledge Management in the Intelligence Enterprise*, Artech House, Inc, Μασαχουσέτη / ΗΠΑ, 2003, σ. 14-15. Επίσης περί επιχειρησιακής και τακτικής στρατιωτικής πληροφόρησης βλέπε Waltz Edward, *Information Warfare, Principles and Operations*, Artech House, Inc, Μασαχουσέτη / ΗΠΑ, 1998, σ. 115, table 4.3

⁴³ Περί στρατηγικής, επιχειρησιακής και τακτικής law enforcement πληροφόρησης αλλά και περί των ειδών / τύπων της τελευταίας βλέπε Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, ό. π., σ. 67-72

⁴⁴ Prunckun Hank, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, The Scarecrow Press, Inc., UK, 2010, σ. 12-15

⁴⁵ Keithy M. D., "Intelligence Fundamentals" στο *Homeland Security and Intelligence*, επιμ. Logan G. K., Praeger, California, 2010, σ. 44

warning) με σκοπό την απόδοση επειγόντων (time-sensitive) πολιτικών, στρατιωτικών ή άλλων ευαίσθητων πληροφοριών στην εθνική ή όποια συμμαχική ηγεσία, β) των *τρεχουσών πληροφοριών* (current intelligence) με σκοπό την ενσωμάτωση / ενοποίηση, εντός συνεκτικών αναφορών, στοιχείων σχετικών με την τρέχουσα / εξελισσόμενη κατάσταση στο πεδίο επιχειρήσεων, γ) της *γενικής στρατιωτικής πληροφόρησης* (general military intelligence) με σκοπό την αποκάλυψη των στρατιωτικών δυνατοτήτων των ανταγωνιστών ή την αποκάλυψη στοιχείων και πλάνων ικανών να επηρεάσουν την (αμερικανική) εθνική ή πολυεθνική / συμμαχική στρατιωτική πολιτική και επιχειρησιακή τακτική, δ) της *ανάλυσης στόχου* (target intelligence) με σκοπό την ανάλυση των εχθρικών μονάδων, διατάξεων, εγκαταστάσεων / υποδομών και την αποκάλυψη σχετικών τρωτοτήτων, ε) της *επιστημονικής / τεχνολογικής πληροφόρησης* (scientific / technical intelligence -S&TI) με σκοπό τον προσδιορισμό του επιστημονικού / τεχνολογικού επιπέδου των ανταγωνιστών είτε επί πολιτικών είτε επί στρατιωτικών εφαρμογών και στ) της *αντικατασκοπίας / αντιπληροφόρησης* (counterintelligence) με σκοπό την αναγνώριση / αντιμετώπιση απειλών εκπορευομένων από αλλοδαπές Υπηρεσίες, μη κρατικούς δρώντες, το διεθνικό έγκλημα, την τρομοκρατία, κ. λ.⁴⁶

Ο Νίκος Κυριαζής γράφει ...*σήμερα ονομάζουμε την προσπάθεια υπεροχής στον τομέα της πληροφόρησης, 'κυριαρχία στην πληροφόρηση'. Στόχος είναι η έγκαιρη και σωστή συλλογή της, η έγκαιρη και σωστή ανάλυση και διοχέτευση προς τους τελικούς χρήστες, πολιτική και στρατιωτική ηγεσία και στρατιωτικές επιχειρησιακές μονάδες, που σημαίνει τοπική, χρονική και προθέσεων εικόνα πληροφόρησης.*⁴⁷ Κατά τούτο: α) *τοπική* ίσον εικόνα πληροφόρησης που καλύπτει το σύνολο της επικρατείας του αντιπάλου / στόχου μη αφήνοντας κενά εντός των οποίων δύναται να συγκεντρωθούν απαρατήρητα δυνάμεις του αντιπάλου / στόχου, β) *χρονική* ίσον διαρκής / εικοσιτετράωρη πληροφοριακή εικόνα με σκοπό την έγκαιρη διάγνωση κινήσεων του αντιπάλου / στόχου και την αποφυγή αιφνιδιασμού και γ) *προθέσεων* ίσον πληροφόρηση που αποκαλύπτει τη βαθύτερη επιδίωξη κάθε ενέργειας του αντιπάλου όπως και τις απόψεις / θέσεις του με σκοπό την έγκαιρη λήψη μέτρων / αντιμετρών. Η πληροφόρηση / ανάλυση προθέσεων οφείλει να αναζητεί / ανακαλύπτει το αίτιο, το λόγο και το στόχο αυτών ακριβώς των προθέσεων και των συνδεδεμένων (με τις προθέσεις) κινήσεων και ενεργειών πριν οι εν λόγω προθέσεις, κινήσεις και ενέργειες τελεσφορήσουν. Ποιες, π. χ., οι προθέσεις του Σαντάτ, ποιος ο στόχος των αιγυπτιακών κινητοποιήσεων πριν από τον πόλεμο του Γιομ Κιπούρ το 1973; Ποιες οι προθέσεις της αργεντίνικης χούντας ως προς τα Φώκλαντ πριν την εισβολή το 1982; Ποιες οι προθέσεις του Σαντάμ Χουσεΐν ως προς το Κουβέιτ πριν την εισβολή το 1990; Το γεγονός τής -και στα τρία παραδείγματα- αποτυχίας τής *πληροφόρησης προθέσεων* ως προς την αποκάλυψη των επίβουλων σχεδιασμών καταδεικνύει την ιδιαίτερη δυσκολία επίτευξης ικανής πληροφόρησης αυτού του τύπου.⁴⁸

Τέλος, ενδιαφέρον παρουσιάζει η άποψη του υπτγου ε. α. Παναγιώτη Μαυρόπουλου. Ο ερευνητής κατατάσσει τις πληροφορίες σε δύο μεγάλες κατηγορίες. Στην πρώτη ανήκουν αυτές που χρησιμοποιούνται για την προσβολή του εχθρού σε κάθε επίπεδο (πολιτικό, στρατιωτικό, οικονομικό κ. λ.) ενώ στη δεύτερη αυτές που

⁴⁶ FM 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2004, σ. 2-5 – 2-7, επίσης βλέπε JP 2-0, *Joint Intelligence*, Joint Chiefs of Staff, Οκτώβριος 2013, σ. I-18 – I-20, Mazumadar Keshav, *Actionable Intelligence*, RIEAS, RIEAS e-Book No 5, Αθήνα, Σεπτέμβριος 2013, σ. 15

⁴⁷ Κυριαζής Νίκος, Σπανός Στέλιος, *Το Πρόσωπο του Πολέμου στον 21^ο Αιώνα*, Εστία, Αθήνα, 2000, σ. 136

⁴⁸ ό. π., σ. 137

αξιοποιούνται στον επηρεασμό της κοινής γνώμης χωρών που τίθενται στο στόχαστρο. Κατά τον τρόπο τούτο οι πληροφορίες της δεύτερης κατηγορίας σκοπό έχουν να διαφωτίσουν περί του ιστορικού, πολιτισμικού, θρησκευτικού κ. λ. υποβάθρου ενός λαού (ενός λαού που ταυτόχρονα αποτελεί *ακροατήριο-στόχο*)⁴⁹, ωστόσο, υποπτευόμαστε πως πρόκειται περισσότερο για ανεπεξέργαστες πληροφορίες παρά για ραφιναρισμένη πληροφόρηση.

Οι πηγές πληροφόρησης

Αν και η λαϊκή φαντασία πριμοδοτεί μια *cloak-and-dagger* δράση, το μεγαλύτερο τμήμα αραφινάριστων πληροφοριών προέρχεται από ανοικτές πηγές. Πάρα ταύτα ο Johnson ανατρέχοντας σε μαρτυρία αναλυτού της CIA (τουλάχιστον για το technical branch της Υπηρεσίας) αναφέρει τα εξής: *Αλήθεια είναι μεν ότι το 60% των δεδομένων προέρχεται από ανοικτές πηγές, το 25% από μια ενδιάμεση κατηγορία γνωστή ως gray area και μόνο το 15% από κατασκοπική δράση αλλά, αν και παρατηρείται μια τάση αποθέωσης της αξίας των ελεύθερων πηγών, συνηθέστατα οι πλέον πολύτιμες πληροφορίες κρύβονται στο τελευταίο 15% -αν το 85%, συμπληρώνουμε, μπορεί να συλλεχθεί από τη δράση οιοδήποτε (ή σχεδόν οιοδήποτε) οργανισμού ή προσώπου, κάτι τέτοιο δεν ισχύει για το εναπομένον ποσοστό. Σχετικά με το gray area intelligence σημειώνουμε ότι πρόκειται για μη κρυφή πληροφόρηση η οποία, ωστόσο, δεν αποτελεί κοινό κτήμα. Ο Johnson την καλεί *inside(r) information* κάτι που σημαίνει πως γνώση του περιεχομένου της έχει μια μικρή κοινότητα (πολιτικό / διπλωματικό, στρατιωτικό, επιστημονικό ή άλλο ειδικό προσωπικό)*⁵⁰ -στην ελληνική τη συναντάμε ως «εσωτερική πληροφόρηση». Οι Shulsky και Schmitt παρουσιάζονται επίσης επιφυλακτικοί ως προς την αξία και χρήση των ανοικτών πληροφοριών υποθέτοντας την ευκολία με την οποία ενδέχεται να καταστούν φορείς προπαγανδιστικών ή ψευδών μηνυμάτων. Η δυνατότητα άμεσης και σε πραγματικό χρόνο πρόσληψης ειδήσεων από το πολιτικό προσωπικό χωρίς, πολλές φορές, τη μεσολάβηση ενός τμήματος ανάλυσης ενέχει κινδύνους. Αυτοί κυρίως σχετίζονται με το μη έλεγχο / αξιολόγησή τους αλλά και με τη μη σύνδεσή τους με άλλα κομμάτια του παζλ, συνεπώς, η πιθανότητα δημιουργίας παρανοήσεων αυξάνεται.⁵¹

Κατά τον Michael Warner οι πηγές ενός μελετητή θεμάτων πληροφόρησης χωρίζονται σε *εσωτερικές* και *εξωτερικές*. Οι πρώτες αναφέρονται στο «φάκελο» της όποιας αποστολής χαρακτηρίζοντας το είδος της τελευταίας, αποδίδοντας λεπτομερειακά το επιχειρησιακό της profile. Συγκεκριμένα πρωτόκολλα καθορίζουν πώς θα αρχειοθετηθεί ένας φάκελος, πώς θα διατηρηθεί, σε ποιους θα αποδοθεί, αν και πότε θα ανοιχτεί, αν θα καταστραφεί. Ο ερευνητής ελέγχει όλα τα σχετικά αρχεία μιας υπόθεσης στην οποία του δίδεται πρόσβαση. Αυτό σημαίνει πως η έρευνα ίσως κρατήσει χρόνια καθώς μια περίπτωση μπορεί να περιγράφεται μέσα από χιλιάδες σελίδες / έγγραφα που, ενδεχομένως, βρίσκονται καταχωρημένα σε διαφορετικές Υπηρεσίες. Πρακτικά, τίποτα δεν επιβάλλει την τήρηση φακέλου. Υπάρχουν υποθέσεις που στερούνται αρχείου λόγω πολιτικών επιταγών ή άλλων κωλυμάτων. Από και πέρα πάντα παραμένει η πιθανότητα εμφάνισης νέων στοιχείων, μαρτυριών κ. λ. Η αναψηλάφηση του αρχείου των επικοινωνιών, εκθέσεις σχετικές με τον

⁴⁹ Μαυρόπουλος Παναγιώτης, *Εισαγωγή στη Θεωρία του Πολέμου και της Στρατηγικής*, Αθήνα, 2012, σ. 174-175

⁵⁰ Johnson L., *Secret Agencies U.S. Intelligence in a hostile world*, ό. π., σ. 1-4

⁵¹ Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, Brassey's, Inc., Washington, D.C., HPIA, 2002³, σ. 173

προϋπολογισμό μιας δράσης, με τα άτομα που έλαβαν μέρος σ' αυτήν, ο έλεγχος ηλεκτρονικών δεδομένων / data κ. λ. ενδέχεται να κομίσουν ενδείξεις ή να παράξουν αποδείξεις του χαρακτήρα ενός εγχειρήματος.

Οι εξωτερικές πηγές αναφέρονται σε ελεύθερα ή απελευθερωμένα στοιχεία. Οι δημοσιογραφικές αναρτήσεις / αναλύσεις αποτελούν μια άλλη εξωτερική / ανοιχτή πηγή με κάποιες Υπηρεσίες (CIA, MI5, MI6) να προβαίνουν σε τακτικές δημοσιεύσεις. Οπωσδήποτε, και σε κάθε περίπτωση, ο ερευνητής πρέπει να διαθέτει εμπειρία, αλλά και διαίσθηση, ώστε να διαχωρίσει το γεγονός από το μύθευμα, το πραγματικό από την ανέξοδη φημολογία.

Πρέπει να σημειωθεί πως τόσο τα άτομα με πρόσβαση σε εσωτερικές όσο και τα άτομα που αξιοποιούν εξωτερικές πηγές αντιμετωπίζουν το πρόβλημα της μη δυνατότητας *συγκριτικής πληροφοριακής ανάλυσης*. Οι πρώτοι δεν μπορούν, τουλάχιστον στα αρχικά στάδια, να μοιραστούν την έρευνά τους με την υπόλοιπη ερευνητική κοινότητα, οι δεύτεροι στερούνται στοιχείων από την πηγή.⁵²

Ένας άλλος τρόπος κατηγοριοποίησης αφορά στις *πρωτογενείς, δευτερογενείς και τριτογενείς* πηγές. Πολύ συνοπτικά αναφέρουμε ότι οι πρώτες βρίσκονται σε άμεση σύνδεση με το προς έρευνα γεγονός (π. χ. μαρτυρίες πρωταγωνιστών), οι δεύτερες αποτελούν συνήθως αναλύσεις ή μεταφράσεις ειδικών, περιγραφές ή εκτιμήσεις από δεύτερο χέρι, σχόλια ή κριτικές από τρίτους κ. λ. ενώ οι τελευταίες διατηρούν ρόλο ευρετηρίου εντός του οποίου εναποθέτονται οι δύο πρώτες. Γίνεται κατανοητό ότι οι πρωτογενείς πηγές σχετίζονται συχνά με εσωτερικές κομίζοντας μέγιστη αξία τη στιγμή που οι δευτερογενείς, συνδεδεμένες με εξωτερικές, φέρουν σχετική χωρίς αυτό να σημαίνει πως η αξιοπιστία των πρώτων είναι αδιαπραγμάτευτη.⁵³

Συμπεράσματα

Ο Martin T. Bimfort γράφοντας, εν έτει 1958, περί των ορισμών του intelligence διαπιστώνει ότι αυτοί ομιλούν κυρίως για συλλογή, ανάλυση και διασπορά πληροφοριών που αφορούν σε ξένες δυνάμεις ή για διαδικασίες παραγωγής ενός τελικού (πληροφοριακού) προϊόντος που σκοπό έχει την επικουρία στον πολιτικό σχεδιασμό. Ο Bimfort παρατηρεί πως δεν γίνεται λόγος για ενέργειες που σχετίζονται με πολιτική δράση και προπαγάνδα, αξιοποίηση ανοικτών πηγών και αντιμετώπιση εσωτερικών απειλών ⁵⁴ παρά: α) την αναφορά σε ξένες δυνάμεις και αλλοδαπούς πράκτορες και β) την αναφορά της National Security Act (1947) στην αντικατασκοπευτική έννοια. Ασφαλώς, συν τω χρόνω, οι υπηρεσίες CI αποκτούν όλο και σημαντικότερη θέση, ο ίδιος μελετητής γράφει: «Η αντιπληροφόρηση αποτελεί οργανικό και όχι αρχιτεκτονικό (συμπληρωματικό) κομμάτι της πληροφόρησης. Είναι ό,τι τα λευκά αιμοσφαίρια και τα αντισώματα. Αν και μια ιδέα αντικατασκοπίας υπάρχει, οφείλουμε να αναπτύξουμε ικανά αμυντικά και επιθετικά μέτρα προκειμένου να προστατευθούν δράσεις και προϊόντα».⁵⁵

Το 1958 ανήκει στο παρελθόν. Από τότε η έννοια «intelligence» εμπλουτίστηκε. Ευρεία γκάμα ορισμών σε θεωρητικό και επιχειρησιακό επίπεδο εμφανίστηκε. Σ'

⁵² Warner M., "Sources and methods for the study of intelligence" στο *Handbook of Intelligence Studies*, επιμ. Johnson L., Routledge, Βρετανία, 2007, σ. 18-26, Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, Ποιότητα, Αθήνα, 2010, σ. 59-60

⁵³ Antoniou Antony, *Open Source Information. The Future of Intelligence*, ό. π., σ. 9-10

⁵⁴ Bimfort T. Martin, "A Definition of Intelligence" στο *Studies in Intelligence*, Volume 2, Number 4, 1958, διαθέσιμο και στην διαδικτυακή τοποθεσία https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm όπου ανατρέξαμε την 4^η Μαρτίου 2016

⁵⁵ Bimfort T. Martin, "A Definition of Intelligence", ό. π.

αυτό συνετέλεσαν λόγοι πολιτικοί, διεύρυνσης της έννοιας της ασφαλείας, τεχνολογικοί κ. λ. Κανείς δεν γνωρίζει αν, ενώ πλησιάζουμε στο τέλος της δεύτερης δεκαετίας του 21^{ου} αιώνα, οι ερευνητές κατόρθωσαν να την αναλύσουν σε άρτιο βαθμό. Αυτό που φαίνεται είναι μια σχετική συμφωνία στον πυρήνα των μελετών. Όσο οι εξελίξεις τρέχουν τόσο οι ορισμοί αναπροσαρμόζονται.

ΠΡΟΣΘΗΚΗ

Ο πληροφοριακός κύκλος

Intelligence και πληροφοριακός κύκλος

Ο Mark Phythian γράφει πως ο επονομαζόμενος *πληροφοριακός κύκλος* συνδέεται με ένα οξύμωρο: αν και όλες οι σύγχρονες μελέτες της πληροφόρησης ανοίγουν με την παρουσίασή του, δεν υφίσταται κάποιος ακριβής «χάρτης» της πληροφοριακής οργάνωσης και διαδικασίας. Περαιτέρω, έρευνες δείχνουν ότι το χάσμα μεταξύ της θεωρητικής απόδοσής του και της πραγματικότητας διευρύνεται -με λίγα λόγια η χρησιμότητά του διερευνάται και όπως σημειώνει ο Robert Clark «όταν πιεστούν οι παράγοντες της πληροφόρησης, τότε, παραδέχονται πως η πληροφοριακή διαδικασία 'δεν λειτουργεί έτσι'». ⁵⁶ Πάρα ταύτα η συγκεκριμένη προσθήκη προσπαθεί να επιδώσει μια εικόνα του φαινομένου 'πληροφοριακός κύκλος', ενός φαινομένου που κατά το μάλλον ή ήττον συμπυκνώνει τόσο τη θεωρία όσο και την πράξη της πληροφοριακής λειτουργίας.

Πληροφοριακός κύκλος καλείται η διαδικασία που ξεκινά με την υποβολή των πληροφοριακών αιτημάτων των κρατικών πολιτικοστρατιωτικών επιτελείων στις Υπηρεσίες και καταλήγει στην ανατροφοδότηση / αναπληροφόρηση μεταξύ των δύο πλευρών. Θεμελιώδη σκοπό αποτελεί η παροχή πληροφόρησης στους οικείους decisionmakers προς βελτίωση της διαδικασίας λήψεως αποφάσεων.

Ανατρέχοντας στο *Words of Intelligence. A Dictionary* διαβάζουμε ότι ο κύκλος της πληροφόρησης αποδίδει σύνολο εργασιών μέσω των οποίων επιτυγχάνεται: α) η κτήση των πληροφοριών, β) η μετατροπή των πληροφοριών σε πληροφόρηση και γ) η μεταφορά της πληροφόρησης στους ενδεδειγμένους λήπτες. Οι εργασίες για τις οποίες κάνουμε λόγο αναφέρονται: α) στον ορισμό των πληροφοριακών απαιτήσεων όπως και στην προετοιμασία του πλάνου συλλογής πληροφοριών (planning and direction), β) στη συλλογή των πληροφοριών (collection), γ) στην αρχική επεξεργασία των πληροφοριών (processing), δ) στη μετατροπή της πληροφορίας σε πληροφόρηση μέσω της αναλυτικής διαδικασίας (production), ε) στην απόδοση της πληροφόρησης στους θεσμικούς λήπτες (dissemination).⁵⁷

Ο Fred Schreier γράφει ότι η πληροφόρηση παράγεται μέσα από επάλληλη διαδικασία έξι σταδίων που συμποσούμενα δομούν τον κύκλο της, ειδικότερα πρόκειται για τα στάδια: α) του ορισμού των πληροφοριακών αναγκών, του σχεδιασμού και των κατευθύνσεων (planning and direction), β) της συλλογής των πληροφοριών (collection), γ) της αρχικής επεξεργασίας των πληροφοριών (processing), δ) της ανάλυσης των πληροφοριών (analysis), ε) της διασποράς του τελικού πληροφοριακού προϊόντος (dissemination) και στ) της ανατροφοδότησης (feedback).

Το πρώτο βήμα αφορά τον προσδιορισμό των πληροφοριακών αναγκών («χρειαζόμαστε πληροφόρηση για εκείνο ή το άλλο θέμα»). Ουσιαστικά, ομιλούμε για την εκ μέρους των παραγωγών πληροφόρησης παραλαβή των πληροφοριακών απαιτήσεων των ανωτάτων κρατικών στελεχών.

Το δεύτερο σχετίζεται με τη συλλογή στοιχείων / δεδομένων ικανών κατά τα φαινόμενα να επιβοηθήσουν στη λύση των τεθέντων ερωτημάτων / προβληματισμών,

⁵⁶ Phythian Mark, "Beyond the Intelligence Cycle?" στο *Understanding the Intelligence Cycle*, επιμ. Phythian Mark, Routledge, Βρετανία, 2013, σ. 1, επίσης βλέπε Clark Robert, *Intelligence Analysis: A Target-Centric Approach*, CQ Press, Washington, D.C., 2003, σ. 11

⁵⁷ Goldman Jan, *Words of Intelligence. A Dictionary*, The Scarecrow Press, Inc., USA, 2006, σ. 80-81

κατ' ουσίαν να επιβοηθήσουν τη διαδικασία λήψεως αποφάσεων εκ μέρους πολιτικών, στρατιωτικών και λοιπών άλλων επιτελικών. Η συλλογή πληροφοριών κατηγοριοποιείται σε συλλογή μέσω: α) ανοικτών πηγών (open source intelligence - OSINT), β) ανθρωπίνου δυναμικού (human intelligence - HUMINT), γ) καταγραφής / υποκλοπής ραδιοσημάτων ή άλλων ηλεκτρομαγνητικών εκπομπών (signal intelligence - SIGINT), δ) λήψεως εικόνων, φιλμ κ. λ. με τη χρήση δορυφορικών συστημάτων, UAVs και άλλων hi-tech μηχανισμών (imagery intelligence - IMINT / τηλεπισκόπηση), ε) αναγνώρισης δυνατοτήτων / χαρακτηριστικών οπλικών εχθρικών συστημάτων (measurement and signatures intelligence - MASINT).

Το τρίτο βήμα έχει να κάνει με τη μετατροπή των συλλεγομένων στοιχείων σε μορφή ικανή προς ανάλυση. Λόγου χάρη, ένα έγγραφο στην αλλοδαπή πριν αναλυθεί πρέπει να μεταφραστεί. Άλλο παράδειγμα σημαίνει το «συμμάζεμα» ενός ευρέος όγκου δεδομένων σε έναν πιο στοχευμένο / διαχειρίσιμο.

Το τέταρτο αναφέρεται στη μετατροπή των πρωτογενών δεδομένων / πληροφοριών (που έχουν περάσει εφόσον κριθεί αναγκαίο από το τρίτο στάδιο) σε πληροφόρηση. Γίνεται κατανοητό πως κάθε πληροφορία δεν δεικνύει πληροφόρηση τη στιγμή που κάθε είδος πληροφόρησης προέρχεται από πληροφορίες.

Το πέμπτο αφορά στη διασπορά του τελικού προϊόντος (της πληροφορίας που έχει μετατραπεί σε πληροφόρηση) στους εντεταλμένους λήπτες ήτοι, στα πρόσωπα των οποίων οι πληροφοριακές ανάγκες εκίνησαν την όλη διαδικασία. Το τελικό προϊόν / πληροφόρηση πρέπει να διακρίνεται / χαρακτηρίζεται από: α) ικανότητα επίλυσης των αρχικών ερωτημάτων / προβληματισμών, β) έγκαιρη απόδοση, γ) ακρίβεια νοήματος, συμπεράσματος, προτάσεων, δ) λογικότητα, ε) διαφάνεια ήτοι, απαλλαγή από στρεβλώσεις εξ αιτίας πολιτικών επιρροών, παραπληροφόρηση, χειραγώγηση / μόχλευση κ. λ. Στοίχημα για τις Υπηρεσίες αποτελεί η παραγωγή πληροφόρησης που από τη μια ανταποκρίνεται στις απαιτήσεις του εντολέα ενώ από την άλλη, εντοπίζοντας περιορισμούς και αδυναμίες, δεν παρασύρει.

Το έκτο και τελικό στάδιο δεν αποτελεί άλλο από διαμοιβή μεταξύ εντολέων και Υπηρεσιών-ών με σκοπό την απάντηση ερωτημάτων σχετικών με το περατωθέν έργο. Ήταν ικανοποιητικό; Βοήθησε τους διαμορφωτές πολιτικής; Περαιτέρω, οι εντολείς, χρήστες πλέον της πληροφόρησης, ίσως ζητήσουν διευκρινήσεις ή επιδώσουν νέα καθήκοντα ανατροφοδοτώντας την όλη διαδικασία.⁵⁸

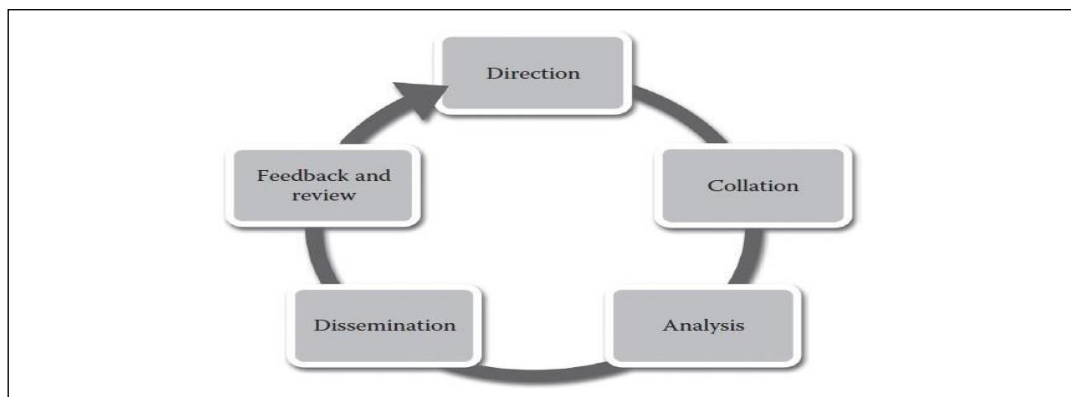
Ο Άντονι Αντωνίου παρουσιάζει ένα παρόμοιο σχήμα με αυτό του Schreier με την διαφορά πως βαπτίζει το πρώτο στάδιο (planning and direction) με τον όρο requirements ήτοι, πληροφοριακές ανάγκες -ποια ζητήματα χρήζουν ιδιαίτερης πληροφόρησης; ποια από αυτά τα ζητήματα απαιτούν αντιμετώπιση κατά προτεραιότητα;⁵⁹

Ο John Buckley κυρώνει ουσιαστικά τις ανωτέρω προσεγγίσεις αντικαθιστώντας το λήμμα *συλλογή* / *collection* με το λήμμα *συν-άθροιση* / *collation*. Ειδικότερα ομιλεί για: α) ορισμό πληροφοριακών αναγκών, β) συν-άθροιση πληροφοριών, γ) ανάλυση πληροφοριών, δ) διασπορά τελικού προϊόντος, ε) πληροφοριακή εκτίμηση και ανατροφοδότηση.⁶⁰

⁵⁸ Schreier Fred, *Transforming Intelligence Services. Making Them Smarter, More Agile, More Effective and More Efficient*, ό. π., σ. 27-32

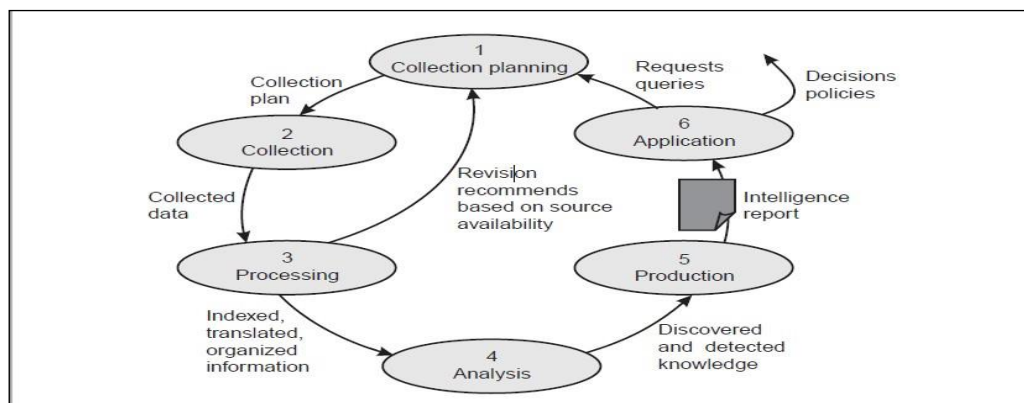
⁵⁹ Antoniou Antony, *Open Source Information. The Future of Intelligence*, ό. π., σ. 15, 16

⁶⁰ Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, ό. π., σ. 150



Εικόνα 2: ο πληροφοριακός κύκλος του Buckley. Η εικόνα ελήφθη από το *Managing Intelligence. A Guide for Law Enforcement Professionals* του John Buckley, CRC Press / Taylor & Francis Group, Florida / USA, 2014, σ. 150

Σύμφωνα με τον Edward Waltz η διαδικασία παραγωγής στρατηγικής και επιχειρησιακής πληροφόρησης συναρτάται με έξι διακριτές φάσεις, πιο συγκεκριμένα: α) τη φάση των κατευθυντηρίων γραμμών και απαιτήσεων (collection planning), β) τη φάση της συλλογής των πληροφοριακών στοιχείων, γ) τη φάση της αρχικής εκκαθάρισης των συλλεχθέντων δεδομένων ή, αλλιώς, τη φάση της προ-ανάλυσης, δ) τη φάση της ανάλυσης των στοιχείων, ε) τη φάση της παραγωγής του τελικού προϊόντος. Το τελευταίο διαχωρίζεται σε (1) *current intelligence report*, (2) *basic intelligence report*, (3) *intelligence estimate*, στ) τη φάση της διασποράς της πληροφόρησης και ταυτόχρονα της διαμοιβής μεταξύ Υπηρεσιών και κρατικής ηγεσίας (application) με σκοπό απαντήσεις σε πιθανές ερωτήσεις της δεύτερης, την εκτίμηση της αξίας / ακρίβειας του αποδιδόμενου προϊόντος κ. λ.⁶¹



Εικόνα 3: ο πληροφοριακός κύκλος κατά τον Waltz, εικόνα ληφθείσα από το *Information Warfare Principles and Operations*, Artech House, Inc., 1998, σ. 116

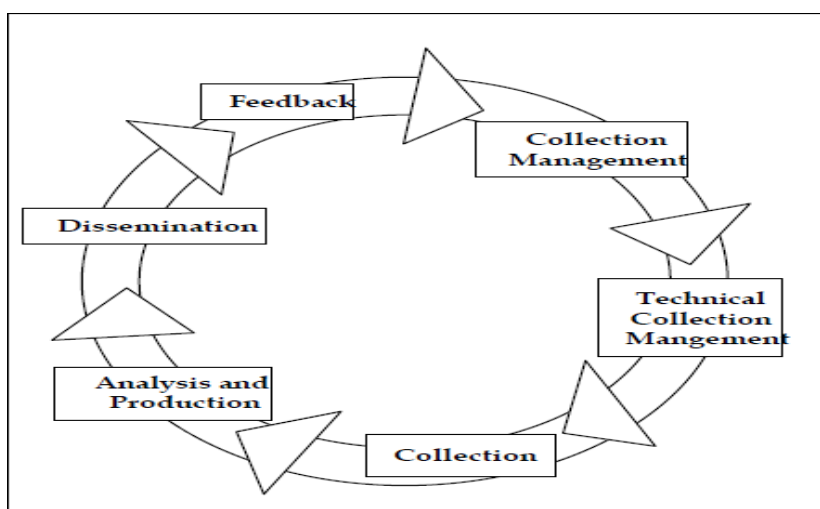
Ο Lock Johnson επισημαίνει ότι ο πληροφοριακός κύκλος δεν δεικνύει τόσο μια ακολουθία διακριτών φάσεων όσο μια διαδικασία αλληλεπίδρασης εντός της οποίας εμπλέκονται παράγοντες των Υπηρεσιών και της πολιτικής.⁶² Σύμφωνα με τον Mark Lowenthal η πληροφοριακή κοινότητα επικοινωνεί με το πολιτικό επιτελείο

⁶¹ Waltz Edward, *Information Warfare Principles and Operations*, ό. π., σ. 113-116

⁶² Johnson Lock, "National Security Intelligence in the United States: A Performance Checklist" στο *Intelligence and National Security*, Volume 26, Number 5, 2011, σ. 607-612

αραιότερα από όσο επιβάλλεται, μάλιστα, σε ορισμένες περιπτώσεις καθόλου με αποτέλεσμα τη δημιουργία ασυνεννοησιών. Ο ίδιος τονίζει ότι η μη απόδοση feedback προσομοιάζει με άρνηση ή ανικανότητα του πολιτικού να ορίσει τις πληροφοριακές του ανάγκες.⁶³ Ο Arthur Hulnick ολοκληρώνει την κριτική του Lowenthal μιλώντας για παθογένειες του πληροφοριακού κύκλου. Πιο συγκεκριμένα γράφει για: α) μια συχνή ασυνεννοησία μεταξύ παραγωγών και εντολέων / ληπτών πληροφόρησης, β) την «ικανότητα» μίας και μόνο μη ορθής πληροφορίας να περιπλέξει τη διαδικασία της ανάλυσης, γ) την, πολλές φορές, μη συμπόρευση μεταξύ συλλεκτικών και αναλυτικών φάσεων, δ) την πιθανή μη αξιοποίηση του τελικού προϊόντος είτε διά λόγους ποιότητας, είτε διά λόγους πολιτικών σκοπιμοτήτων.⁶⁴

Αναφορικά με τους θεσμούς / οργανισμούς σημειώνουμε ότι ουσιαστικά δεν παρατηρείται διαφοροποίηση της απόδοσης του πληροφοριακού κύκλου σε σχέση με τα ήδη κατατεθέντα⁶⁵ τόσο το αμερικανικό National Institute for Public Policy⁶⁵ όσο το FBI⁶⁶, η CIA⁶⁷ και το ODNI⁶⁸ επιβεβαιώνουν τους άνω ερευνητές.



Εικόνα 4: Αποτύπωση του πληροφοριακού κύκλου κατά το National Institute for Public Policy. Η εικόνα ελήφθη από *Modernizing Intelligence: Structure and Change for the 21st Century*, επιμ. Victory C. B., National Institute for Public Policy, 2002, σ. 11

⁶³ Lowenthal M., *Intelligence. From Secrets to Policy*, CQPress, Washington, D. C., 2003², σ. 41-52

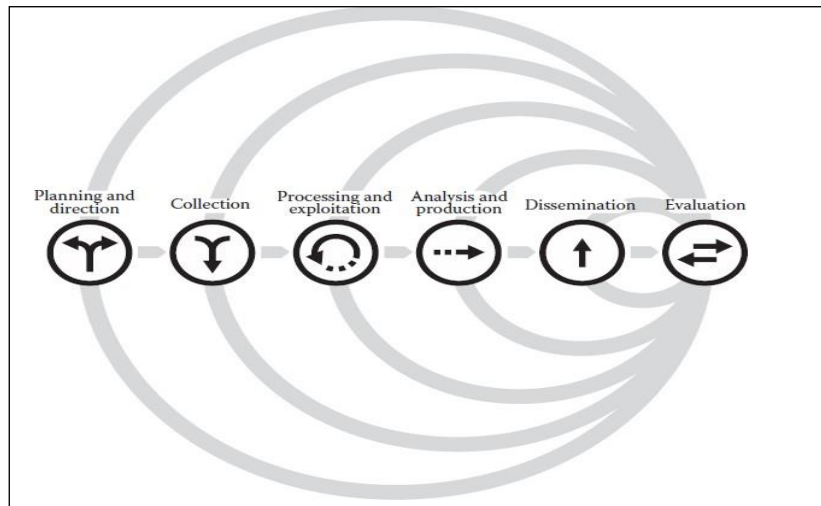
⁶⁴ Hulnick S. Arthur, "What's Wrong With The Intelligence Cycle?" στο *Strategic Intelligence*, Volume 2, επιμ. Johnson Lock, USA, 2007, σ. 1-10

⁶⁵ *Modernizing Intelligence: Structure and Change for the 21st Century*, επιμ. Victory C. B., National Institute for Public Policy, 2002, σ. 113

⁶⁶ Carter L. D., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, U.S. Department of Justice, 2004, σ. 65, επίσης βλέπε "Intelligence Cycle" στη δικτυακή σελίδα <https://www.fbi.gov/about-us/intelligence/intelligence-cycle> εις την οποία καταφύγαμε την 3^η Αυγούστου 2015

⁶⁷ *Encyclopedia of Espionage, Intelligence, and Security*, Volume 1, επιμ. Lerner K., Lerner B., Gale, HPIA, 2004, σ. 117, Turner Michael, *Historical Dictionary of United States Intelligence*, The Scarecrow Press, Inc., USA, 2006, σ. 97, Smith, W. Thomas, Jr., *Encyclopedia of the Central Intelligence Agency*, Facts On File, Inc., New York, 2003, σ. 137, επίσης στην ηλεκτρονική τοποθεσία https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/page_46.pdf όπου καταφύγαμε την 29 Μαΐου 2016

⁶⁸ *U.S. National Intelligence. An Overview 2013*, ODNI, σ. 4-6 και 29-56 στη δικτυακή τοποθεσία https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf όπου καταφύγαμε την 3^η Μαΐου 2016



Εικόνα 5. Ο πληροφοριακός κύκλος κατά το ODNI. Η εικόνα ελήφθη από το *U.S. National Intelligence. An Overview 2013*, ODNI, σ. 4

Σχετικά με τον στρατιωτικό πληροφοριακό κύκλο τονίζουμε την ομοιότητά του με τον κύκλο που αποδίδεται εκ του ODNI παρά τις όποιες μικροδιαφορές. Ο στρατιωτικός ερευνητής Geraint Evans προτείνει έναν κύκλο οκτώ βημάτων, αναλυτικότερα: α) του σχεδιασμού (planning), β) των κατευθύνσεων κατά βαθμό προτεραιότητας (direction and prioritization), γ) της συλλογής στοιχείων κατά προτεραιότητα (collection and prioritization), δ) της προ-αναλυτικής διαδικασίας (processing), ε) της αναλυτικής διαδικασίας (analysis), στ) της παραγωγής του τελικού προϊόντος (production), ζ) της διασποράς του τελικού προϊόντος (dissemination), η) της συζήτησης επί του τελικού προϊόντος (review).

Στο κέντρο του κύκλου εμφανίζεται η λεγόμενη «συνεχής εκτίμηση του επιχειρησιακού περιβάλλοντος όπως και των προθέσεων της διοίκησης». Τα οκτώ βήματα, σαν αριθμός, σχετίζονται με την αυστηρή ιεραρχική φύση των στρατιωτικών οργανισμών και την ανάγκη επισταμένης λογοδοσίας που χαρακτηρίζει το στρατιωτικό πεδίο.⁶⁹

Αυτά που πρωτίστως οφείλουμε να συγκρατήσουμε είναι τα εξής: α) ο πληροφοριακός κύκλος και η παραγόμενη πληροφόρηση λειτουργούν προς εξυπηρέτηση του ανωτάτου πολιτικού και στρατιωτικού προσωπικού και της διαδικασίας λήψεων αποφάσεων, β) όσον αφορά στην θεωρητική απόδοσή του αξιοσημείωτες διαφορές μεταξύ μελετητών ή Υπηρεσιών δεν υπάρχουν, γ) ο πληροφοριακός κύκλος δεν πρέπει να συγχέεται με τα τέσσερα στοιχεία / μέρη του intelligence ήτοι, τη συλλογή, την ανάλυση, την αντικατασκοπία (counterintelligence) και την κεκαλυμμένη δράση (covert action).⁷⁰ Τέλος, κατά τον Michael Handel η επιτυχία της πληροφοριακής διαδικασίας σχετίζεται με: α) τη διαθεσιμότητα πρωτογενών στοιχείων, β) την ικανότητα των αναλυτών να διακρίνουν μεταξύ σχετικών και μη σχετικών πληροφοριών ως προς την ικανοποίηση των όποιων

⁶⁹ Evans G., “Rethinking military intelligence failure -Putting the wheels back on the intelligence cycle” στο *Defense Studies*, Volume 9, Number 1, 2009, σ. 22-46

⁷⁰ Παρί των τεσσάρων στοιχείων / μερών της πληροφόρησης βλέπε Johnson L., *Secret Agencies. U.S. Intelligence in a hostile world*, ό. π., σ. 4 και Godson R., *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, Transaction Publishers, N. Jersey / ΗΠΑ, 2001, σ. 1-26. Τέλος, για ό,τι πιο αναλυτικό περί κύκλου πληροφόρησης βλέπε Omand David, “The Cycle of Intelligence” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, Βρετανία, 2014, σ. 59-70

πολιτικών ή στρατιωτικών αναζητήσεων, κατευθύνσεων, προβληματισμών, ερωτημάτων, σχεδιασμών κ. λ., γ) την ικανότητα των αναλυτών να πλησιάζουν την αλήθεια των καταστάσεων αποδίδοντας χρήσιμο τελικό προϊόν στην ηγεσία, δ) το επίπεδο της πολιτικής παρέμβασης στην πληροφοριακή διαδικασία.⁷¹

Counterintelligence και πληροφοριακός κύκλος

Ένα ερώτημα που πιθανώς εγείρεται είναι το εξής: υπάρχει διαφορά μεταξύ του κλασικού πληροφοριακού κύκλου και του πληροφοριακού κύκλου της αντικατασκοπίας;

Ο Hulnick σημειώνει πως το πρώτο στάδιο της αντικατασκοπευτικής λειτουργίας σχετίζεται με την αναγνώριση κινδύνων και την ταυτοποίηση ομάδων ή ατόμων που τους εκπροσωπούν. Οι σχετικές πληροφορίες προσπορίζονται είτε από ανοικτές πηγές, είτε από πηγές των υπηρεσιών επιβολής νόμου ή, τέλος, από ειδικευμένα τμήματα συλλογής των αντιπληροφοριακών οργανισμών. Πλείστες όσες χώρες όπως και το σύνολο των βιομηχανοποιημένων κρατών διατηρεί τέτοια τμήματα με εξαίρεση τις ΗΠΑ. Στις τελευταίες η συλλογή πληροφοριών σχετικών με την εθνική αντικατασκοπία προέρχονται από τις law enforcement υπηρεσίες (βλέπε περίπτωση FBI).⁷²

Το δεύτερο κομμάτι ενός αντικατασκοπευτικού σχεδιασμού σχετίζεται με την αμυντική ή επιθετική στρατηγική. Η πρώτη αφορά, π. χ., σε φυσική προστασία υποδομών / εγκαταστάσεων, σε διαβάθμιση πληροφοριών, σε έλεγχο προσωπικού κ. λ. Η δεύτερη αναφέρεται στη χειραγώγηση του αντιπάλου μέσω, συνηθέστατα, διείσδυσης στο πληροφοριακό του δίκτυο.⁷³

Το τρίτο βήμα, συνεχίζει ο συγγραφέας, έχει να κάνει με μια μάλλον ιδιότυπη σχέση μεταξύ των αντικατασκοπευτικών οργανισμών και των υπηρεσιών επιβολής νόμου. Πρόκειται για συνεργασία που καθίσταται αναγκαία εφόσον αποφασιστεί η σύλληψη του υπόπτου προσώπου για, π. χ., κατασκοπία -σημειώνουμε ότι τέτοιο δικαίωμα σπάνια έχει μια υπηρεσία Αντιπληροφοριών.⁷⁴

Το τέταρτο, προαιρετικό και υπό προϋποθέσεις, βήμα αφορά στη δημοσιοποίηση μιας πετυχημένης αντικατασκοπευτικής επιχείρησης. Ο στόχος διττός: α) ενισχύεται το προφίλ της Υπηρεσίας που οργάνωσε και εκτέλεσε τη δράση τόσο σε θεσμικό / γραφειοκρατικό επίπεδο όσο και σε επίπεδο κοινής γνώμης και β) αποστέλλεται μήνυμα στους όποιους επίβουλους χαρακτήρες πως «το σύστημα λειτουργεί».⁷⁵

Κατά τα ανωτέρω γίνεται φανερό ότι: α) συλλογή και προφανώς ανάλυση πληροφοριών αποτελούν κοινό τόπο τόσο στον κλασικό πληροφοριακό όσο στον αντιπληροφοριακό κύκλο, β) από τον κύκλο της αντιπληροφόρησης απουσιάζει το στάδιο της διασποράς και το ανάλογο της ανατροφοδότησης. Αυτό συμβαίνει διότι οι υπηρεσίες Αντικατασκοπίας δεν εφοδιάζουν, θεωρητικά, την ηγεσία με στοιχεία προκειμένου να στηριχθεί / βελτιωθεί η διαδικασία λήψεως αποφάσεων, γ) οι υπηρεσίες Αντικατασκοπίας μετέχουν στην εκτέλεση κρατικών σχεδιασμών (ή, αλλιώς, συνεργάζονται με άλλες κρατικές υπηρεσίες) και δ) η δημοσιοποίηση μιας αντικατασκοπευτικής επιτυχίας δεν είναι πάντα απαγορευτική. Σημειώνουμε μόλα ταύτα την εμφάνιση ενός *ιδιότυπου* feedback σε κείμενα που ασχολούνται με την

⁷¹ Handel M., *War, Strategy, and Intelligence*, Frank Cass & Co. Ltd., UK, 1989, σ. 187

⁷² Hulnick Arthur, "Intelligence theory: seeking better models" στο *Understanding the Intelligence Cycle*, επιμ. Phythian Mark, Βρετανία, 2013, σ. 156

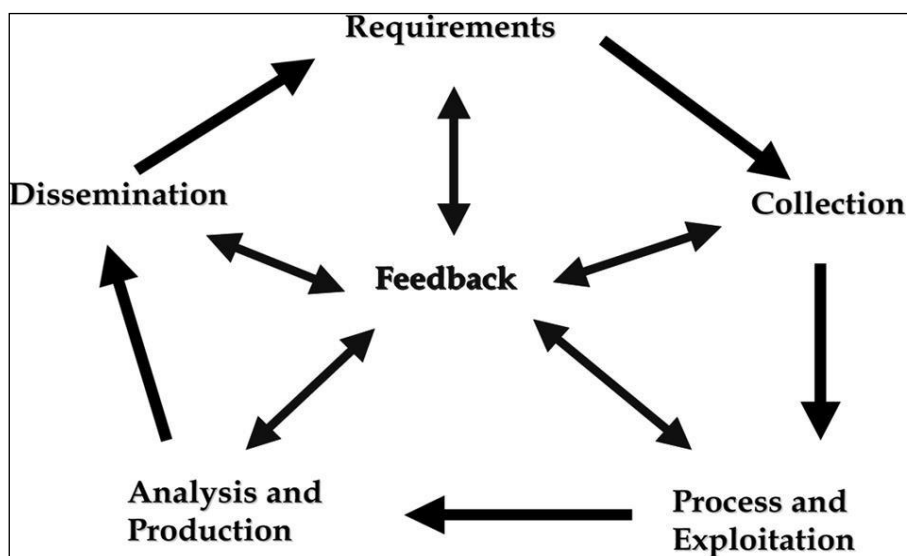
⁷³ ibid

⁷⁴ Hulnick Arthur, "Intelligence theory: seeking better models", ό. π., σ. 156-157

⁷⁵ ό. π., σ. 157

αντιπληροφόρηση. Δεν πρόκειται για αναφορά στο κλασικό πληροφοριακό feedback αλλά στην γνώση της αντίδρασης της αντίπαλης πλευράς σε περίπτωση που επιχειρείται μια παραπλανητική κίνηση εις βάρος της.

Αν από την άλλη μεριά ανατρέξουμε στο πρότυπο του Thomas C. Bruneau δεν θα διαπιστώσουμε καμία διαφορά μεταξύ πληροφοριακού και αντιπληροφοριακού κύκλου. Παρά το ότι ο Bruneau μιλά για intelligence και όχι για counterintelligence, η ενασχόλησή του με τρόπους πάταξης του τρομοκρατικού φαινομένου εμπεριέχει την ιδέα του αντικατασκοπευτικού σχεδιασμού σε ίδιο αν όχι σε πληθωρικότερο βαθμό σε σύγκριση με την ιδέα της κατασκοπευτικής δράσης. Μόνη ίσως διαφοροποίηση η εμφάνιση της ανατροφοδοτικής λειτουργίας σε κάθε σημείο του κύκλου προφανώς υπό την έννοια της αδιαλείπτου συνεργασίας Υπηρεσιών και πολιτικοστρατιωτικής ηγεσίας.⁷⁶



Εικόνα 6: ο (αντι)πληροφοριακός κύκλος κατά τον Thomas C. Bruneau. Η εικόνα ελήφθη από άρθρο του ίδιου με τίτλο “Democracy and Effectiveness: Adapting Intelligence for the Fight Against Terrorism” στο *International Journal of Intelligence and CounterIntelligence* εν έτει 2008

Εντούτοις αυτό που προσωπικά παρατηρούμε είναι πως εντός του αντιπληροφοριακού κύκλου ‘χάνεται’ ή δεν αποδίδεται ξεκάθαρα το κομμάτι της επιθετικής αντικατασκοπίας παρά την τοποθέτηση του Hulnick περί σχετικής στρατηγικής. Επί τη βάσει ποίου σκοπού θα λειτουργήσει η τελευταία; Θα δραστηριοποιηθεί με στόχο τη συλλογή πληροφοριών; Ή μήπως την παραπλάνηση του αντιπάλου; Αν ζητούμενο είναι η παραπλάνηση, τότε, μήπως αυτονομείται; Ή μήπως σ’ αυτήν την περίπτωση η διασπορά και η ανατροφοδότηση δεικνύουν απαραίτητα συστατικά; Επί τη βάσει αυτών των ερωτημάτων τόσο η θέση Hulnick όσο και αυτή του Bruneau προβληματίζουν. Η πρώτη εμπεριέχει την επιθετική αντιπληροφόρηση χωρίς ωστόσο χρεία διασποράς και ανατροφοδότησης. Η δεύτερη εμποτίζει την επιθετική αντικατασκοπία εντός της κατασκοπίας, ωστόσο, αν και το

⁷⁶ Bruneau T., “Democracy and Effectiveness: Adapting Intelligence for the Fight Against Terrorism” στο *International Journal of Intelligence and CounterIntelligence*, Volume 21, Issue 3, 2008, σ. 452-454

counterespionage ⁷⁷ παράγει positive intelligence δεν είναι espionage. Σε κάθε περίπτωση φαίνεται πως ο αντιπληροφοριακός κύκλος είναι στριφνότερος από τον πληροφοριακό επιβεβαιώνοντας τόσο τον Phythian όσο και τον Clark σχετικά με τη μη ύπαρξη ακριβούς «χάρτη» πληροφοριακής, με την ευρύτερη έννοια, οργάνωσης και διαδικασίας.

⁷⁷ Για την παρούσα μελέτη *counterespionage* ίσον *επιθετική αντικατασκοπία*. Πρόκειται για εκτύπωση με την οποία συμφωνεί ικανή μερίδα μελετητών. Για άλλους ωστόσο *counterespionage* ίσον μια, κατά το μάλλον ή ήττον, διαφορετική λέξη περί του πεδίου του *counterintelligence*. Για περισσότερες διευκρινήσεις βλέπε στο κεφάλαιο 4 της παρούσης

ΚΕΦΑΛΑΙΟ 3

Περί της θεωρίας της πληροφόρησης

...all attempts to develop ambitious theories of intelligence have failed

Walter Laqueur¹

Περί οιονεί θεωρίας πληροφόρησης

Αν προσπαθήσουμε να ανακαλύψουμε μια *Θεωρία Πληροφόρησης (Intelligence Theory)* θα βρεθούμε μπροστά είτε σε ένα αδιέξοδο είτε σε μια πλειάδα αποφάνσεων που αυτοπροσδιορίζονται υπό αυτή την ιδιότητα με τη σημαντικότητα, ωστόσο, να έγκειται μάλλον στην προσπάθειά τους να εξηγήσουν τι σημαίνει «intelligence», πώς κατανοείται ή ποιες προκλήσεις οφείλει να αντιμετωπίσει παρά κάτι άλλο. Ο David Kahn βεβαιώνει, εν έτει 2001, πως αν και το πεδίο υφίσταται εδώ και μια πενηνταετία ουσιαστικά δεν υπάρχει κάποια σχετική περί τη θεωρία πληροφόρησης πρόοδος. Μαζί του συμφωνούν τόσο ο Michael Warner όσο και ο Walter Laqueur παρά το ότι, όπως επισημαίνει ο Loch Johnson, μια όλο και αυξανόμενη παραγωγή άρθρων, εργασιών ή έργων πάνω σε θέματα πληροφόρησης καθίσταται φανερή.²

Πράγματι στις ΗΠΑ δομείται μια εκτεταμένη εργογραφία γύρω από την έννοια και τον ορισμό της πληροφορίας, τις δράσεις, τα ζητούμενα, τους προβληματισμούς κ. λ. -όλα αυτά υποθετικά απαιτούν ή κατατείνουν σε μια σχετική θεωρία. Το *Strategic Intelligence for American World Policy* του Sherman Kent φαίνεται πως χάραξε το δρόμο, από τότε έχουν ξεκινήσει γύρω αντιπαραθέσεων γύρω από το νόημα της πληροφόρησης, τις σχέσεις των Υπηρεσιών με το κράτος και την κοινωνία, ασφαλώς τη διαδικασία της ανάλυσης, τον πληροφοριακό κύκλο κ. ο. κ. Ωστόσο, και σύμφωνα με τον Philip Davies, πρόκειται για «διένεξη» που δεν αφορά στη δημιουργία μιας θεωρίας αλλά, καλύτερα, ενός «χάρτη» περί τη λειτουργία και χρήση της πληροφόρησης.³

Θεωρητικές πληροφοριακές αναζητήσεις

Ο Johnson τονίζει ότι *...μια καλή θεωρία πρέπει να διακρίνεται για την εξηγητική της ισχύ, τη λιτότητά της και, τέλος, για τη (δυννητική) διαψευσιμότητά της*. Ο ίδιος ευελπιστεί στην παραγωγή μιας οιονεί *grand theory* που θα υπηρετήσει το πεδίο ως ενιαίο πλαίσιο⁴ τη στιγμή που άλλοι ερευνητές, όπως ο Richard Betts, υποστηρίζουν πως κάτι τέτοιο δεν είναι εφικτό. Ο τελευταίος, σε αντίθεση με τον Johnson, διατείνεται πως το μόνο προσδόκιμο είναι, ίσως, μια δημιουργία «μικρών θεωριών» (*middle range theories*) που θα κληθούν να απαντήσουν σε επιμέρους προβληματισμούς όπως, π. χ., αυτού που γεννάται υπό την έποψη μιας αιφνίδιας επίθεσης με σκοπό τη μεγιστοποίηση στον όποιο βαθμό μιας δυνατότητας επιτυχούς

¹ Laqueur W., *A World of Secret. The Uses and Limits of Intelligence*, Basic Books, N.Y., 1985, σ. 8

² Bay Sebastian, *Intelligence Theories. A Literary Overview*, Lund University, Sweden, 2007, σ. 4

³ Davies Phillip, "Theory and intelligence reconsidered" στο *Intelligence Theory. Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, UK, 2009, σ. 189

⁴ Johnson L., "Sketches for a theory of strategic intelligence" στο *Intelligence Theory: Key questions and debates*, ό. π., σ. 33-53

αντίδρασης, βελτιώνοντας αυτό που ο ίδιος καλεί *batting average*.⁵ Ο Mark Phythian, κάπου στη μέση, διερωτάται αν οι σημερινές απαιτήσεις πρέπει να ικανοποιηθούν υπό το πρίσμα μιας ολιστικής απάντησης ή να αντιμετωπιστούν τμηματικά.⁶ Όπως και να τεθεί το ζήτημα η επιθυμία των θεωρητικών του χώρου κατατείνει είτε σε μία «θεωρία» είτε σε «(υπο)θεωρίες» πληροφοριών. Οι Peter Gill, James Sheptycki κ. ά. βεβαιώνουν πως μια ικανή θεωρητική προσέγγιση θα επιφέρει αλλαγές στον τρόπο λειτουργίας των Υπηρεσιών, στον τρόπο σκέψης των scholars και των policymakers⁷ τη στιγμή που η Jennifer Sims προβληματίζεται τονίζοντας πως εφόσον οι πληροφοριακοί ορισμοί δεν είναι ξεκάθαροι, τότε, μια θεωρητική αποτύπωση δεν μπορεί να επιτευχθεί.⁸

Ο Ohad Leslau ρωτά: «πώς εμπλέκεται μια Υπηρεσία στο λεγόμενο *decisionmaking process*;»⁹ Ο μελετητής υποστηρίζει ότι η όποια εμπλοκή καθρεπτίζει τόσο το βαθμό επιρροής ενός πληροφοριακού οργανισμού στο κρατικό σύστημα ασφαλείας όσο και την ευφυΐα των πολιτικών ηγετών. Μέσω της κατάθεσής του υποδηλώνει το εξής: η θέση μιας Υπηρεσίας στην κορυφαία πολιτική διαδικασία, αυτή της λήψεως αποφάσεων, δεν είναι εκ προοιμίου ορισμένη ή δεδομένη. Μια θεωρία οφείλει να ορίζει εκείνες τις παραμέτρους ή μεταβλητές που βοηθούν τον ερευνητή να ποιοτικοποιήσει / ποσοτικοποιήσει την παρουσία της πληροφόρησης εντός του (τελευταίου) σταδίου του οποίου κατάληξη αποτελεί η τελική απόφαση και κρίση δράσης. Εντούτοις δεν υπάρχει κάποιο μέτρο ελέγχου ποιότητας της τελικής πληροφόρησης, άλλωστε, αυτή η ποιότητα εξαρτάται, όπως ο ίδιος γράφει, από αστάθμητους παράγοντες, ειδικότερα / ιδιαίτερα χαρακτηριστικά και καταστάσεις όπως πιέσεις, επιμέρους σχέσεις, συμφέροντα, ιδεοληψίες κ. λ.^{10, 11}

Ο Stephen Marrin προτείνει μια σύζευξη ακαδημαϊκών και επιχειρησιακών τοποθετήσεων προκειμένου να επιτευχθεί η αναβάθμιση της αναλυτικής διαδικασίας.¹² Επισημαίνει την απουσία ανεξαρτήτων εργαστηρίων με αποκλειστική περιοχή ερεύνης την πληροφορία ομιλώντας για μια ...*absence of significant*

⁵ Betts R., "Analysis, war, and decision: why intelligence failures are inevitable" στο *Intelligence Theory: Key questions and debates*, ό. π., σ. 104

⁶ Phythian M., "Intelligence theory and theories of international relations: shared worlds or separate worlds?" στο *Intelligence Theory: Key questions and debates*, ό. π., σ. 54

⁷ Bay Sebastian, *Intelligence Theories. A Literary Overview*, ό. π., 2007, σ. 7-8

⁸ Sims J., *Understanding Friends and Enemies: The Context for American Intelligence Reform*, Georgetown University Press, Washington, D.C., 2005, σ. 15

⁹ Επιτρέπεται μια Υπηρεσία να εμπλέκεται στην πολιτική απόφαση; Οφείλει να ανταλλάσει απόψεις με το κυβερνητικό προσωπικό; Οφείλει να ενδιαφέρεται για τον εσωτερικό / εξωτερικό κρατικό σχεδιασμό; Να είναι «πολιτικά προσανατολισμένη»; Τα συγκεκριμένα ερωτήματα απασχολώντας ήδη από τη δεκαετία του 1950 εξακολουθούν να πυροδοτούν συζητήσεις -για μια εικόνα βλέπε Hilsman Roger, "Intelligence and Policy-Making in Foreign Affairs" στο *World Politics*, Volume 5, Issue 1, 1952, σ. 1-45, Davis Jack, "The Kent-Kendall Debate of 1949" στο *Studies in Intelligence*, Volume 35, Number 5, 1992, σ. 91-103, Davis Jack "Sherman Kent's Final Thoughts on Analyst-Policymaker Relations" στο *Occasional Papers: Volume 2, Number 3*, Central Intelligence Agency, The Sherman Kent Center for Intelligence Analysis, Washington, June 2003

¹⁰ Leslau Ohad, "The Effect of Intelligence on the Decisionmaking Process" στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 3, 2010, σ. 426-445

¹¹ Οι James Wirtz και Richard Betts προσπαθούν να αποδώσουν, μεταξύ άλλων, κάποιους τρόπους «μέτρησης» της συμμετοχής / σπουδαιότητας της πληροφορίας στην πολιτική απόφαση. Υπήρξε έγκυρη; Υπήρξε έγκαιρη; Προβλέφθηκαν γεγονότα; Κατά πόσο έπαιξε ανασταλτικό / υποστηρικτικό ρόλο στην κατάληξη μιας πράξης; Για περισσότερες πληροφορίες βλέπε *Toward a Theory of Intelligence. Workshop Report* σε επιμέλεια Treverton Gregory, Jones Seth, et. al., RAND, Santa Monica, 2006, σ. 26-28

¹² Marrin St., "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful" στο *Intelligence and National Security*, Volume 27, Number 3, 2012, σ. 398-399

*intelligence-related think tanks which have traditionally been the sinew or connective tissue between scholars and practitioners.*¹³ Μόλα ταύτα δεν πτοείται ευελπιστώντας σε μια οργανωμένη προσπάθεια εντός του ακαδημαϊκού χώρου με στόχο τη δημιουργία και έλεγχο γνώσης και θεωρίας που θα υπηρετήσει τα τμήματα της ανάλυσης, άλλωστε, όπως ο ίδιος αναφέρει, αρκετά intelligence schools συνδεδεμένα με πανεπιστήμια και Υπηρεσίες λειτουργούν σ' αυτή την κατεύθυνση. Τονίζει πως η πρόταση δημιουργίας του CIA University κινητροδοτήθηκε, μεταξύ άλλων, από τη φιλοδοξία κατασκευής μιας θεωρητικής αλλά και πρακτικής μεθόδου σχετικά με τη «δουλειά του αναλυτή», από την προοπτική θεμελίωσης ενός οργανισμού εντός του οποίου *...knowledgeable insiders could collaborate with insightful outsiders to develop both the theory and practice of intelligence analysis tradecraft...*, ωστόσο, ο ίδιος ουδέποτε αναφέρεται ευθέως σε μια θεωρία πληροφορίας ή (υπο)θεωρία πληροφοριακής ανάλυσης.¹⁴

Ο John Ehrman επικεντρώνει στην απουσία μιας θεωρίας αντικατασκοπίας. Υποστηρίζει πως αυτή η έλλειψη οδηγεί τις αμερικανικές Υπηρεσίες σε διάπραξη ουσιωδών σφαλμάτων. Αναζητά λύσεις ως προς το ζήτημα της θεωρίας αλλά και του ορισμού της πληροφορίας, ωστόσο, όπως διασαφηνίζει, η αντικατασκοπία ως πεδίο δεν φαίνεται να απασχολεί σε ικανό βαθμό τους ακαδημαϊκούς κύκλους. Ο ερευνητής αφήνει να εννοηθεί ότι η μη θεωρία ανατροφοδοτεί την απουσία ενδιαφέροντος και το αντίστροφο. Προσπαθεί να καταρτίσει ένα αρχικό σχέδιο μιας αντικατασκοπευτικής θεωρητικής κατασκευής ορμώμενος από το ερώτημα *...what are we talking about when we talk about CI?*¹⁵ Ο Μύρωνας Βαρουχάκης υποστηρίζει πως ο, κατά Ehrman, ορισμός της αντικατασκοπίας ως «μελέτη της οργάνωσης και της συμπεριφοράς των αλλοδαπών πληροφοριακών υπηρεσιών με σκοπό τη χρήση της παραγόμενης γνώσης» δεικνύει ένα πρώτο βήμα. Ο ίδιος υποθέτει πως μέσα από case-by-case μελέτες θα αποκαλυφθούν κάποια από τα χαρακτηριστικά που δομούν το προφίλ ατόμων επιρρεπών στην κλοπή και απόδοση εγχώριων μυστικών σε ξένες δυνάμεις ούτως ειπείν, ατόμων που η αντικατασκοπία οφείλει να εξουδετερώσει.¹⁶

Τον Ιούνιο του 2005 έλαβε χώρα στην Ουάσιγκτον μια ολοήμερη σύνοδος υπό την αιγίδα του Office of the Director of National Intelligence (ODNI) και του Research AND Development (RAND) Institute με αντικείμενο την πληροφορία. Σε κάποιο από τα εκδοθέντα πρακτικά υπό τον τίτλο *Toward a Theory of Intelligence* ανακαλύπτουμε μια αποτύπωση της προηγηθείσας προσπάθειας δημιουργίας ενός πλαισίου εντός του οποίου μπορεί να φιλοξενηθεί μια θεωρία πληροφορίας. Το εν λόγω ντοκουμέντο αναφέρεται στις τέσσερις συνεδρίες της συνόδου ξεκινώντας με την υπό τον τίτλο *What is Intelligence Theory* αναφορά. Στο πρώτο τμήμα των εργασιών κλήθηκαν να παρουσιάσουν οι Warner, Kahn και Gill. Ο πρώτος δεν προχώρησε σε μια συγκεκριμένη πρόταση καταθέτοντας πως πρώτα απ' όλα πρέπει να δοθεί ένας ορισμός περί την πληροφορία. Ο δεύτερος αναφέρθηκε σε μια ιστορική, μαθηματική και ψυχολογική απεικόνισή της. Σύμφωνα με την πρώτη, η έλλειψη πληροφόρησης αντικαθίσταται (ή πρέπει να αντικαθίσταται) από την ισχύ, η πληροφόρηση συνιστά έναν βοηθητικό και όχι έναν κύριο παράγοντα πολεμικής κατίσχυσης και, τέλος, η πληροφόρηση συνθέτει ένα ικανό στοιχείο αμύνης αλλά όχι

¹³ Marrin St., "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful", ό. π., σ. 420

¹⁴ ό. π., σ. 420-422

¹⁵ Ehrman John, "What are We Talking About When We Talk about Counterintelligence?" στο *Studies in Intelligence*, Volume 53, Number 2, 2009, σ. 5-6

¹⁶ Varouhakis Miron, "An Institution-Level Theoretical Approach for Counterintelligence" στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 3, 2011, σ. 495-499

επίθεσης. Η μαθηματική θεώρηση αντιλαμβάνεται την πληροφορία ως κομμάτι γνώσης ικανό να ποσοτικοποιηθεί εντός μαθηματικών και στατιστικών μοντέλων προκειμένου να αξιολογηθεί -πρόκειται για θέση που δεν διευκρινίζεται περαιτέρω. Η ψυχολογική προσέγγιση υποστηρίζει πως μια υπηρεσία Πληροφοριών πιθανότατα δεν στερείται πληροφοριακών εισροών αλλά χρόνου ανάλυσης και, άρα, αντίδρασης / απόκρισης. Ο Gill επιμένει πως μια θεωρία πληροφορίας πρέπει να ικανοποιεί τόσο τους academics όσο και τους practitioners, πως δεν υπάρχει κάτι που εγγενώς αντιβαίνει σε ένα συγκερασμό των δύο αναζητήσεων. Μια καλή επιλογή μπορεί να εξηγήει την έννοια της πληροφορίας ικανοποιώντας τους πρώτους αλλά ταυτόχρονα να αποτίνεται στους δεύτερους και στις ανάγκες τους ...*a good theory of intelligence should, by definition, be useful for intelligence*, δηλώνει ο ερευνητής. Επισημάνει τη δυσκολία απάντησης στο ερώτημα «τί είναι γνώση;», πρόκειται για κάτι ανεξάρτητο της αντίληψης του ανθρώπου ή, μήπως, εξαρτάται από αυτήν; Αν ισχύει το δεύτερο, τότε, η πληροφορία / γνώση προφανώς υποκειμενικοποιείται με ό,τι αυτό συνεπάγεται για μια θεωρία περίξ αυτής. Εν τέλει οι εργασίες του Ινστιτούτου καταλήγουν στην εξής απόφαση: *μια θεωρία πληροφορίας το λιγότερο που δύναται να συνεισφέρει είναι στην καλύτερη κατανόηση της πληροφορίας per se.*¹⁷ Ασφαλώς πρόκειται για διαπίστωση με την αναζήτηση μιας θεωρίας πληροφορίας να μην τελεσφορεί.

Περί της αδυναμίας δόμησης μιας θεωρίας στρατηγικής πληροφόρησης

Ο Thomas Quiggin γράφει ότι κάθε μελετητής που φιλοδοξεί να δομήσει μια θεωρία στρατηγικής πληροφόρησης οφείλει να κατέχει αρχές πολιτικής επιστήμης και διεθνών σχέσεων, να γνωρίζει περί του ρόλου της γραφειοκρατίας, να έχει διαβάσει στατιστική, ψυχολογία, κοινωνιολογία, να είναι οικείος με τα του στρατιωτικού πεδίου κ. λ. Αν μια εμπειρισταωμένη άποψη περί όλων αυτών δεν είναι εύκολο να αποκτηθεί, υπάρχει, επίσης, κάτι άλλο: η μυστικότητα που χαρακτηρίζει το χώρο των πληροφοριών όπως και η πολυπλοκότητα που διακρίνει την πληροφοριακή κοινότητα.¹⁸ Από την άλλη και σύμφωνα με τους Bruce Berkowitz και Allan Goodman ...*οι αναλυτές παρουσιάζονται διστακτικοί στην υιοθέτηση κάτι τόσο αφηρημένου όσο μια [πληροφοριακή] θεωρία, επιπλέον, ...δεν υπάρχει κανείς μαγικός τρόπος να παραχθεί [τέλεια] πληροφοριακή εκτίμηση / αξιολόγηση.*¹⁹ Ως φαίνεται το εγγενές περιβάλλον του πεδίου (συνθετότητα, εχεμύθεια / κρυψίνια, επιφυλακτικότητα / συντηρητικότητα) δεν πριμοδοτεί πιθανότητες δημιουργίας μιας θεωρίας στρατηγικής πληροφόρησης.

Το *Intelligence Theory: Key Questions and Debates* (2009) συγκαταλέγεται στα κύρια έργα αφιερωμένα στη θεωρία της πληροφορίας. Οι δεκατρείς συνεισφέροντες συγγραφείς επιχειρούν να ενισχύσουν τη μελέτη της πληροφόρησης, να εισφέρουν στην αμερικανική πολιτική ασφαλείας, να ενημερώσουν το κοινό και, πρωτίστως, να προετοιμάσουν το έδαφος για μία ή περισσότερες «θεωρίες» εξηγώντας την πρακτική του πεδίου αποσαφηνίζοντας, παράλληλα, πλήθος ιδεών που αναπτύσσονται εντός αυτού. Πάρα ταύτα ο James Webb προβαίνει σε ένα δεικτικό σχόλιο τονίζοντας πως είναι οι ανάγκες της σπουδής όπως και οι επιμέρους της εξήγησης της διαδικασίας συλλογής, ανάλυσης, παραγωγής και χρήσης πληροφορίας, του επιχειρείν, των

¹⁷ *Toward a Theory of Intelligence. Workshop Report* σε επιμέλεια Treverton Gregory, Jones Seth, et. al., ό. π., σ. 3-7

¹⁸ Quiggin Thomas, *Seeing the Invisible. National Security Intelligence in a Uncertain Age*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2007, σ. 59

¹⁹ Berkowitz Bruce, Goodman Allan, *Strategic Intelligence and American National Security*, Princeton University Press, New Jersey / USA, 1989, σ. 85

επιτυχιών / αποτυχιών, της διαφοράς μεταξύ κατασκοπίας και αντικατασκοπίας κ. λ. που ωθούν σε μια «θεωρία» που περισσότερο φιλοδοξεί να αποδώσει definitions παρά κάτι διάφορο. Ο Webb τονίζει πως ο κάματος των συγγραφέων δεν καταλήγει σε μια θεωρία ή, τουλάχιστον, σε μια συμπαγή θεωρία. Ο μελετητής εντοπίζει τρία προβλήματα: α) το πρώτο αφορά στη μάχη των ορισμών²⁰, β) το δεύτερο συνδέεται με μια διάσταση απόψεων σχετικά με την ταυτότητα του χώρου. Πρέπει ο τελευταίος να ακολουθήσει μια αυτόνομη πορεία έξω από το πλαίσιο της Πολιτικής Επιστήμης και των Διεθνών Σχέσεων; Πώς αυτό δικαιολογείται όταν διατηρούνται φωνές που τον τοποθετούν εντός του ρεαλιστικού παραδείγματος; γ) το τρίτο σχετίζεται με την τάση ορισμένων (Betts, Hastedt, Skelley, Sims κ. λ.) να περιορίσουν την προσπάθεια δημιουργίας θεωρίας σχεδόν αποκλειστικά γύρω από τη θεραπεία της πληροφοριακής αποτυχίας που, οξύμωρο, κάποιοι από αυτούς (π. χ. Betts) θεωρούν αναπόφευκτη. Όμως οι Υπηρεσίες ποτέ δεν αποδίδουν στο φως της δημοσιότητας το σύνολο των αρχείων τους ώστε να αποδειχθεί αν αυτή (η αποτυχία) αποτελεί κανόνα ή εξαίρεση. Οι Richard Kerr και Jack Davis τοποθετούνται λέγοντας πως οι επιτυχίες της CIA υπερτερούν αριθμητικά των αποτυχιών κατά το δεύτερο, τουλάχιστον, μισό του 20^{ου} αιώνα²¹ τη στιγμή που η μελέτη των τελευταίων (των αποτυχιών) δεν προσδίδει κάτι ουσιαστικό στην οικοδόμηση μιας «θεωρίας πληροφορίας». Ο Webb διαφωνεί προσθέτοντας, ωστόσο, πως μια ικανή προσέγγιση πρέπει να διακρίνεται για την ευρύτητά της και όχι να αναλώνεται μονοδιάστατα.²²

Κατά τους Johnson και Allison M. Shelton η αναζήτηση των ευρύτερων σκοπών, των ορισμών, της μεθοδολογίας, του tradecraft του πεδίου όπως και η διευθέτηση θεσμικών αλλά και ηθικών προβληματισμών συνθέτουν μόνο κάποια από τα principal debates του χώρου²³ -όλα αυτά υπογραμμίζουν τη ζωντάνια και την ποικιλοχρωμία μιας ατζέντας που, εντούτοις, στερείται κεντρικής θέσεως / θεωρίας. Ο Davies διαφοροποιείται / τοποθετείται επί του θέματος λέγοντας λίγο έως πολύ πως ...η δημιουργία μιας θεωρίας πληροφορίας σχετίζεται αντιστρόφως ανάλογα με μια

²⁰ ...των πάρα πολλών, είτε «informational», είτε «organizational», ορισμών, όπως καταθέτει ο Warner. Ο ερευνητής παραθέτει ένα πλήθος, εντός αυτού και τον δικό του ...*intelligence is secret, state activity to understand or influence foreign entities*. Μόλα ταύτα δεν φαίνεται ικανοποιημένος καθώς, όπως ο ίδιος γράφει, ...*without a clear idea of what intelligence is, how can we develop a theory to explain how it works?* Ουσιαστικά ο Warner υποστηρίζει πως δεν υπάρχει καν ικανός ορισμός πληροφόρησης, πόσο μάλλον θεωρία -για περισσότερα βλέπε Warner M., “Wanted: A Definition of ‘Intelligence’” στο *Studies in Intelligence*, Volume 46, Number 3, 2002, σ. 15-22

²¹ Παρά το ότι ο επιχειρησιακός της CIA και καθηγητής John Gentry φαίνεται να διαφωνεί -περί τούτου βλέπε Gentry John, “The ‘Professionalization’ of Intelligence Analysis: A Skeptical Perspective” στο *International Journal of Intelligence and CounterIntelligence*, Volume 29, Issue 4, 2016, σ. 649

²² Webb M. J., “Intelligence in Public Literature. Intelligence Theory: Key Questions and Debates” στο *Studies in Intelligence*, Volume 53, Number 2, 2009, σ. 35-37. Συμπληρώνουμε πως ο B. Fischhoff είναι από τους ερευνητές που στηρίζει τη μελέτη του φαινομένου «πληροφοριακή αποτυχία» αρκεί αυτή να μην κατατράχεται από θεωρήσεις τύπου «φταίει η κακοτυχία». Μαζί του συμφωνούν οι Kjetil A. Hatlebrekke και M. L. R. Smith γράφοντας ουσιαστικά ότι αρχή της λύσης ενός προβλήματος αποτελεί η παραδοχή του ήτοι, η παραδοχή του γεγονότος του αναπόφευκτου της πληροφοριακής αποτυχίας εντός της ροής του χρόνου -για μια εικόνα βλέπε Fischhoff B., “For those Condemned to Study the Past: Reflections on Historical Judgment” στο *New Directions for Methodology of Behavioural Science: Fallible Judgments in Behavioural Research*, επιμ. Shweder A. R., Fiske W. D., Jossey-Bass, San Francisco, 1980, σ. 83 και Hatlebrekke A., K., Smith, M. L. R., “Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure” στο *Intelligence and National Security*, Volume 25, Number 2, 2010, σ. 181

²³ Που γενικά κατηγοριοποιούνται ως «ιστορικά», «θεωρητικά», «εμπειρικά / hands-on» -για περισσότερες λεπτομέρειες βλέπε Johnson L., Shelton Al., “Thoughts on the State of Intelligence Studies: A Survey Report” στο *Intelligence and National Security*, Volume 28, Number 1, 2013, σ. 109-112

πετυχημένη πληροφοριακή διαδικασία²⁴ αποσυνδέοντας πλήρως δύο περιοχές για τις οποίες έχει γίνει τόση κουβέντα και μετατρέποντας το ...*for every complex problem there is a simple solution which is wrong* του H. L. Mencken²⁵ σε εφιάλτη κάθε επίδοξου εφευρέτη θεωρητικών κατασκευών που προτείνονται ή προεκτείνονται στην πραγματική ζωή και δράση.

Κλείνουμε με μια εικόνα της σοβιετικής θεωρίας και πράξης της πληροφόρησης. Ο Alexander Orlov ξεκαθαρίζει πως αυτό που απασχόλησε τη σκέψη των ειδικών της ΕΣΣΔ σχετίστηκε ουσιαστικά με το λειτουργικό / επιχειρησιακό δόγμα ήτοι, με απόδοση υποχρεώσεων / καθηκόντων και ανάπτυξη τακτικισμών. Στην πραγματικότητα δεν διαφαίνεται διάθεση συζήτησης θεωρητικής υφής. Για την ΚGB θεωρία και πράξη είναι ένα και αυτό αρκεί να προάγονται οι εξής επτά βασικές δραστηριότητες: α) πολιτική / διπλωματική πληροφόρηση, β) στρατιωτική πληροφόρηση, γ) οικονομική πληροφόρηση, δ) παραπληροφόρηση, ε) διείσδυση εντός αλλοεθνών Υπηρεσιών, στ) χειραγώγηση γεγονότων, επιρροή επί ξένων κυβερνήσεων, ζ) βιομηχανική πληροφόρηση. Διευκρινίζουμε ότι: α) για τις ρωσικές Υπηρεσίες πληροφόρηση σημαίνει προϊόν ανάλυσης στοιχείου / δεδομένου που εκμαιεύεται με επίβουλο / μυστικό τρόπο από μη φανερές πηγές ή, αλλιώς, πληροφόρηση = tradecraft product και β) πέρα των επτά κύριων δραστηριοτήτων προβλέπονται, επίσης, σχεδιασμοί με σκοπό την αποτροπή υπονομευτικών ή επαναστατικών / τρομοκρατικών ενεργειών.²⁶ Κατά συνέπεια το σοβιετικό πληροφοριακό μοντέλο αν μη τι άλλο είναι: α) ξεκάθαρο / λιτό, β) στερούμενο ιδιαίτερου θεωρητικού υποβάθρου, γ) προσηλωμένο στην κατασκοπευτική / αντικατασκοπευτική πράξη.

Συμπεράσματα

Ο Warner είναι ξεκάθαρος. Κατ' ουσίαν δεν υφίσταται θεωρία πληροφόρησης τη στιγμή, μάλιστα, που ακόμα και οι ορισμοί της διαπραγματεύονται. Προκειμένου να υπάρξει, συνεχίζει, πρέπει να εμφανιστεί κάτι πιο συμπαγές ως (ακαδημαϊκή) απόδοση. Οι ερευνητές του χώρου οφείλουν όπως αναδιφήσουν εντός παλαιότερων και νεωτέρων περιστατικών είτε προς επιβεβαίωση είτε προς δοκιμασία των υποθέσεων που πρεσβεύουν. Ίσως τότε ιδέες και απόψεις περίξ μιας θεωρίας πληροφοριών επικεντρώσουν σε μια σχέση αίτιου - αιτιατού.²⁷ Επιπλέον, υποθέτουμε πως δεν υπάρχει κάποιος αναπόδραστος λόγος προβολής των θέσεων των Θετικών Επιστημών περί ανάπτυξης θεωρίας²⁸ εντός του πεδίου των αντίστοιχων Πολιτικών

²⁴ Davies Phillip, "Theory and intelligence reconsidered" στο *Intelligence Theory. Key questions and debates*, ό. π., σ. 191

²⁵ ό. π., σ. 186

²⁶ Orlov Alexander, "The Theory and Practice of Soviet Intelligence" στο *Studies in Intelligence*, Volume 7, Number 2, 1963, σ. 45-65, διαθέσιμο και στο https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm εις το οποίο ανατρέξαμε την 29^η Φεβρουαρίου 2016, επίσης, Ορλόφ Αλ., *Εγχειρίδιο κατασκοπείας και ανταρτοπολέμου. Η εκπαίδευση των Σοβιετικών πρακτόρων σε επιχειρήσεις παρακολούθησης, παραπλάνησης και ανορθόδοξου πολέμου*, μτφρ. Παράσχος Ιωάννης, Eurobooks, Αθήνα, 2015, σ. 21-43, 155-172

²⁷ Warner M., "Theories of intelligence: the state of play" στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014, 2014, σ. 32

²⁸ Μάλιστα ο Davies τονίζει πως ...*there is no a priori need for the social sciences[...] to have theory in order to be "scientific", any more than there is an absolute necessity that they be quantitative* either -για περισσότερα βλέπε Davies Phillip, "Theory and intelligence reconsidered" στο *Intelligence Theory. Key questions and debates*, ό. π., σ. 187. Ο Phythian γράφει πως το debate περί του τι συνιστά θεωρία συνεχίζεται όπως συνεχίζεται το ανάλογο περί του αν το πεδίο των IR χρήζει στήριξης στις

και κατ' επέκταση εντός του πεδίου της πληροφορίας / πληροφόρησης. Αν μια θεωρία²⁹ αποτελεί εξηγητικό και προβλεπτικό εργαλείο, τότε, η μελέτη της πληροφορίας μάλλον εξηγεί κατά περίπτωση και λιγότερο προβλέπει υπό την κλασική θετικιστική έννοια. Μάλιστα ο Stan Taylor γράφει πως εντός των κοινωνικών επιστημών η εξηγητική δύναμη μιας 'θεωρίας' είναι, κατά κάποιο τρόπο, πιο σημαντική από την αντίστοιχη της προβλεπτικής ακριβώς διότι *...all of the controls necessary for a predictive theory are not available*.³⁰

Όπως και να έχει και παρά τα όποια αποτελέσματα της συζήτησης, η μελέτη του ακαδημαϊκού και πρακτικού πεδίου της πληροφορίας / πληροφόρησης είτε με την επικουρία μιας θεωρίας είτε όχι δύναται να οδηγήσει τους scholars σε μια έγκυρη κατανόηση των πραγμάτων, τους practitioners σε πιθανές προεικονίσεις και τους policy makers σε έγκαιρους χειρισμούς που καλούνται να απλωθούν σε ποικίλες περιοχές του χρονικού ορίζοντα. Το τελευταίο επιβεβαιώνει την εργαλειακή χρεία και την αξίωσή της να αντιμετωπιστεί με ιδιαίτερη προσοχή από το σύνολο των συνεισφερόντων στην παραγωγή πολιτικής αρκεί να γίνει αποδεκτή ως ad hoc και μόνο οδηγός. Τέλος, δεν πρέπει να λησμονούμε το δυαδικό χαρακτήρα της πληροφόρησης. Αν και η γνώση / αλήθεια γύρω από τον κόσμο είναι σημαντική, αποτελώντας επίμονη θήρα για τις Υπηρεσίες όπως το (ανεπίσημο) μότο «And ye shall know the truth and the truth shall make you free» της CIA αφήνει να εννοηθεί, αυτή ακριβώς η γνώση / αλήθεια δεν ωφελεί να αποτελέσει αντικείμενο έμμονων θεωρητικολογήσεων ή αυτοσκοπό παρά, μάλλον, οδό και πράξη προς τη νίκη, άλλωστε, κατά τον καθηγητή George Stein *...information in itself is a key aspect of*

αρχές της κλασικής επιστήμης. Για τον Waltz μια θεωρία εξηγεί υποθέσεις και νόμους που υπόκεινται στην παρατήρηση ή στη μέτρηση αποτελώντας (η θεωρία) γενίκευσή τους. Το γενικό pattern ακολουθεί την πορεία: *Υπόθεση → Νόμος → Θεωρία* και όπως ο Waltz σημειώνει *...a theory is born in conjecture and is viable if the conjecture is confirmed*. Ο Phythian υποστηρίζει ότι η παρουσία «μοντέλων» υποβοηθά στη «θεωρητικοποίηση». Το κύριο μοντέλο σπουδής της πληροφόρησης σχετίζεται με τον πληροφοριακό κύκλο, άρα, ο τελευταίος συνδέεται ή δύναται να συνδεθεί με μια θεωρία (ή, ίσως, θεωρίες). Το πρόβλημα εντοπίζεται στο ότι αυτός αποτελεί προβολή των σκέψεων και της εργασίας των practitioners (άρα των υποθέσεων των συγκεκριμένων ανθρώπων) τη στιγμή που η πραγματικότητα είναι πιο περίπλοκη από αυτή που και ο πλέον έμπειρος αναλυτής φαντάζεται -για όλα αυτά βλέπε Phythian Mark, "Intelligence theory and theories of international relations. Shared world or separate worlds?" στο *Intelligence Theory. Key questions and debates*, ό. π., σ. 55-56. Σ' αυτό το σημείο ενσκήπτει (και) κάτι άλλο. Η Jennifer Sims διατείνεται ότι μια υπόθεση ενδέχεται να είναι ορθή αλλά για το χ λόγο να μην επιβεβαιώνεται -για περισσότερα βλέπε Sims J., "Defending adaptive realism. Intelligence theory comes of age" επίσης στο *Intelligence Theory. Key questions and debates*, ό. π., σ. 153

²⁹ Δεν υπάρχει καν ξεκάθαρος ορισμός του λήμματος «θεωρία» όπως ο ίδιος ο van Evera καταθέτει προτείνοντας πολύ απλά πως...*θεωρία είναι μια διατύπωση γενικού περιεχομένου που περιγράφει και εξηγεί τις αιτίες ή τα αποτελέσματα διαφορετικών φαινομένων αποτελούμενων από αιτιώδεις νόμους ή υποθέσεις, ερμηνείες και προϋποτιθέμενες συνθήκες* -για περισσότερες πληροφορίες βλέπε van Evera, Stephen, *Εισαγωγή στη μεθοδολογία της πολιτικής επιστήμης*, μτφρ. Συλογίου Έλ., Ποιότητα, Αθήνα, 2009⁴, σ. 21-84. Περαιτέρω, αλλιώς σημαίνεται ο όρος στις φυσικές και αλλιώς στις κοινωνικές επιστήμες. Στις πρώτες μια σφιχτοδεμένη θεωρία μπορεί να αναπτυχθεί, στις δεύτερες εμφιλοχωρεί ο ανθρώπινος παράγοντας -βλέπε, μεταξύ πολλών άλλων, Hollis M., Smith St., *Explaining and Understanding International Relations*, Oxford University Press, Βρετανία, 1990, σ. 1-15 και Ember Carol, Ember Melvin, *Cross-Cultural Research Methods*, AltaMira Press, Βρετανία, 2009, σ. 33-42. Εντούτοις, ακόμα και στις επονομαζόμενες «σκληρές» επιστήμες παρουσιάζονται πεδία *ελεύθερα θεωρίας* (theory-free domain). Τέτοια δεικνύουν η βιοχημεία ή η γενετική των οποίων η έρευνα δεν επαφίεται σε κάποιο μοντέλο τη στιγμή που τα αποτελέσματά της αποδίδονται ως σώμα γνώσεων γύρω από συγκεκριμένες χημικές αντιδράσεις που εμπλουτίζεται συν τω χρόνω -για περισσότερα βλέπε *Toward a Theory of Intelligence. Workshop Report*, ό. π., σ. 20

³⁰ Taylor A. Stan, "Definitions and Theories of Counterintelligence" στο *Strategic Intelligence*, Volume 4, επιμ. Johnson K. Loch, Praeger Security International, 2007, σ. 1

*national power and more importantly, is becoming an increasingly vital national resource that supports diplomacy, economic competition, and the effective employment of military forces.*³¹

³¹ Stein G., “Information Warfare” στο *Air Power Journal*, Volume 9, Number 1, 1995, σ. 30-39

ΚΕΦΑΛΑΙΟ 4

Περί των υπηρεσιών εθνικής Αντικατασκοπίας (Counterintelligence -CI)

Counterintelligence... the core mission simply stated... Combating Adversarial Intelligence Threats

Mark L. Reagan, Σχης ε. α.¹

Μια υπηρεσία CI εκτελεί την αποστολή της αντιμετωπίζοντας κάθε μέρα τις απειλές που θέτουν οι ξένες πληροφοριακές Υπηρεσίες, να γιατί λέμε πως πρόκειται για έναν σιωπηλό πόλεμο

Stuart Herrington, Σχης ε. α.²

«...η πιο μυστική από τις μυστικές πληροφοριακές δραστηριότητες ... η καρδιά του κρεμμυδιού»

The Church Committee³

Η έννοια «αντικατασκοπία» περιλαμβάνει κάθε είδους 'human and technical' δραστηριότητες, εκτελούμενες τόσο στο εσωτερικό όσο στο εξωτερικό με σκοπό την αναγνώριση, εκτίμηση, εξουδετέρωση αλλά και διαχείριση αλλότριων πληροφοριακών απειλών ... η αντικατασκοπία εγγενώς δεν αποτελεί παρά ένα στρατηγικό εργαλείο εθνικής ασφαλείας

Michelle van Cleave⁴

...[CI] σημαίνει πληροφόρηση ιδιαίτερου είδους, συν κάτι ακόμα

Francis McNamara⁵

Στοιχεία / αρχές περί υπηρεσιών CI. Λεξικά, ερευνητές, θεσμοί

Η δράση της αντικατασκοπίας συνθέτει μία εκ των δύο βασικών δομών μιας ενιαίας υπηρεσίας Πληροφοριών ή, αλλιώς, έναν από τους δύο πυλώνες ενός ενιαίου πληροφοριακού δικτύου / μηχανισμού χωρίς αυτό να σημαίνει πως δεν δύναται να λειτουργήσει αυτόνομα (ως Υπηρεσία). Φαινομενικά, ιδιαίτερη δυσκολία στην απόδοση ορισμού δεν παρουσιάζεται, ωστόσο, πλήθος ερευνητών (Shulsky, Schmitt, Lowenthal) υποστηρίζουν το αντίθετο: μία δήλωση της μορφής «αντικατασκοπία σημαίνει καταδίωξη του αντιπάλου πράκτορα» δεν καλύπτει ιδιαίτερα.⁶

¹ *Terms & Definitions of Interest for Counterintelligence Professionals*, επιμ. Reagan M., 2014, σ. 55

² Reagan Mark, *Introduction to U.S. Counterintelligence. "CI 101--A Primer"*, 2005, σ. 17, διαθέσιμο στο http://c.ymcdn.com/sites/www.cicentre.com/resource/resmgr/reports/ci_101_primer_july_2005.pdf όπου καταφύγαμε τη 13^η Σεπτέμβρη 2016

³ Senate Report # 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, US Government Printing Office, Washington, D.C., Απρίλιος 1976, σ. 171

⁴ *Terms & Definitions of Interest for Counterintelligence Professionals*, ό. π., σ. 55

⁵ Reagan Mark, *Introduction to U.S. Counterintelligence. "CI 101--A Primer"*, ό. π., σ. 6

⁶ Ο Alberto Gutierrez, και όσον αφορά στο πεδίο της αντικατασκοπίας, επαναπιστώνει τη φράση «wilderness of mirrors» του ποιητή T. S. Elliot στον James Jesus Angleton. Ο Angleton μέσω αυτής προσπαθεί να αποδώσει τα τεχνάσματα και την πολυπλοκότητα που χαρακτηρίζει το χώρο περιγράφοντας τον περισσότερο ως αντανάκλαση πραγματικότητας παρά ως καθαντή πραγματικότητα -για μια άποψη βλέπε "CIA: James Angleton" στην διαδικτυακή τοποθεσία http://wais.stanford.edu/Governments/gov_ciajamesatleto.htm όπου καταφύγαμε την 21^η Μαρτίου 2015

Ο Paul Redmond γράφει ότι αν οι ορισμοί CI αναφέρονται στην αντιμετώπιση φαινομένων κατασκοπίας, σαμποτάζ και τρομοκρατίας, στον ίδιο χρόνο αναφέρονται σε ποικιλία δραστηριοτήτων, πρακτορικών δεξιοτήτων, μέσων και σκοπών. Ο ίδιος καταγράφει μαρτυρία της επιχειρησιακού van Cleave κατά την οποία ...*παρατηρούνται τεράστιες διαφορές στην κατανόηση του 'τι σημαίνει αντικατασκοπία', του 'πώς εκτελείται', του 'ποια βασική ορολογία οφείλει να ακολουθείται'...*⁷ Π. χ. είναι χαρακτηριστικό ότι η γερμανική Ομοσπονδιακή Υπηρεσία Πληροφοριών (BND) χρησιμοποιεί τον όρο «gegenspionage» προκειμένου αναφοράς στην καταδίωξη της αντίπαλης κατασκοπίας τη στιγμή που η αντίστοιχη Υπηρεσία Εσωτερικής Ασφαλείας (BfV) χρησιμοποιεί τον όρο «spionageabwehr».⁸

Ο Todd E. Gleghorn υποστηρίζει ότι οι περί CI ορισμοί κατηγοριοποιούνται σε «ευρείς» και «στενότερους». Στους πρώτους ανήκουν ορισμένοι που έχουν αποδοθεί από την αμερικανική κυβέρνηση σε σειρά επισήμων εγγράφων. Κατά τον τρόπο τούτο η *Executive Order* [EO / 1981] 12333 ορίζει πως ...*CI σημαίνει συλλογή πληροφοριών και εκτέλεση αποστολών με σκοπό την προστασία έναντι κατασκοπευτικών (espionage) ενεργειών, άλλων εχθρικών πληροφοριακών δράσεων, σαμποτάζ ή δολοφονιών από ή εκ μέρους ξένων δυνάμεων, οργανισμών ή ατόμων, ή δράση κατά τρομοκρατικών σχεδιασμών, αλλά, πάντως, όχι εκτέλεση προγραμμάτων ασφαλείας γύρω από το προσωπικό, τα φυλασσόμενα ντοκουμέντα, εν γένει τη φυσική προστασία και τις επικοινωνίες.*⁹ Ασφαλώς έχει προηγηθεί η *National Security Act* του 1947 ορίζοντας ακριβώς τα ίδια μη κάνοντας, ωστόσο, αναφορά σε κάποια «μη εκτέλεση προγραμμάτων ασφαλείας». ¹⁰ Ένας άλλος ευρύς ορισμός είναι αυτός που καταθέτει ο A. C. Wasemiller. Ο Wasemiller γράφει πως καθήκον μιας υπηρεσίας *εσωτερικής αντικατασκοπίας (internal counterintelligence)* αποτελεί η προάσπιση της νόμιμης κυβέρνησης έναντι «κρυφών επιθέσεων». Κατά τούτη την έννοια μια υπηρεσία internal CI επιφορτισμένη με την ανάσχεση εχθρικών μυστικών δράσεων σκοπεύει στο μπλοκάρισμα πράξεων κατασκοπίας (espionage), επιθετικής εχθρικής αντικατασκοπίας (counterespionage), υπονόμευσης (subversion) και δολιοφθοράς (sabotage).¹¹ Ακόμα πιο ευρύς είναι ο ορισμός του Frederick Hitz σύμφωνα με τον οποίο ...*CI σημαίνει ερευνητική εργασία (detective work) υψηλών / ειδικών απαιτήσεων εστιάζοντας σε επιχειρησιακές λεπτομέρειες που αφορούν σε έναν κόσμο μυστικών συναντήσεων, ανταλλαγών μηνυμάτων και πληροφοριών...*¹² Τέλος, μεταφέρουμε τη σκέψη του Thomas Powers κατά τον οποίο ...*η αντιπληροφόρηση είναι για την πληροφόρηση ό,τι είναι η επιστημολογία για τη φιλοσοφία. Και οι δύο βρίσκουν τις ρίζες τους στη θεμελιώδη ερώτηση «με ποιο τρόπο αναγνωρίζουμε τα πράγματα;». Και οι δύο αμφισβητούν αυτά που θεωρούμε, ή είμαστε διατεθειμένοι να δεχτούμε, ως αλήθεια.*¹³

Στη δεύτερη κατηγορία εντάσσονται ορισμοί όπως ...*[ως]δράση CI ορίζεται η συλλογή στοιχείων γύρω από τις πληροφοριακές επιχειρήσεις και τις σχετικές δυνατότητες του*

⁷ Redmond J. Paul, "The Challenges of Counterintelligence" στο *The Oxford Handbook of National Security Counterintelligence*, επιμ. Johnson Loch, Oxford University Press, New York, 2010, σ. 538

⁸ ό. π., σ. 539

⁹ U.S. President Executive Order "United States Intelligence Activities, Executive Order 12333", *Federal Register* 46, number 59941, 4 Δεκεμβρίου 1981, διαθέσιμο και στη διαδικτυακή τοποθεσία <http://fas.org/irp/offdocs/eo12333.htm> όπου ανατρέξαμε την 8^η Μαρτίου 2015

¹⁰ *National Security Act of 1947*, διαθέσιμο και στο <http://www.intelligence.senate.gov/nsaact1947.pdf> όπου ανατρέξαμε την 8^η Μαρτίου 2015

¹¹ Wasemiller C. A., "The Anatomy of Counterintelligence" στο *Studies in Intelligence*, Volume 13, Number 1, 1969, διαθέσιμο στο https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol13no1/html/v13i1a02p_0001.htm εις το οποίο καταφύγαμε την 5^η Μαΐου 2016. Ο Wasemiller αναφέρεται κυρίως σ' αυτό που ονομάζει εσωτερική αντικατασκοπία (internal CI). Πρόκειται για υπηρεσία-ίες εσωτερικής ασφαλείας αν αναλογιστούμε ότι την επιθετική αντικατασκοπευτική δράση (counterespionage) την αποδίδει στις υπηρεσίες εθνικής αντικατασκοπίας (national CI)

¹² Ehrman John, "Toward a Theory of CI. What are We Talking About When We Talk about Counterintelligence?" στο *Studies in Intelligence*, Volume 53, Number 2, Ιούνιος 2009, σ. 7

¹³ *ibid*

αντιπάλου. Με άλλα λόγια CI δεν σημαίνει άλλο από προσπάθεια ξεσκεπάσματος των εχθρικών πληροφοριακών assets¹⁴ ή ...CI σημαίνει δράση προστασίας των οικείων μυστικών, αποφυγή χειραγώγησης εκ μέρους του αντιπάλου, ενδεχομένως πληροφοριακή χειραγώγηση του προς όφελός μας.¹⁵ Ο Gleghorn βασισμένος στην ΕΟ 12333 γράφει ότι μια υπηρεσία Αντικατασκοπίας «αναγνωρίζει, αποτιμά, εξουδετερώνει και χειραγωγεί τις δράσεις αντίπαλων Υπηρεσιών ή τρομοκρατικών ομάδων» τονίζοντας ότι «η χειραγώγηση ανήκει στο κομμάτι του counterintelligence που καλείται counterespionage».¹⁶ Περαιτέρω, καταγράφουμε τον ορισμό του John Ehrman κατά τον οποίο ...CI είναι η μελέτη της οργάνωσης και συμπεριφοράς των αλλοδαπών πληροφοριακών οργανισμών και η χρήση της παραγόμενης εκ της συγκεκριμένης μελέτης γνώσης.¹⁷ Παρατηρούμε πως αυτό που κατηγοριοποιεί τους ορισμούς CI σε πιο «κλειστούς» σχετίζεται με μια σαφέστερη ή και αποκλειστική αναφορά σε δράσεις αλλοδαπών μυστικών υπηρεσιών και στην αντιμετώπισή τους. Στην περίπτωση που η συζήτηση περιστρέφεται γύρω από «εχθρικές ενέργειες» και σε τρόπους αποσόβησής τους, τότε, προσεγγίζουμε την αντικατασκοπευτική δράση με ευρύτερο πνεύμα.

Λεξικά, εγκυκλοπαίδειες, εγχειρίδια περί του αντικειμένου

Στη σελίδα 71 του *Historical Dictionary of International Intelligence* του Nigel West διαβάζουμε πως ως υπηρεσία Αντικατασκοπίας ορίζεται η υπηρεσία της οποίας η δράση σχετίζεται με τη μελέτη των αντιπάλων δικτύων πληροφοριών και την προσπάθεια διείσδυσης εντός αυτών. Το λεγόμενο *order of battle* του εχθρού αποτελεί διακαή πόθο μιας Υπηρεσίας με απώτερο σκοπό τη γνώση γύρω από τα πρόσωπα που το συνθέτουν, την παρακολούθησή τους, τον έλεγχό τους, τη χειραγώγησης τους κ. λ. Προκειμένου να επιτευχθεί κάτι τέτοιο πρέπει να αξιοποιηθούν είτε φίλιοι πράκτορες (με σκοπό την εισχώρηση στο ξένο στρατόπεδο), είτε αντίπαλο προσωπικό που προθυμοποιείται να συνεργαστεί αποσκοπώντας ή διαπράττοντας διπλή πρακτόρευση.¹⁸

Έναν παρόμοιο ορισμό βρίσκουμε στη σελίδα 114 του *Historical Dictionary of British Intelligence* του ιδίου μελετητή. Σύμφωνα μ' αυτόν, η διείσδυση μιας υπηρεσίας Αντικατασκοπίας στο αντίπαλο στρατόπεδο απαρτίζει τη μια από τις δύο βασικές της αποστολές. Η άλλη σχετίζεται με την προστασία / στεγανοποίηση του φίλιου δικτύου πληροφοριών.¹⁹

Στο *Historical Dictionary of United States Intelligence* του Michael Turner διαβάζουμε ότι αντικατασκοπία σημαίνει διαδικασία αναγνώρισης / εξουδετέρωσης αλλοδαπών πληροφοριακών δραστηριοτήτων. Ο ερευνητής σημειώνει πως αν και ο αντικατασκοπευτικός σχεδιασμός στις ΗΠΑ μοιράζεται κατά βάσει μεταξύ FBI, στο εσωτερικό, και CIA, στο εξωτερικό, όλες οι Υπηρεσίες μετέρχονται, στον έναν ή άλλο βαθμό, αντικατασκοπευτικών πρακτικών.²⁰ Κατ' αυτόν τον τρόπο δεικνύεται η

¹⁴ *Modernizing Intelligence: Structure and Change for the 21st Century*, επιμ. Victory C. Bernard, National Institute for Public Policy, USA, 2002, σ. 99

¹⁵ Godson Roy, *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, Transaction Publishers, N. Jersey / ΗΠΑ, 2001, σ. 2

¹⁶ Gleghorn E. T., *Exposing the Seams: The Impetus for Reforming U.S. Counterintelligence* (διατριβή κατατεθειμένη στο Naval Postgraduate School), Monterey / California, 2003, σ. 6-11

¹⁷ Ehrman John, "Toward a Theory of CI. What are We Talking About When We Talk about Counterintelligence?", ό. π., σ. 6

¹⁸ West N., *Historical Dictionary of International Intelligence*, The Scarecrow Press, Inc., ΗΠΑ, 2006, σ. 71

¹⁹ West N., *Historical Dictionary of British Intelligence*, The Scarecrow Press, Inc., ΗΠΑ, 2005, σ. 114

²⁰ Turner M., *Historical Dictionary of United States Intelligence*, The Scarecrow Press, Inc., ΗΠΑ, 2006, σ. 41

διάχυση της έννοιας CI εντός του συνόλου των πληροφοριακών θεσμών ως απαραίτητο στοιχείο λειτουργίας τους.

Στον πρώτο τόμο του *Encyclopedia of Espionage, Intelligence, and Security* ως δράση αντικατασκοπίας καταγράφεται εκείνη που λαμβάνει χώρα προκειμένου να αναγνωρισθεί (identify / identification), να παρακαμφθεί (circumvent / circumvention) ή να εξουδετερωθεί (neutralize / neutralization) η αντίστοιχη κακόβουλων κατασκοπευτικών δικτύων. Ο σχεδιασμός ερείδεται στην ικανότητα ορθής χρήσης των πληροφοριακών πόρων, με λίγα λόγια στην ορθή αξιολόγηση και αξιοποίηση της ληφθείσας πληροφορίας.²¹

Η Joint Publication (JP) 1-02, *Dictionary of Associated Terms*, του 2010 αλλά και η JP 2-01.2, *CI & HUMINT in Joint Operations*, του 2011 ορίζουν ως counterintelligence μια σειρά δράσεων με σκοπό την αναγνώριση, αποδιοργάνωση, εξαπάτηση αλλά και προστασία έναντι ξένων δυνάμεων, οργανισμών, ατόμων, τρομοκρατικών ή άλλων γκρουπ που προτίθενται να κατασκοπεύσουν, υπονομεύσουν / σαμποτάρουν, εκτελέσουν πολιτικά κτυπήματα / δολοφονίες κ. λ.²² Τον ίδιο ορισμό ανακαλύπτουμε στο Army Field Manual 2-0, *Intelligence*, του Department of the Army (2010) -τα εγχειρίδια στηρίζονται στην EO 12333.²³

Κατά την JP 2-0, *Joint Intelligence* του 2013 μια υπηρεσία CI εντέλλεται όπως: (1) ερευνήσει περί επίβουλων εσωτερικών / εξωτερικών στοιχείων (CI investigations), (2) συλλέξει δεδομένα περί αλλοδαπών Υπηρεσιών, εξωτερικών απειλών και τρομοκρατικών δικτύων (CI collection), (3) αναλύσει, εκτιμήσει, παράξει και διασπείρει πληροφόρηση στους αρμόδιους φορείς (CI analysis and production), (4) προβεί σε σειρά ειδικών επιχειρήσεων παρεμπόδισης, εξουδετέρωσης αλλά και μόχλευσης αλλότριων προσπαθειών κατασκοπίας και συγκεκαλυμμένων δράσεων (CI operations²⁴), (5) προβεί σε αλληλουχία χρηστικών / λειτουργικών (functional) ενεργειών με σκοπό την υποστήριξη πληροφοριακών / επιχειρησιακών σχεδιασμών

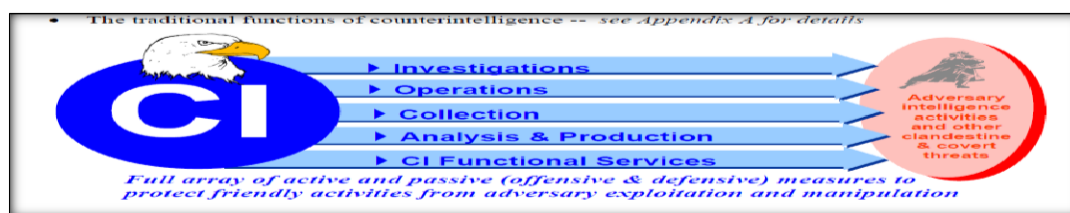
²¹ *Encyclopedia of Espionage, Intelligence, and Security*, volume 1, επιμ. Lerner K., Lerner B., Gale, ΗΠΑ, 2004, σ. 274-275

²² JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 16 July 2014), σ. 58

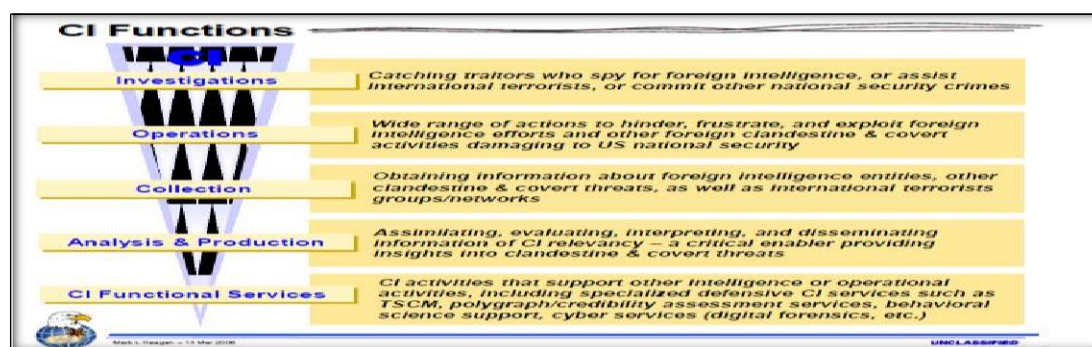
²³ Army Field Manual 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2010, σ. 6-1

²⁴ Αναφερόμαστε σε δράσεις σχεδιασμένες να αναγνωρίζουν, εξουδετερώνουν / αποτρέπουν, χειραγωγούν τις προσπάθειες συλλογής πληροφοριών εκ μέρους εχθρικών Υπηρεσιών ή / και τρομοκρατικών δικτύων. Πιο συγκεκριμένα επιχειρούν να: α) αποδιοργανώσουν, εξουδετερώσουν / καταστρέψουν, ποδηγητήσουν τη δράση αλλότριων πληροφοριακών οργανισμών, β) στρατολογήσουν ή παρακινήσουν σε αυτομόληση προσωπικό αλλοδαπών Υπηρεσιών, γ) συλλέξουν πληροφόρηση περί στόχων, τρόπων λειτουργίας, ειδικότερων δυνατοτήτων και τρωτοτήτων αντιπάλων οργανισμών, δ) δημιουργήσουν βάσεις δεδομένων (περί επιχειρήσεων ένθεν και εκείθεν, δυνητικών απειλών κ. λ.), ε) συλλέξουν τεχνικό εξοπλισμό αλλοδαπών Υπηρεσιών προς ανάλυση, εκτίμηση και ανάπτυξη τεχνικών αντιμέτρων, στ) αποκαλύψουν παρελθοντικές, τρέχουσες ή σχεδιαζόμενες εχθρικές espionage δράσεις, ζ) παράξουν πληροφόρηση προς υποστήριξη HUMINT επιχειρήσεων, η) συμβάλουν στην εξυπηρέτηση στρατιωτικών πρωτοκόλλων ασφαλείας και ανάλογων που σχετίζονται με (στρατιωτικές) μη πολεμικές επιχειρήσεις όπως και στο λεγόμενο peacekeeping, θ) παράξουν πληροφόρηση προς υποστήριξη της διαδικασίας λήψεως αποφάσεων -περί τούτων βλέπε JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 16 July 2014), σ. 59 και Secretary of the Navy Instruction (SECNAVINST) 3850.2C, Department of the Navy Counterintelligence, 20 Ιουλίου 2005. Ο John Ehrman κατηγοριοποιεί τα CI operations σε: α) δράσεις διείσδυσης εντός αλλοδαπών Υπηρεσιών μέσω στρατολόγησης πρακτόρων που ανήκουν ακριβώς σ' αυτές τις αλλοδαπές Υπηρεσίες, β) δράσεις διείσδυσης μέσω οικείων πρακτόρων ή συλληφθέντων αντιπάλων που εξαναγκάζονται να αλλάξουν στρατόπεδο και γ) δράσεις επιτήρησης / παρακολούθησης συγκεκριμένων ατόμων ή στόχων -για περισσότερα βλέπε Ehrman John, "Toward a Theory of CI. What are We Talking About When We Talk about Counterintelligence?" στο *Studies in Intelligence*, ό. π., σ. 15-16

αλλά και εξειδικευμένων αμυντικών CI λειτουργιών (CI functional services²⁵) όπως *Technical Surveillance Countermeasures -TSCM, polygraph / credibility assessment, behavioral science support, cyber services* με σκοπούς που ήδη έχουν περιγραφεί στη JP 1-02, στη JP 2-01.2 ή στο FM 2-0.^{26, 27} Το ίδιο έγγραφο τονίζει την ανάγκη στενής συνεργασίας μεταξύ υπηρεσιών εσωτερικών / εξωτερικών Πληροφοριών, υπηρεσιών ασφαλείας / προστασίας υποδομών αλλά και διωκτικών αρχών με το ενδιαφέρον να στρέφεται στη δημιουργία ενός εν εγρηγόρσει πλέγματος αμύνης έναντι εθνικών κινδύνων σχετιζομένων με τις (αμερικανικές) ένοπλες δυνάμεις, την έρευνα και τεχνολογία, την οικονομία, τις Υπηρεσίες καθαυτές.²⁸



Εικόνα 7: Τα καθήκοντα μιας υπηρεσίας CI. Η εικόνα ελήφθη από τη σελίδα 17 του *Introduction to U.S. Counterintelligence. "CI 101--A PRIMER"* (2005) του Mark Reagan



Εικόνα 8: Τα καθήκοντα μιας υπηρεσίας CI. Η εικόνα ελήφθη από τη σελίδα 66 του *Terms & Definitions of Interest for Counterintelligence Professionals* (επιμέλεια Mark Reagan)

²⁵ Παρεμφερής όρος, αν και μάλλον ευρύτερος, εμφανίζεται στο FM 2-0. Πρόκειται για το λεγόμενο *technical services and support* με σκοπό τη συνεισφορά στην έρευνα και συλλογή πληροφοριών (CI investigations, CI collection), γενικά στις CI επιχειρήσεις (CI operations) και στην τεχνική υποστήριξη των τελευταίων. Κάποιες από τις αρμοδιότητες αφορούν στο TSCM, στην προστασία των πληροφοριακών δικτύων αλλά και των υπολογιστικών ανάλογων (information and computer networks) του αμερικανικού στρατού και του DoD μέσω ανάληψης κυβερνοχωρικών CI δραστηριοτήτων (cyber CI activities), στην εφαρμογή της μεθόδου ανάληψης ψεύδους (polygraph examinations), στην υποστήριξη πληροφοριακών προγραμμάτων του στρατεύματος κ. λ. -για μια καλύτερη εικόνα βλέπε Army Field Manual 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2010, σ. 6-2 – 6-3

²⁶ Πρόκειται για τις πέντε λειτουργίες μιας υπηρεσίας Αντικατασκοπίας (CI Functions), επίσης βλέπε *counterintelligence activities* αντί *counterintelligence functions* [Department of Defense Directive (DoDD) O-5240.02, *Counterintelligence*, 2007, JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 16 July 2014), JP 2-01.2, *CI & HUMINT in Joint Operations*, DoD, Μάρτιος 2011]

²⁷ Ειδικότερα περί *functional services* βλέπε Department of Defense, *CI Functional Services Integrated Group Handbook, Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services*, Φεβρουάριος 2009 αλλά και Department of Defense Instruction (DoDI), *Counterintelligence Functional Services*, 5240.16, Αύγουστος 2012

²⁸ JP 2-0, *Joint Intelligence*, 2013, σ. B-9, επίσης βλέπε *Terms & Definitions of Interest for Counterintelligence Professionals*, ό. π., 2014, σ. 66



Εικόνα 9: μια άλλη αποτύπωση των καθηκόντων / λειτουργιών μιας υπηρεσίας CI. Η εικόνα ελήφθη από τη σελίδα 29 του *Introduction to U.S. Counterintelligence. "CI 101--A PRIMER"* (2005) του Mark Reagan

Η JP 2-01, *Joint and National Intelligence Support to Military Operations*, του 2012 σχετίζει τις, στρατιωτικές κατά κύριο λόγο, CI δράσεις με το λεγόμενο Indication and Warning System (I&W) και την προστασία του προσωπικού του DoD (force protection). Πέρα των γνωστών καθηκόντων συλλογής δεδομένων, η αντικατασκοπία προχωρά σε επιλεκτική εξέταση ατόμων προερχομένων από την αλλοδαπή (μετανάστες, πρόσφυγες, αποσκιρτήσαντες πράκτορες), στη λήψη συνεντεύξεων / αναφορών / απενημερώσεων (και) στρατιωτικού ενδιαφέροντος (interviews & debriefing), στην επισκόπηση ανοικτών πηγών ενημέρωσης (media, internet) κ. λ. Η JP 2-01 εκλαμβάνει το όλο εγχείρημα ως πλαίσιο εντός του οποίου συμποσούνται / αναλύονται κάθε είδους σχετικές πληροφορίες προερχόμενες ακόμα και από το χώρο των αστυνομικών / διωκτικών αρχών ή την όποια αξιόπιστη περί «υπόπτων δραστηριοτήτων» πηγή. Περαιτέρω, η 2-01 αποδίδει στην αντικατασκοπία τεχνικές συλλογής πληροφοριών παρόμοιες με αυτές που χρησιμοποιούνται στο πληροφοριακό HUMINT υποδηλώνοντας ότι μια πληρέστερη διαδικασία συλλογής αλλά και επεξεργασίας / μετατροπής της πληροφορίας σε πληροφόρηση απαιτεί συνεργασία σε επίπεδο Υπηρεσιών (στρατιωτικών και μη) και σε επίπεδο επί μέρους ενεργειών [βλέπε, π. χ., περί Joint Force Counterintelligence and Human Intelligence Staff Element (J-2X)].²⁹

Τέλος, η FM 3-24 / MCWP 3-33.5, *Counterinsurgency*, του 2006 σημειώνει σε αδρές γραμμές ότι αντικατασκοπία σημαίνει εκμηδενισμό των αντιπάλων προσπάθειών συλλογής πληροφοριών, επίσης, ανίχνευση, αναγνώριση, εξουδετέρωση και χειραγώγηση κάθε είδους επίβουλων πληροφοριακών δραστηριοτήτων είτε αυτές εκπορεύονται από φίλιους δρώντες, συμμάχους, ανταγωνιστές ή εχθρούς.³⁰

Οι ερευνητές του πεδίου

Ο Roy Godson εμβάλλει δίπλα στους όρους *identification* και *neutralization* τον όρο *exploitation* συνδέοντάς τον με την τακτική της παραπληροφόρησης. Ο ίδιος δεν

²⁹ JP 2-01, *Joint and National Intelligence Support to Military Operations*, 2012, σ. III-39. Για κάποιες λεπτομέρειες περί 2X δράσεων βλέπε συνδυαστικά FM 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2010, σ. 6-3 και *Terms & Definitions of Interest for Counterintelligence Professionals*, ό. π., 2014

³⁰ FM 3-24 / MCWP 3-33.5, *Counterinsurgency*, Headquarters, Department of the Army, Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., December 2006, σ. 3-30

θεωρεί απαραίτητη μια ιδιαίτερη συζήτηση περί αμυντικής ή επιθετικής στάσης -τόσο η άμυνα όσο και η επίθεση αποτελούν συνδεδεμένες δράσεις. Η πρώτη συλλέγει / αναλύει στοιχεία περί των αντιπάλων πληροφοριακών οργανισμών με σκοπό την προστασία των κρατικών μυστικών και τη διασφάλιση μη εξαπάτησης της πολιτείας εκ μέρους εξωγενών παραγόντων. Η δεύτερη συνεισφέρει στο κτίσιμο μιας προωθημένης στρατηγικής με σκοπό την εξυπηρέτηση οικείων συμφερόντων εντός του πεδίου των διεθνών σχέσεων, επιπλέον, είναι η αντικατασκοπία και μόνο αυτή που ως θεσμός διαθέτει την τεχνογνωσία ώστε να αμυνθεί ή / και να επιτεθεί στον όποιο αντίπαλο, μόνο αυτή δύναται να τον κατανοήσει και, άρα, να προ-νοήσει. Για τον Godson η άμυνα δεν συνιστά μια στατική λειτουργία ενώ, τέλος, το σημαντικότερο τμήμα μιας αντικατασκοπευτικής δράσης εξελίσσεται στο εξωτερικό καταρρίπτοντας τον ισχυρισμό περί αποστολών αποκλειστικά εγχωρίου περιβάλλοντος.³¹ Συνοπτικά, κατά τον μελετητή τα κυριότερα προϊόντα της αμερικανικής αντικατασκοπίας σχετίζονται με: α) την *εθνική αντιπληροφοριακή εκτίμηση* (*national CI estimates*) με σκοπό μια συνολική / περιεκτική αποτίμηση κινδύνων προερχομένων εξ αλλοδαπών Υπηρεσιών και κρατικών / μη κρατικών δρώντων, β) αναφορές περί δραστηριοτήτων αλλοδαπών Υπηρεσιών, περί του προσωπικού των τελευταίων, περί του *modus operandi* αυτών κ. λ. γ) την ουδετεροποίηση / χειραγώγηση αλλοδαπών Υπηρεσιών, δ) τη *θετική πληροφόρηση* (*positive intelligence*). Οι υπηρεσίες CI δύνανται να παράξουν πληροφόρηση σχετική με προθέσεις, προτεραιότητες, δυνατότητες / τρωτότητες αλλοδαπών κυβερνήσεων, οργανώσεων, κινημάτων, ομάδων κ. λ. Πρόκειται για πληροφόρηση που προέρχεται από αντικατασκοπευτικές επιχειρήσεις διείσδυσης εντός αλλοδαπών Υπηρεσιών με την προϋπόθεση πως οι τελευταίες αποτελούν μηχανισμό πολιτικής του κράτους που υπηρετούν³² -ουσιαστικά ο Godson μιλά για κατασκοπία.

Ο Mark Lowenthal διακρίνει τουλάχιστον τρεις μορφές αντικατασκοπευτικής δράσης που περιστρέφονται γύρω από: α) τη *συλλογή* της πληροφορίας, β) την *άμυνα* με σκοπό τον τορπιλισμό των προσπαθειών διείσδυσης του αλλότριου παράγοντα εντός της οικείας περιμέτρου³³ και γ) την *επίθεση* με προοπτική τη χειραγώγηση των αντιπάλων Υπηρεσιών.³⁴ Αν για τα αμυντικά ή / και τα επιθετικά καθήκοντα δεν υπάρχει κάτι προς ιδιαίτερο σχολιασμό, αυτό που παρατηρούμε αφορά στη διάθεση του ερευνητή να υπάγει με ξεχωριστό τρόπο τη διαδικασία συλλογής πληροφοριών στο πινάκιο καθηκόντων μιας υπηρεσίας CI. Είναι φανερό πως ο Lowenthal εκτιμά αμέριστα ένα κομμάτι εργασιών τη στιγμή που δεν αναφέρετε, όπως πολλοί άλλοι κάνουν, σ' αυτό της *ανάλυσης* της πληροφορίας. Πάρα τούτα αίσθησή μας αποτελεί πως συλλογή και ανάλυση συνθέτουν γι' αυτόν ό,τι εντάσσει εντός της *αναλυτικής* (*analytical*) περιοχής μιας Υπηρεσίας με την άμυνα και την επίθεση να εντάσσονται

³¹ Godson R., *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, ό. π., σ. xxviii

³² Godson R., "Intelligence: an American View" στο *British and American Approaches to Intelligence*, επιμ. Robertson G. K., Royal United Services Institute, USA, 1987, σ. 20-25

³³ Σημαντικό ρόλο σ' αυτό παίζει το λεγόμενο *information security -infosec* με σκοπό την προστασία της πληροφορίας και των πληροφοριακών συστημάτων έναντι επίβουλων προσπαθειών μη εξουσιοδοτημένων προσεγγίσεων, προσβάσεων ή εισόδων. Κατά την Joint Security Commission II Report η διασφάλιση των informational networks δεικνύει κύριο καθήκον του infosec -για περισσότερα βλ. Joint Security Commission II Report, Αύγουστος 1999, σ. 18, JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 16 July 2014), JP 3-13, *Information Operations*, Νοέμβριος 2012 (Incorporating Change 1 November 2014) αλλά και *National Intelligence: A Consumer's Guide*, ODNI, Μάιος 2009

³⁴ Lowenthal M., *Intelligence. From Secrets to Policy*, CQPress, Washington, D.C., HΠΑ, 2008⁴, σ.

στην αντίστοιχη επιχειρησιακή (operational).³⁵ Από τη μεριά του ο Eric Timm γράφει πως κύριο επιχειρησιακό καθήκον ενός αντιπληροφοριακού τμήματος αποτελεί η δημιουργία καναλιών (εν είδει chokepoints) των οποίων τη διέλευση δεν μπορεί να αποφύγει ο αντίπαλος πράκτορας. Τα συγκεκριμένα σημεία ελέγχου θα παγιδεύσουν τον τελευταίο υπό την προϋπόθεση πως έχουν αναλυθεί προθέσεις και σχεδιασμοί.³⁶

Η Michelle van Cleave στο *Counterintelligence and National Security* αναφέρεται στις τέσσερις επιχειρησιακές λειτουργίες του CI ήτοι, *identification, assessment, neutralization* και *exploitation*. Πρόκειται για δράσεις εκτελούμενες έναντι ξένων δυνάμεων, τρομοκρατικών ομάδων, οντοτήτων που επιβουλεύονται την αμερικανική ασφάλεια στο εσωτερικό και στο εξωτερικό. Η πρώτη δράση σχετίζεται με την αναγνώριση της επίβουλης οντότητας, η δεύτερη με την εκτίμηση της απειλής και των δυνατοτήτων του αντιπάλου, η τρίτη με την εξουδετέρωση του τελευταίου (defensive CI) και η τέταρτη με την χειραγώγησή του (offensive CI).³⁷ Αναφορικά με τους στρατηγικούς στόχους του CI και επί τη βάση του *The National Counterintelligence Strategy of the United States* του 2005 η van Cleave σημειώνει ότι αυτοί αφορούν: α) στην καταπολέμηση των πληροφοριακών επιχειρήσεων των τρομοκρατικών ομάδων. Πρόκειται για επίβουλες δράσεις συλλογής πληροφοριών, στρατολόγησης, διαχείρισης ανθρωπίνων πόρων, εξαπάτησης. Ουσιαστικά αναφερόμαστε σε επιχειρήσεις όμοιες με αυτές των κρατικών Υπηρεσιών, β) στην απόκτηση πλεονεκτήματος έναντι των ξένων Υπηρεσιών διά της κτήσεως πληροφοριών περίξ αυτών ή μέσω αυτών (positive intelligence) με απώτερο σκοπό την αδρανοποίηση / εξαπάτηση τους γ) στην προστασία κρίσιμων αμυντικών τεχνολογιών, δ) στην εξουδετέρωση αλλοδαπών πληροφοριακών D&D (Denial & Deception) επιχειρήσεων όπως και προπαγανδιστικών «επιχειρήσεων επιρροής», ε) στην προστασία των αμερικανικών consortiums έναντι προσπαθειών κλοπής οικονομικών / εμπορικών μυστικών από ξένους ανταγωνιστές, στ) στην επικουρία της διαδικασίας παραγωγής πολιτικής εθνικής ασφαλείας, ζ) στη δόμηση ενός Εθνικού Αντιπληροφοριακού Συστήματος με σκοπό την εκτέλεση της εθνικής στρατηγικής ασφαλείας και αντιπληροφόρησης στον 21^ο αιώνα.³⁸

Στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, υπό την επιμέλεια των Jennifer Sims και Burton Gender, ανιχνεύουμε έναν αναλυτικότερο ορισμό. Σύμφωνα μ' αυτόν η αντικατασκοπία δεν είναι άλλο από alter ego της κατασκοπίας. Ορισμένοι έχουν οδηγηθεί στην απόφαση πως οι πληροφορίες δεν παίζουν ιδιαίτερο ρόλο στην έκβαση μιας μάχης (ακριβώς λόγω αποτυχιών στρατευμάτων που διέθεταν ικανές, θεωρητικά τουλάχιστον, υπηρεσίες Πληροφοριών), πως η ισχύς και μόνο είναι αυτή που οδηγεί στη νίκη. Τα πράγματα

³⁵ Lowenthal M., *Intelligence. From Secrets to Policy*, CQPress, Washington, D.C., ΗΠΑ, 2008⁴, σ. 113

³⁶ Timm W. Eric, "Countersabotage--a Counterintelligence Function" στο *Studies in Intelligence*, Volume 7, Number 2, διαθέσιμο στη διαδικτυακή τοποθεσία https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a06p_0001.htm όπου καταφύγαμε την 5^η Μαΐου 2016

³⁷ Για μια πληρέστερη εικόνα βλέπε van Cleave, Michelle, *Counterintelligence and National Security*, National Defense University Press, Washington, D.C., 2007, σ. 5-11 αλλά και "Guide to the Study of Intelligence. What is Counterintelligence? A Guide to Thinking and Teaching about CI" στο *The Intelligence Journal of U.S. Intelligence Studies*, Volume 20, Number 2, 2013, σ. 59-65 της ίδιας

³⁸ van Cleave, Michelle, *Counterintelligence and National Security*, ό. π., σ. 14-20, επίσης NCIX Publication 2005-10007, *The National Counterintelligence Strategy of the United States*, Office of the National Counterintelligence Executive, Washington, D.C., Μάρτιος 2005 και *The National Counterintelligence Strategy of the United States*: NCIX Speech (CI for the 21st Century Conference), 4-5 Μαρτίου 2005, διαθέσιμο στην ιστοσελίδα <https://fas.org/irp/news/2005/03/ncix030505.pdf> εις την οποία ανατρέξαμε την 21^η Σεπτεμβρίου 2016

δεν είναι, ίσως, ακριβώς έτσι. Όταν δύο οντότητες δεν χαρακτηρίζονται από μια άξια λόγου ικανότητα σύλληψης και ανάλυσης πληροφορίας, τότε, η ισχύς αναπόφευκτα καταφαίνεται ως μοναδικό μέσον καταβολής του αντιπάλου. Όταν όμως μια πλευρά, και δη και η αδύναμη, κατορθώσει να αποκτήσει τον έλεγχο στον πόλεμο των πληροφοριών, τότε, η νίκη επί της δυνατότερης δεν εμφανίζει κάτι ανεξήγητο.³⁹ Επιχειρησιακά ένας αντικατασκοπευτικός ιστός στοχεύει στην απόκρουση της κατασκοπευτικής επίβουλης δραστηριότητας ή, καλύτερα, ξεκινά από τη συγκεκριμένη πρόθεση. Αυτό μεταφράζεται σε δράσεις αμυντικού και αργότερα επιθετικού χαρακτήρα που κατηγοριοποιούνται εντός τεσσάρων τακτικισμών. Ομιλούμε για την τακτική της παθητικής άμυνας (*passive defense*), της ενεργητικής άμυνας (*active defense*), της παθητικής επίθεσης (*passive offense*) και της ενεργητικής επίθεσης (*active offense*), ειδικότερα:

- Παθητική άμυνα καλείται η δράση που σκοπό έχει την ανάπτυξη ενός δικτύου ασφαλείας προς αποφυγήν διαρροών ευαίσθητων πληροφοριών. Το συγκεκριμένο δίκτυο συνήθως δομείται υπό ενός συνδυασμού ύπαρξης ηλεκτρονικών συστημάτων ασφαλείας προηγμένης τεχνολογίας και ενεργοποίησης παραδοσιακών πρακτικών όπως δημιουργία δυσκολοπροσβάσιμων χώρων αποθήκευσης / ταξινόμησης δεδομένων χαρακτηριζομένων από την ύπαρξη υπογείων εγκαταστάσεων, την παρουσία αδιάρρηκτων θυρών, αδιάτρητων τοιχίων κ. λ. Ωστόσο το στάδιο αυτό έχει να κάνει περισσότερο με την ασφάλεια παρά, μάλλον, με την αντικατασκοπευτική πολυπλοκότητα και σκέψη καθαυτή. Η τελευταία δεν επιζητά μόνο την περίβλεψη του χώρου αλλά (και) το «γιατί» της όποιας αστοχίας. Αυτό σημαίνει ότι μια οπή στον προστατευτικό ιστό ενδέχεται να αποτελέσει αρχή έρευνας που θα οδηγήσει στην αποκάλυψη αδυναμιών και στο ξεσκέπασμα, στον ίδιο χρόνο, αντιπάλων στρατηγικών, πλάνων και δυνατοτήτων. Προσθέτουμε πως απαραίτητη προϋπόθεση κάτι τέτοιου αποτελεί: α) η άμεση ανεύρεση του σπασμένου κρίκου ώστε να ελεγχθεί ποικιλοτρόπως η επιζήμια δράση προτού μια ανεπανόρθωτη βλάβη ενσκήψει και β) η επιτυχής απάντηση στο «γιατί» ο αντίπαλος στόχευσε στο δεδομένο σημείο.
- Ενεργητική άμυνα καλείται η δράση που σκοπό έχει την απόκτηση πληροφοριών περί των αντιπάλων κατασκοπευτικών σχεδιασμών ή / και την αποδιοργάνωση / αποσυντονισμό των τελευταίων. Κάτι τέτοιο λαμβάνει χώρα είτε διά της παρακολούθησης / επιτήρησης (*surveillance*) των επίβουλων στοιχείων, είτε διά της αξιοποίησης προσωπικού του αντιπάλου που έχει αποσκιρτήσει (*defector*)⁴⁰, είτε διά της χρήσεως διπλών πρακτόρων (οι όροι «*double agent*», «*pole*», «*dangle*» αποδίδουν στην ουσία, με τον έναν ή άλλο τρόπο, αυτό που νοείται διά του όρου «διπλός πράκτορας») προς αλίευση πληροφοριών.
- Η παθητική επίθεση σχετίζεται με μια προσπάθεια επηρεασμού του αντιπάλου προς την κατεύθυνση λήψης αποφάσεων που εξυπηρετούν τα συμφέροντα τού κράτους που προβαίνει σ' αυτήν την τακτική. Κάτι τέτοιο επιτυγχάνεται διά της «έμμεσης» παραπληροφόρησης μέσω, π. χ., της τέχνης του καμουφλάζ (όσον

³⁹ Sims J., "Twenty-first-Century Counterintelligence. The Theoretical Basis for reform" στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, Washington, D.C., 2009, σ. 19-20

⁴⁰ Ένας πράκτορας που έχει αποσκιρτήσει (*defector*) δεν αποτελεί διπλό πράκτορα (*double agent*) καθώς οι προθέσεις και η ταυτότητά του καθίστανται άμεσα γνωστές με την εκδήλωση της φυγής του, ωστόσο, τα κίνητρα είναι παρόμοια με αυτά του δευτέρου -για περισσότερες λεπτομέρειες βλέπε Turner M., *Historical Dictionary of United States Intelligence*, The Scarecrow Press, Inc., ΗΠΑ, 2006, σ. 49 και Goldman J., *Words of Intelligence*, The Scarecrow Press, Inc., ΗΠΑ, 2006, σ. 34

αφορά σε στρατιωτικές επιχειρήσεις) επενδύοντας στη δυνατότητα του εχθρού να συλλέξει την κακόβουλη πληροφορία αλλά και στη μη ικανότητά του να αποκρυπτογραφεί την παγίδα που κρύβεται πίσω από τη φαινομενική επιτυχία.⁴¹

- Μόλις παραπάνω αναφερθήκαμε στην έμμεση παραπληροφόρηση υπό την ελπίδα πως η πληροφορία θα συλλεχθεί ως θήρα από τις αντίπαλες Υπηρεσίες. Η τακτική της ενεργητικής επίθεσης, ωστόσο, εμπεριέχει έναν πλέον προωθημένο ελιγμό. Κατά τον τρόπο τούτο δεν περιμένουμε τον αντίπαλο να συλλέξει μέσω ιδίων πόρων την πληροφορία αλλά την περνάμε σ' αυτόν απευθείας με την συνηθέστατη αξιοποίηση, και πάλι, διπλών πρακτόρων⁴² που απολαμβάνουν ένα ικανό επίπεδο *bona fide* -πρόκειται μάλλον για τη δυσκολότερη αποστολή.⁴³

Αποσαφήνιση: Ασφάλεια και Αντικατασκοπία

*Αντικατασκοπία (CI) δεν σημαίνει ασφάλεια (security)...Η πρώτη ξεπερνά την αμιγώς αμυντική φύση της δεύτερης*⁴⁴

Ο William R. Johnson γράφει ότι *...security is a dimension of clandestinity in espionage, counterespionage, counterintelligence, adultery, and poker. It is to these activities what style is to a writer, an athlete, or a musician, but it is not itself a work, a game, or a performance. Its purpose is prophylactic: it excludes toxic and infectious organisms and conserves vital fluids*⁴⁵, επίσης πως *...people like to confuse counterintelligence (CI) with security. In practice, the two are related but not identical.*⁴⁶ Ο Robert P. Hanssen σημειώνει ότι *...it's not [CI] security work. Security protects. It does not attack. CI attacks the actor. It attacks the opposition intelligence structures. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart*

⁴¹ Ένα εκπληκτικό παράδειγμα αναφέρεται στις σελίδες 17-18 του *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence* του Roy Godson. Πρόκειται, ίσως, για τη διασημότερη υπόθεση παραπληροφόρησης στην παγκόσμια πολεμική ιστορία με τους Συμμάχους να πείθουν τους Γερμανούς πως η περίφημη απόβαση στη Νορμανδία (Operation Fortitude Plan) κάθε άλλο παρά στη συγκεκριμένη τοποθεσία θα λάβει χώρα. Οι δυτικοί τοποθετώντας ομοιώματα τανκ (dummy tanks) στις ακριβώς απέναντι από το γαλλικό Καλαί βρετανικές ακτές έσπρωξαν τους Ναζί να πιστέψουν σε έναν σχεδιασμό που ποτέ δεν έλαβε σάρκα και οστά. Η απόβαση, τελικά, επιχειρήθηκε και περατώθηκε 200 χιλιόμετρα δυτικότερα με τους Γερμανούς να πιάνονται εξαπίνης. Οι Σύμμαχοι εκμεταλλεύτηκαν τόσο την εγγύτητα των βρετανικών ακτών από τις αντίστοιχες του Καλαί όσο και τη γνώση πως οι Γερμανοί διέθεταν ικανότητες κατόπτευσης χώρου πετυχαίνοντας τον αιφνιδιασμό μέσω της τέχνης του καμουφλάζ και της έμμεσης παραπληροφόρησης

⁴² Στην ανωτέρω υποσημείωση αναφερθήκαμε στην προετοιμασία για την απόβαση στη Νορμανδία αποδίδοντας ένα παράδειγμα παθητικής επίθεσης εκ μέρους της συμμαχικής αντικατασκοπίας. Ωστόσο, η όλη επιχείρηση στηρίχτηκε σε ένα ευρύτερο πρόγραμμα παραπληροφόρησης των Γερμανών από τους Βρετανούς. Πρόκειται για το Double Cross System που λάβαινε χώρα σχεδόν από την έναρξη του πολέμου -βλέπε μεταξύ άλλων Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, Brassey's, Inc., Washington, D.C., 2002³, σ. 112-113, Sims J., "Twenty-first-Century Counterintelligence. The Theoretical Basis for reform" στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, ό. π., σ. 23 και West N., "Double Cross - MI5 in World War Two" στην ιστοσελίδα http://www.bbc.co.uk/history/worldwars/wwtwo/mi5_ww2_01.shtml εις την οποία ανατρέξαμε την 6^η Απριλίου 2013

⁴³ Για τους τέσσερις σχεδιασμούς αμυντικής και επιθετικής αντικατασκοπευτικής δράσης βλέπε Sims J., "Twenty-first-Century Counterintelligence. The Theoretical Basis for reform" στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, ό. π., σ. 21-23

⁴⁴ Reagan Mark, *Introduction to U.S. Counterintelligence. "CI 101--A Primer"*, 2005, σ. 11

⁴⁵ Johnson R. W., "Clandestinity and Current Intelligence" στο *Studies in Intelligence*, Volume 20, Number 3, 1976, σ. 26

⁴⁶ Johnson R. W., *Thwarting Enemies at Home and Abroad. How to Be a Counterintelligence Officer*, Georgetown University Press, Washington, D.C., 2009, σ. 1

security.⁴⁷ Ο George P. Morse επικουρεί τονίζοντας το εξής: “[t]he security effort seeks primarily to protect its assigned material against compromise, deliberate or accidental, while the counter-espionage effort operates actively to identify, thwart, mislead, and destroy an opposing espionage capability”.⁴⁸ Από τη μεριά του ο Angelo Codevilla υποστηρίζει πως ...counterintelligence... is often confused with security-that is, merely with protecting secrets and protecting against subversion. Yet whereas the objective of security is to cut and prevent all contacts between hostiles and those who are to be protected the objective of CI is to engage hostile intelligence, control what it knows, and if possible control what it does. In principle, neither security people nor CI people deny the validity of the others approach, but CI people think of security as flatfooted cops, and the latter think of the former as game-playing spooks.⁴⁹ Ο Wasemiller κάνει λόγο για counterintelligence δράσεις (counterintelligence activities) που κατηγοριοποιούνται σ’ αυτές της ασφαλείας (security) και σ’ αυτές της αντικατασκοπίας (counterespionage). Οι πρώτες σχετίζονται με την παρουσία παθητικών / στατικών μέτρων προστασίας έναντι εχθρικών ή κεκαλυμμένων ενεργειών. Οι δεύτερες ουσιαστικά αναφέρονται σε επιθετικές μεθοδεύσεις μέσω πρακτικών διείσδυσης στο αντίπαλο πληροφοριακό στρατόπεδο, πρακτικών που καταλήγουν στη χειραγώγηση του τελευταίου.⁵⁰ Ο John Bruce Lockhart τονίζει πως οι έννοιες counterintelligence και security είναι αλληλένδετες. Γράφει ότι η δεύτερη εντέλλεται όπως: α) επιβλέπει άτομα που διαθέτουν πρόσβαση σε διαβαθμισμένες πληροφορίες, β) επιβλέπει την περίμετρο κρίσιμων εθνικών υποδομών, βλέπε, π. χ., στρατιωτικών εγκαταστάσεων, με σκοπό την αποσόβηση υπονομευτικών, αποσταθεροποιητικών, τρομοκρατικών κ. λ. ενεργειών, γ) προστατεύει το απόρρητο οικείων μυστικών δράσεων, δ) προστατεύει την οικεία χώρα από επίβουλές δραστηριότητες ξένων χωρών και μυστικών υπηρεσιών.⁵¹

Στο ίδιο μοτίβο, με αποκλειστικό σκοπό ωστόσο την ακεραιότητα των Υπηρεσιών, ο Stan Taylor καταγράφει τα εξής προαπαιτούμενα «αντικατασκοπευτικής ασφαλείας»: α) έλεγχο υποψηφίου προσωπικού Υπηρεσιών (pre-employment personnel security), β) έλεγχο εν ενεργεία προσωπικού Υπηρεσιών (in-service personnel security), γ) ασφάλεια χώρων παραγωγής / καταχώρησης πληροφόρησης (facility security), δ) ασφάλεια επικοινωνιών Υπηρεσιών (communications security), ε) κατηγοριοποίηση πληροφοριών / διαμερισματοποίηση δεδομένων (classification / compartmentalization), στ) [Counter]Signals Intelligence δράση με σκοπό το σπάσιμο επικοινωνιών αλλοδαπών Υπηρεσιών, την ενδεχόμενη αποκάλυψη ατόμων που επιβουλεύονται οικείους πληροφοριακούς οργανισμούς ή εγχώρια συμφέροντα.⁵²

Ο William Johnson χρησιμοποιώντας παρεμφερείς όρους μιλά για: α) personnel security, β) physical security (αντί για facility security) και γ) επιχειρησιακή ασφάλεια (operational security) ενσωματώνοντας σ’ αυτήν τις πρακτικές του compartmentalization και του need-to-know.⁵³

⁴⁷ Παράθεμα στο άρθρο “Diary of a Spy” του Paul M. Rodriguez στο περιοδικό *Insight on the News* της 16^{ης} Ιουλίου 2001, επίσης βλέπε *Terms & Definitions of Interest for DoD Counterintelligence Professionals*, Defense Intelligence Agency, 2011, σ. 152

⁴⁸ Morse P. G., *America Twice Betrayed: Reversing Fifty Years of Government Security Failure*, Bartleby Press Inc, USA, 1995, σ. 50

⁴⁹ Codevilla A., *Informing Statecraft: Intelligence for a New Century*, The Free Press, USA, 1992, σ. 26

⁵⁰ Wasemiller C. A., “The Anatomy of Counterintelligence” στο *Studies in Intelligence*, Volume 13, Number 1, 1969, διαθέσιμο στο https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol13no1/html/v13i1a02p_0001.htm εις το οποίο καταφύγαμε την 5^η Μαΐου 2016

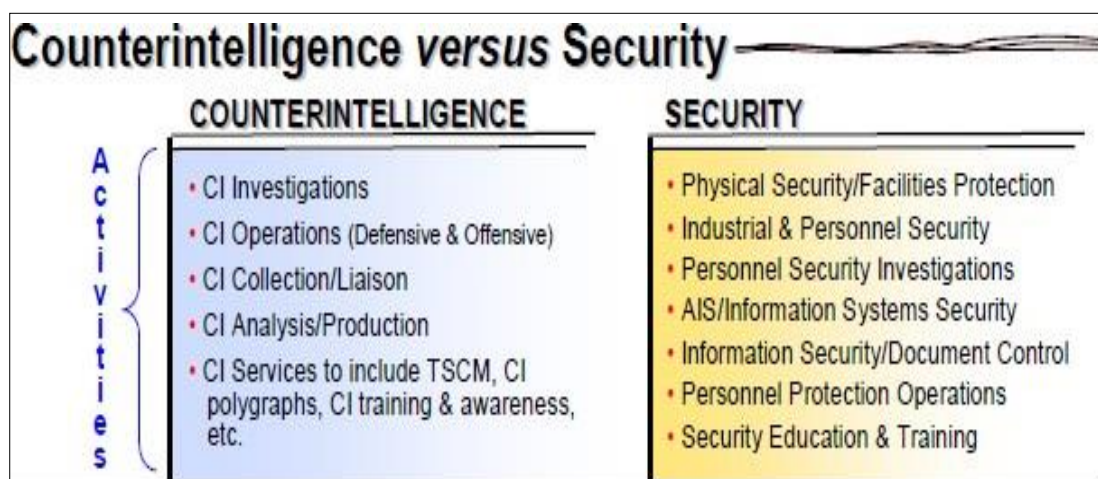
⁵¹ Lockhart John, “Intelligence: A British View” στο *Approaches to Intelligence*, επιμ. Robertson K., Macmillan, London, 1987, σ. 43-44

⁵² Taylor Stan, “Definitions and Theories of Counterintelligence” στο *Strategic Intelligence*. Volume 4, επιμ. Johnson Lock, Praeger Security International, USA, 2007, σ. 5-7

⁵³ Johnson William, *Thwarting Enemies at Home and Abroad. How to Be a Counterintelligence Officer*, ό. π., σ. 1-2

Κατά τη Senate Report # 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, (Church Committee Report, Απρίλιος 1976), η αμυντική δράση ενός αντικατασκοπευτικού σχεδιασμού (της όποιας Υπηρεσίας, οργανισμού κ. λ.) επιλαμβάνεται της ασφάλειας / ελέγχου: α) του εντεταλμένου προσωπικού, β) του χώρου / εγκαταστάσεων και γ) των επιχειρησιακών πλάνων. Η επιθετική έκφανση ή, αλλιώς, counterespionage κατευθύνεται στη διείσδυση εντός της αντιπάλου Υπηρεσίας με σκοπό τη χειραγώγηση / έλεγχο της τελευταίας.⁵⁴

Η Senate Select Committee on Intelligence (SSCI) Report 99-522 του αμερικανικού Κογκρέσου με τίτλο *Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs* (1986) τονίζει ότι ...[c]ounterintelligence measures deal directly with foreign intelligence service activities, while security programs are indirect defensive actions that minimize vulnerabilities. Τέλος, στην Intelligence Community Directive (ICD) 700 του Office of the Director of National Intelligence αναφέρεται πως “CI and security shall be regarded as interdependent and mutually supportive disciplines with shared objectives and responsibilities associated with the protection of secrets and assets. CI gathers information and conducts activities to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. Security programs establish appropriate personnel, physical, information, operations, industrial and technical security, safeguards, and countermeasures to protect information and information systems, operations, resources, technologies, and facilities from threats”.⁵⁵



Εικόνα 10: η διαφορετικότητα μεταξύ αντικατασκοπίας και ασφαλείας. Η εικόνα ελήφθη από τη σελίδα 11 του *Introduction to U.S. Counterintelligence. “CI 101--A PRIMER”* (2005) του Mark Reagan

Σύμφωνα με τον Vincent Bridgeman η δράση της αντικατασκοπίας εκλαμβάνεται ως επικουρία στην πορεία προς τη λήψη αποφάσεων. Κατ’ αυτόν τον τρόπο ένα σχετικό τμήμα οφείλει: α) να κατανοήσει τις (πληροφοριακές) ανάγκες ενός πολιτικού επιτελείου, β) να κατανοήσει τη φύση της διαδικασίας λήψεως αποφάσεων

⁵⁴ Senate Report # 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, US Government Printing Office, Washington, D.C., Απρίλιος 1976, σ. 166

⁵⁵ ICD 700, *Protection of National Intelligence*, Office of the Director of National Intelligence, 7 Ιουνίου 2012, έγγραφο διαθέσιμο και στο <http://fas.org/irp/dni/icd/icd-700.pdf> όπου καταφύγαμε την 4^η Ιουλίου 2015, επίσης ανέτρεξε στο Terms & Definitions of Interest for Counterintelligence Professionals, ό. π., σ. 283-285

και γ) να αποδεχτεί πως αντίστοιχη δράση και προσπάθειες διεξάγουν και οι Υπηρεσίες του αντιπάλου προσπαθώντας να τις μπλοκάρει. Εν γένει μια υπηρεσία Αντικατασκοπίας επιβάλλεται: α) να προβαίνει σε *παθητική* ή / και *ενεργητική άρνηση* (*passive / active denial*) εισόδου του αντιπάλου στο φίλιο δίκτυο πληροφοριών είτε βελτιώνοντας τα μέτρα ασφαλείας είτε εμπλέκοντάς τον σε ανώφελα *operational*, όπως τα ονομάζει ο Bridgeman, *games*. Σε κάθε περίπτωση αντικειμενικό στόχο αποτελεί η μη απόκτηση, από τον ανταγωνιστή, πλεονεκτήματος που δύναται να κεφαλαιοποιηθεί εντός της δικής του διαδικασίας λήψεως αποφάσεων, β) να ενημερώνει και να διαφωτίζει (*insight*) την πολιτεία ως προς τις προθέσεις των «άλλων», να προειδοποιεί ως προς τις κατασκοπευτικές ικανότητες και σχεδιασμούς αυτών, γ) να συμβάλλει στη χειραγώγηση (*manipulation*) των αποφάσεων του ξένου παράγοντα χρησιμοποιώντας το ίδιο το πληροφοριακό του δίκτυο μέσω επιχειρήσεων παραπληροφόρησης (*deception operation*).⁵⁶ Οι τρεις αναφερόμενες διακριτές δράσεις δεν αποκλείεται να συμπέσουν ή να παρουσιάσουν επιχειρησιακές επικαλύψεις. Χαρακτηριστικό είναι πως αν και συμβάλουν στη διαδικασία λήψεως αποφάσεων του εγχώριου επιτελείου αποσκοπούν, ταυτόχρονα, σε μια *αρνητική μεθόδευση* ως προς την αντίστοιχη του ανταγωνιστή.⁵⁷ Κατ' αυτήν την έννοια παρατηρείται ένας αέναος πόλεμος κατασκοπίας (της μιας πλευράς) και αντικατασκοπίας (της άλλης πλευράς) ως προς τα εξής: α) αν μια υπηρεσία εξωτερικών Πληροφοριών κινείται στην κατεύθυνση συλλογής στοιχείων, τότε, μια υπηρεσία Αντικατασκοπίας πρέπει να υπονομεύσει ή να χειραγωγήσει την προσπάθεια της πρώτης (καθήκον Α), κάτι όχι τόσο δύσκολο αν η «κατασκοπευτική στόχευση» είναι «αναμενόμενη και λογική», β) αν ένας κατασκοπευτικός σχεδιασμός οδηγεί, μέσα από τη συλλογή και ανάλυση πληροφορίας, σε μια προεικόνιση (*anticipation*), τότε, ένας αντικατασκοπευτικός ανάλογος οφείλει να στρεβλώσει αυτήν ακριβώς την προεικόνιση (καθήκον Β). Προκειμένου να επιτευχθεί κάτι τέτοιο απαιτείται η σε βάθος γνώση του συγκεκριμένου μηχανισμού (*anticipatory mechanism*) του αντιπάλου, γ) ένα πληροφοριακό δίκτυο επικοινωνεί με την κεντρική διοίκηση μέσω διαύλων μεταφέροντας στοιχεία και δεδομένα. Αν κάποιοι από τους διαύλους δεν δύναται να χειραγωγηθούν, τότε, πρέπει να αποκοπούν ή να πληγεί η αξιοπιστία τους -πρόκειται για μια ακόμα αποστολή (καθήκον Γ) μιας αντικατασκοπευτικής Υπηρεσίας, δ) μια υπηρεσία εσωτερικών Πληροφοριών δεν δρα μόνο κατά μιας εχθρικής εξωτερικών αλλά, επίσης, κατά της αναλόγου Υπηρεσίας του αντιπάλου. Αν η τελευταία προστατεύει τα κρατικά μυστικά αρνούμενη την πρόσβαση σ' αυτά, τότε, η πρώτη οφείλει να σπάσει τον προστατευτικό κλοιό. Αν επίσης η τελευταία επιχειρεί μια προσπάθεια παραπληροφόρησης, τότε, η πρώτη πρέπει να την ακυρώσει (καθήκον 4). Η τελευταία διπλή αποστολή δεικνύει, κατά την

⁵⁶ Bridgeman Vincent, "Defense Counterintelligence" στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, ό. π., σ. 128. Επιπλέον, κατά τον Christopher Felix αιώτερος στόχος μιας υπηρεσίας CI είναι να ...διεισδύσει στο αντίπαλο πληροφοριακό σύστημα: να καταστεί, χωρίς να γίνει αντιληπτή, λειτουργικό τμήμα του, των εκτιμήσεων και των επιχειρήσεων του εχθρού... [Μια πετυχημένη διείσδυση] τοποθετεί τον επιχειρών στην καρδιά των επίβουλων προθέσεων και δράσεων... Περαιτέρω, και σημαντικότερο, καθιστά τον τελευταίο ικανό ελέγχου των ανταγωνιστικών υπολογισμών, στοχεύσεων και κινήσεων επηρεάζοντας και χειραγωγώντας το απέναντι στρατόπεδο -για μια ιδέα βλέπε Felix Christopher, *A Short Course in the Secret War*, Madison Books, Lanham / Maryland, 2001, σ. 121

⁵⁷ Bridgeman Vincent, "Defense Counterintelligence" στο *Vaults Mirrors and Masks. Rediscovering Counterintelligence*, ό. π., σ. 128-129. Επίσης, ο Ehrman στη σελίδα 7 του "Toward a Theory of CI. What are We Talking About When We Talk about Counterintelligence?", μεταφέρει έναν συνοπτικότερο ορισμό του Bridgeman κατά τον οποίο ...η αντικατασκοπία αποτελεί ευρύ υποσύνολο του πληροφοριακού πεδίου με καθήκον την παρακολούθηση των δραστηριοτήτων των ανταγωνιστικών μυστικών υπηρεσιών. Πυρήνα της αποστολής δεικνύει η αποκρυπτογράφηση της εξάρτησης του αντιπάλου από τα πληροφοριακά δίκτυα και η αξιοποίηση της συγκεκριμένης γνώσης

Jennifer Sims, τη δυσκολότερη που μια υπηρεσία Αντικατασκοπίας καλείται να εκπληρώσει. Τα καθήκοντα Α, Β, Γ, Δ είναι αντιστοίχως γνωστά ως: *Countercollection*, *Counteranticipation*, *Countertransmission* και *Counterdenial / Counterdeception*.⁵⁸ Είναι φανερό πως για μια επιτυχή έκβαση απαιτείται: α) γνώση του τρόπου σκέψης και δράσης του αντιπάλου, β) γνώση των άμεσων προτεραιοτήτων του, γ) κατάλληλη υποστήριξη σε μέσα / προσωπικό, δ) σύνδεση των αντικατασκοπευτικών σχεδιασμών με την πολιτική αναγκαιότητα.

Οι Gökhan Kuloglu, Zakir Gül και Sefika Sule Erçetin τοποθετούνται γράφοντας ότι μια υπηρεσία CI επιφορτίζεται με: α) την παρεμπόδιση διείσδυσης εχθρικών στοιχείων εντός του προστατευόμενου δικτύου πληροφοριών, β) τη διασφάλιση μη διαρροών οικείων διαβαθμισμένων πληροφοριών σε τρίτα πρόσωπα, γ) την προστασία της εγχώριας τεχνολογικής κοινότητας προς αποφυγή διασποράς hi-tech data στο εξωτερικό, δ) την αποτροπή, εν γένει, κάθε είδους κατασκοπευτικής ενέργειας εις βάρος του κράτους που υπηρετεί, ε) την αποτροπή υπονομευτικής δράσης εκ μέρους γνωστών ή αγνώστων παραγόντων, στ) την αποσόβηση ενεργειών σαμποτάζ και ζ) το μπλοκάρισμα εκδήλωσης τρομοκρατικών ή άλλων πολιτικά κινητροδοτούμενων πράξεων βίας.⁵⁹

Κατά τους ίδιους αμυντική αντικατασκοπία σημαίνει: α) δράση *φυσικής προστασίας* (*physical security*) με αναφορά στην περιφρούρηση φυσικών χώρων εντός των οποίων διαφυλάσσονται διαβαθμισμένες πληροφορίες, β) *έλεγχος προσωπικού* (*personnel security*) με σκοπό τη διασφάλιση στρατολόγησης ικανών προσώπων αλλά και το συνεχές τσεκάρισμα κατά τη διάρκεια της θητείας τους, γ) *διαβάθμιση πληροφορίας* (*information security*) με αποστολή την κατηγοριοποίησή της, δ) *προστασία τηλεπικοινωνιών* (*communications security -COMSEC*) με πλέον γνωστό περί τούτου οργανισμό την αμερικανική National Security Agency -NSA.⁶⁰

Όσον αφορά στην επιθετική αντικατασκοπία επισημαίνουν πως οι κύριες προτεραιότητες σχετίζονται με την: α) *ανίχνευση* και *εξιχνίαση* (*detection*) περιπτώσεων παραβιάσεων του κώδικα ασφαλείας διαβαθμισμένων πληροφοριών, β) *παραπληροφόρηση* (*deception*) του αντιπάλου, γ) *εξουδετέρωση / παράλυση* (*neutralization / paralysis*) των επίβουλων ενεργειών του εχθρού.⁶¹ Οι τρεις επιστήμονες ενσωματώνουν στην επιθετική αντικατασκοπία ενέργειες *detection* και *neutralization / paralysis*. Οι συγκεκριμένες δράσεις ενδέχεται να κατηγοριοποιηθούν επίσης εντός του πλαισίου της ενεργητικής άμυνας, αυτό, ωστόσο, εξαρτάται από τη θέαση του ερευνητή -οι τρεις χαρακτηρίζουν ως δράση επιθετικής αντικατασκοπίας οτιδήποτε αφορά σε εμπλοκή της οικείας Υπηρεσίας με έξωθεν πρόσωπα είτε

⁵⁸ Sims J., "Twenty-first-Century Counterintelligence. The Theoretical Basis for reform" στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, ό. π., σ. 25-36

⁵⁹ Kuloglu G., Gül Z., Erçetin S., "Counter-Intelligence as a Chaotic Phenomenon and Its Importance in National Security" στο *Chaos Theory in Politics*, επιμ. Banerjee Santo, Erçetin Sefika, Tekin Ali, Springer, 2014, σ. 183

⁶⁰ ό. π., σ. 178-183. Ο Frederick Wethering προσθέτει στα καθήκοντα της αμυντικής αντικατασκοπίας: α) την ασφάλεια πληροφοριακών συστημάτων (*computer security / infosec*), β) τα τεχνικά αντίμετρα ασφαλείας (*technical security countermeasures / TSCM*), γ) την υπό τριών κυρίως μορφών -στατική, ευέλικτη, ηλεκτρονική- παρακολούθηση (*surveillance*) -για μια εικόνα βλέπε Wethering Frederick, "Counterintelligence: The Broken Triad" στο *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 3, 2000, σ. 265-284. Για περισσότερες λεπτομέρειες επί του θέματος βλέπε Prunckun Hank, *Counterintelligence. Theory and Practice*, Rowman & Littlefield Publishers, USA, 2012, σ. 81-162 αλλά και Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, CRC Press, Florida, 2014, σ. 288-293

⁶¹ Kuloglu G., Gül Z., Erçetin S., "Counter-Intelligence as a Chaotic Phenomenon and Its Importance in National Security" στο *Chaos Theory in Politics*, ό. π., σ. 183-185 και Prunckun Hank, *Counterintelligence. Theory and Practice*, ό. π., σ. 171-206

πρόκειται για παρεμπόδιση, εξουδετέρωση, σύλληψη ή απέλαση, είτε σχετίζεται με την εκβίαση τους, εκμίσθωση ή χειραγώγησή τους κ. λ.

Οι Shulsky και Schmitt γράφουν πως αντικατασκοπία, γενικά, σημαίνει συλλογή / ανάλυση πληροφορίας και ανάληψη δράσεων με σκοπό την προστασία των οικείων πληροφοριακών σχεδιασμών και του κράτους καθ'αυτού. Υπό μίας άλλης οπτικής, η «αντικατασκοπευτική αρμοδιότητα» της Υπηρεσίας Α του κράτους Χ συμπίπτει, τουλάχιστον, με το «κατασκοπευτικό εύρος» της Υπηρεσίας Β του κράτους Ψ εάν και εφόσον κάθε αντίπαλη ύποπτη δραστηριότητα πρέπει να εκμηδενιστεί.⁶² Υπό μίας στενότερης, αντικατασκοπία ίσον αποτροπή κτήσεως πληροφοριών από αλλότριο παράγοντα προς κατοχύρωση πλεονεκτήματος όπως αυτό μπορεί να σχηματισθεί / κεφαλαιοποιηθεί στο στίβο της πολιτικής και στρατιωτικής δράσης. Οι Shulsky και Schmitt επικεντρώνουν στην αποδόμηση του μηχανισμού λήψεως πληροφοριών του ανταγωνιστή.⁶³ Αυτό δύναται να επιτευχθεί με την ενεργοποίηση τόσο παθητικών όσο και επιθετικών μέτρων. Ωστόσο, και πριν απ' όλα, οφείλουμε να διασαφηνίσουμε το είδος και τον τρόπο διαφύλαξης / κατηγοριοποίησης των ευαίσθητων δεδομένων που βρίσκονται στα χέρια μας -πρόκειται για τη διαβάθμιση της πληροφορίας, *classification of information* για τους δύο μελετητές. Δεύτερο βήμα αποτελεί ο έλεγχος του προσωπικού με άδεια κυκλοφορίας εντός των διαδρόμων των μυστικών Υπηρεσιών με το τρίτο να αναλαμβάνει τη διασφάλιση του χώρου διατήρησης χαρακτηρισμένων εγγράφων, στοιχείων, δεδομένων κ. λ.⁶⁴ Αν οι δράσεις για τις οποίες κάναμε μόλις τώρα λόγο εμπίπτουν της *διαβάθμισης της πληροφορίας* ή της *ασφάλειας της εσωτερικής περιμέτρου*, άρα, των παθητικών μέτρων, τότε, ό,τι απομένει σχετίζεται με την επιθετική τακτική μιας υπηρεσίας CI. Οι Shulsky και Schmitt δηλώνουν πως η τελευταία επιχειρεί μέσω, συνηθέστατα, διπλών πρακτόρων να ανακαλύψει τον τρόπο «με τον οποίο σκέπτεται και δρα ο αντίπαλος» προς ματαίωση / χειραγώγηση των σχεδιασμών του, ο όρος, δε, *counterespionage*, αποδίδει τον τακτικισμό.⁶⁵

⁶² Στις υποσημειώσεις τέλους και πιο συγκεκριμένα στην υποσημείωση 1 της σελίδας 214 του *Silent Warfare. Understanding the World of Intelligence* τονίζεται πως ο όρος *counterintelligence* ορισμένες φορές αφορά σε αποτροπή σαμποτάζ / δολιοφθοράς ή αποσόβηση δολοφονιών διαπραττομένων εκ μέρους ή προς όφελος ξένων δυνάμεων, οργανισμών, προσώπων ή διεθνών τρομοκρατικών ομάδων [βλέπε επίσης στο 50 USC 401a (War and National Defense, page 70) στο <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap15-sec401a.pdf> όπου καταφύγαμε τη 16^η Μαρτίου 2015]. Από τη στιγμή που τέτοιου είδους επιχειρήσεις προσομοιάζουν με ανάλογες covert action και με την προϋπόθεση πως αυτές εκτελούνται από μυστικές υπηρεσίες, τότε, μια υπηρεσία CI υποχρεούται όπως αναπτύξει σχετικές (αντι)μεθόδους

⁶³ Πιο συγκεκριμένα ο Shulsky χρησιμοποιεί τον όρο *denial* προκειμένου να αποδώσει την προσπάθεια μπλοκαρίσματος κάθε πληροφοριακής οδού μέσω της οποίας ο αντίπαλος θα μπορούσε να φτάσει σε στοιχεία που πρέπει να παραμείνουν εν κρυπτώ -για περισσότερες λεπτομέρειες ανέτρεξε στο Shulsky A., "Elements of Strategic Denial and Deception" στο *Strategic Denial and Deception*, επιμ. Godson R., Wirtz J, Transaction Publishers, New Brunswick / New Jersey, 2002, σ. 15

⁶⁴ Για όλα αυτά κατάφυγε στο Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 99-108. Στις συγκεκριμένες σελίδες περιλαμβάνεται επίσης μια συνεκτική αναφορά για την ταξινόμηση της πληροφορίας, για το πρόβλημα της υπερβολικής σπουδής διαφύλαξης αυτής (*overclassification*) αλλά και περί του αντιθέτου φαινομένου (*underclassification*)

⁶⁵ Η αξία μιας πετυχημένης χρήσης διπλών πρακτόρων καταφαίνεται μέσα από τα αποτελέσματα του σχεδίου *Double-Cross System* του οποίου κύρια κατάληξη υπήρξε η απόβαση στη Νορμανδία τον Ιούνιο του 1944. Ο John Masterman, αξιωματούχος της MI5 και οργανωτής του πλάνου, εξηγεί πως μέσω αυτού επεδιώχθη και, κατά το μάλλον ή ήττον, επετεύχθη: α) έλεγχος του γερμανικού κατασκοπευτικού συστήματος, β) σύλληψη κατασκόπων επί βρετανικού εδάφους, γ) απόκτηση ικανής εικόνας περί του τρόπου σκέψης / δράσης των γερμανικών μυστικών Υπηρεσιών, δ) απόκτηση πληροφοριών περί κωδικών και κρυπτογραφημάτων των Γερμανών, ε) αποκάλυψη των γερμανικών προθέσεων / σχεδιασμών, στ) χειραγώγηση των τελευταίων και ζ) παραπληροφόρηση του εχθρού

Οι Kalaris και McCoy σε άρθρο τους στο *International Journal of Intelligence and Counterintelligence* με τίτλο “Counterintelligence for the 1990s” καταγράφουν πλήθος ορισμών προερχομένων από διάφορους ερευνητές του πεδίου. Έτσι, σύμφωνα με τον Scott D. Breckinridge, η έννοια / αποστολή μιας υπηρεσίας Αντικατασκοπίας δεν είναι ιδιαιτέρως προσδιορίσιμη. Αυτό συμβαίνει διότι η μυστικότητα που επιβάλλεται δεν αφήνει έδαφος προσέγγισης και ευχέρεια κατασκευής ορισμών· οι όποιοι ορισμοί παραμένουν ασαφείς και σκοτεινοί εξαιρουμένων ίσως κάποιων αυτονόητων. Ο Arthur A. Zuehlke, ειδικός αναλυτής σοβιετικών θεμάτων, χαρακτηρίζει την αντικατασκοπευτική δράση ως δράση τριών επιπέδων: του *προληπτικού* (*preventive*), του *αμυντικού* (*defensive*) και του *επιθετικού* (*aggressive*) επιπέδου. Ο Norman L. Smith, υψηλόβαθμο στέλεχος της CIA, δηλώνει πως ...η αντικατασκοπία ίσως δεικνύει την πλέον απαιτητική δραστηριότητα των υπηρεσιών Πληροφόρησης. Ένας ικανός «κυνηγός πρακτόρων» πρέπει να διαθέτει φαντασία, επινοητικότητα, διορατικότητα και ικανότητα ανάλυσης των καταστάσεων.⁶⁶

Στο “Guide to the Study of Intelligence. What is Counterintelligence? A Guide to Thinking and Teaching about CI” της Michelle van Cleave αναφέρεται ότι ...[counterintelligence] is both an intelligence discipline and a national security mission με σκοπό τη σύλληψη αντιπάλων πρακτόρων όπως και την προστασία / επικουρία εγχώριων πληροφοριακών επιχειρήσεων, ομιλούμε, γράφει η van Cleave, περί «μιας διανοητικής προσπάθειας / άσκησης μαθηματικής σχεδόν πολυπλοκότητας». ⁶⁷ Ένα τμήμα / υπηρεσία CI, συνεχίζει η συγγραφέας, περιλαμβάνει τόσο τον πληροφοριακό (counterintelligence information) όσο και τον επιχειρησιακό (counterintelligence activity) βραχίονα. Ο πρώτος συλλέγει στοιχεία, ο δεύτερος ανακόπτει, αποδιοργανώνει ή χειραγωγεί τον αντίπαλο.⁶⁸

Σκοπό κάθε Υπηρεσίας αποτελεί η απόδοση τελικών στοιχείων στην ηγεσία προς εξυπηρέτηση οικείων σχεδιασμών. Η επίτευξη, ωστόσο, ενός πλάνου δεν έχει να κάνει μόνο με το τι γνωρίζουμε αλλά, επίσης, με μια προσπάθεια απόκρυψης αυτών

σχετικά με βρετανικά / συμμαχικά σχέδια και δυνητικές δράσεις -για όλα αυτά βλέπε Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 110-114

⁶⁶ Kalaris G., McCoy L., “Counterintelligence for the 1990s” στο *International Journal of Intelligence and CounterIntelligence*, Volume 2, Issue 2, 1988, σ. 179-180

⁶⁷ van Cleave, M., “Guide to the Study of Intelligence. What is Counterintelligence? A Guide to Thinking and Teaching about CI”, ό. π., σ. 58, επίσης βλέπε Felix Christopher, *A Short Course in the Secret War*, Madison Books, Lanham / Maryland, 2001, σ. 126. Παρατηρούμε ότι εντός των καθηκόντων συμπεριλαμβάνεται και η «σύλληψη αντιπάλων πρακτόρων». Πρόκειται για σημείο που πυροδοτεί συζητήσεις καθώς η συγκεκριμένη αποστολή σχετίζεται με την αστυνομική αρχή παρά με έναν πληροφοριακό οργανισμό. Όσον αφορά στις ΗΠΑ χαρακτηριστική είναι η ύπαρξη του The Office of Investigations and Counterintelligence του Department of State με ερευνητικές και ανακριτικές αρμοδιότητες που, ωστόσο, εκδιπλώνονται σε στενή συνεργασία με το FBI. Το Bureau of Diplomatic Security (επίσης του Department of State) δεικνύει διαφορετική περίπτωση, εντούτοις, καταγράφονται ομοιότητες μεταξύ των λόγων ύπαρξης των δύο θεσμών -για μια ιδέα βλέπε στην ιστοσελίδα <http://www.state.gov/m/ds/terrorism/c8653.htm> όπου καταφύγαμε τη 16^η Μαρτίου 2015. Στη JP 2-0 (σ. B-4) διαβάζουμε ότι ...[intelligence] interrogation ονομάζεται η συστηματική διαδικασία χρήσης ανακριτικών μεθόδων, από εντεταλμένα εκ του DoD πρόσωπα, με σκοπό την εκμαίευση στοιχείων / πληροφοριών από άτομα που έχουν συλληφθεί ή κρατούνται -για περισσότερες λεπτομέρειες βλέπε JP 2-0, *Joint Intelligence*, Οκτώβριος 2013, επίσης FM 2-22.3, *Human Intelligence Collector Operations*, Headquarters, Department of the Army, Washington, D.C., Σεπτέμβριος 2006 αλλά και DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, Οκτώβριος 2008

⁶⁸ van Cleave, M., “Guide to the Study of Intelligence. What is Counterintelligence? A Guide to Thinking and Teaching about CI”, ό. π., σ. 59, επίσης βλέπε Moravej K., Diaz G., “Critical Issues in Contemporary Counter-Intelligence” στο *UNISCI Discussion Papers*, Number 13, Ιανουάριος 2007, σ. 54-59

ακριβώς που ελέγχουμε. Αν η πρώτη επιδίωξη σχετίζεται με τη συλλογή / ανάλυση (υπό την έννοια της κατασκοπίας), τότε, η δεύτερη αφορά στην αντικατασκοπευτική δράση. Οι Jensen, McElreath και Graves τονίζουν ότι η τελευταία συνθέτει τμήμα της πληροφοριακής διαδικασίας εμποτίζοντας κάθε σχετικό οργανισμό επιδιώκοντας τη θωράκιση του τελευταίου έναντι εσωτερικών / εξωτερικών απειλών χωρίς να παραγνωρίζεται η επιθετική διάσταση.⁶⁹

Ο Arthur Hulnick επιβεβαιώνει ότι ένα σύγχρονο αντικατασκοπευτικό πλάνο δεν περιορίζεται στο κυνήγι των αλλοδαπών Υπηρεσιών. Οφείλει να ασχοληθεί με: α) την αντιμετώπιση ενεργειών υπονομευτικού χαρακτήρα (anti-subversion, anti-sabotage), β) την καταδίωξη της τρομοκρατίας, γ) την πάταξη του οργανωμένου εγκλήματος, δ) το κλείσιμο διαδρομών διακίνησης ναρκωτικών ουσιών, ε) το anti-trafficking -ο μελετητής σχετίζει τμήμα της αντιπληροφόρησης με τις law enforcement Υπηρεσίες.⁷⁰ Ο Hulnick δεν χρησιμοποιεί το παραδοσιακό μοτίβο της συλλογής, ανάλυσης, διασποράς και ανατροφοδότησης προκειμένου να περιγράψει τη διαδικασία. Κατ' αυτόν πέντε είναι τα επιχειρησιακά βήματα: α) αναγνώριση στόχου (identification), β) διείσδυση εντός στόχου (penetration), γ) ανάλυση / αξιοποίηση πληροφοριών (exploitation), δ) πρόληψη ή έμμεση καταστολή επίβουλων δράσεων (interdiction) - στην περίπτωση της ενεργούς καταστολής αναλαμβάνουν συνήθως οι υπηρεσίες επιβολής νόμου, ε) διακοίνωση επιτυχούς αποτελέσματος (claim success).⁷¹ Σχετικά με το πέμπτο στάδιο ο Hulnick αναφέρει ότι οι Αρχές (αποφεύγοντας να μιλήσει για υπηρεσίες Αντικατασκοπίας) συχνά αφήνουν να διαφανούν, ή και παρουσιάζουν, τα αποτελέσματα επιτυχών επιχειρήσεων. Δεν πρόκειται για κάτι συνηθισμένο στον κόσμο των Υπηρεσιών -ένα συχνά μνημονευόμενο σλόγκαν της CIA τονίζει ότι «μυστικό της επιτυχίας είναι να κρατάς μυστική την επιτυχία».⁷² Ωστόσο ο μελετητής σ' αυτό το σημείο υποστηρίζει πως μεταξύ πληροφοριακών και κατασταλτικών εγχειρημάτων υπάρχει διαφορά. Σε αντίθεση με επιτυχίες των πρώτων, κάποιες επιτυχίες των δεύτερων αποκαλύπτονται προκειμένου να αισθανθεί ο πολίτης ότι τα χρήματα που ξοδεύονται για την ασφάλειά του πιάνουν τόπο.⁷³

Αποσαφήνιση: Espionage vs Counterespionage. Υπηρεσίες Ασφαλείας και Πληροφοριών

Επειδή όροι όπως *espionage* και *counterespionage* αναφέρονται συχνά ωφελεί μια συγκριτική παρουσίαση. Espionage καλείται η δράση που σκοπεύει στην υποκλοπή πληροφοριών από τον αντίπαλο μέσω πρακτορικών τακτικισμών -ουσιαστικά αυτό καλείται να πράξει μια υπηρεσία εξωτερικών Πληροφοριών. Ωστόσο, μια τέτοια ενέργεια αν και συνδεδεμένη με την έννοια της πληροφόρησης (intelligence) συχνά διαχωρίζεται από αυτήν λόγω του 'επιθετικού', κρυφού και επικινδύνου χαρακτήρα της.⁷⁴ Ανατρέχοντας στη σελίδα 93 του *Historical Dictionary of United States Intelligence* ανακαλύπτουμε ότι espionage καλείται η δράση που εκτελείται από πρόσωπα (human intelligence action -HUMINT), ωστόσο, στη σελίδα 158 του ιδίου αναφέρεται πως ο συγκεκριμένος σχεδιασμός εξυπηρετείται επίσης από τεχνολογικά παράγωγα (χάρτες, φωτογραφίες, τηλεπισκοπήσεις κ.

⁶⁹ Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA, 2013, σ. 166-171

⁷⁰ Hulnick S. Arthur, "What's Wrong With The Intelligence Cycle?" στο *Strategic Intelligence*, Volume 2, επιμ.: Johnson Lock, USA, 2007, σ. 10-14

⁷¹ ό. π. σ. 14-15

⁷² Hulnick S. Arthur, *Fixing the Spy Machine*, Praeger Publishers, USA, 1999, σ. 81

⁷³ Hulnick S. Arthur, "What's Wrong With The Intelligence Cycle?", ό. π., σ. 15-16

⁷⁴ *Encyclopedia of Espionage, Intelligence, and Security*, volume 1, επιμ. Lerner K., Lerner B., Gale, HPIA, 2004, σ. 413

λ.)· αν επικεντρώσουμε στο HUMINT αντιλαμβανόμαστε τη σύνδεση μεταξύ espionage και επικινδυνότητας.⁷⁵ Στο Army Regulation (AR) 381-12 του DoD ως espionage περιγράφεται η κατοχή, μεταφορά, λήψη ή διασπορά πληροφοριών σχετικών με την εθνική (αμερικανική) άμυνα και ασφάλεια από άτομα που προτίθενται (ή υπάρχουν λόγοι να πιστεύεται πως προτίθενται) να βλάψουν τη χώρα ή να εξυπηρετήσουν ξένες δυνάμεις.⁷⁶ Ο William R. Johnson ήδη από το 1976 γράφει πως ...*espionage σημαίνει κλοπή πληροφοριών σε παράβαση της όποιας εθνικής νομοθεσίας από άτομο που καλείται 'πράκτορας / agent'* ... *Espionage δεν συνθέτει μια εμπιστευτική αγορά πληροφοριών ή μια βιαστική, ενδεχομένως βίαιη, πράξη που δεν συμβιβάζεται με δημοκρατικά ιδεώδη αλλά, μάλλον, μια σιωπηρή, κρυφή ενέργεια που προσπαθεί να αποφύγει κάθε βίαιη εξέλιξη υπηρετώντας, ταυτόχρονα, το έθνος.*⁷⁷ Αναφορικά με το counterespionage ο Felix στο *A Short Course in the Secret War* (2001⁴) γράφει ότι ...*[counterespionage] is a widely misunderstood branch of secret operations... CE is an offensive operation, a means of obtaining intelligence about the opposition by using -or, more usually, attempting to use- the opposition's operations. CE is a form of secret intelligence operation, but it is a form so esoteric, so complex and important as to stand by itself.* Στη Senate Report # 94-755 αναφέρεται ότι ..*counterespionage (CE) is the offensive, or aggressive, side of counterintelligence. It involves the identification of a specific adversary and a knowledge of the specific operation he is conducting. Counterespionage personnel must then attempt to counter these operations by infiltrating the hostile service (called penetration) and through various forms of manipulation. Ideally, the thrust of the hostile operation is turned back against the enemy.*⁷⁸ Τα ίδια καταγράφονται λίγο έως πολύ στη σελίδα 23 του *Words of Intelligence* του Jan Goldman⁷⁹ επί τη βάση των FM 1-02, της EO 12333 και της DoD Instruction 5240.16.⁸⁰ Στις σελίδες 1-3 του *Thwarting Enemies at Home and Abroad. How to Be a Counterintelligence Officer* του William Johnson σημειώνεται η τάση ταύτισης της έννοιας «αντικατασκοπία / counterintelligence» με την έννοια «ασφάλεια / security» όπως και με την αντίστοιχη του «counterespionage». Αλλά η δεύτερη είναι μόνο ένα κομμάτι της πρώτης, το αμυντικό. Το άλλο κομμάτι, το επιθετικό, καλείται counterespionage (CE). Το counterespionage, συνεχίζει ο Johnson, δεικνύει τον απώτερο στόχο του counterintelligence ήγουν, τη χειραγωγήση, την παραπληροφόρηση αλλά και την κλοπή μυστικών μέσα από τις ίδιες τις Υπηρεσίες του αντιπάλου -όταν εκμαιεύουμε ένα μυστικό από μια, π. χ., πολιτική υπηρεσία προβαίνουμε σε espionage, όταν παρεισδύουμε σε μια υπηρεσία Πληροφοριών προβαίνουμε σε counterespionage.⁸¹ Ουσιαστικά counterespionage σημαίνει κατασκοπία του αντίπαλου κατασκόπου. Ο Johnson γράφει: «counterespionage δεν είναι άλλο από κλοπή πληροφοριών μέσω πράκτορα (συνήθως καλείται διπλός πράκτορας) που έχει διεισδύσει στον αντίπαλο πληροφοριακό μηχανισμό». ⁸² Τέλος, ο Ehrman αναφερόμενος στο counterespionage κάνει λόγο κυρίως για «κυνήγι του αντιπάλου κατασκόπου», ίσως, τονίζουμε, σ' αυτή την περίπτωση δυνάμεθα να ομιλήσουμε και για 'ενεργητική άμυνα' ή για

⁷⁵ Turner M., *Historical Dictionary of United States Intelligence*, ό. π., σ. 93, 158. Σε ότι αφορά στους ανθρώπινους πόρους προσθέτουμε πως στο χώρο των αμερικανικών αστυνομικών αρχών προτιμάται η χρήση του ακρωνυμίου CHIS (Covert Human Intelligence Source) παρά του όρου «πράκτορας / agent» -για μια πληρέστερη άποψη βλέπε West N., *Historical Dictionary of British Intelligence*, ό. π., σ. 118.

⁷⁶ AR 381-12, *Subversion and Espionage Directed Against the US Army*, DoD, 15 Ιανουαρίου 1993, διαθέσιμο στην ιστοσελίδα http://www.soft-vision.com/ao_vets/pdf/sub_esp_against%20USArmy.pdf όπου καταφύγαμε την 9^η Μαΐου 2016

⁷⁷ Johnson R. W., "Clandestinity and Current Intelligence" ό. π., σ. 25

⁷⁸ *Terms & Definitions of Interest for DoD Counterintelligence Professionals*, ό. π., σ. 31

⁷⁹ Goldman Jan, *Words of Intelligence*, ό. π., σ. 23

⁸⁰ FM 1-02, *Operational Terms and Graphics*, Department of the Army, Marine Corps Combat Development Command. Department of the Navy, Washington, D.C., 21 Σεπτεμβρίου 2004, *Executive Order 12333* και DoD Instruction 5240-16, *Counterintelligence Functional Services*, US DoD, 27 Αυγούστου 2012

⁸¹ Johnson William, *Thwarting Enemies at Home and Abroad. How to Be a Counterintelligence Officer*, ό. π., σ. 1-3

⁸² Johnson R. W., "Clandestinity and Current Intelligence", ό. π., σ. 25-26

‘αμυντικό counterespionage’. Ο ίδιος σημειώνει πως πρόκειται για εξαιρετικά δύσκολη αποστολή που ενδέχεται να μην τελεσφορήσει πριν την πάροδο ετών (οι υποθέσεις Ames και Hanssen το αποδεικνύουν) έχοντας στο μεταξύ δεσμεύσει σημαντικό όγκο έμψυχων και άψυχων πόρων. Πάρα ταύτα η κατάληξη του εγχειρήματος (σύλληψη και ομολογία, παγίδευση και συνεργασία του υπόπτου κ. λ.) εμπλουτίζει τη μεθοδολογία αντιμετώπισης περιστατικών espionage.⁸³

Παρατηρούμε πως τα διάφορα λεξικά, εγκυκλοπαίδειες, εγχειρίδια και συγγραφικά σχετικά έργα αλληλεπικαλύπτονται ή αν διαφοροποιούνται αυτό συμβαίνει χωρίς να επηρεάζεται κάτι ουσιαστικά. Ο Nigel West, υπό ευρείας οπτικής, αποδίδει το counterespionage στις υπηρεσίες Ασφαλείας. Οι Lerner και Lerner όπως και ο Turner αποδίδουν το espionage στις υπηρεσίες εξωτερικών Πληροφοριών. Ο πρώην διοικητής της ΕΥΠ Παύλος Αποστολίδης κάνει σαφές πως οι υπηρεσίες Ασφαλείας καλούνται να προστατεύσουν τον εσωτερικό χώρο τονίζοντας πως εντός των καθηκόντων συγκαταλέγονται αποστολές αντικατασκοπίας, αντιδολιοφθοράς, αντιπροπαγάνδας και αντιανατρεπτικών σχεδιασμών, συνεπώς, η αντικατασκοπία εμπίπτει του πεδίου των υπηρεσιών Ασφαλείας χωρίς όμως να γίνεται περαιτέρω λόγος για αμυντική ή επιθετική έκφανση. Άλλοι μελετητές, υπό μία στενότερη οπτική, διατείνονται πως οι υπηρεσίες Ασφαλείας, ουσιαστικά law enforcement, πρέπει να περιορίζονται στην καταδίωξη εγκλημάτων των οποίων η τέλεση ενδέχεται να επηρεάσει την εσωτερική σταθερότητα. Τι σημαίνει όμως αυτό; Μήπως σε κάποια εγκλήματα εμπλέκονται άτομα που βρίσκονται στις παρυφές ή εντός τρομοκρατικών οργανώσεων με συνδέσμους ακόμα και στο εξωτερικό; Μια υπηρεσία Αντιτρομοκρατίας δύναται να ενταχθεί τόσο στο law enforcement όσο και στο (counter)intelligence; Μία απάντηση που μπορεί να δοθεί, έστω με διάθεση ομογενοποίησης, είναι ότι όλες οι Υπηρεσίες λειτουργούν διά της χρήσης και αξιοποίησης της πληροφορίας χωρίς κάποια ακλόνητα στεγανά να απομονώνουν, τουλάχιστον, κάποιες από αυτές.⁸⁴

Ο Dave Szady, ανώτατο στέλεχος του Bureau, δηλώνει ότι το πεδίο της αντικατασκοπίας «είναι πολύ ευρύτερο από αυτό της κατασκοπίας (espionage). Το counterintelligence αφορά στην προστασία της υψηλής τεχνολογίας, της οπλικής και στρατιωτικής ικανότητας, των διαβαθμισμένων πληροφοριών και άλλων στρατηγικής σημασίας για την εθνική ευμάρεια συστημάτων. Επίσης αφορά στην προστασία εμπορικών / οικονομικών μυστικών όπως και στην αποτροπή επιχειρήσεων ή εκστρατειών παραπληροφόρησης που θα μπορούσαν να βλάψουν τις ΗΠΑ».⁸⁵

Τέλος, δεν μπορούμε να μην σταθούμε στον Νικόλαο Ο. Αρχιμανδρίτη, γενικό διευθυντή της πάλαι ποτέ ελληνικής Αστυνομίας Πόλεων, και στο πρωτοποριακό του πολυσέλιδο έργο, μοναδικό στα ελληνικά χρονικά, *Ψυχολογικός Πόλεμος. Κατασκοπεία. Αντικατασκοπεία* (1960). Στο συγκεκριμένο, η αντικατασκοπία περιγράφεται ως ...*οργανωμένη αντιμετώπιση από το κράτος και στο εσωτερικό της χώρας και στις ξένες χώρες, προληπτικώς και κατασταλτικώς, των ενεργειών των*

⁸³ Ehrman John, “Toward a Theory of CI. What are We Talking About When We Talk about Counterintelligence?” στο *Studies in Intelligence*, ό. π., σ. 16-17

⁸⁴ Μία ολιγοσέλιδη μελέτη περί των Υπηρεσιών εκπονήθηκε το 2007 από τον πρώην Διοικητή της ΕΥΠ Παύλο Αποστολίδη υπό την αιγίδα του ΕΛΙΑΜΕΠ με τίτλο *Οι Υπηρεσίες Πληροφοριών στο Εθνικό Σύστημα Ασφαλείας. Η περίπτωση της ΕΥΠ*. Ο προσεκτικός αναγνώστης θα διαγνώσει πως κάτω από την «ομπρέλα της πληροφόρησης» βρίσκουν θέση τόσο οι υπηρεσίες Ασφαλείας όσο και αυτές της Κατασκοπίας / Αντικατασκοπίας. Κάτι τέτοιο δεν είναι τυχαίο καταδεικνύοντας τη συγγένεια των συγκεκριμένων Υπηρεσιών εντός ενός συστήματος συγκοινωνούντων δοχείων -για περισσότερες πληροφορίες βλέπε Αποστολίδης Παύλος, «Οι Υπηρεσίες Πληροφοριών στο Εθνικό Σύστημα Ασφαλείας. Η περίπτωση της ΕΥΠ» στη διαδικτυακή τοποθεσία http://www.eliamep.gr/wp-content/uploads/2008/07/apostolidies_eyp_gr.pdf όπου ανατρέξαμε τη 17^η Απριλίου 2016

⁸⁵ “Focus on Counterintelligence”, συνέντευξη με τον βοηθό διευθυντή του FBI Dave Szady, 20 Ιουλίου 2004, διαθέσιμη στο <https://archives.fbi.gov/archives/news/stories/2004/july/szady072004> εις το οποίο καταφύγαμε την 16^η Σεπτεμβρίου 2016

κατασκοπευτικών υπηρεσιών των αντίπαλων κρατών.⁸⁶ Ο ίδιος συνεχίζει τονίζοντας ότι οι υπηρεσίες κατασκοπίας και αντικατασκοπίας κάθε κράτους αποτελούν τμήματα των υπηρεσιών Πληροφοριών του κράτους τούτου ...και συνεργάζονται πάρα πολύ, τόσο μάλιστα, ώστε πολλές φορές να μην μπορεί κανείς να ξεχωρίσει αν μια ενέργεια που αφορά ξένη χώρα, αποτελεί κατασκοπεία εις βάρος της χώρας αυτής ή αντικατασκοπεία με σκοπό την πρόληψη ή εξουδετέρωση της κατασκοπείας που ενεργεί αυτή.⁸⁷ Συμπληρωματικά, αλλού αναφέρει πως ...κάθε κράτος πρέπει να έχει άριστα οργανωμένες τις υπηρεσίες κατασκοπείας κυρίως για τις ξένες εχθρικές χώρες, της αντικατασκοπείας δε κυρίως για το εσωτερικό της χώρας. Μπορεί όμως να υπάρχουν επιδιώξεις της κατασκοπείας μιας χώρας που θα πρέπει να πραγματοποιηθούν μέσα σ' αυτή την ίδια τη χώρα (π. χ. κλοπή μυστικών από μια ξένη πρεσβεία αντίπαλου κράτους), καθώς και επιδιώξεις της αντικατασκοπείας που θα πρέπει να πραγματοποιηθούν σε ξένη χώρα (π. χ. η αντικατασκοπεία μιας χώρας στέλνει όργανά της στην πρεσβεία της που λειτουργεί σε αντίπαλη χώρα για να ματαιώσει τις ενέργειες της ξένης κατασκοπείας εις βάρος της πρεσβείας αυτής).⁸⁸

Θεσμοί και Αντικατασκοπία

Ήδη από το 1947 το αμερικανικό Κογκρέσο πιστοποιεί ότι ο όρος «αντιπληροφόρηση» σχετίζεται ...με συλλογή πληροφοριών και διεξαγωγή επιχειρήσεων με σκοπό την προστασία έναντι κατασκοπευτικών ή / και άλλων πληροφοριακών σχεδιασμών, υπονομευτικών προθέσεων ή πλάνων πολιτικών δολοφονιών εκτελουμένων από ή στο όνομα ξένων κυβερνήσεων, οργανισμών, προσώπων, διεθνών τρομοκρατικών δικτύων⁸⁹ -πρόκειται για ορισμό που αν και δεν κάμει λόγο για ζητήματα εσωτερικής τρομοκρατίας ή οργανωμένου εγκλήματος παραμένει χρηστικός.⁹⁰

Περί τα μέσα της δεκαετίας του 1950 η U.S. Senate's Church Committee προβαίνει σε έναν ορισμό σύμφωνα με τον οποίο μια υπηρεσία CI αποτελεί οργανισμό του οποίου η δράση σκοπεύει στην αναγνώριση / καταστολή εχθρικών κινήσεων τελουμένων υπό ξένων Υπηρεσιών. Η προστασία της αμερικανικής κυβέρνησης από ενέργειες αλλοδαπών πρακτόρων όπως και ο έλεγχος / χειραγώγηση των τελευταίων δεικνύει μια ακόμα υποχρέωση ενός ικανού αντικατασκοπευτικού ιστού.⁹¹

Η National Security Council Intelligence Directive No. 5 (NSCID No 5), *U.S. Espionage and Counterintelligence Activities Abroad* του 1958 ορίζει την αντικατασκοπία ως δραστηριότητα με σκοπό: α) την καταστροφή των επίβουλων ξένων πληροφοριακών επιχειρήσεων, β) την προστασία και ασφάλεια του έθνους έναντι κατασκοπευτικών ενεργειών, δολιοφθορών και υπονόμευσης, γ) τη διασπορά πληροφόρησης σε αρμοδίους φορείς περίξ εχθρικών μυστικών ενεργειών και δ) τη διείσδυση εντός ομάδων ή οργανώσεων ικανών προς τέτοια δράση.⁹²

⁸⁶ Αρχιμανδρίτης Νικόλαος, *Ψυχολογικός Πόλεμος. Κατασκοπεία. Αντικατασκοπεία*, Αθήνα, 1960, σ. 555

⁸⁷ *ibid*

⁸⁸ Αρχιμανδρίτης Νικόλαος, *Ψυχολογικός Πόλεμος. Κατασκοπεία. Αντικατασκοπεία*, ό. π. σ. 559

⁸⁹ United States Congress, *National Security Act of 1947*, 1947, σ. 6, διαθέσιμο στην ιστοσελίδα <https://www.ncsc.gov/training/resources/nsaact1947.pdf> όπου ανατρέξαμε την 3^η Αυγούστου 2015

⁹⁰ Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, ό. π., σ. 166

⁹¹ Kalaris G., McCoy L., "Counterintelligence for the 1990s" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 182

⁹² NSCID No 5, *U.S. Espionage and Counterintelligence Activities Abroad*, Απρίλιος 1958, σ. 1

Στη Senate Report # 94-755 διαβάζουμε πως CI σημαίνει πληροφοριακή δραστηριότητα διακριτή από άλλες ανάλογες. Σκοπό αποτελεί η αναγνώριση / εξουδετέρωση των εχθρικών πληροφοριακών δράσεων, επίσης, η προστασία του (αμερικανικού) έθνους, των πολιτών, θεσμών και υποδομών έναντι απειλών κατασκοπίας, δολιοφθοράς κ. λ. εντός και εκτός επικρατείας. Ουσιαστικά οι άνθρωποι της αντικατασκοπίας βρίσκονται σε διαρκή πόλεμο με τις ανταγωνιστικές Υπηρεσίες' «εν τη απουσία ενός αποτελεσματικού αντιπληροφοριακού σχεδιασμού», σημειώνει Αμερικανός ειδικός, «οι εχθροί μας δύναται να λειτουργούν εντός ενός ευνοϊκού γι' αυτούς περιβάλλοντος». Στο ίδιο έγγραφο, και παραπέμποντας στις σελίδες 48-49 του *Report of the Commission on Government Security* του 1957, σημειώνεται ότι ...[CI] δύναται επίσης να σημαίνει απαιτητή γνώση προκειμένου να προστατευθεί / διατηρηθεί η στρατιωτική, οικονομική και παραγωγική ισχύς των ΗΠΑ, να διασφαλιστεί η κυβέρνηση έναντι κατασκοπευτικών, υπονομευτικών ή άλλων μυστικών δράσεων των οποίων απώτερο σκοπό αποτελεί η τρώση ή η καταστροφή των *Ηνωμένων Πολιτειών*.⁹³ Περαιτέρω, η έννοια counterintelligence, στα πρότυπα της έννοιας intelligence, εκλαμβάνεται ως: α) προϊόν / product, βλέπε πληροφόρηση περίξ του «εχθρού», β) δραστηριότητα / activity, βλέπε αμυντική (security) / επιθετική (counterespionage), γ) οργανισμός / organization, βλέπε π. χ. CIA, FBI κ. λ.⁹⁴ -τονίζουμε ότι στο “Counterintelligence for National Security” του *Studies in Intelligence* το «προϊόν / product» αντικαθίσταται από τη «γνώση / knowledge».⁹⁵ Σχετικά με τις έννοιες «counterespionage», «countersabotage», «countersubversion», η Senate Report # 94-755 ορίζει πως: α) counterespionage σημαίνει επιθετική δράση με σκοπό την απομείωση των επιχειρησιακών δυνατοτήτων των αλλότριων πληροφοριακών οργανισμών όπως και την ανίχνευση / εξουδετέρωση της αλλοδαπής κατασκοπευτικής δραστηριότητας. Η διείσδυση εντός εχθρικών ομάδων, οργανισμών κ. λ., η χειραγώγηση / παραπληροφόρηση αυτών δεικνύουν πρακτικές του counterespionage, β) countersabotage σημαίνει δράση με σκοπό την αποκάλυψη και εξουδετέρωση σχεδιασμών δολιοφθοράς. Η διείσδυση εντός υπόπτων σχηματισμών, η χειραγώγηση τους, η παραπληροφόρηση τους δεικνύουν επίσης πρακτικές του countersabotage, γ) countersubversion σημαίνει δράση με σκοπό την εξουδετέρωση ανατρεπτικών / υπονομευτικών ενεργειών. Οι πρακτικές που εξυπηρετούν το countersubversion είναι όμοιες με τις άνω αναφερθέντες. Και οι τρεις counter-δράσεις ανήκουν στο πεδίο του counterintelligence.⁹⁶

Το DoD στην 5240.02 Directive της 17^{ης} Μαρτίου 2015 τονίζει ότι δραστηριότητες CI εκτελούνται προς ανίχνευση, αναγνώριση, εκτίμηση, αντιμετώπιση / εξουδετέρωση σχεδιασμών κατασκοπίας, σαμποτάζ, εξεγέρσεων, υπονομεύσεων, πολιτικών δολοφονιών, τρομοκρατικών κτυπημάτων εκπορευομένων από ή στο όνομα ξένων δυνάμεων, οργανισμών, προσώπων κ. λ. ήτοι, με σκοπό την προάσπιση της αμερικανικής εθνικής ασφαλείας / συμφέροντος ή, εναλλακτικά, της ασφαλείας / συμφέροντος του DoD (προσωπικού, πληροφοριών, εγκαταστάσεων, projects). Ειδικότερα προβλέπεται: α) αντιμετώπιση της κατασκοπίας, της διεθνούς τρομοκρατίας και των εσωτερικών, εντός του DoD και των περίξ αυτού οργανισμών,

⁹³ Senate Report # 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, US Government Printing Office, Washington, D.C., Απρίλιος 1976, σ. 163, επίσης, *Report of the Commission on Government Security*, US Government Printing Office, Washington, D.C., 1957, σ. 48-49

⁹⁴ Senate Report # 94-755, ό. π., σ. 165-166, 169-171

⁹⁵ “Counterintelligence for National Security” στο *Studies in Intelligence*, Volume 2, Number 4, διαθέσιμο στην ιστοσελίδα https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm εις την οποία καταφύγαμε την 3^η Σεπτέμβρη 2016

⁹⁶ Senate Report # 94-755, ό. π., σ. 620

απειλών, β) υποστήριξη του πλέγματος προστασίας των ενόπλων δυνάμεων και ευρύτερα των πόρων του DoD, γ) επικουρία στην προστασία υποδομών που αφορούν σε δυνητικές στρατιωτικές επιχειρήσεις⁹⁷, δ) επικουρία στην προστασία ερευνητικών / αναπτυξιακών προγραμμάτων όπως και στη διαφύλαξη των προϊόντων τους.⁹⁸

Το Office of Intelligence and Analysis (OIA) του αμερικανικού Department of Homeland Security (DHS) βεβαιώνει ότι η σχετική με απειλές εσωτερικής ασφαλείας πληροφόρηση συλλέγεται, αναλύεται και διασπείρεται κατά τας ανάγκες στο σύνολο των συνδεδεμένων με το DHS επιτελικών, στον ιδιωτικό επιχειρηματικό τομέα όπως και εντός της υπόλοιπης πληροφοριακής κοινότητας. Κατά το Office πέντε είναι οι κύριες απειλές, ειδικότερα: α) η απειλή που προέρχεται από παραβίαση χερσαίων, θαλασσίων, εναερίων και εικονικών (virtual) συνόρων με τον παραβάτη να υποστασιοποιείται από κρατικές και μη κρατικές οντότητες, β) η απειλή που προέρχεται από τη ριζοσπαστικοποίηση και τον εξτρεμισμό, γ) η απειλή που προέρχεται από ομάδες ή άτομα που εισέρχονται στις Ηνωμένες Πολιτείες με αδιευκρίνιστες προθέσεις, δ) η απειλή που αφορά σε σαμποτάρισμα κρισίμων κρατικών υποδομών ή σε υπονόμηση / καταστροφή εθνικών πόρων, ε) η απειλή που προέρχεται από τη διασπορά όπλων μαζικής καταστροφής όπως και από τη διασπορά επιβαρυντικών για την ανθρώπινη υγεία στοιχείων.⁹⁹

Domestic Intelligence / Homeland Security Intelligence

Η έννοια «domestic intelligence» εμφανίζεται στις ΗΠΑ μετά το κτύπημα της 11^{ης} Σεπτεμβρίου. Αποτέλεσμα αυτού του κτυπήματος υπήρξε η δημιουργία του U.S. Department of Homeland Security (DHS). Ο Bruce Berkowitz γράφει ότι η εσωτερική πληροφόρηση, αντικείμενο του DHS, σκοπό έχει να εφοδιάσει κρατικούς αξιωματούχους, αρχές και, αν κριθεί απαραίτητο, το ευρύ κοινό με την καλύτερη δυνατή γνώση περί δυνητικών απειλών που επιβουλεύονται τη χώρα. Διαφέρει τόσο από την εξωτερική πληροφόρηση που ασχολείται με το εκτός των συνόρων περιβάλλον όσο και από το law enforcement που επικεντρώνει στη σύλληψη προσώπων και, ενδεχομένως, στην αποτροπή νέων εγκλημάτων.¹⁰⁰ Κατά τον μελετητή η εσωτερική πληροφόρηση πληρώνει το (πληροφοριακό) κενό μεταξύ των δύο αναφερομένων πεδίων, ένα κενό που παρατηρήθηκε με την τραγωδία των Δίδυμων Πύργων· πρακτικά ο Berkowitz μιλά για αποτροπή τρομοκρατικών ενεργειών.

Ο Gregory Treverton, παρά το γεγονός της μνημόνευσης των Todd Masse και David Heyman που επισημαίνουν την υπαρκτή ασυμφωνία ως προς τον ορισμό του domestic intelligence και τον προβληματισμό που αυτό επιφέρει σε επιχειρησιακό επίπεδο, προσδιορίζει το έργο της εσωτερικής πληροφόρησης ως ...*προσπάθεια κυβερνητικών οργάνων να συλλέξουν, αξιολογήσουν και αξιοποιήσουν πληροφορίες που: α) αναφέρονται σε πρόσωπα / οργανισμούς εντός των Ηνωμένων Πολιτειών ή πρόσωπα / οργανισμούς που*

⁹⁷ Αναφερόμαστε στο Defense Critical Infrastructure Program (DCIP) -για μια άποψη βλέπε DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, Αύγουστος 2007, επίσης ανέτρεξε στη δικτυακή τοποθεσία <http://www.prim.osd.mil/init/dcipcadat.html> στην οποία καταφύγαμε την 25^η Ιουνίου 2015

⁹⁸ DoDD 5240.02, *Counterintelligence*, Μάρτιος 2015. Στο ίδιο paper καταγράφονται νομοθετήματα και οδηγίες επί τη βάση των οποίων ασκείται, τουλάχιστον όσον αφορά στο DoD, η CI λειτουργία (EO 12333, DoDD 5240.01, DoD 5240.1-R, DoDD 5400.11, DoDI 1000.29, DoDI 1100.22 κ. λ.) εντός και εκτός επικρατείας, τονίζεται, δε, η εμπλοκή του πεδίου σε κάθε είδος επιχειρήσεων, προγραμμάτων, σχεδιασμών, ασκήσεων, δογμάτων, στρατηγικών, πολιτικών και πληροφοριακών αρχιτεκτονικών εκπορευομένων εκ του Office of Secretary of Defense (OSD)

⁹⁹ Collins A. Pamela, Baggett K. Ryan, "Private Security Intelligence and Homeland Security" στο *Homeland Security and Intelligence*, επιμ. Logan G. Keith, Praeger, California, 2010, σ. 136-137

¹⁰⁰ Berkowitz Bruce, "Homeland Security Intelligence: Rationale, Requirements, and Current Status" στο *Analyzing Intelligence. Origins, Obstacles, and Innovations*, επιμ. George Roger, Bruce James, Georgetown University Press, Washington, D.C., 2008, σ. 281

σχετίζονται με την αμερικανική πολιτεία και βρίσκονται στο εξωτερικό και β) δεν συνδέονται [οι πληροφορίες] απαραίτητα με έρευνες γύρω από καταγεγραμμένες εγκληματικές πράξεις. Ο συγγραφέας τονίζει πως ο όρος «πληροφόρηση / intelligence» απαντάται όλο και συχνότερα εντός των υπηρεσιών law enforcement ως «intelligence-led policing». Αν και οι ορισμοί του intelligence-led policing ποικίλουν, η συλλογή, ανάλυση και εργαλειοποίηση της πληροφορίας αποτελεί κοινό τόπο και μάλιστα όχι μόνον προς διαλεύκανση εγκλημάτων αλλά και προς αποσόβηση έκνομων δραστηριοτήτων ¹⁰¹ -κύριο μέλημα του Treverton δεικνύει η πάταξη της τρομοκρατίας και των συνδεδεμένων μ' αυτήν εγκληματικών δικτύων.

Το ίδιο ισχύει λίγο έως πολύ και για τον Richard Posner. Κατ' αυτόν, το domestic intelligence (ή domestic national security intelligence) αφορά στην πληροφόρηση περί απειλών εθνικής ασφαλείας, βίαιων πολιτικώς κινητροδοτούμενων δραστηριοτήτων εντός των ΗΠΑ και στην αντιμετώπισή τους. Οι συγκεκριμένοι κίνδυνοι δύναται να εκπορεύονται από εσωτερικά ή εξωτερικά τρομοκρατικά δίκτυα όπως επίσης από κατασκόπους ή δολιοφθορές ξένων δυνάμεων.¹⁰²

Σ' αυτό ακριβώς το σημείο τονίζουμε ότι αν η τρομοκρατία συνήθιζε να πονοκεφαλιάζει τις κρατικές υπηρεσίες Ασφαλείας, τα πράγματα έχουν αλλάξει. Μια τρομοκρατική ενέργεια ενδέχεται να εκπορεύεται από εξωτερικούς κρατικούς ή μη κρατικούς παράγοντες, άρα, η εμπλοκή της αντικατασκοπίας στο ζήτημα καθίσταται μάλλον απαραίτητη. Επιπλέον, μια τρομοκρατική τοπική ή διεθνής οργάνωση δύναται να συνδέεται με το τοπικό ή διεθνές οργανωμένο έγκλημα, συνεπώς, η παρουσία του law enforcement στην αντιμετώπιση του φαινομένου κρίνεται επίσης ουσιαστική.

Το National Counterintelligence Executive τονίζει, διά μέσου του *The National Counterintelligence Strategy of the United States of America* (2009), ότι η αμερικανική αντικατασκοπευτική κοινότητα συνενώνοντας επιμέρους στοιχεία / υπηρεσίες και δράοντας ως σύνολο οφείλει να ανταποκριθεί στις προτεραιότητες: α) της προστασίας του έθνους έναντι αλλότριων κατασκοπευτικών απειλών και απειλών ηλεκτρονικής διείσδυσης, β) της προάσπισης της ακεραιότητας του πληροφοριακού συστήματος, γ) της υποστήριξης εθνικών πολιτικών και αποφάσεων, δ) της προστασίας της αμερικανικής οικονομίας, των συνδεδεμένων μ' αυτήν εμπορικών μυστικών, της ημεδαπής σχετικής τεχνογνωσίας κ. λ., ε) της κάλυψης των αμερικανικών ενόπλων δυνάμεων, στ) της βελτίωσης της εκπαίδευσης και της επιμόρφωσης του εντεταλμένου CI προσωπικού, ζ) της προώθησης ενός διαλόγου με ιδιωτικούς και ακαδημαϊκούς φορείς περί κινδύνων κλοπής πληροφοριών μέσω ηλεκτρονικών και (δια)δικτυακών εργαλείων, πληροφοριών που κατά βάσει αφορούν στην αμερικανική επιχειρηματικότητα, στην τεχνολογία αιχμής, σε ερευνητικά και αναπτυξιακά επιστημονικά προγράμματα κ. λ.¹⁰³

¹⁰¹ Treverton Gregory, *Reorganizing U.S. Domestic Intelligence. Assessing the Options*, RAND Corporation, Santa Monica, 2008, σ. 15-16, επίσης βλέπε *The Challenge of Domestic Intelligence in a Free Society. A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, επιμ. Jackson A. Brian, RAND, Santa Monica, 2009, σ. 3-4. Στον ίδιο τόμο συναντάμε ως κομμάτι του domestic intelligence το λεγόμενο domestic counterterrorism intelligence με ξεκάθαρη αναφορά στην πάταξη της τρομοκρατίας. Ουσιαστικά όταν ομιλούμε για εσωτερική πληροφόρηση, domestic intelligence ή homeland security intelligence ομιλούμε για μια σύνθεση CI και law enforcement υπηρεσιών

¹⁰² Posner A. Richard, *Remaking Domestic Intelligence*, Hoover Institution Press Publication, USA, 2005, σ. 1

¹⁰³ *The National Counterintelligence Strategy of the United States of America*, Office of the National Counterintelligence Executive (NCIX-2010-002), 2009. Το έγγραφο του 2009 έρχεται να συμπληρώσει το αντίστοιχο του 2005 κατά το οποίο η αμερικανική αντικατασκοπία εντέλλεται όπως: α) συνεισφέρει στον πόλεμο κατά της παγκόσμιας τρομοκρατίας, β) προβεί σε προληπτικές *proactive* δράσεις αλλάζοντας το παλαιότερο *reactive* δόγμα, γ) προστατεύσει τις ευαίσθητες τεχνολογίες ασφαλείας, δ) προασπίσει την ολοκλήρωση των οικείων πληροφοριακών επιχειρήσεων, ε) εμποδίσει την εκτέλεση

Στα εισαγωγικά μέρη του *The National Counterintelligence Strategy of the United States* του 2005 διαβάζουμε ότι μια αλλοδαπή υπηρεσία Πληροφοριών στοχεύει: α) στη συλλογή / αποκάλυψη κρίσιμων στοιχείων εθνικής σπουδαιότητας μέσω διείσδυσης εντός των αμερικανικών Υπηρεσιών, β) στη χειραγώγηση γεγονότων και στη διαστρέβλωση της πραγματικότητας προς παγίδευση της αμερικανικής ηγεσίας μέσω τακτικισμών παραπληροφόρησης και κεκαλυμμένων επιχειρήσεων, γ) στην αναγνώριση, αποδιοργάνωση ή καταστροφή των αμερικανικών στοχεύσεων περιλαμβανομένης της συλλογής δεδομένων, της εκτέλεσης ευαίσθητων εγχειρημάτων πληροφοριακού, στρατιωτικού ή διπλωματικού ενδιαφέροντος και δ) στην απόκτηση αμερικανικών τεχνολογιών ικανών να συνεισφέρουν στις οικείες στρατιωτικές και οικονομικές εξελίξεις. Η αμερικανική στρατηγική αντικατασκοπίας προκειμένου να απαντήσει στις συγκεκριμένες προκλήσεις σχεδιάζει / επιχειρεί την: α) αναγνώριση, εκτίμηση, εξουδετέρωση ή χειραγώγηση των πληροφοριακών δραστηριοτήτων ξένων δυνάμεων, τρομοκρατικών γκρουπ, διεθνών εγκληματικών οργανώσεων κ. λ., β) προστασία πληροφοριακών και αναλυτικών δυνατοτήτων με σκοπό την αποτροπή εχθρικής διείσδυσης, χειραγώγησης κ. λ., γ) επιβολή ευαίσθητων επιχειρήσεων εθνικής σημασίας, δ) διαφύλαξη στοιχείων που σχετίζονται με την ασφάλεια της χώρας, των κρίσιμων εθνικών υποδομών και των τεχνολογιών αιχμής. Η επιχειρησιακή επίτευξη του όλου πλάνου απαιτεί την εμπλοκή των αντικατασκοπευτικών assets ήτοι, του counterespionage, της αντιπαραπλάνησης, εν γένει, των επιθετικών τακτικών¹⁰⁴, ασφαλώς, των αμυντικών πρακτικών ασφαλείας.

Ανατρέχοντας στις εισαγωγικές σελίδες των *The National Counterintelligence Strategy of the United States of America* των 2007 και 2008 επιβεβαιώνουμε τον περί αντικατασκοπίας ορισμό όπως αυτός δίδεται στην EO 12333, ανακαλύπτουμε τα νομοθετήματα εκ των οποίων αντλεί αρμοδιότητες η αμερικανική κοινότητα CI, το φάσμα δραστηριοτήτων της τελευταίας και τον σημαίνων ρόλο του The National Counterintelligence Policy Board.¹⁰⁵ Σημειώνουμε, δε, ότι ο περί αντικατασκοπίας ορισμός που ανευρίσκεται στο *Fundamental Elements of the Counterintelligence Discipline* (2006) αποτελεί ουσιαστικά μεταφορά από την EO 12333.¹⁰⁶

Στη σελίδα iii του *The National Counterintelligence Strategy of the United States of America* του 2009 καταγράφονται οι σκέψεις / επιδιώξεις του Dennis C. Blair, Διευθυντού της αμερικανικής Πληροφοριακής Κοινότητας -Director of National Intelligence (DNI). Σύμφωνα μ' αυτές η εθνική αντικατασκοπευτική στρατηγική -αποτελώντας τμήμα της ευρύτερης πληροφοριακής στρατηγικής- οφείλει όπως συνεισφέρει στο κτίσιμο ικανών πολιτικών ασφαλείας χρησιμοποιώντας τόσο αμυντικές όσο και επιθετικές τακτικές. Στις σελίδες v και vi του ιδίου, ο Robert M. Bryant, Διευθυντής του Office of the National Counterintelligence Executive, συνεπικουρεί τον Blair δηλώνοντας πως μια εθνική πληροφοριακή /

επίβουλων αλλότριων πληροφοριακών σχεδιασμών / επιχειρήσεων, στ) εποπτεύσει το οικονομικό παίγνιο με σκοπό την προστασία της εγχώριας βιομηχανίας από ανάλογα κατασκοπευτικά πλάνα αλλοδαπών δυνάμεων, ζ) συνεισφέρει στην επιτυχία εθνικών πλάνων ασφαλείας, στρατιωτικών σχεδιασμών και δράσεων που άπτονται του διεθνούς πολιτικού στίβου -περί τούτων βλέπε στο *The National Counterintelligence Strategy of the United States*, Office of the National Counterintelligence Executive, Μάρτιος 2005

¹⁰⁴ *The National Counterintelligence Strategy of the United States*, Office of the National Counterintelligence Executive, Μάρτιος 2005

¹⁰⁵ *The National Counterintelligence Strategy of the United States of America*, Office of the National Counterintelligence Executive των ετών 2007 και 2008

¹⁰⁶ *Fundamental Elements of the Counterintelligence Discipline. Universal Counterintelligence Competencies*, National Counterintelligence Institute, Office of the National Counterintelligence Executive, Office of the Director of National Intelligence, 2006, σ. 8

αντιπληροφοριακή στρατηγική ενισχύει το όλο Intelligence Enterprise. Ο Bryant υπενθυμίζει μία εκ των αναφορών του *The National Intelligence Strategy of the United States of America* του 2009 (Mission Objective 4: Integrate Counterintelligence) κατά την οποία η αντικατασκοπία επιβάλλει την παρουσία της εντός κάθε πληροφοριακής διαδικασίας. Από κει και πέρα η κοινότητα της αντιπληροφόρησης οφείλει να επικεντρώσει στα ακόλουθα: α) ανίχνευση απειλών εκ των έσω, β) διείσδυση εντός αλλοδαπών Υπηρεσιών, γ) εμπλοκή με το πεδίο του κυβερνοδιαστήματος προς αντιμετώπιση κυβερνοενεργειών στρεφόμενων κατά κρίσιμων εθνικών υποδομών, δ) διασφάλιση της απρόσκοπτης κίνησης της παραγωγικής / εφοδιαστικής αλυσίδας.¹⁰⁷

Στο *National Counterintelligence Strategy of the United States of America* του 2016 διαβάζουμε ότι αποστολή της CI κοινότητας καθίσταται: α) η βαθύτερη κατανόηση των σχεδιασμών, προθέσεων, tradecraft κ. λ. των αλλοδαπών υπηρεσιών Πληροφοριών, β) η αποδιοργάνωση των εχθρικών αλλοδαπών υπηρεσιών Πληροφοριών προκειμένου να μην ευδοχωθούν αντιαμερικανικοί σχεδιασμοί, γ) η αποκάλυψη, αποτροπή και απομείωση κινδύνων προερχομένων από εσωτερικά στοιχεία (insiders) με πρόσβαση σε ευαίσθητα δεδομένα, δ) η προστασία ευαίσθητων δεδομένων / assets προκειμένου αποφυγής κλοπής, αλλοίωσης, χειραγώγησης, εκμετάλλευσης εκ μέρους αλλότριων πληροφοριακών οργανισμών, ε) η αναγνώριση / αντιμετώπιση κυβερνοδραστηριοτήτων αλλοδαπών πληροφοριακών οντοτήτων με σκοπό την κλοπή ευαίσθητων πληροφοριών αμερικανικών ηλεκτρονικών δικτύων.¹⁰⁸

Το Office of the Director of National Intelligence μέσω του *The National Intelligence Strategy of the United States of America* του 2014 υπογραμμίζει πως μια υπηρεσία Αντικατασκοπίας προβλέπει, αναγνωρίζει και αποτρέπει κακόβουλες προσπάθειες αλλοδαπών πληροφοριακών οργανισμών ή υπηρεσιών ασφαλείας, ατόμων ή ομάδων των οποίων οι σκοποί ποικίλουν. Κάποιοι από αυτούς ενδέχεται να αφορούν στην εκμείωση ευαίσθητων οικονομικών, διπλωματικών, στρατιωτικών, τεχνολογικών ντοκουμέντων, στην παρεμπόδιση των λειτουργιών του αμερικανικού συστήματος ασφαλείας και πληροφοριών, στον επηρεασμό της πολιτικής των ΗΠΑ. Οι υπηρεσίες Αντιπληροφόρησης προκειμένου να ανατρέψουν τα κακόβουλα πλάνα πρέπει: α) να κατανοούν, να προβλέπουν και να εισδύουν εντός των ολοένα και εξελισσόμενων ξένων μυστικών υπηρεσιών, β) να αναπτύσσουν / εφαρμόζουν κανονισμούς / πρακτικές ασφαλείας προς αποτροπή «εσωτερικών περιστατικών», γ) να μηδενίζουν τη διαρροή / κλοπή κρίσιμων τεχνολογικών δεδομένων και πληροφοριών, δ) να εξουδετερώνουν ή, έστω, να αποδυναμώνουν τις ανταγωνιστικές προσπάθειες εκμετάλλευσης των αδυναμιών της αμερικανικής παραγωγικής / εφοδιαστικής αλυσίδας.¹⁰⁹ Τα προηγούμενα θεωρούνται σημεία απαραίτητα προς πλήρωση καθώς, όπως τονίζει ο DNI James R. Clapper, οι ΗΠΑ ...*αντιμετωπίζουν τις πλέον ποικίλες απειλές στην εντός των πενήντα ετών προσωπικής μου πορείας στο χώρο των Υπηρεσιών. Κατά την έννοια που σημαντικές αλλαγές στο εξωτερικό και εσωτερικό περιβάλλον λαμβάνουν χώρα, οφείλουμε να σταθούμε έτοιμοι προ προκλήσεων και ευκαιριών που κάνουν την εμφάνισή τους στον 21^ο αιώνα.*¹¹⁰

¹⁰⁷ *The National Counterintelligence Strategy of the United States of America*, Office of the National Counterintelligence Executive (NCIX-2010-002), 2009, σ. iii, v-vi, επίσης, *The National Intelligence Strategy of the United States of America*, ODNI, Αύγουστος 2009, σ. 7-8

¹⁰⁸ *National Counterintelligence Strategy of the United States of America*, National Counterintelligence and Security Center, ODNI, 2016, σ. 3-7

¹⁰⁹ *The National Intelligence Strategy of the United States of America*, ODNI, 2014, σ. 10

¹¹⁰ *DNI Unveils 2014 National Intelligence Strategy*, ODNI, Σεπτέμβριος 2014, διαθέσιμο στη δικτυακή τοποθεσία του ODNI <http://www.dni.gov/index.php/newsroom/reports-and-publications/204->

Περαιτέρω στη σελίδα 17 του ιδίου αφήνεται να εννοηθεί πως η αντικατασκοπία συνθέτει αδιαχώρητο τμήμα του όλου πληροφοριακού παιγνίου υπό την έννοια της μη ύπαρξης ευκρινών διαχωριστικών τομών καθώς κατά τον Clapper ...η πληροφοριακή κοινότητα λειτουργεί προκειμένου να εφοδιάζει τους πολιτικούς και στρατιωτικούς ηγέτες με το μέγιστο δυνατό [πληροφοριακό] πλεονέκτημα ως προς τη διαδικασία λήψεως αποφάσεων. Κατανοούμε, τώρα περισσότερο από ποτέ, ότι ο καλύτερος τρόπος επίτευξης του σκοπού σχετίζεται με μια πλήρη ενοποίηση των εθνικών πληροφοριακών δυνατοτήτων.¹¹¹

Μελέτη της CIA εν έτει 1969 περιγράφει τις λειτουργίες / σκοπούς του CI ως εξής: «γενικά μιλώντας, οι λειτουργίες μιας υπηρεσίας Αντικατασκοπίας σχετίζονται με την προστασία της νόμιμης κυβέρνησης έναντι επιθέσεων... η αντικατασκοπία εμπλέκεται με υποθέσεις εχθρικής υπόγειας (clandestine) και κεκαλυμμένης (covert) δράσης. Υπόγεια δράση είναι η δράση κατά την οποία ο εχθρός επιθυμεί την αποσιώπησή της. Κεκαλυμμένη δράση είναι αυτή κατά την οποία δεν επιθυμείται κάλυψη· στην πραγματικότητα είναι πιθανό να εκδηλωθεί μέσω ενός άρθρου, μιας εκπομπής, μιας τρομοκρατικής ενέργειας. Αυτό που καλείται να αποκρυφτεί σχετίζεται με την ταυτότητα του δρώντα. Σκοπό μιας υπηρεσίας CI δεικνύει η συλλογή οιοδήποτε στοιχείου που αφορά σ' αυτά τα δύο είδη επίβουλων ενεργειών και στα άτομα που τις εκτελούν. Μόνο αποδίδοντας στην κυβέρνηση ολοκληρωμένη πληροφόρηση περί των εχθρών της και με την προϋπόθεση ότι αυτοί δεν θα λάβουν γνώση, μια υπηρεσία Αντικατασκοπίας κάνει αυτό για το οποίο σχεδιάστηκε και δημιουργήθηκε». ¹¹² Χρόνια αργότερα (2003), στο *Encyclopedia of the Central Intelligence Agency* διαβάζουμε ότι ...counterintelligence δεικνύει όρο ευρύτερο του counterespionage. Σημαίνει ολική αντικατασκοπευτική δράση. Πρόκειται για δράση μέσω της οποίας συλλέγεται η πληροφόρηση, προστατεύεται η Υπηρεσία καθαυτή από επίβουλες πρακτορικές ενέργειες, ακυρώνονται σχεδιασμοί σαμποτάζ, πολιτικών δολοφονιών και λοιπών δραστηριοτήτων διεξαγομένων από εχθρικές κυβερνήσεις ή άλλες κακόβουλες οντότητες όπως τρομοκρατικές ομάδες, παραστρατιωτικά γκρουπ κ. λ.¹¹³

Από τη μεριά του το FBI, ως κύριος αμερικανικός αντικατασκοπευτικός οργανισμός, βεβαιώνει ότι εντέλλεται όπως εντοπίσει / καταδιώξει αλλοδαπές Υπηρεσίες και οργανώσεις που μετέρχονται ανθρωπίνων πόρων και τεχνικών μέσων προκειμένου να συλλέξουν πληροφορίες που αφορούν στις Ηνωμένες Πολιτείες και να επηρεάσουν αρνητικά τους αμερικανικούς σχεδιασμούς και συμφέροντα. ¹¹⁴ Χαρακτηριστικό είναι πως η EO 12333 -επικαιροποιημένη από τις αντίστοιχες 13355 (2004) και 13470 (2008)- δεν αποκλείει αντικατασκοπευτική δράση της CIA στο

[reports-publications-2014/1114-dni-unveils-2014-national-intelligence](#)

[strategy?tmpl=component&format=pdf](#) όπου καταφύγαμε την 3^η Νοεμβρίου 2015

¹¹¹ *The National Intelligence Strategy of the United States of America*, Office of the Director of National Intelligence, 2014, σ. 17

¹¹² Wasemiller C. A., "The Anatomy of Counterintelligence", *Studies in Intelligence*, Volume 13, Issue 1, 1969, σ. 14-15

¹¹³ Smith T. W., Jr., *Encyclopedia of the Central Intelligence Agency*, Facts On File, Inc., New York, 2003, σ. 66

¹¹⁴ "What is the FBI's foreign counterintelligence responsibility?", διαθέσιμο στη διαδικτυακή τοποθεσία <https://www.fbi.gov/about/faqs/what-is-the-fbis-foreign-counterintelligence-responsibility> εις την οποία ανατρέξαμε την 1^η Σεπτεμβρίου 2016

εσωτερικό των ΗΠΑ σε συνεργασία με το FBI και ανάλογη δραστηριότητα εκ μέρους του FBI στο εξωτερικό σε συνεννόηση με τη CIA.¹¹⁵

Ανατρέχοντας σε ιστοσελίδα της U.S. Intelligence Community διαβάζουμε ότι «η αντικατασκοπία επιζητά να αναγνωρίσει, να κατανοήσει, να διαβαθμίσει και να αντιμετωπίσει τις πληροφοριακές απειλές ξένων δυνάμεων που βάλουν κατά των Ηνωμένων Πολιτειών. Αντικατασκοπία σημαίνει κάτι παραπάνω από σύλληψη κατασκόπων, σημαίνει εξουδετέρωση όλων των επιχειρήσεων του foreign intelligence».¹¹⁶

Όσον αφορά στη βρετανική θεσμική αντίληψη περί αντικατασκοπίας αυτή αποτυπώνεται, μεταξύ άλλων, στην *British Security Service Act of 1989* κατά την οποία ...[αντικατασκοπία] σημαίνει δράση υπέρ της εθνικής ασφαλείας, έναντι απειλών κατασκοπίας, τρομοκρατίας ή σαμποτάζ εκ μέρους ξένων δυνάμεων, έναντι ενεργειών που βάλουν κατά της κοινοβουλευτικής δημοκρατίας.¹¹⁷

Τέλος, κλείνουμε με έναν λιτό ορισμό, αντιπροσωπευτικό της KGB, όπως μεταφέρθηκε από τον Vasili Mitrokhin, ειδικότερα: «αντικατασκοπευτική δραστηριότητα είναι η δραστηριότητα που εκτελείται από ειδικές κρατικές υπηρεσίες έναντι ξένων πληροφοριακών υπηρεσιών και ατόμων στρατολογημένων από αυτές».¹¹⁸

Η MI5 εντός του πλέγματος των βρετανικών Υπηρεσιών

Το *National Intelligence Machinery* του 2000 τονίζει πως εντός του βρετανικού πληροφοριακού πλέγματος η MI5: α) συλλέγει, αναλύει και αξιολογεί πληροφοριακά δεδομένα, β) αντιμετωπίζει κατασκοπευτικές απειλές εκτελώντας δράσεις κατά μόνας ή συνεργατικά, γ) ενημερώνει τους κυβερνητικούς φορείς για τη φύση των απειλών προτείνοντας σχετικά μέτρα ασφαλείας. Η Υπηρεσία δεν ασκεί εκτελεστικά καθήκοντα. Η εμπλοκή της σε συλλήψεις ή διώξεις εξαρτάται από το βαθμό συνεργασίας με τις δικαστικές αρχές -σε τέτοιου είδους επιχειρήσεις οι τελευταίες έχουν τον πρώτο λόγο.¹¹⁹ Το *National Intelligence Machinery* του 2010 αναφέρεται τόσο στους κινδύνους όσο στην αντιμετώπιση της κατασκοπίας, της τρομοκρατίας και της αποσταθεροποιητικής δράσης κάνοντας λόγο, κυρίως, για επίβουλες ενέργειες πρακτόρων ξένων δυνάμεων. Πέρα τούτων η MI5 εντέλλεται όπως: α) προστατεύσει την κοινοβουλευτική δημοκρατία από απειλές που προέρχονται λόγω πολιτικών, οικονομικών ή άλλου είδους αναταραχών, β) προστατεύσει την οικονομική / κοινωνική ευημερία των πολιτών της Βρετανίας εξ απειλών εκπορευομένων από κέντρα εκτός χώρας, γ) συνεισφέρει στις προσπάθειες αστυνομικών και άλλων δικαστικών αρχών περί την πάταξη του εγκλήματος.¹²⁰ Το ίδιο έγγραφο, κάνοντας μνεία στις εθνικές κυβερνητικές πολιτικές ασφαλείας, σημειώνει πως αυτές δραστηριοποιούνται προς: α)

¹¹⁵ *Executive Order 12333 United States Intelligence Activities*, 4 Δεκεμβρίου 1981, παράγραφοι 1.8, 1.14 στα National Archives στη διαδικτυακή τοποθεσία <http://www.archives.gov/federal-register/codification/executive-order/12333.html#3.6> εις την οποία ανατρέξαμε την 1^η Σεπτέμβρη 2016

¹¹⁶ Στο <https://www.intelligencecareers.gov/icprotecting.html> εις το οποίο καταφύγαμε την 16^η Σεπτεμβρίου 2016

¹¹⁷ *British Security Service Act 1989*, The Stationery Office, Λονδίνο 2000, διαθέσιμο στην τοποθεσία https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/260780/4779.pdf εις την οποία καταφύγαμε την 4^η Σεπτεμβρίου 2016

¹¹⁸ Ehrman John, “Toward a Theory of CI. What are We Talking About When We Talk about Counterintelligence?” στο *Studies in Intelligence*, ό. π., σ. 7

¹¹⁹ *National Intelligence Machinery*, The Stationery Office, Λονδίνο 2000, σ. 9-10, διαθέσιμο και στο https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/250868/0114301808.pdf όπου καταφύγαμε την 3^η Δεκεμβρίου 2015

¹²⁰ *National Intelligence Machinery*, Cabinet Office, 2010, σ. 10-12, διαθέσιμο στη διαδικτυακή τοποθεσία https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf όπου ανατρέξαμε την 3^η Δεκεμβρίου 2015

προστασία της Βρετανίας και των βρετανικών κτήσεων, των βρετανικών συμφερόντων και περιουσιακών στοιχείων από μια ποικιλία απειλών περιλαμβανομένων της κατασκοπίας και της τρομοκρατίας, β) προστασία και προώθηση της βρετανικής αμυντικής και εξωτερικής πολιτικής, γ) προστασία της βρετανικής οικονομικής θέσεως, δ) καταστολή του οργανωμένου εγκλήματος.¹²¹

Από τη μεριά τους οι Peter Gill και Mark Phythian γράφουν πως η MI5 εξουσιοδοτείται στην αντιμετώπιση εσωτερικών απειλών αμέσως ή εμμέσως διά: α) εκτέλεσης συλλογής, ανάλυσης και αξιολόγησης / αξιοποίησης πληροφοριών, β) εκτέλεσης ορισμένων εκ των προτέρων πληροφοριακών ενεργειών, μεταξύ αυτών και της κεκαλυμμένης δράσεως, γ) συνεργασίας με την κυβέρνηση, απόδοσης στην τελευταία σχετικών προτάσεων, εργαλειοποίησης μέτρων ασφαλείας κ. λ., δ) συνεργασίας με άλλους οργανισμούς, θεσμούς και κυβερνητικά σώματα εντός Ηνωμένου Βασιλείου αλλά και Υπηρεσίες εκτός αυτού.¹²²

Αλλά ποιες οι απειλές για τις οποίες γίνεται λόγος; Ποιες οι περιοχές κύριας ενασχόλησης της MI5; Κατά την περίοδο 1990/1 η Υπηρεσία αφιέρωνε το 50% των πόρων / ενεργητικού της στην αντιμετώπιση της αλλοδαπής κατασκοπίας, το 37% στην αντιμετώπιση της τρομοκρατίας, το 12.5% στην αντιμετώπιση υπονομευτικών / ανατρεπτικών κινήσεων, 0% στην αντιμετώπιση του οργανωμένου εγκλήματος. Την περίοδο 1998/9 τα ποσοστά αντιστοίχως έχουν ως εξής: 24.4%, 63,1%, 0%, 8,3%. Την περίοδο 2004/5 τα ποσοστά αντιστοίχως έχουν ως εξής: 11.5%, 77%, 0%, 4,6%. Την περίοδο 2009/10 τα ποσοστά αντιστοίχως διαμορφώνονται ως εξής: 3.3%, 95.6%, 0%, 0%. Σημειώνουμε πως η αντιμετώπιση της τρομοκρατίας αφορά τόσο στην εσωτερική όσο και στη διεθνή με την πρώτη να αντιπροσωπεύεται στην περίοδο 2009/10 από ένα 16,3%, τη στιγμή που η δεύτερη εκτινάσσεται στο 79,3% -είναι φανερό πως η πάταξη του τρομοκρατικού φαινομένου απασχολεί εσχάτως την MI5 σχεδόν αποκλειστικά, εντυπωσιάζει, δε, το γεγονός της υποχώρησης, ως συμπεραίνεται, του κατασκοπευτικού κινδύνου.¹²³

Συμπεράσματα

Ο αριθμός των περίξ της έννοιας CI ορισμών αλλά και η περί των καθηκόντων των σχετικών Υπηρεσιών συζήτηση φαίνεται να δικαιώνουν την van Cleave ως προς το πολυδιάστατο του πεδίου. Η αντικατασκοπευτική πρακτική, που σημειωτέον διαχέεται κατά τον έναν ή άλλο τρόπο εντός του συνόλου των υπηρεσιών ασφαλείας, πληροφόρησης και law enforcement, δεν σχετίζεται μόνο με προκλήσεις ασφαλείας. Μένοντας σ' αυτά που θεωρούμε σημαντικότερα σημειώνουμε πως: α) CI σημαίνει τόσο άμυνα (security) όσο και επίθεση (counterespionage) φέροντας στο μυαλό την εικόνα της ασπίδας που προστατεύει και του ξίφους που επιτίθεται, το έργο των Andrew, Mitrokhin *The Sword and the Shield*, β) η αντικατασκοπία αφορά στην προάσπιση αλλά και προώθηση εθνικών πολιτικών, στρατιωτικών, οικονομικών, κοινωνικών συμφερόντων, γ) η αντικατασκοπία εμπλέκεται πλέον στον αντιτρομοκρατικό αγώνα και στον έλεγχο δράσεων στον κυβερνοχώρο, δ) μια υπηρεσία CI ενδέχεται να δεικνύει αυτόνομη υπηρεσία εσωτερικών Πληροφοριών ή να εντάσσεται εντός μεικτού πληροφοριακού σχεδιασμού, ε) αντικατασκοπία και κατασκοπία, αν και διακριτά πεδία, δεικνύουν το alter ego το ένα του άλλου, στ) κατά το προηγούμενο, καθόλου δεν αποκλείεται η παραγωγή «εξωτερικής ή θετικής πληροφόρησης» από μια υπηρεσία CI, ζ) μια υπηρεσία CI δραστηριοποιείται τόσο στο εσωτερικό όσο στο εξωτερικό. Η άποψη της δράσης αποκλειστικά σε εγχώριο περιβάλλον είναι στρεβλωτική εκτός, ίσως, αν μιλάμε αποκλειστικά για δράσεις ασφαλείας, η) η αντικατασκοπευτική λειτουργία δύναται να επιβοηθήσει / επηρεάσει τόσο την οικεία διαδικασία λήψεως αποφάσεων όσο την ανάλογη εξωτερικών

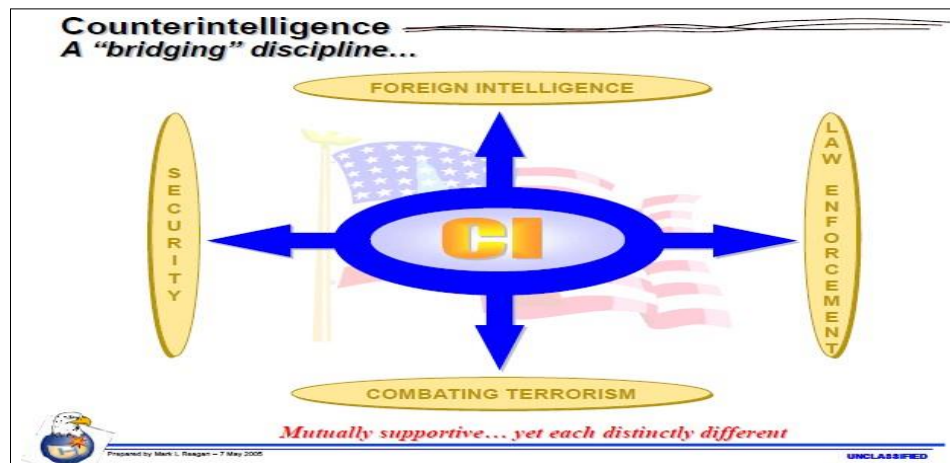
¹²¹ *National Intelligence Machinery*, Cabinet Office, 2010, σ. 19-20

¹²² Gill P., Phythian M., *Intelligence in an Insecure World*, Polity Press, UK / USA, 2012², σ. 16

¹²³ ό. π., σ. 59

δυνάμεων / δρώντων. Η van Cleave σημειώνει πως ...[η] αντικατασκοπία εμμέσως δύναται να συνεισφέρει στην αμερικανική παραγωγή πολιτικής μέσω αποκάλυψης πλάνων, προθέσεων και δυνατοτήτων ξένων δυνάμεων που στοχεύουν τις Ηνωμένες Πολιτείες προβαίνοντας σε πληροφοριακές επιχειρήσεις. Η θετική [positive] πληροφόρηση που μια υπηρεσία Αντικατασκοπίας μπορεί να παράξει υποβοηθά την αμερικανική εξωτερική και αμυντική πολιτική εφόσον η ηγεσία εκτιμήσει ορθά την πολυτιμότητά της.¹²⁴

Το πεδίο CI είναι τόσο δαιδαλώδες, ίσως αόριστο, που επιδέχεται πλήθος προσεγγίσεων πέραν της αρχικής, βασικής και κοινά αποδεκτής ήτοι, της καταδίωξης της αντίπαλης κατασκοπίας, της διαφύλαξης των εσωτερικών μυστικών και της προάσπισης της εθνικής ασφαλείας. Φαίνεται ότι στον 21^ο αιώνα γεφυρώνει έννοιες όπως «ασφάλεια / εσωτερική ασφάλεια», «εξωτερική πληροφόρηση», «law enforcement», «αντιτρομοκρατία» ή αποτελεί κοινό δεσμό για αυτές. Συντομότερα, δύναται να θεωρηθεί μέσος χώρος μεταξύ του πεδίου της εξωτερικής πληροφόρησης και του ανάλογου της επιβολής νόμου και τάξεως. Πιθανότατα η κεντρική του παρουσία το καθιστά πλέον σκοτεινό και απρόσιτο, η, δε, αντικατασκοπευτική κουλτούρα ωφελεί να εμποτίσει κάθε πολιτικό, στρατιωτικό, οικονομικό, ασφαλείας, τεχνολογικό / επιστημονικό ή άλλο σημαντικό οργανισμό.



- Counterintelligence can be viewed as a "bridge" between law enforcement and foreign intelligence... information obtained by any of these disciplines may potentially be of value and use to the others



Εικόνες 11 και 12: ο κεντρικός / κομβικός ρόλος της αντιπληροφόρησης εντός του φάσματος των Υπηρεσιών. Οι εικόνες ελήφθησαν από τις σελίδες 10 και 14 του *Introduction to U.S. Counterintelligence. "CI 101--A PRIMER"* (2005) του Mark Reagan

¹²⁴ van Cleave, M., *Counterintelligence and National Security*, ό. π., σ. 3

ΚΕΦΑΛΑΙΟ 5

Περί της στρατιωτικής αντικατασκοπίας

Στρατιωτική αντικατασκοπία: θεμελιώδη καθήκοντα

Θεσμικά, η στρατιωτική πληροφόρηση / αντιπληροφόρηση αφορά στην στρατηγική / τακτική υποστήριξη επιχειρήσεων των ενόπλων δυνάμεων. Όσο ευρύτερα ορίζονται αυτές οι επιχειρήσεις τόσο πιθανότερη είναι μια εισπήδηση των στρατιωτικών Υπηρεσιών εντός της πολιτικής και κοινωνικής ζωής. Ακραίο παράδειγμα τα λεγόμενα «κράτη εθνικής ασφαλείας / national security states»: τα τελευταία πριμοδοτούν στο μέγιστο τις λειτουργίες των στρατιωτικών πληροφοριακών οργανισμών με σκοπό τον έλεγχο της ημεδαπής κοινωνίας, ίσως, δε, περισσότερο από την καταδίωξη του αλλοδαπού πράκτορα. Στις αρχές της δεκαετίας του 1980 Υπηρεσίες με αυτού του είδους τις ανησυχίες (ουσιαστικά υπηρεσίες εσωτερικής Ασφαλείας) ευρίσκοντο σε Λατινική Αμερική και Ανατολική Ευρώπη. Μόλα ταύτα ακόμα και δημοκρατικά καθεστώτα δεν δίστασαν να μετέλθουν σχετικών πρακτικών. Χαρακτηριστική είναι η περίπτωση κατά την οποία ο αμερικανικός στρατός χρησιμοποιήθηκε από το πολιτικό σύστημα προς διεξαγωγή παράνομων εσωτερικών δραστηριοτήτων υπό τον μανδύα της αντικατασκοπευτικής αναγκαιότητας και της πάταξης του κομμουνιστικού φόβητρου κατά την μετά το 1947 περίοδο.¹ Με το πέρασμα των ετών η δημοκρατικοποίηση των Υπηρεσιών στα πρώην αυταρχικά καθεστώτα, αν όχι και σε ορισμένα φιλελεύθερα, εκδηλώθηκε με την μεταλλαγή αυτών των Υπηρεσιών από στρατιωτικές σε πολιτικές, βλέπε, π. χ., την περίπτωση της Βραζιλίας² ή της Ελλάδας. Πρόσφατα, ερευνητές όπως ο Stephen Dycous, ο Kevin Haggerty ή ο Richard Ericson υποθέτουν ή και φοβούνται την επιστροφή των στρατιωτικών Υπηρεσιών στο κοινωνικό και πολιτικό γίγνεσθαι μέσω της αναβάθμισης του αγώνα κατά της τρομοκρατίας.³

Σύμφωνα με τον αμερικανικό στρατό ξηράς ο ρόλος της στρατιωτικής αντικατασκοπίας αφορά στην εξασφάλιση μυστικότητας / προστασίας που οφείλει να χαρακτηρίζει / καλύπτει τα σχετικά σώματα / όπλα. Κατ' αυτήν την έννοια μια στρατιωτική υπηρεσία CI μεταξύ άλλων: α) ανιχνεύει, αναγνωρίζει, αξιολογεί, αντιμετωπίζει, εξουδετερώνει, χειραγωγεί τις αντίπαλες προσπάθειες συλλογής πληροφοριών τόσο σε περίοδο ειρήνης όσο και συρράξεων κάθε έντασης, β) επιλαμβάνεται του ελέγχου προσωπικού (personnel security) με σκοπό τη μη διαρροή πληροφοριών, γ) επωμίζεται το καθήκον της ασφάλειας πληροφοριών, δ) αναλαμβάνει τη φυσική προστασία (physical security) χώρων, εγκαταστάσεων κ. λ., ε) αναλαμβάνει τη διαφύλαξη φίλιων πληροφοριών (essential elements of friendly information -EEFI)⁴, στ) επιλαμβάνεται της ασφάλειας κίνησης / κινητοποίησης του στρατεύματος, ζ) αντιμετωπίζει την τρομοκρατική απειλή, η) προβαίνει σε ψυχολογικές επιχειρήσεις, θ) προβαίνει σε παραπλάνηση του εχθρού στο πεδίο της

¹ Βλέπε στο Jensen M. Joan, *Army Surveillance in America, 1775-1980*, Yale University Press, USA, 1991

² Cepik Marco, "Structural change and democratic control of intelligence in Brazil" στο *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, επιμ. Bruneau C. Tomas., Boraz C. Steven, University of Texas Press, Austin, 2007, σ. 149-169

³ Dycous Stephen, "The role of military intelligence in homeland security" στο *Louisiana Law Review*, 64, 2004, σ. 779-807, Haggerty Kevin, Ericson Richard, "The militarization of policing in the information age" στο *Journal of Political and Military Sociology*, 27, 1999, σ. 233-255

⁴ Department of the Army, *U.S. Army Counterintelligence Handbook*, Skyhorse Publishing, Inc., 2013, σ. 1-2

μάχης, ι) προστατεύει τις όπισθεν του μετώπου γραμμές (rear area security) με ό,τι αυτό σημαίνει για την επιμελητεία, διοικητική μέριμνα, εφοδιαστική ικανότητα των φίλιων δυνάμεων, ια) επιβλέπει τις εσωτερικές επικοινωνίες και ηλεκτρονικά συστήματα, ιβ) επιλαμβάνεται της προστασίας τμημάτων / δυνάμεων που σταθμεύουν στο εξωτερικό και των οποίων η παρουσία συνιστά στόχο πρακτόρων, σαμποτέρ ή τρομοκρατών (Counterintelligence Force Protection Source Operations -CFSO, Antiterrorism Force Protection -AT/FP), ιγ) επιφορτίζεται της κάλυψης επιχειρήσεων που δεν αφορούν σε ένοπλη αντιπαράθεση (Operations Other Than War -OOTW, Civil-military affairs).⁵

Οι στρατιωτικές αντικατασκοπευτικές επιχειρήσεις διακρίνονται σε δύο τύπους, τις ειδικές (*special*) και τις γενικές (*general*). Οι πρώτες περιλαμβάνουν άμεση / έμμεση εμπλοκή με αλλοδαπές πληροφοριακές Υπηρεσίες (Foreign Intelligence Services -FIS) δια της χρήσεως τόσο ανθρωπίνων όσο τεχνικών πόρων. Οι δεύτερες διακρίνονται για την αμυντική τους φύση με κύριο σκοπό την υποστήριξη των προγραμμάτων προστασίας των ενόπλων δυνάμεων -ουσιαστικά κάθε στρατιωτική αντικατασκοπευτική επιχείρηση / δραστηριότητα υπηρετεί αυτόν τον σκοπό.⁶

Τόσο οι ειδικές όσο και οι γενικές επιχειρήσεις στηρίζονται σε πληροφορία / πληροφόρηση που δομείται στο γνωστό βηματισμό του πληροφοριακού κύκλου. Οι αμερικανικές ειδικές στρατιωτικές CI επιχειρήσεις εκτελούνται υπό την αιγίδα του National Foreign Counterintelligence Program ακολουθώντας την Army Regulation (AR) 381-47 (S), *US Army Offensive Counterespionage Activities*, (Ιούλιος 1990). Συντίθενται εξ επιθετικών CI επιχειρήσεων, επιχειρήσεων Counterespionage (CE) και ορισμένων αμυντικών προγραμμάτων με στόχευση ξένους πληροφοριακούς οργανισμούς. Οι αμερικανικές γενικές στρατιωτικές CI επιχειρήσεις, ευρύτερες και κατά βάσει αμυντικού χαρακτήρα, περιλαμβάνουν / χαρακτηρίζονται από: α) συμβουλευτικά / επικουρικά προγράμματα με σκοπό την επαύξηση ασφαλείας του όποιου υποστηριζόμενου στρατιωτικού οργανισμού, β) προγράμματα τεχνικής υποστήριξης Technical Surveillance Countermeasures (TSCM), TEMPEST (έρευνες επί τεχνικών ζητημάτων ηλεκτρονικών εκπομπών), εκτέλεση προγραμμάτων πολύγραφου (ανιχνευτής ψεύδους / polygraph), C-SIGINT κ. λ., γ) παρουσία αυτοματοποιημένων συστημάτων ασφαλείας με σκοπό την προστασία πληροφοριακών networks, hardware, software, e-data κ. λ., δ) υποστηρικτικά προγράμματα υπέρ πληροφοριακών HUMINT, SIGINT και IMINT δραστηριοτήτων,

⁵ FM 34-60, *Counterintelligence*, Headquarters, Department of the Army, Washington, D.C., Οκτώβριος 1995, chapter 1, επίσης βλέπε FM 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., Μάιος 2004, σ. 1-31 αλλά και Army Regulation (AR) 381-20, *Military Intelligence. The Army Counterintelligence Program*, Headquarters, Department of the Army, Washington, D.C., Νοέμβριος 1993, σ. 1, 10, 12. Περί Force Protection Source Operations -CFSO όπως και περί Antiterrorism Force Protection -AT/FP βλέπε αντιστοίχως MCWP 2-14, *Counterintelligence*, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., Σεπτέμβριος 2000, σ. 7-12 – 7-13 και Rokosz F. Ronald, Hash H. Charles, “Army Antiterrorism Force Protection” στο *Joint Force Quarterly*, Φθινόπωρο / Χειμώνας 1997-1998, σ. 110-117. Σχετικά με το κομμάτι Operations Other Than War -OOTW / Civil-military affairs, αυτό αναφέρεται σε: α) επιχειρήσεις εκκένωσης περιοχών με άμαχο πληθυσμό (noncombatant evacuation operations), β) έλεγχο εξοπλισμών, γ) υποστήριξη των εγγόριων πολιτικών αρχών, δ) ανθρωπιστική βοήθεια (humanitarian assistance -HA), ε) βοήθεια σε ζητήματα ασφαλείας, στ) παροχή βοήθειας σε κρατική οντότητα από άλλη ή άλλες ανάλογες, ζ) υποστήριξη επιχειρήσεων κατά του εμπορίου ναρκωτικών, η) πόλεμο έναντι του τρομοκρατικού φαινομένου, θ) επιχειρήσεις διατήρησης ειρήνης (peacekeeping operations), ι) επιβολή ειρήνης (peace enforcement), ια) επίδειξη ισχύος (show of force), ιβ) υποστήριξη εξεγέρσεων, ιγ) υποστήριξη καταστολής εξεγέρσεων -για μια άποψη βλέπε Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 8-9

⁶ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 23

ε) υποστηρικτικά υπέρ των αρχών επιβολής νόμου προγράμματα· τα συγκεκριμένα προγράμματα εκτελούνται υπό αυστηρών όρων και περιορισμών, στ) υποστηρικτικά προγράμματα ανακούφισης πληγέντων από φυσικές καταστροφές περιοχών.⁷

Εντός του Army FM 2-0, *Intelligence*, (2010), καταγράφονται τα εξής: α) CI σημαίνει σύνολο δράσεων με σκοπό την ανίχνευση, αναγνώριση, παρακολούθηση, εξουδετέρωση αλλά και χειραγώγηση των αντίπαλων πληροφοριακών οργανισμών και δραστηριοτήτων, β) η αποστολή της αμερικανικής πολιτικής / στρατιωτικής αντικατασκοπίας σχετίζεται με διεξαγωγή συντονισμένων, διεξοδικών ερευνών σε περίπτωση διάπραξης εγκλημάτων κατά της εθνικής ασφαλείας (1), διεξαγωγή επιχειρήσεων με σκοπό την υποστήριξη στρατιωτικών προγραμμάτων / αποστολών (2), συλλογή, ανάλυση και παραγωγή πληροφόρησης περίξ δραστηριοτήτων αλλοδαπών Υπηρεσιών ή διεθνών τρομοκρατικών ομάδων (3), παροχή τεχνικών υπηρεσιών προς ικανοποίηση των προηγούμενων απαιτήσεων (4), εκτέλεση επιθετικών ενεργειών έναντι ξένων πληροφοριακών οργανισμών και οργανισμών ασφαλείας (foreign intelligence and security services -FISS) όπως και διεθνών τρομοκρατικών οργανώσεων (international terrorist organizations -ITO) που συνθέτουν απειλή για την ασφάλεια των ενόπλων δυνάμεων, τους σχεδιασμούς του υπουργείου Αμύνης (DoD) αλλά και για συμμαχικές χώρες (5), γ) οι αποστολές της αμερικανικής στρατιωτικής Αντικατασκοπίας αναφέρονται σε counterespionage, προστασία ενόπλων δυνάμεων, προστασία ερευνητικών και τεχνολογικών στρατιωτικών προγραμμάτων, κυβερνητική / διαδικτυακή αντικατασκοπία (cyber CI).⁸

Στο Secretary of the Navy Instruction (SECNAVINST) 3850.2C του αμερικανικού Department of the Navy αναφέρεται ότι αντικατασκοπία σημαίνει συλλογή πληροφοριών και διεξαγωγή επιχειρήσεων προς αντιμετώπιση αλλότριων κατασκοπευτικών πλάνων, σχεδιασμών σαμποτάζ, πολιτικών δολοφονιών κ. λ. Εντός του ιδίου καταγράφονται οι γνωστές CI δράσεις, ήτοι: α) *CI Investigations* με έμφαση στη διαλεύκανση υποθέσεων κατασκοπίας ή υπονομευτικών δράσεων όπως αυτές ορίζονται εντός του κειμένου όπως και στην πληροφόρηση πολιτικών και στρατιωτικών προϊσταμένων περίξ απειλών ασφαλείας, β) *CI Operations* με σκοπό την ανίχνευση, αναγνώριση, εξουδετέρωση, καταστροφή, χειραγώγηση κ. λ. στρατηγημάτων αλλοδαπών Υπηρεσιών ή τρομοκρατικών οργανώσεων που στοχεύουν / βάλλουν κατά του DoD. Επιπλέον προβλέπεται στρατολόγηση ή παρακίνηση σε αποσκίρτηση αλλογενών ατόμων / πρακτόρων, εκτίμηση δυνατοτήτων / τρωτοτήτων ξένων δρώντων, συμβολή στο οικείο human intelligence, συμβολή στην προστασία οικείων δυνάμεων που σταθμεύουν εκτός επικρατείας, επικουρία σε επιχειρήσεις peacekeeping και άλλων μη πολεμικής υφής, υφαρπαγή ανταγωνιστικών τεχνολογικών gadgets / εξοπλισμών προς ανάπτυξη αντιμέτρων κ. λ., γ) *Counterintelligence Collection* με αποστολή την κτήση πληροφοριών, δ) *Counterintelligence Analysis and Production* με αρμοδιότητα στην ανάλυση πληροφοριών και στην τροπή των τελευταίων σε πληροφόρηση, ε) *Counterintelligence Functional Services* με έμφαση στην αμυντική αντικατασκοπία.⁹

Από τη μεριά της η αμερικανική πολεμική αεροπορία εισάγει τον όρο *counterinformation* (CI). Πρόκειται για σειρά εφαρμογών που στοχεύουν στην

⁷ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 24-28

⁸ Army Field Manual 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2010, σ. 6-1 – 6-2

⁹ SECNAVINST 3850.2C, *Department of the Navy Counterintelligence*, Department of the Navy, Washington, D.C., Ιούλιος 2005, επίσης βλέπε SECNAVINST 3850.4A, *Technical Surveillance Countermeasures Program*, Department of the Navy, Washington, D.C., Αύγουστος 2014

επίτευξη πληροφοριακής ανωτερότητας επί του αντιπάλου μέσω αδρανοποίησης / εξουδετέρωσης ή / και επηρεασμού των πληροφοριακών καναλιών του. Η ευρύτητα του όρου καταφαίνεται (και) από την, μάλλον, γενική διακήρυξη πρόθεσης παρεμπόδισης του ανταγωνιστή στον αγώνα επίτευξης πληροφοριακού πλεονεκτήματος. Η άρνηση πληροφορίας, η διακοπή λειτουργίας ή / και η αποδόμηση του αντιπάλου συστήματος, η εξαπάτηση κ. λ. υποδηλώνουν δρόμους επιτυχίας. Οι counterinformation δράσεις χωρίζονται σε αμυντικές και επιθετικές με το counterintelligence να κατατάσσεται στις πρώτες. Σύμφωνα με αυτήν την προσέγγιση counterintelligence σημαίνει προστασία πληροφοριών, εγκαταστάσεων, τεχνολογικών καινοτομιών, επιχειρησιακών σχεδιασμών κ. λ. Και εδώ ο όρος σχετίζεται με αμυντική προσπάθεια, είναι δε χαρακτηριστικό ότι τακτικισμοί όπως deception και counterdeception κατατάσσονται στον ευρύτερο counterinformation και όχι στον counterintelligence σχεδιασμό.¹⁰ Το αμερικανικό Air Force Office of Special Investigations (AFOSI) μεταξύ άλλων δραστηριοποιείται στην αντιτρομοκρατική έρευνα (antiterrorism survey), στην εκτίμηση απειλών (threat assessment), στην εκτίμηση τρωτοτήτων επιχειρήσεων HUMINT (Human Intelligence Vulnerability Assessments -HVAs) όπως και στην υποστήριξη επιχειρήσεων μέσω αντικατασκοπευτικών σχεδιασμών (counterintelligence force support operations)¹¹ -όλες οι αναφερόμενες δράσεις εντάσσονται στα counterintelligence functional services.¹²

Στην MCWP 2-14 (2000) του U.S. Marine Corps / Department of the Navy αναφέρεται ότι οι δράσεις CI δεικνύουν τμήμα ολικής προσπάθειας με κίνητρο την εκμηδένιση απειλών αντιπάλων μυστικών υπηρεσιών που στοχεύουν το σύνολο των οικείων εντασσομένων μονάδων στο σχεδιασμό της Marine Air Ground Task Force (MAGTF) ή / και των συνεργαζομένων δυνάμεων. Σε ευρύτερο επίπεδο τονίζεται η κύρια αποστολή ήτοι, η αναγνώριση / εξουδετέρωση κινδύνων εκπορευόμενων από αλλότριους πληροφοριακούς ή άλλους οργανισμούς / πρόσωπα. Δεν παραλείπονται αναφορές στην ανάγκη εξάλειψης των εγχώριων αδυναμιών μέσω ενός ικανού πλέγματος ασφαλείας, στη χρησιμότητα της παραπλάνησης / παραπληροφόρησης, στην ανάγκη δημιουργίας κλίματος αβεβαιότητας στον εχθρό ως προς τις οικείες δυνατότητες, ελλείψεις και προθέσεις.¹³

¹⁰Air Force Doctrine Document 2-5, *Information Operations*, U.S. Air Force, 1998, σ. 9-19, επίσης βλέπε *Cornerstones of Information Warfare*, Department of the Air Force, Washington, D.C., 1995 στο <http://www.csse.monash.edu.au/courseware/cse468/2006/cornerstones-iw.html> όπου ανατρέξαμε την 23^η Απριλίου 2015 ή / και στο <http://www.c4i.org/cornerstones.html> με ημερομηνία καταφυγής επίσης την 23^η Απριλίου 2015

¹¹ Air Force Policy Directive 71-1, *Special Investigations, Criminal Investigations and Counterintelligence*, Department of the Air Force, Ιανουάριος 2010, σ. 5. Περί AFOSI και αντικατασκοπευτικού προγραμματισμού βλέπε προαιρετικά Air Force Instruction 71-101, Volume 4, *Special Investigations, Counterintelligence*, Department of the Air Force, Νοέμβριος 2011

¹² Αναφερόμαστε σε αμυντικές αντικατασκοπευτικές δράσεις προς: α) αναγνώριση / αντιμετώπιση τρομοκρατικών σχεδιασμών, κατασκοπευτικών κινήσεων, πλάνων σαμποτάζ αλλά και στρατηγημάτων ξένων Υπηρεσιών, β) υποστήριξη ευρύτερων πληροφοριακών δράσεων ή / και σχεδιασμών του DoD -για μια άποψη βλέπε Air Force Policy Directive 71-1, *Special Investigations, Criminal Investigations and Counterintelligence*, Ιανουάριος 2010, σ. 11

¹³ Ειδικότερα, και μεταξύ άλλων, συνεκτιμώνται τακτικές που αφορούν σε δράσεις *force protection, operations security, counterreconnaissance, deception, communication / information systems security, information and personnel security, physical security* υπό την προϋπόθεση τεσσάρων μεθοδολογικών βημάτων ήτοι, *CI estimate, CI survey(s), CI plan, CI measures*. Τα τελευταία (CI measures) αναγνωρίζονται σε *άρνησης (denial), ανίχνευσης (detection)* και *παραπλάνησης (deception)*. Συνηθέστατα οι CI Marine Air-Ground Task Force / CI MAGTF επιχειρήσεις σκοπό έχουν είτε την επίρρωση της στρατιωτικής ασφαλείας (military security) είτε της δημόσιας πολιτικής / αστικής ανάλογης (civil security). Προκειμένου επιμέρους Marine Expeditionary Force (MEF) μονάδων και

Όσον αφορά στις διαβαθμίσεις δράσεων διακρίνουμε την στρατηγική, την επιχειρησιακή και την τακτική. Η πρώτη σχετίζεται με εθνικούς (π. χ. DoD's) όσο και διεθνείς (π. χ. NATO's) σχεδιασμούς εκτελώντας κάθε είδους αποστολών CI [CI investigations / operations, offensive CI, research / technology protection, Special Assess Program (SAP) support, Special Operations Forces (SOF) support κ. λ.]. Η δεύτερη (επιχειρησιακή) συνήθως αποδίδεται στο Army Service component command -ASCC (Στρατός Ξηράς) αλλά και σε διοικήσεις μεικτών ή μη ενόπλων σχηματισμών επικεντρώνοντας σε συγκεκριμένα θέατρα με καθήκον την προστασία των επιχειρησιακών βάσεων από ενέργειες αλλοδαπών Υπηρεσιών ή εξτρεμιστικών οργανισμών, την υποστήριξη των επιχειρήσεων μάχης όταν η τακτική αντικατασκοπία δεν δύναται να εξυπηρετήσει την περιοχή των ενεργειών (area of operations -AO). Κατά την αντίστροφη φορά η επιχειρησιακή αντικατασκοπία ενδέχεται, όταν αυτό κριθεί απαιτητό, να συνδράμει τη στρατηγική ανάλογη. Η τρίτη (τακτική) εμπλέκεται με κάθε είδους CI δραστηριότητες που αποτείνονται σε / εξυπηρετούν σχηματισμούς επιπέδου Σώματος Στρατού (και ελασσόνων) με σκοπό κυρίως την προστασία των συγκεκριμένων δυνάμεων και των διοικητικών / επιχειρησιακών βάσεων από εχθρική στοχοποίηση.¹⁴

Ουσία των στρατιωτικών CI αποστολών αποτελεί η προστασία του στρατεύματος. Η αντικατασκοπία, φύσει πολυεπίπεδη, επιχειρεί την απομείωση των εχθρικών πληροφοριακών απειλών, την στοχοποίηση των εχθρικών πληροφοριακών assets.¹⁵ Κατά τα ανωτέρω, τρία θεωρούνται τα κύρια στρατιωτικά CI υποπεδία. Πρόκειται για τα υποπεδία του Counter-HUMINT, του Counter-SIGINT και του Counter-IMINT, ειδικότερα:

- Το C-HUMINT απαιτεί εφαρμογή τόσο επιθετικών όσο αμυντικών μέτρων προς ελαχιστοποίηση των δυνατοτήτων συλλογής πληροφοριών του αντιπάλου διά ανθρωπίνων πόρων. Άλλες κινήσεις αφορούν σε: α) παραγωγή και διασπορά πληροφορίας περίξ οργανισμών, τοποθεσιών ή προσώπων που ενδιαφέρουν κατά τον έναν ή άλλο τρόπο τις υπηρεσίες CI, β) εφαρμογή ελέγχου προσωπικού (personnel security investigation -PSI), γ) επιμόρφωση / ενημέρωση προσωπικού επί ζητημάτων ασφαλείας, δ) αναζήτηση υπόπτων κατασκοπίας ή τέλεσης τρομοκρατικών κτυπημάτων, ε) απενημέρωση (debriefing) ήτοι, αποτίμηση αποτελεσμάτων της όποιας εκτελεσθείσης αποστολής με στόχο τη συλλογή πληροφοριών αντικατασκοπευτικού ενδιαφέροντος, στ) προσέγγιση ατόμων / ομάδων όπως εκτοπισθέντες, πρόσφυγες, συνεργάτες του αντιπάλου, αποσκιρτήσαντες, γνώστες των αντιπάλων στρατηγικών προθέσεων / δυνατοτήτων κ. λ. Στην πλειοψηφία των περιπτώσεων, η ανάπτυξη του CI προσωπικού αφορά σε περιοχές όπισθεν του πολεμικού μετώπου. Άλλες αποστολές περιλαμβάνουν / σχετίζονται με: α) ανάπτυξη τοπικού δικτύου πληροφοριών, β) παροχή υπηρεσιών ασφαλείας υπέρ τοπικών κρισίμων υποδομών / εγκαταστάσεων, γ) επίβλεψη / αξιολόγηση της αποτελεσματικότητας των μέτρων ασφαλείας, δ) συνεργασία με μονάδες Civil Affairs (CA) προκειμένου καταγραφής της στάσης / διάθεσης του τοπικού πληθυσμού,

πάντα σε σχέση με το CI / HUMINT μεταξύ άλλων προβλέπονται: α) επιχειρήσεις τακτικού επιπέδου συμπεριλαμβανομένου του αντίστοιχου CFSO, β) επίβλεψη προσωπικού, γ) εκτέλεση περιορισμένων CI ερευνών, δ) εκτέλεση αντιμέτρων τεχνικής επιτήρησης -technical surveillance countermeasures (TSCM) με σημαντικό ρόλο να αποδίδεται στα λεγόμενα HUMINT Support Teams (HST) -για μια λεπτομερέστερη άποψη βλέπε MCWP 2-14, ό. π., σ. 1-1 – 1-10, 3-10 – 3-15

¹⁴ Army Field Manual 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2010, σ. 6-6 – 6-7

¹⁵ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 4

αντιμετώπισης / εξουδετέρωσης απειλών κ. λ., ε) συνεργασία με μονάδες της στρατιωτικής αστυνομίας (Military Police -MP) με σκοπό την αποκάλυψη ατόμων που ενδιαφέρουν την στρατιωτική αντικατασκοπία.¹⁶

Επιθετικές / αμυντικές C-HUMINT επιχειρήσεις

OFFENSIVE	DEFENSIVE
Targeting for fire and maneuver	Deception operations (OPSEC)
Counterespionage operations	Physical security
Counterreconnaissance	Information security
Countersabotage	Personnel security
Counterterrorism	
Penetration and exploitation operations	

Εικόνα 13: επιθετικές και αμυντικές C-HUMINT επιχειρήσεις. Η εικόνα ελήφθη από τη σελίδα 28 του *U.S. Army Counterintelligence Handbook* (2013) του U.S. Department of the Army

- Οι επιχειρήσεις C-SIGINT, περιλαμβανομένης της παρακολούθησης / ελέγχου της ασφάλειας επικοινωνιών (communications security -COMSEC), εκτελούνται με σκοπό την αποκάλυψη των εχθρικών SIGINT δυνατοτήτων όπως και της βελτίωσης: α) της ασφάλειας των οικείων στρατιωτικών δυνάμεων, β) του ποσοστού επιβιωσιμότητας (survivability) αυτών, γ) της κινητικότητας (mobility) αυτών. Επιπλέον σχετίζονται: α) με παροχή στοιχείων προς αναγνώριση φίλων επικοινωνιακών / ηλεκτρονικών (communications / electronics C-E) τρωτοτήτων, β) με απόδοση προτάσεων περί σχετικών αντιμέτρων, γ) με έλεγχο αποτελεσματικότητας αντιμέτρων. Οι C-SIGINT επιχειρήσεις χαρακτηρίζονται από επιθετικές όσο και αμυντικές παραμέτρους. Αναπτύσσονται στη γνώση: α) των δυνατοτήτων του εχθρικού SIGINT, β) των δυνατοτήτων των οικείων και φίλων C-E συστημάτων, γ) των σχεδιασμών / προθέσεων των εχθρικών δυνάμεων όπως και (δ) επί τη βάση της ανάγκης λήψεως μέτρων άρνησης πληροφορίας στον αντίπαλο.¹⁷

Επιθετικές / αμυντικές C-SIGINT επιχειρήσεις

OFFENSIVE	DEFENSIVE
Targeting for fire and maneuver	Radio OPSEC countermeasures
Electronic attack	Use of secure telephone
	Signals security (SIGSEC) procedures
	Deception operations

Εικόνα 14: επιθετικές και αμυντικές C-SIGINT επιχειρήσεις. Η εικόνα ελήφθη από τη σελίδα 34 του *U.S. Army Counterintelligence Handbook* (2013) του U.S. Department of the Army

¹⁶ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 28-34

¹⁷ ό. π., σ. 34

- Οι επιχειρήσεις C-IMINT σκοπό έχουν την εξουδετέρωση των εχθρικών IMINT δυνατοτήτων οι οποίες ενδέχεται να υποστασιοποιούνται μέσω: α) λήψεως εναερίων απεικονίσεων, β) χρήσεως υπέρυθρων αισθητήρων, γ) χρήσεως ραδιοεντοπιστών (radar), δ) χρήσεως ηλεκτρο-οπτικών αισθητήρων, ε) χρήσεως πολυφασματικών / ψηφιακών απεικονιστικών μηχανισμών. Οι επιχειρήσεις IMINT στηρίζονται / εξαρτώνται από: α) την πολυμορφική πολυανιχνευτική (diverse multi-sensor) δυνατότητα συλλογής πληροφοριών, β) την αναγνώριση εδάφους (reconnaissance) μέσω επανδρωμένων ή μη (manned / unmanned) πτητικών μέσων, γ) τη μελέτη των καιρικών φαινομένων, δ) τη μελέτη της χωρογεωγραφίας, ε) την ανάπτυξη των εχθρικών δυνάμεων. Η συλλογή πληροφοριών περίξ εχθρικών IMINT εγχειρημάτων ενδέχεται να προέρχεται από: α) αιχμαλώτους πολέμου (enemy prisoner of war -EPW), β) αναφορές της πολεμικής αεροπορίας, γ) τακτική / στρατηγική αναγνώριση, δ) επιχειρήσεις HUMINT, ε) satellite reconnaissance advance notice -SATRAN, στ) αναφορές αντιαεροπορικών / αντιπυραυλικών μονάδων (air defense artillery -ADA), συνοπτικά ρεπορτάζ (SPOT reports) τύπου SALUTE (size, activity, location, unit, time, equipment) περίξ των εχθρικών IMINT υποδομών / εγκαταστάσεων.¹⁸

Επιθετικές / αμυντικές C-IMINT επιχειρήσεις

OFFENSIVE	DEFENSIVE
Action of ADA	Deception operations
	OPSEC countermeasures
Targeting for fire and maneuver	Aerial platform tracking

Εικόνα 15: επιθετικές και αμυντικές C-IMINT επιχειρήσεις. Η εικόνα ελήφθη από τη σελίδα 36 του *U.S. Army Counterintelligence Handbook* (2013) του U.S. Department of the Army

Στις τρεις άνω κύριες στρατιωτικές CI επιχειρήσεις έρχεται να προστεθεί η διαδικασία της (αντι)πληροφοριακής έρευνας ως, επίσης, βασικό καθήκον / αρμοδιότητα. Ο όρος διακρίνεται για την ευρύτητά του, έτσι, η κατηγοριοποίηση έστω σε δύο, σύμφωνα με τον αμερικανικό στρατό, τύπους κρίνεται θετική. Κατά τον τρόπο τούτο διεξάγονται: α) αντικατασκοπευτικές έρευνες (CI investigations) και β) έρευνες / μελέτες ικανότητας / καταλληλότητας λήψεως διαβαθμισμένων πληροφοριών από ορισμένο, κατά περίπτωση, προσωπικό (personnel security investigations).¹⁹ Ειδικότερα:

- Οι αντιπληροφοριακές έρευνες (CI investigations) δεικνύουν έρευνες «εθνικής ασφαλείας» υπό την αιγίδα του στρατεύματος. Από την Army Regulation 381-12, *Subversion and Espionage Directed Against The US Army*, (Ιανουάριος 1993), μέχρι την Army Regulation 381-12, *Threat Awareness and Reporting Program*, (Ιούνιος 2016), καταγράφεται η ανάγκη αναφοράς εκ μέρους πολιτικού και στρατιωτικού προσωπικού κάθε είδους υπόπτων δραστηριοτήτων.²⁰ Οι (ύποπτες)

¹⁸ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 36-38

¹⁹ ό. π., σ. 17

²⁰ Βλέπε, π. χ., Army Regulation 381-12, *Threat Awareness and Reporting Program*, Headquarters, Department of the Army, Washington, D.C., Ιούνιος 2016, σ. 1

κύριες δραστηριότητες που εμπίπτουν της ερευνητικής δικαιοδοσίας της αμερικανικής στρατιωτικής αντικατασκοπίας σχετίζονται με κατηγορίες / υποθέσεις: α) εθνικής προδοσίας (treason), β) κατασκοπίας ανεξαρτήτου συνθηκών ειρήνης ή πολέμου (espionage), γ) κατασκοπίας εν καιρώ πολέμου υπέρ του εχθρού (spying), δ) υπονόμευσης / πρόκλησης στάσεως εντός του στρατεύματος (subversion), ε) στάσεως, συνομωσίας, σχεδιασμών ανατροπής της κυβέρνησης (sedition), στ) δολιοφθοράς εκ μέρους αλλοδαπών Υπηρεσιών (sabotage), ζ) τρομοκρατικών ενεργειών κατά του στρατεύματος, η) αυτομόλησης πολιτικού / στρατιωτικού προσωπικού σε εξωτερικές δυνάμεις, θ) ασφάλειας επικοινωνιών, ι) αντιμέτρων τεχνικής παρακολούθησης (technical surveillance countermeasures -TSCM).²¹

- Οι μελέτες ικανότητας / καταλληλότητας λήψεως διαβαθμισμένων πληροφοριών (personnel security investigations) σχετίζονται με το γεγονός της μη εκ των προτέρων εξουσιοδότησης / δικαιώματος κατοχής τέτοιων από άτομα λόγω και μόνο της θέσεως / αξιώματος (by virtue of) που διατηρούν.²² Η απόδοση αυτής της σημαντικότητας δεδομένων έχει να κάνει με την διεκπεραίωση και μόνο συγκεκριμένων καθηκόντων. Πρόσωπα επιφορτισμένα μ' αυτά καλούνται να επιβεβαιώσουν την αξιοπιστία που οφείλει να τα χαρακτηρίζει πριν γίνουν παραλήπτες απόρρητου υλικού. Σημειώνουμε ότι υπό την πίεση δεδομένων κατά περίπτωση συνθηκών δύναται η απόδοση περιορισμένου δικαιώματος πρόσβασης (limited access authorization -LAA) διαβαθμισμένων πληροφοριών στο όποιο εντεταλμένο / ηλεγμένο προσωπικό.²³

Στρατιωτική αντικατασκοπία: πολυεπίπεδη αντικατασκοπία (multidisciplinary counterintelligence -MDCI) και τεχνικά αντίμετρα παρακολούθησης (technical surveillance countermeasures -TSCM) vs ανταγωνιστικών τεχνολογικών μηχανισμών συλλογής πληροφοριών

Η αντίπαλη τεχνολογική συλλεκτική ικανότητα πληροφοριών συνιστά πονοκέφαλο, πέραν αυτού των κλασικών HUMINT απειλών, που οφείλει να αντιμετωπιστεί -το συγκεκριμένο καθήκον αναλαμβάνει η λεγόμενη στρατιωτική *Πολυεπίπεδη Αντικατασκοπία (Multidisciplinary Counterintelligence -MDCI)*.

Πρώτιστο μέλημα / αρχή τής MDCI αποτελεί η χαρτογράφηση των ικανοτήτων τεχνικής υποστήριξης συλλογής πληροφοριών του αλλότριου παράγοντα. Αυτό, σε δεύτερο βαθμό, υποβοηθά στην αποκάλυψη πιθανών οικείων εσωτερικών τρωτοτήτων. Τα κύρια μέτρα σχετίζονται με την: α) προστασία επικοινωνιών ήτοι, με προγράμματα communications security -COMSEC. Η χρήση οπτικών ινών έχει δυσκολέψει την προσπάθεια υποκλοπής μηνυμάτων. Αντίθετα, η χρήση ραδιοσημάτων για επικοινωνιακούς σκοπούς παρουσιάζεται ευάλωτη²⁴, β) μείωση

²¹ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 17-18, 164-175

²² Βλέπε AR 380-5, *Department of the Army Information Security Program*, Headquarters, Department of the Army, Washington, D.C., Σεπτέμβριος 2000, στο <https://fas.org/irp/doddir/army/ar380-5.pdf> εις το οποίο καταφύγαμε την 10^η Οκτωβρίου 2016

²³ Department of the Army, *U.S. Army Counterintelligence Handbook*, ό. π., σ. 21-22

²⁴ Αρχικά οι ραδιοεπικοινωνίες λάβαιναν χώρα μέσω κωδικοποιημένων ή κρυπτογραφημένων μηνυμάτων. Η μη γνώση των κωδικών δεν επέτρεπε τη μετάφραση του μηνύματος. Τα «ασφαλή τηλέφωνα» εδείκνυν, επίσης, ένα τρόπο προστασίας αλλά αντεδείκνυτο για επικοινωνίες μακρινών αποστάσεων. Η πλευρά που επιχειρεί την υποκλοπή στοχεύει, συνηθέστατα, σε διαβαθμισμένες πληροφορίες. Κάποια αντίμετρα που μπορούν να ληφθούν έχουν να κάνουν με τον επανασχεδιασμό του επικοινωνιακού δικτύου, τη συχνή αλλαγή κωδικών, τη γενικευμένη χρήση οπτικών ινών -για

των ηλεκτρομαγνητικών εκπομπών επικοινωνιακών και άλλων μηχανισμών (*emanations security*), γ) χρήση τεχνικών αντιμέτρων (*usage of technical countermeasures*) προς εξουδετέρωση πλεονεκτημάτων που παρέχει στον αντίπαλο ένας, π. χ., επικοινωνιακός ή τηλεπισκοπικός δορυφόρος. Ως αντίμετρα προτείνονται οι ηλεκτρομαγνητικές παρεμβολές, το καμουφλάζ, η μη σταθερή θέση των προς κατόπτευση (κινητών) στόχων, η διακοπή των δραστηριοτήτων που τίθενται στο στόχαστρο κ. λ.²⁵

Κατά την FM 34-7 *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations* (1993) η πολυεπίπεδη αντικατασκοπία: α) συλλέγει στοιχεία σχετικά με αλλοδαπές υπηρεσίες Πληροφοριών και οργανισμούς Ασφαλείας, β) εξουδετερώνει τις προσπάθειες των άνω θεσμών να εισέλθουν εντός του οικείου δικτύου πληροφόρησης, γ) επιβοηθά στη λήψη προστατευτικών μέτρων ως προς τη διεξαγωγή μιας στρατιωτικής ή μυστικής επιχείρησης (*Operations Security -OPSEC*), δ) επικουρεί στην καταστολή στασιαστικών κινημάτων, στην πάταξη του τρομοκρατικού φαινομένου όπως και στην καταδίωξη ομάδων που ασκούνται στο διεθνικό υψηλής έντασης έγκλημα, ε) συμμετέχει στην προστασία ευαίσθητων επιχειρήσεων εν καιρώ ειρήνης ή κρίσεων (*peacetime contingency operations -PCO*) κατά την εκτέλεση των οποίων απαιτείται άμεση ανάπτυξη περιορισμένων στρατιωτικών δυνάμεων προς επιβολή αποφάσεων οργανισμών της διεθνούς κοινότητας.²⁶ Η τελευταία αποστολή συνδέεται με δράσεις που μεταξύ άλλων ίσως απαιτήσουν μάχη χαμηλής έντασης ²⁷ (*Low Intensity Conflict -LIC*). Η αναλυτική διαδικασία της πολυεπιπέδου αντικατασκοπίας όσον αφορά στο συγκεκριμένο σημείο αποσκοπεί: α) στη 'φυσική' εκτίμηση της δυνητικής περιοχής μάχης (έδαφος, καιρικές συνθήκες κ. λ.), β) στην εκτίμηση της τιθέμενης απειλής (ποιος απειλεί, είδος απειλής, πιθανός χρόνος εκδήλωσης, πιθανό σημείο εκδήλωσης, τρόπος εκδήλωσης κ. λ.), γ) στην εκτίμηση των οικείων τρωτοτήτων επικοινωνιών, πληροφόρησης, σχεδιασμού / υποστήριξης μάχης κ. λ., δ) στην επιλογή / ανάπτυξη αντιμέτρων για την θεραπεία των συγκεκριμένων τρωτοτήτων, ε) στην εκτίμηση της δράσης των αντιμέτρων σε σχέση με την πορεία της επιχείρησης.²⁸

Περαιτέρω, εντός των καθηκόντων της MDCI εμπεριέχεται η αναγνώριση: α) διαδρομών εχθρικών δορυφορικών συστημάτων που υπερίπτανται εγχώριων ή μη εδαφών, β) ζωνών οπισθοφυλακής εντός των οποίων ενδέχεται να δράσει αιφνιδιαστικά ο αντίπαλος, γ) περιοχών που δέχτηκαν ασυνήθιστη εχθρική ηλεκτρονική δραστηριότητα, δ) ευάλωτων οικείων θέσεων και υποδομών υπό την έννοια του φόβου εκδήλωσης ενός σαμποτάζ ή μιας υπονομευτικής ενέργειας.²⁹

Είναι φανερό πως η MDCI συνθέτει είδος εντός του οποίου συνεργάζονται ο ανθρώπινος παράγοντας και ο παράγοντας των επιστημών της φυσικής, της μηχανικής, της οπτικής, των ηλεκτρονικών εφαρμογών, της μετεωρολογίας, της διαστημικής κ. λ. Πάρα τούτα, και ενώ υποτίθεται ένας οιονεί παραγκωνισμός του

περισσότερα βλέπε Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, Brassey's, Inc., Washington, D. C., ΗΠΑ, 2002³, σ. 116

²⁵ Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 114-116

²⁶ FM 34-7 *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations*, Headquarters, Department of the Army, Washington, D.C., 1993

²⁷ Για μια ιδέα περί των βασικών αρχών του όρου βλέπε FM 34-7 *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations*, Headquarters, Department of the Army, Washington, D.C., 1993

²⁸ FM 34-7 *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations*, Appendix C «Multidiscipline Counterintelligence Support to Low-Intensity Conflict Operations», ό. π.

²⁹ FM 34-60 *Counterintelligence*, Chapter 4 "CI Analysis and Production", Headquarters, Department of the Army, Washington, D.C., 1995, σ. 9

ανθρώπου από τις «μηχανές», η αναλυτική διαδικασία που εξαρτάται από την αντίληψη του φυσικού προσώπου δεν μπορεί να υποκατασταθεί από κάποιο software. Κατ' αυτήν την έννοια και σύμφωνα με την FM 34-60 *Counterintelligence* του 1995 ένας αναλυτής MDCI μεταξύ άλλων: α) διερευνά το εύρος της αντίπαλης πολυεπίπεδης κατασκοπευτικής απειλής όσον αφορά σε τεχνολογικά μέσα συλλογής πληροφορίας, β) εξετάζει τρόπους εξαπάτησης του ανταγωνιστή, γ) καταθέτει προτάσεις ως προς την αξιοποίηση των κενών ασφαλείας του τελευταίου, δ) εστιάζει την προσοχή σε αλλότριους στόχους / assets εφευρίσκοντας τρόπους ουδετεροποίησης, χειραγώγησης ή καταστροφής αυτών, ε) συμμετέχει στον εντοπισμό οικείων προβληματικών σημείων και αναγκών, στ) προτείνει λύσεις ως προς την ανακούφιση των τελευταίων.³⁰

Στην MCWP 2-14 (2000) και στις σελίδες 7-28 – 7-31 γίνεται αναφορά σε αντίμετρα επίβουλων επιχειρήσεων τεχνικής επιτήρησης (technical surveillance countermeasures -TSCM). Το TSCM συνθέτει σύνολο βασικών αμυντικών, αλλά όχι μόνο, αντικατασκοπευτικών πρακτικών με σκοπό την προστασία των εγχωρίων ηλεκτρονικών / τηλεπικοινωνιακών συστημάτων / σημάτων (audio, video, digital, computer signals κ. λ.) που τελούν υπό το φάσμα απειλής ξένων Υπηρεσιών. Ένα TSCM πρόγραμμα επιχειρεί κατά κύριο λόγο τον εντοπισμό / αντιμετώπιση των όποιων εχθρικών hi-tech μηχανισμών / πόρων / δυνατοτήτων υποκλοπής μέσω τεσσάρων βημάτων ήτοι, της ανίχνευσης (detection), της ακύρωσης / εκμηδένισης (nullification), της απομόνωσης (isolation) αλλά και της ενημέρωσης / εκπαίδευσης (education) του οικείου προσωπικού.³¹

Η DoDI 5240.05 αποδίδει στο TSCM τεχνικές προς ...ανίχνευση, εξουδετέρωση και παραπλάνηση εχθρικών τεχνολογιών αναγνώρισης, παρακολούθησης και επιτήρησης όπως και τεχνικές προς αντιμετώπιση περιστατικών που αφορούν σε μη εξουσιοδοτημένη [τεχνική] πρόσβαση σε πληροφοριακό υλικό.³² Στη Joint Publication 1-02 της 8^{ης} Νοεμβρίου 2010 τονίζεται ότι TSCM σημαίνει σύνολο πρακτικών με σκοπό την ανίχνευση / εξουδετέρωση μιας ποικιλίας εχθρικών τεχνολογιών εισχώρησης σε ευαίσθητες περιοχές. Μια τέτοια τεχνολογία περιλαμβάνει τη χρήση οπτικών, ηλεκτρο-οπτικών, ηλεκτρομαγνητικών, ακουστικών κ. λ. μέσων μετάδοσης πληροφοριών -την πιθανότητα αυτής της μετάδοσης καλείται να αναστείλει ένα TSCM πρόγραμμα.³³ Η Intelligence Community Standard (ICS) 700-1 επισημαίνει πως TSCM δεν δηλώνει άλλο από σχεδιασμούς φυσικής / τεχνικής υφής με σκοπό την αντιμετώπιση εχθρικών δυνατοτήτων επιτήρησης / παρακολούθησης και υποκλοπής, εικόνων, συνομιλιών, γενικότερα, κρίσιμων πληροφοριών.³⁴ Η ICD 702 μη διαφοροποιούμενη από τα ήδη αναφερόμενα κάνει λόγο για συγκεκριισμό δύο διακριτών πεδίων ήτοι, της αντικατασκοπίας και της ασφαλείας.³⁵ Παρόμοιες αποτυπώσεις ανακαλύπτουμε στο *Redefining Security: A Report to the Secretary of*

³⁰ FM 34-60 *Counterintelligence*, Chapter 4 “CI Analysis and Production”, ό. π., σ. 3

³¹ MCWP 2-14, ό. π., σ. 7-28 – 7-31. Επικουρικά βλέπε στη σελίδα 7-30 περί TSCM Survey, TSCM Inspection και TSCM Pre-construction Assistance. Στη σελίδα 7-28 καταγράφεται η διαφοροποίηση μεταξύ TSCM και TEMPEST (Transient Electromagnetic Pulse Emanation Standard), ειδικότερα περί TEMPEST βλέπε *Terms & Definitions of Interest for Counterintelligence Professionals*, επιμ. Reagan M., 2014, σ. 320-321

³² DoDI 5240.05, *Technical Surveillance Countermeasures (TSCM)*, Department of Defense, Απρίλιος 2014

³³ JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 16 July 2014), σ. 255

³⁴ ICS 700-1, *Glossary of Security Terms, Definitions, and Acronyms*, ODNI, Απρίλιος 2008, σ. 27

³⁵ ICD 702, *Technical Surveillance Countermeasures*, ODNI, Φεβρουάριος 2008

Defense and the Director Central Intelligence της Joint Security Commission³⁶, στην FM 2-22.2³⁷ επίσης στα Army Regulation (AR) 381-14 του 1986, του 2002 και του 2015.³⁸

Ο Frederick Wattering αποδίδει το TSCM ως *technical security countermeasures*. Η χρησιμοποίηση της λέξης *security* αντί της λέξης *surveillance* δεν είναι τυχαία καθώς όπως σημειώνει ...TSCM σημαίνει σύνολο διαδικασιών με σκοπό την ανίχνευση προσπαθειών «τεχνικών παρεισδύσεων» ξένων Υπηρεσιών εντός οικείων περιβαλλόντων προς άγρα πληροφοριών... Οι συγκεκριμένες προσπάθειες / σχεδιασμοί σχετίζονται με ηλεκτρονικές ηχητικές και όχι φωτογραφικές / οπτικές υποκλοπές. Τα TSCMs, συνεχίζει ο ερευνητής, δεικνύουν καθήκον όλων των ανά τον κόσμο μεγάλων υπηρεσιών Ασφαλείας και Πληροφοριών.³⁹

Η συλλογή της πληροφορίας όλο και περισσότερο επαφίεται στην υψηλή τεχνολογία -η πολυεπίπεδη αντικατασκοπία εξυπηρετεί εκ πρώτης όψεως έναν στόχο: την αντιμετώπιση των τεχνολογικών κατασκοπευτικών ατού του αντιπάλου. Η κωδικοποίηση, η κρυπτογράφηση, η κάλυψη, η παραλλαγή δεικνύουν κάποιους τρόπους μέσω των οποίων δυνάμεθα να αμυνθούμε ή / και να επιτεθούμε. Η χρήση, π. χ., του καμουφλάζ ενισχύει την προσπάθεια «σβησίματος» στοιχείων με έναν, ωστόσο, διττό χαρακτήρα / σκοπό: α) την απόκρυψη υπό την κλασική έννοια της προστασίας και β) την απόκρυψη → συνακόλουθη «ηθελημένη επίδειξη» υπό την έννοια της επιθετικής παραπλάνησης.

Κατά τον τρόπο τούτο και επί τη βάσει των ανωτέρω υποστηρίζουμε ότι: α) η πολυεπίπεδη αντικατασκοπία επωμίζεται το καθήκον αντιμετώπισης της πολυεπίπεδης (τεχνικής) κατασκοπίας, β) η πολυεπίπεδη αντικατασκοπία αν και κάνει χρήση υψηλής τεχνολογίας δεν μπορεί παρά να διατηρήσει τον άνθρωπο ως κύριο παράγοντα στη διαδικασία ανάλυσης / εκτίμησης δεδομένων, γ) οι σκοποί της αμυντικής πολυεπίπεδης αντικατασκοπίας δεν διαφέρουν από αυτούς της κλασικής, συμπεριλαμβανομένης της αντιμετώπισης νέων απειλών (τρομοκρατία, οργανωμένο έγκλημα) -ό,τι διαφέρει σχετίζεται με τα μέσα, δ) η επιθετική πολυεπίπεδη αντικατασκοπία χρησιμοποιώντας μεθόδους χειραγώγησης / εξαπάτησης εισδύει εντός του ανταγωνιστικού δικτύου, ουσιαστικά κατασκοπεύει ή χειραγωγεί τον αντίπαλο στα πρότυπα του κλασικού counterespionage.

³⁶ Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Φεβρουαρίου 1994, σ. 61

³⁷ FM 2-22.2, *Counterintelligence*, Headquarters, Department of the Army, Washington, D.C., Οκτώβριος 2009, σ. 6-5

³⁸ AR 381-14, *Technical Surveillance Countermeasures*, Headquarters, Department of the Army, Washington, D.C., Οκτώβριος 1986, AR 381-14, *Technical Counterintelligence*, Headquarters, Department of the Army, Washington, D.C., Σεπτέμβριος 2002, AR 381-14, *Technical Surveillance Countermeasures*, Headquarters, Department of the Army, Washington, D.C., Φεβρουάριος 2015

³⁹ Wattering L. Frederick, "Counterintelligence: The Broken Triad", *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 3, 2000, σ. 277

Στρατιωτική αντικατασκοπία: τακτική παραπλάνηση / αντιπαραπλάνηση⁴⁰

Η παραπλάνηση

Ο πόλεμος βασίζεται στην παραπλάνηση

Sun Tzu⁴¹

Είναι απολύτως σημαντικό να διαδίδετε φήμες εντός του εχθρικού στρατοπέδου σχετικά με κάποια σχέδιά σας, κατόπιν, πράττετε κάτι άλλο...

Αυτοκράτωρ Μαυρίκιος
The Strategikon, 600 μ. Χ.

Οι μάχες κερδίζονται με αιματοχυσία και ελιγμό. Όσο ικανότερος είναι ο διοικητής τόσο μεγαλύτερη είναι η συνεισφορά του στον δεύτερο. Όσο λιγότερο ικανός είναι τόσο αποζητά την πρώτη

Winston Churchill⁴²

Ως στρατιωτική παραπλάνηση ορίζεται η τέχνη της εξαπάτησης του εχθρού με σκοπό την ανάληψη (ή μη) δράσεως εξ αυτού, δράσεως της οποίας το αποτέλεσμα συντείνει στην αποδυνάμωση της στρατηγικής ή τακτικής του θέσεως

Charles Cruickshank⁴³

Ουσιαστική επιθετική αποστολή μιας υπηρεσίας CI δεικνύει η διενέργεια επιχειρήσεων παραπληροφόρησης / παραπλάνησης του αντιπάλου. Αυτό σημαίνει πως στον ίδιο χρόνο επιφορτίζεται με την προστασία έναντι ανάλογων εχθρικών δράσεων -πρόκειται για τη λεγόμενη *counterdeception* αναγκαιότητα και πρακτική. Η Cynthia Grabo γράφει, εν έτει 2004, πως η έννοια *παραπλάνηση*, ως αντικείμενο, συνθέτει ένα από τα λιγότερο ανεπτυγμένα στο χώρο της μελέτης της (αντι)πληροφόρησης με πλήθος στρατιωτικών παρουσιάσεων να μη λαμβάνουν υπόψη τη σημασία της εξαπάτησης στον πόλεμο. Η ίδια επικεντρώνει σε δύο αιτίες με πρώτη την όχι συχνή εκδήλωσή της (τουλάχιστον αυτό συμβαίνει σε καιρό ειρήνης) και δεύτερη τη μυστικότητα με την οποία περιβάλλεται.⁴⁴

Ο Clausewitz, παρά το ότι δεν δίδει έμφαση στη σημαντικότητα της παραπλάνησης στον πόλεμο, σημειώνει πως η αδύναμη πλευρά έχει κάθε λόγο να καταφύγει σ' αυτήν ως τελευταία ελπίδα.⁴⁵ Κάτι τέτοιο συνεπάγεται την ύπαρξη μιας αντίστροφης σχέσεως μεταξύ ισχύος και κινήτρου προσφυγής σε σχεδιασμούς εξαπάτησης. Ο Michael Handel γράφει πως η συγκεκριμένη παρατήρηση βρίσκει συχνά την απόδειξή της εντός της σύγχρονης στρατιωτικής ιστορίας ξεκινώντας από

⁴⁰ Στο παρόν κεφάλαιο οι όροι *παραπλάνηση*, *παραπληροφόρηση*, *εξαπάτηση*, *deception*, *misinformation*, *disinformation* κ. λ. αποδίδουν λίγο έως πολύ το ίδιο νόημα

⁴¹ Sun Tzu, *The Art of War*, μτφρ. Griffith B. Samuel, Oxford University Press, New York, 1973, σ. 66

⁴² Churchill W., *The World Crisis: 1915*, Charles Scribner's Sons, New York, 1923, σ. 5

⁴³ Cruickshank Charles, *Deception in World War II*, Oxford University Press, New York, 1980, σ. i

⁴⁴ Grabo C., *Anticipating Surprise. Analysis for Strategic Warning*, University Press of America, Inc., USA, 2004, σ. 120-121

⁴⁵ Carl von Clausewitz, *On War*, επιμ. / μτφρ. Howard M., Paret P., Princeton University Press, Princeton, 1976, σ. 203. Ο J. Bowyer, προς επίρρωση του Clausewitz, γράφει, λ. χ., πως η Ρώμη χρησιμοποίησε την παραπλάνηση ενόσω υπήρξε μικρή και αδύναμη. Όταν μεταμορφώθηκε σε αυτοκρατορία η συγκεκριμένη πρακτική παρήκμασε. Οι αδύναμοι αντίπαλοί της κατέρρεαν μπροστά στην ισχύ της, μια ισχύ που εργαλειοποιόταν μέσω άμεσης προσέγγισης -για μια εικόνα βλέπε Bowyer J., *Cheating*, New York, St. Martin's, 1980, σ. 22-23

τον Β' Π. Π. με τους Βρετανούς να κινητροδοτούνται πολύ περισσότερο στη χρήση «τεχνασμάτων» από τους ισχυρότερους Γερμανούς.⁴⁶

Σύμφωνα με τους Shulsky και Schmitt εξαπάτηση σε βάρος ανταγωνιστού σημαίνει κατά βάσει αποπροσανατολισμό του τελευταίου σε πολιτικό, στρατιωτικό ή οικονομικό επίπεδο. Αντικειμενικός σκοπός του διαπράττοντα τον ελιγμό είναι η αντίδραση του ανταγωνιστικού παράγοντα με τρόπο που υπηρετεί το συμφέρον του πρώτου τη στιγμή που ο δεύτερος πιστεύει ακριβώς το αντίθετο, ότι, δηλαδή, εξυπηρετεί το δικό του.⁴⁷ Είναι η παραπληροφόρηση συνδεδεμένη με την έννοια της *πληροφοριακής αποτυχίας (intelligence failure)*; Οπωσδήποτε η επιτυχία της μιας πλευράς υπαινίσσεται την αστοχία της άλλης, ωστόσο, το ποσοστό συμμετοχής μιας επιχείρησης παραπληροφόρησης στη λανθασμένη εκτίμηση του αντιπάλου δεν μπορεί να μετρηθεί.⁴⁸ Οι επιχειρήσεις παραπληροφόρησης αν και συνηθίζονται σε περιόδους πολέμου, δεν αποκλείονται σε ανάλογες ειρήνης -βέβαια στην τελευταία περίπτωση δύσκολα αποκαλύπτονται έστω και αν έχουν κυλήσει έτη.⁴⁹ Οι Shulsky και Schmitt προβαίνοντας σε έναν ακόμα διαχωρισμό ομιλούν για *τακτική και στρατηγική παραπληροφόρηση / παραπλάνηση* με την πρώτη να λαμβάνει χώρα συχνότερα.⁵⁰

⁴⁶ Handel Michael, "Intelligence and Deception" στο *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, επιμ. George Roger, Kline Robert, Rowan & Littlefield Publishers, Inc., USA, 2006, σ. 360

⁴⁷ Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 117

⁴⁸ Άλλωστε η παραπλάνηση σχετίζεται με την οικεία ικανότητα άρνησης (denial) πληροφοριών στον αντίπαλο -για μια άποψη κατάφυγε στο Shulsky A., "Elements of Strategic Denial and Deception" στο *Strategic Denial and Deception*, επιμ. Godson R., Wirtz J, Transaction Publishers, New Brunswick / New Jersey, 2002, σ. 16. Για μια σύνδεση των εννοιών denial και deception, γνωστές ως D&D, βλέπε Devin D. Jessee, "Tactical Means, Strategic Ends: Al Qaeda's Use of Denial and Deception" στο *Terrorism and Political Violence*, Volume 18, Issue 3, 2006, σ. 367-388 και Godson R., Wirtz J., "Strategic Denial and Deception" στο *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 4, 2000, σ. 424-426. Από τη μεριά του ο Edward Waltz εναλλάσσει τον όρο *denial* / *άρνηση* με τον όρο *dissimulation* / *απόκρυψη*. Σχετικά με την παραπλάνηση (deception ή simulation) σημειώνει πως αυτή διακρίνεται σε *m-type* και *a-type*. Η πρώτη επιχειρεί την πλασματική μείωση του περιβάλλοντος ασάφειας οδηγώντας το θύμα, μέσω μιας αίσθησης σιγουριάς, μακριά από την αλήθεια. Η δεύτερη επιχειρεί την πλασματική επαύξηση του περιβάλλοντος ασάφειας με σκοπό την αποδιοργάνωση της λειτουργίας λήψεως αποφάσεων του δεχόμενου την εξαπάτηση. Η παραπλάνηση τύπου *m-type* καλείται από τον Waltz και *misdirection deception*, η, δε, τύπου *a-type* καλείται και *ambiguity deception* -για μια εικόνα βλέπε Waltz Edward, *Knowledge Management in the Intelligence Enterprise*, Artech House, Inc., Norwood / Massachusetts, 2003, σ. 229, Daniel D., Herbig K., "Propositions on Military Deception" στο *Strategic Military Deception*, επιμ. Daniel D., Herbig K, Pergamon, New York, 1982, σ. 5, Waltz Edward, *Information Warfare Principles and Operations*, Artech House, Inc., Norwood / Massachusetts, 1998, σ. 211. Για μια περαιτέρω ανάλυση γύρω από ειδικότερους τύπους, είδη και κατηγορίες παραπλάνησης βλέπε Bennett Michael, Waltz Edward, *Counterdeception Principles and Applications for National Security*, Artech House, Inc., Norwood / Massachusetts, 2007, σ. 20-33. Τέλος παραθέτουμε τα λόγια του John Yurechko, αξιωματούχου της DIA, σε σχετική ενημέρωση στο Department of Defense την 8^η Οκτωβρίου 2002: *...denial and deception are interrelated. Denial is the basis for a successful deception. One cannot manipulate or blur the truth or lie convincingly unless the truth is first concealed* -για περισσότερα βλέπε Caddell J., *Deception 101-Primer on Deception*, σ. 18 στα <http://www.au.af.mil/au/awc/awcgate/ssi/deception.pdf> και <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=3787> όπου καταφύγαμε την 9^η Αυγούστου 2014

⁴⁹ Όπως και δυσκολότερα πετυχαίνουν καθώς η αντίδραση του υποψήφιου θύματος δεν επηρεάζεται από την πίεση του χρόνου και, εν γένει, την πολεμική άμεση αναγκαιότητα

⁵⁰ Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 117-118, επίσης, Bennett Michael, Waltz Edward, *Counterdeception Principles and Applications for National Security*, ό. π., σ. 8. Όσον αφορά στα προαπαιτούμενα μιας πετυχημένης επιχείρησης παραπλάνησης τονίζουμε την αναγκαιότητα: α) ελέγχου κατά το δυνατό των καναλιών συλλογής πληροφοριών του αντιπάλου και κατ' επέκταση ελέγχου της πληροφοριοδότησής του, β) παροχής πειστικών μεν,

Ο John Bowyer Bell υποστηρίζει ότι παραπλάνηση σημαίνει ενσυνείδητη προσπάθεια ενός δρώντα να μεταλλάξει την αντίληψη ενός άλλου μεταφέροντας χειραγωγημένες εικόνες στο περιβάλλον του τελευταίου. Η όλη δράση βασίζεται στη χρήση τεχνασμάτων βάσει των οποίων παρουσιάζονται ή αποκρύπτονται γεγονότα / δεδομένα, ανύπαρκτα στην πρώτη περίπτωση, υπαρκτά στη δεύτερη. Ουσιαστικά ομιλούμε για επιχείρηση επιβολής του αναληθούς έναντι του αληθούς με την αντίδραση του στόχου να υποδεικνύει την επιτυχία ή αποτυχία του επιτιθέμενου προδιαγράφοντας τη συνέχιση, την προσαρμογή ή τη διακοπή του εγχειρήματος.⁵¹

Ο Conley Hampton, επισμηναγός της αμερικανικής πολεμικής αεροπορίας, τονίζει το κρίσιμο της παραπλάνησης εν καιρώ πολέμου. Σύμφωνα με τα γραφόμενά του μια σχετική επιτυχία δύναται να επιφέρει στον αντίπαλο: α) κατασπατάληση υλικών και ανθρωπίνων πόρων, β) άσκοπη διασπορά δυνάμεων, γ) αποδυνάμωση στο πεδίο μάχης, δ) ενίσχυση θέσεων σε λάθος τόπο και χρόνο, ε) διάσπαση προσοχής, στ) απομείωση ετοιμότητας, ζ) τρώση βεβαιότητας και η) επαύξηση σύγχυσης. Όλα αυτά κατατείνουν σε μειωμένο πολεμικό κόστος για τον επιχειρών την παραπλάνηση και σε αντίστοιχο αυξημένο για τον δέχοντα. Ο ίδιος διαχωρίζει την παραπλάνηση σε αμυντική και επιθετική με την πρώτη να ασκείται στην απόκρυψη των δυνατοτήτων και προθέσεων μας (μορφή άρνησης / denial) και τη δεύτερη να επικεντρώνει σε επιθετικές επιδιώξεις. Τέλος, μια άλλη μορφή κατηγοριοποίησης αφορά: α) στο θέατρο των πολεμικών τεκταινομένων και β) στον πλήρη (στρατηγικό) αιφνιδιασμό του αντιπάλου κάτι, οπωσδήποτε, πολύ φιλόδοξο.⁵²

Ο Joseph W. Caddell κάνει διάκριση μεταξύ των λέξεων *disinformation* και *misinformation*. Αν και οι δύο μεταφράζονται στην ελληνική ως *παραπληροφόρηση*, ο μελετητής υιοθετεί τη χρήση της πρώτης ως *εσκεμμένη παραπληροφόρηση*, άρα, παραπλάνηση, σε αντίθεση με τη δεύτερη που υποδηλώνει, απλώς, μια λανθασμένη πληροφορία.⁵³ Σχετικά με προβληματισμούς εύρους ή φύσης παραπλάνησης ακολουθείται η προσέγγιση των Shulsky, Schmitt και Hampton.

Συνεχίζοντας την περί ορισμών έρευνα διαπιστώνουμε ότι οι Donald Daniel και Katherine Herbig ορίζουν την παραπλάνηση ως ...σκοπίμως στρεβλή παρουσίαση της πραγματικότητας προς χειραγώγηση των πιστεύω του αντιπάλου και κατ' επέκταση των ενεργειών του με τελική κατάληξη την απόκτηση πλεονεκτήματος εκ μέρους του

αναληθών δε πληροφοριών, γ) ανατροφοδότησης (feedback)· η ανατροφοδότηση είναι ιδιαίτερος σημαντική καθώς επιτρέπει στον παραπληροφορών να αντιληφθεί την επιτυχία ή μη του εγχειρήματός του -για περισσότερες λεπτομέρειες βλέπε Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 118-121. Οι Roy Godson και James Wirtz συμπληρώνουν τα άνω προαπαιτούμενα προσθέτοντας σ' αυτά τη γνώση της αμυντικής κουλτούρας του αντιπάλου, κατηγοριοποιούν, δε, μια δράση D&D στις ασύμμετρες επιχειρήσεις επισημαίνοντας, σε δεύτερο χρόνο, την αξία χρήσης υψηλής τεχνολογίας ως προς την επιτυχία της -για μια πληρέστερη εικόνα κατέφυγε στο Godson R., Wirtz J., "Strategic Denial and Deception" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 426, 430-431

⁵¹ Bell B. J., "Toward a Theory of deception" στο *International Journal of Intelligence and CounterIntelligence*, Volume 16, Issue 2, 2003, σ. 244, 246

⁵² Hampton C., *A history of camouflage, concealment and deception*, εργασία κατατεθειμένη στο Air War College, Alabama / USA, 1988, σ. 3-4

⁵³ Ο ίδιος προβαίνει σε μια ακόμα σημείωση αντιδιαστέλλοντας τις έννοιες *fabrication* και *manipulation*. Και οι δύο αναφέρονται στο deception, αν και με διαφορετικό τρόπο, με την πρώτη να δηλώνει την ψευδή πληροφόρηση και τη δεύτερη την τεχνικά ορθή που, ωστόσο, παρουσιάζεται με ασαφή τρόπο προς εξαπάτηση του λήπτη -για περισσότερες λεπτομέρειες βλέπε Caddell J., *Deception 101-Primer on Deception*, σ. 1-2 στη διαδικτυακή τοποθεσία <http://www.au.af.mil/au/awc/awcgate/ssi/deception.pdf> με ημερομηνία ανάκτησης τη 19^η Ιουλίου 2014

οργανωτή της επιχείρησης. Το αποτέλεσμα της παραπληροφόρησης δύναται να εκτιμηθεί μόνο σε σύγκριση με το αποκομισθέν ποσό ωφελείας του τελευταίου.⁵⁴

Ο Jon Latimer στο *Deception in Warfare* ορίζει την παραπλάνηση ως χειραγώγηση της αντίληψης του αντιπάλου υπό την έποψη τεσσάρων βασικών στόχων, αναλυτικότερα: α) της εξαπάτησής του γύρω από τις προθέσεις του ασκών τον σχεδιασμό, β) του αποπροσανατολισμού του με σκοπό την ανάληψη πρωτοβουλιών κάθε άλλο παρά ωφελίμων για τα συμφέροντά του, γ) του αιφνιδιασμού του και δ) της μείωσης (οικείων) απωλειών σε περίπτωση μάχης. Όσον αφορά στα προαπαιτούμενα μιας επιτυχημένης σχετικής δράσης δεν διαφοροποιείται ουσιαστικά από την JP 3-13.4.⁵⁵

Ο Barton Whaley συμφωνεί εμμέσως με τον Latimer γράφοντας ότι παραπλάνηση δεν σημαίνει κάτι διάφορο από «στρέβλωση αλήθειας» με σκοπό ...τη διακήρυξη του ψεύδους μπροστά στα μάτια της τελευταίας. Ο ίδιος κατηγοριοποιεί την παραπλάνηση σε δράση με σκοπό την απόκρυψη της πραγματικότητας -*dissimulation* και σε δράση με σκοπό την ενεργητική εξαπάτηση του αντιπάλου -*simulation*. Πριν τη χάραξη ενός σχεδιασμού παραπληροφόρησης το όποιο επιτελείο οφείλει να λάβει υπόψη τους στρατηγικούς σκοπούς της ηγεσίας και να σταθμίσει την (προσδοκώμενη) αντίδραση του αντιπάλου. Κατόπιν επιχειρείται: α) προσδιορισμός μέσων εγχειρίματος, β) απόκρυψη πραγματικότητας, γ) απόδοση χαλκευμένων πληροφοριών, δ) έλεγχος αποδοχής ή μη της χειραγωγημένης πληροφόρησης από τον αντίπαλο.⁵⁶

Ο Michael Handel θεωρεί πως η παραπλάνηση δεν είναι τίποτα άλλο από εκδήλωση δράσεως προκειμένου να πολλαπλασιαστούν οι οικείες πιθανότητες κατίσχυσης. Ο ερευνητής επισημαίνει ότι μια πετυχημένη παραπλάνηση μεταξύ άλλων: α) εξαπατά τον εχθρό σχετικά με τις προθέσεις μας και β) εξαπατά τον εχθρό σχετικά με τις δυνατότητές μας.⁵⁷

Οι Charles Fowler και Robert Nesbit επικεντρώνουν στους κανόνες μιας πετυχημένης παραπλάνησης. Σύμφωνα με αυτούς απαιτείται: α) να αφεθεί ο αντίπαλος στην πίστη των πραγμάτων που τον ικανοποιεί, β) να υπάρξει ικανή ανατροφοδότηση / αναπληροφόρηση, γ) να διατηρηθεί η μυστικότητα της επιχείρησης, δ) να συνάδει (η επιχείρηση) με το masterplan εξυπηρετώντας τους ευρύτερους σκοπούς του.⁵⁸ Η van Cleave τονίζει δύο απαραίτητες συνιστώσες: α) ο ανταγωνιστής δεν πρέπει να ανακαλύψει τι επιζητούμε να αποκρύψουμε και β)

⁵⁴ Daniel D, Herbig K., *Strategic Military Deception*, Pergamon, N. Υόρκη, 1982, σ. 3, 5

⁵⁵ Latimer J., *Deception in Warfare*, Overlook Press, Woodstock, New York, 2001, σ. 62 και Martin Charmaine, *Military Deception Reconsidered* (διατριβή κατατεθειμένη στο Naval Postgraduate School), Monterey / California, 2008, σ. 13. Σχετικά με το φλέγον ζήτημα των απωλειών ο Scot Macdonald ανατρέχοντας στον A. Brown σημειώνει πως κατά την εισβολή στη Νορμανδία, εν μέσω παραπλανητικών σχεδιασμών εις βάρος των Γερμανών, οι αμερικανικές δυνάμεις απώλεσαν 34.000 στρατιώτες. Κατά τη διάρκεια της προέλασης από τη Γαλλία προς τη Γερμανία, όταν η πρακτική της παραπλάνησης ατόνησε, αν δεν απουσίασε εντελώς, οι αμερικανικές απώλειες έφτασαν τις 86.000 -για λεπτομέρειες βλέπε Macdonald Sc., *Propaganda and Information Warfare in the Twenty-First Century*, Routledge, UK, 2007, σ. 72

⁵⁶ Whaley B., "Toward a General Theory of Deception" στο *Military Deception and Strategic Surprise*, Frank Cass and Co. Ltd, London, 1982, σ. 182-189, επίσης βλέπε Grabo C., *Anticipating Surprise. Analysis for Strategic Warning*, ό. π., σ. 122-128

⁵⁷ Handel M., "Intelligence and Deception" στο *Military Deception and Strategic Surprise*, ό. π., σ. 122-132

⁵⁸ Fowler C., Nesbit R., "Tactical Deception in Air-Land Warfare" στο *Journal of Electronic Defense*, Ιούνιος 1995, σ. 42-44, 76

οφείλουμε να γνωρίζουμε κάθε τι που ο τελευταίος σκέπτεται ειδικά όταν η σκέψη του έρχεται σε αντίθεση με αυτό που επιχειρούμε να του υποβάλλουμε.⁵⁹

Η αμερικανική σχολή σκέψης γύρω από τις επιχειρήσεις πληροφόρησης / πληροφοριακές επιχειρήσεις ή, αλλιώς, τον πληροφοριακό πόλεμο (information operations -IO / information warfare -IW) κατανοεί την παραπλάνηση ως ...μέσον εξαπάτησης του αντιπάλου με σκοπό την ανάληψη εξ αυτού δράσεως που κάθε άλλο παρά εξυπηρετεί τα συμφέροντά του.⁶⁰ Αλήθεια είναι πως ενωρίτερα η στρατιωτική παραπλάνηση είχε οριστεί κατά τι πληρέστερα ως ...δράση με σκοπό την απόκρυψη σχεδιασμών ή τη λανθασμένη εκτίμηση από τους αντιπάλους decisionmakers ή την απόδοση χειραγωγημένης πληροφόρησης περί οικείων ή φίλιων στρατιωτικών δυνατοτήτων, προθέσεων ή δυνητικών επιχειρήσεων ... δράση που κατατείνει στην ανάληψη κινήσεων [εκ μέρους του αντιπάλου] που ουσιαστικά πριμοδοτούν την επιτυχία των ημών σχεδιασμών.⁶¹

Βάσει δόγματος του 2005 της πολεμικής αεροπορίας των ΗΠΑ η στρατιωτική παραπλάνηση εμπίπτει της έννοιας των επιχειρήσεων επηρεασμού (influence operations) με κύριο στόχο την επίτευξη καθοδήγησης της σκέψης και της συμπεριφοράς του ανταγωνιστή προς όφελος του «καθοδηγητή». Το συγκεκριμένο δόγμα αντιλαμβάνεται την παραπληροφόρηση -την πληροφορία καθαυτή- ως όπλο μιας συνολικότερης προσπάθειας που έχει να κάνει με τη λεγόμενη πληροφοριακή υπερεπάρκεια / ανωτερότητα (information superiority) -ακριβώς αυτή η ανωτερότητα δεικνύει το *raison d'être* του πληροφοριακού πολέμου.⁶²

⁵⁹ Η ίδια συμπληρώνει την ανάγκη ύπαρξης ανατροφοδότησης (feedback loop, όπως γράφει) μνημονεύοντας τα λόγια του ιστορικού F. H. Hinsley κατά τον οποίο ...*We were able to locate, early on, the entire German espionage network in Britain, eliminate parts of it and use others to feed Hitler disinformation. We were also able to learn Hitler's thinking about where and when the invasion would eventually come, play to his prejudices and hunches, and learn when and whether he took our bait. We were reading his mind all the time...* -για περισσότερα βλέπε van Cleave, M., "Guide to the Study of Intelligence. What is Counterintelligence? A Guide to Thinking and Teaching about CI" στο *The Intelligence Journal of U.S. Intelligence Studies*, Volume 20, Number 2, 2013, σ. 64, επίσης, "The Masters of Deception: At England's Bletchley Park, recalling the Code-Breakers and Illusion-Makers", *The Washington Post*, 31 Μαΐου 1999, C-1

⁶⁰ JP 3-13, *The U.S. Joint Doctrine for Information Operations*, 1998

⁶¹ JP 3-58, *The U.S. Joint Doctrine for Military Deception*, 1996. Κατά τον ορισμό της JP 3-58 η παραπλάνηση αφορά σε κάθε επίπεδο πολέμου ενώ αποτελεί, ειδικότερα, υποπεδίο της διοίκησης / ελέγχου της πολεμικής προσπάθειας (Command and Control Warfare -C2W). Η JP 3-13.4 (2006), αναθεωρημένη έκδοση της 3-58, εκλαμβάνει την επιτυχημένη παραπλάνηση ως άμεση συνεισφορά στην εκπλήρωση του όποιου σκοπού διά της επιβολής ανάληψης (ή μη) εκ μέρους του αντιπάλου δράσεως κατατείνουσας στο επιθυμητό για μας αποτέλεσμα. Οι θεμελιώδεις αρχές μιας επιχείρησης στρατιωτικής παραπλάνησης (military deception -MILDEC) αφορούν: α) στην *εστίαση* του στόχου όπου στόχος ίσον το εχθρικό επιτελείο λήψεως αποφάσεων (*focus*), β) στην *πρόκληση* συγκεκριμένης (αντί)δράσης εκ μέρους του αντιπάλου (*objective*), γ) στην *εξ ημών κεντρική διαχείριση* του σχεδιασμού (*centralized planning and control*), δ) στην *εξασφάλιση μυστικότητας* (*security*), ε) στην *εύρεση καταλλήλου χρόνου* διεξαγωγής αυτής (*timeliness*), στ) στην *απόλυτη ενσωμάτωση* της δράσης εντός του ευρύτερου στρατηγικού πλάνου (*integration*). Αναφορικά με τις τεχνικές που ακολουθούνται γίνεται λόγος για: α) *αντιπερισπασμούς* (*feints*) κατά τους οποίους επιχειρείται η παραπλάνηση του αντιπάλου περίξ του τόπου και του χρόνου εκτέλεσης των όποιων δράσεων, β) *παρουσιάσεις / επιδείξεις* (*demonstrations*) κατά τις οποίες επιδιώκεται η ανάληψη άστοχης δράσης εκ μέρους του ανταγωνιστή, γ) *τεχνάσματα* (*ruses*) κατά τα οποία επιχειρείται η απόδοση ψευδών ή αντικρουόμενων πληροφοριών και δ) *εκθέσεις* (*displays*) διά των οποίων εκτελούνται «επιχειρήσεις πειθούς» σχετικά με υπαρκτές ή μη δυνατότητες οικείων στρατευμάτων -για περισσότερες πληροφορίες βλέπε JP 3-13.4, *Military Deception*, 2006, σ. viii, I-7

⁶² Hutchinson William, "Information Warfare and Deception" στο *Informing Science*, Volume 9, 2006, σ. 217

Το D&D δεν αποτελεί πρακτική μόνο κρατικών δρώντων. Τρομοκρατικές όσο και εγκληματικές οργανώσεις και δίκτυα κτίζουν σ' αυτό με σκοπό τη μη (ή, έστω, τη μη έγκαιρη) κινητοποίηση των αρχών. Το άθροισμα άρνησης πληροφορίας και παραπλάνησης (που ισούται δυνητικά με την εκδήλωση ενός πετυχημένου αιφνιδιασμού) εκτινάσσει τις πιθανότητες του δρώντα επιτυγχάνοντας απόκρυψη ισχυρών και ανίσχυρων σημείων, διαθέσεων, επιχειρησιακών μεθόδων, χρόνου εκτέλεσης σχεδιασμών κ. λ. Από την άλλη μεριά ενδείξεις ή δεδομένα που παραπέμπουν σε τέτοιου είδους συμπεριφορές αποτελούν δείκτη υπόπτων καταστάσεων -πρόκειται για σημεία που οι υπηρεσίες Ασφαλείας και Πληροφοριών οφείλουν να λάβουν υπόψη με ιδιαίτερη προσοχή.⁶³

Κλείνοντας περί εγχειρημάτων παραπλάνησης συνοπτικά αναφέρουμε ότι οι μελετητές επικεντρώνουν κατά κύριο λόγο στη μυστικότητα των δράσεων και έπονται ο καθορισμός των στόχων, η ανάγκη κεντρικού συντονισμού, η επιλογή καταλλήλου χρόνου, η εκτίμηση της αντίδρασης, η επιλογή καναλιών διοχέτευσης παραποιημένων πληροφοριών, η ανατροφοδότηση κ. λ. Η R. Bhalla αναλύοντας τον Βρετανό ιστορικό M. R. D. Foot προσθέτει την ανάγκη κατανόησης της οπτικής του αντιπάλου, τη διατήρηση ικανών μυστικών υπηρεσιών και δη και υπηρεσιών Αντικατασκοπίας και βέβαια την ύπαρξη ικανών επικοινωνιακών συνδέσμων.⁶⁴ Οι Roy Godson και James Wirtz συμφωνούν με τα προαναφερθέντα, ωστόσο, και όσον αφορά σε μια ευρύτερη D&D επιχείρηση, τονίζουν: α) τη ανάγκη 'συντονισμού' των εγχώριων media με τον σχεδιασμό παραπλάνησης σε επίπεδο ανοικτών πηγών, β) την ανάγκη γνώσης της ιδιοσυγκρασίας και της ιστορίας του αντιπάλου, γ) την ανάγκη ύπαρξης εναλλακτικού σχεδίου και, εμμέσως, την ανάγκη εγκατάλειψης του πλάνου σε περίπτωση διαφαινόμενης αποτυχίας.⁶⁵

Παράδειγμα (Ι): Μια αμυντική στρατιωτική τακτική παραπλάνηση

Κατά την FM 3-13 (FM 100-6) μια αμυντική στρατιωτική παραπλάνηση εκτελούμενη από τον δρώντα Α έναντι του δρώντα Β συνοδεύεται από μία ή περισσότερες εκ των κάτωθι προσδοκιών: α) ακύρωση των σχεδίων επίθεσης του δρώντα Β κατά του Α, β) καθυστερημένη ανάπτυξη της, γ) εκδήλωσή της σε λάθος χρόνο ή / και χώρο, δ) δημιουργία λανθασμένης αντίληψης στον επιτιθέμενο γύρω από τις αμυντικές δυνατότητες του βαλλομένου⁶⁶ -μέρος αυτών επιτεύχθηκαν στη Μάχη του Κουρσκ το 1943.

Την άνοιξη του συγκεκριμένου έτους οι Γερμανοί ανασυντάσσονταν μετά από σειρά ηττών στο ανατολικό μέτωπο και κυρίως μετά τη συντριβή της 6^{ης} Στρατιάς στο Στάλινγκραντ. Οι δυνάμεις τους στην περιοχή του Κουρσκ αναπεπταμένες κυματοειδώς σκοπούσαν στην περικύκλωση των ανδρών του Κεντρικού Μετώπου και του Μετώπου Βορονέζ. Η επίθεση θα εξαπολυόταν ταυτόχρονα στη βόρεια και νότια εσοχή της γραμμής των σοβιετικών δυνάμεων, θα έδινε, δε, σε περίπτωση επιτυχίας, την ευκαιρία στη Βέρμαχτ να βρεθεί στην καρδιά του κυρίως όγκου των αντιπάλων μεραρχιών. Ο Στάλιν μαθαίνοντας κατά το Μάιο περί του γερμανικού σχεδίου αποφασίζει να αναλάβει πρωτοβουλία, ωστόσο, οι επιτελικοί του τον πείθουν να μην κινηθεί. Το πλάνο τους στηρίζεται στην άμυνα / απορρόφηση των αρχικών κυμάτων επίθεσης του εχθρού και εν συνεχεία στην αντεπίθεση. Ο ρωσικός στρατός αφού βεβαιώνεται ότι οι Γερμανοί δεν γνωρίζουν για τη διαρροή των

⁶³ Kass L., London Ph., "Surprise, Deception, Denial and Warning: Strategic Imperatives" στο *Orbis*, Volume 57, Number 1, 2013, σ. 75-76

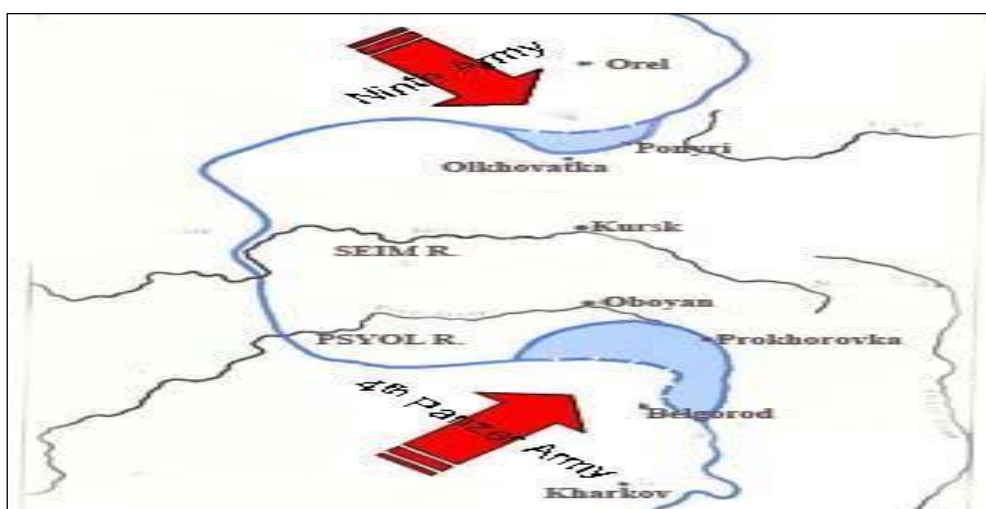
⁶⁴ Bhalla R., *Finding Virtue in Strategic Denial and Deception*, (διατριβή κατατεθειμένη στο Graduate School of Arts and Sciences of Georgetown University), ΗΠΑ, 2011, σ. 9-16

⁶⁵ Godson R., Wirtz J., "Strategic Denial and Deception" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 426-427

⁶⁶ FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques and Procedures*, Headquarters, Department of the Army, Washington, D.C., 2003, σ. 4-13

σχεδίων τους, διασπείρει αντιαρματικές και κατά προσωπικού νάρκες στην προβλεπόμενη περιοχή κινήσεως του χιτλερικού σχηματισμού ξεκινώντας παράλληλα μια μεγάλη επιχείρηση εξαπάτησης. Περιληπτικά η επιτυχία της τελευταίας στηρίχτηκε: α) στον λεπτομερή σχεδιασμό και στην αποσαφήνιση των προσδοκιών, β) στην συμπόρευση στόχων, μέσων, πόρων, γ) στην επιλογή του χρόνου έναρξης των επιχειρήσεων, δ) στη μη προσπάθεια απόκρυψης των αμυντικών προετοιμασιών, ε) στην απόκρυψη του βάθους και της πολυπλοκότητας των τελευταίων, στ) στην απόκρυψη των εφεδρειών πίσω από τις πρώτες γραμμές, ζ) στην εξαπάτηση των γερμανικών αναγνωριστικών με τη χρήση ομοιωμάτων οχημάτων, τη δημιουργία ψεύτικων εγκαταστάσεων, ανύπαρκτων αεροδιαδρόμων κ. λ.

Η γερμανική επιχείρηση, με έναρξη την 5^η Ιουλίου, μέσα σε δύο περίπου εβδομάδες βαλτώνει εντός ενός εκτεταμένου πεδίου που από βορρά προς νότο οριοθετείται από μια γραμμή σχήματος πι διακοσίων σαράντα χιλιομέτρων τη στιγμή που το πλάτος μεταξύ του δυτικότερου και του ανατολικότερου σημείου της προεξοχής Κουρσκ μετρούσε εκατόν είκοσι -η αξιοποίηση του χώρου και η επιλογή του χρόνου από σοβιετικής πλευράς υπήρξε ιδανική, από τα μέσα Ιουλίου το γερμανικό εγχείρημα φαινόταν καταδικασμένο.⁶⁷



Εικόνα 16: Αποτύπωση του θεάτρου μαχών με τα βέλη να δεικνύουν τη γερμανική επίθεση σε βορρά και νότο της γραμμής Κουρσκ. Η εικόνα έχει αντιγραφεί από το https://www.google.gr/?gfe_rd=cr&ei=73H0U_78LiK0AWS8YDoAQ#q=map+of+battle+of+Kursk+photos όπου ανατράξαμε την 20^η Αυγούστου 2014

Αν για την επιτυχία μιας στρατιωτικής τακτικής παραπλάνησης συνεργάζονται πλήθος παραγόντων από την πολιτική ηγεσία, τα επιτελικά γραφεία, τα όπλα του στρατεύματος κ. λ., στο παρόν θα μείνουμε στη συνεισφορά των πληροφοριακών οργανισμών. Οι ρωσικές Υπηρεσίες έδρασαν υποδειγματικά, βέβαια, κάτι τέτοιο δεν ισχύει για τις γερμανικές οι οποίες απέτυχαν: α) να εκτιμήσουν το βάθος της σοβιετικής άμυνας και τις δυνατότητές της, β) να εντοπίσουν τις θέσεις των κύριων σοβιετικών σχηματισμών εντός της προεξοχής Κουρσκ, γ) να αναγνωρίσουν τις προπαρασκευαστικές ενέργειες του στρατού του αντιπάλου υποεκτιμώντας μάλιστα το ηθικό του λόγω της κοντινής γερμανικής επιτυχίας (της τελευταίας στο ανατολικό μέτωπο) στη μάχη για την ανακατάληψη της πόλης Kharkov στις αρχές του 1943.

Κατά την περιγραφή, η γερμανική αποτυχία αποτελεί τη μία όψη του νομίσματος με τη σοβιετική επιτυχία να συνθέτει την άλλη. Οι ρωσικές Υπηρεσίες κατόρθωσαν να παραπλανήσουν τις γερμανικές αντίστοιχες έχοντας γνώση των μέσων συλλογής που οι τελευταίες διέθεταν και αξιοποιώντας ένα πλήθος τακτικών κάλυψης, απόκρυψης και

⁶⁷ FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques and Procedures*, ό. π., σ. 4-13 – 4-14

εικονικών αποκαλύψεων / εκθέσεων που, τελικά, συνέβαλαν στο πέρασμα των Ρώσων από την άμυνα στην επίθεση.^{68, 69}

Παράδειγμα (II): Η στρατιωτική τακτική παραπλάνηση στην επίθεση

Η FM 3-13 ομιλώντας περί επιθετικής στρατιωτικής παραπλάνησης τονίζει ότι ο ασκών το σχεδιασμό δύναται να πετύχει: α) πρωτοβουλία κινήσεων, β) επιτήρηση στόχου, γ) συντήρηση σκοπών, δ) επιθυμητό ρυθμό διεξαγωγής επιχειρήσεων, ε) επιλογή πεδίου δράσεων, στ) απόκρυψη μεγέθους και χρόνου έναρξης ενεργειών, ζ) απόκρυψη δυνάμεων, η) μυστικότητα πλάνων και θ) μείωση κόστους μάχης, απωλειών έμψυχου / άψυχου δυναμικού.⁷⁰

Το καλοκαίρι του 1942 οι συμμαχικές δυνάμεις υπό τον Μοντγκόμερι καταφέρουν να ανακόψουν την πορεία του Africa Corps του Ρόμμελ. Η γραμμή που τους χωρίζει εκκινεί από το Ελ Αλαμίν της Αφρικής εκτεινόμενη νοτίως σε βάθος περίπου 55 χιλιομέτρων. Η φτωχή επιμελητεία καθλώνει τον Ρόμμελ, ο, δε, Μοντγκόμερι γνωρίζει πως αιφνδιασμός εκ μέρους του δεν μπορεί να επιτευχθεί. Η λογική υποδηλώνει ως πλέον πρόσφορο σημείο επίθεσης των Συμμάχων το βόρειο υπό την προοπτική ικανής επικοινωνίας και εφοδιασμού -η αντικατασκοπία των Γερμανών το έχει αντιληφθεί. Ο Μοντγκόμερι γνωρίζοντας πως ιδιαίτερες επιλογές δεν υπάρχουν επιδιώκει τη δημιουργία ευνοϊκού συσχετισμού, οι Γερμανοί, με λίγα λόγια, πρέπει να μετακινήσουν το βάρος αμύνης νοτίως αποδυναμώνοντας το προς τις μεσογειακές ακτές τμήμα. Πως θα πείθονταν; Τα κάτωθι αντιπροσωπεύουν σημεία της απάντησης: α) θωρακισμένοι συμμαχικοί σχηματισμοί ξεκινούν διεξαγωγή ασκήσεων στον νότιο τομέα, η περιορισμένη, δε, λόγω σκόνης, ορατότητα, επιτείνει τις ανησυχίες των αντιπάλων, β) πράκτορες των Γερμανών (γνωστοί στη συμμαχική αντικατασκοπία) ενημερώνονται περί υποτιθέμενων προβλημάτων των μηχανοκίνητων μονάδων του Μοντγκόμερι. Κατ' αυτόν τον τρόπο η όποια επιχείρηση κατά του Ρόμμελ υποτίθεται πως αναβάλλεται τουλάχιστον μέχρι τις αρχές του Νοέμβρη, γ) παραλλάσσονται τεθωρακισμένα και μονάδες πυροβολικού του βορείου τομέα, δ) ομοιώματα μονάδων

⁶⁸ της Elder James, *The Operational Implications of Deception at the Battle of Kursk* για το School of Advanced Military Studies / U.S. Army Command and General Staff College, Κάνσας, 1989, σ. 24-26

⁶⁹ Όλα αυτά, ασφαλώς, υπό την προϋπόθεση της πρότερης γνώσης των ναζιστικών σχεδίων. Όπως επισημάναμε ο Στάλιν είχε πληροφορηθεί περί των προθέσεων των Γερμανών ήδη δύο -κατά τον Τέρι Κράουντι τέσσερις- μήνες πριν τον Ιούλιο του 1943. Αυτό που δεν γνωρίζουμε είναι αν η πληροφόρηση οφείλεται στη δράση του 4^{ου} Αντικατασκοπευτικού Τμήματος του Κόκκινου Στρατού και στο δίκτυό του στην Ελβετία ή στις βρετανικές Υπηρεσίες. Η ταυτότητα του πληροφοριοδότη «Βέρθερ» μέχρι τουλάχιστον και το 2007 δεν είχε αποκαλυφθεί. Αν η επιτυχία σχετίζεται με τη βρετανική αντικατασκοπία, τότε, σχετίζεται με το επίτευγμα του σπασίματος του γερμανικού κρυπτογραφικού μηχανισμού Enigma, ωστόσο, είναι γνωστό ότι οι Βρετανοί δεν επιθυμούσαν να ενημερώσουν καν τους συμμάχους περί τούτου. Αν έχει να κάνει με τη σοβιετική αντικατασκοπία, τότε, ενδεχομένως ο Βέρθερ απετέλεσε πρόσωπο πολύ κοντά τον Χίτλερ -ο Ράινχαρντ Γκέλεν, υπεύθυνος της γερμανικής αντικατασκοπίας στο ανατολικό μέτωπο, κατονομάζει στα απομνημονεύματά του τον Μάρτιν Μπόρμαν ως κατάσκοπο των Σοβιετικών. Αν συμβαίνει κάτι τέτοιο (ο Κράουντι απορρίπτει την εμπλοκή των Βρετανών), τότε, βρισκόμαστε μπροστά σε μια τεράστια πληροφοριακή ρωσική επιτυχία και, ταυτόχρονα, μπροστά σε μια καταστροφική αντικατασκοπευτική γερμανική αποτυχία - για περισσότερες λεπτομέρειες βλέπε Κράουντι Τ., *Ιστορία της Κατασκοπίας*, μτφρ. Μηλιάρης Γ., Lector, Αθήνα, 2007, σ. 425-428. Πέρα τούτων ο Robert Stephan κάνει λόγο για τη δράση του Αλεξάντερ Ντεμιάνοφ (υπηρεσιακό ψευδώνυμο «Χάινε»). Ο Ντεμιάνοφ έχοντας εισχωρήσει στην Άμπμπερ τροφοδοτούσε τους υποτιθέμενους προϊσταμένους του με παραπλανητικά στοιχεία ήδη από το 1942 (επιχείρηση «Μοναστήρι»). Αν και ορισμένοι αξιωματικοί της Άμπμπερ τον έθεσαν στο στόχαστρο ως σοβιετικό πράκτορα, ο Γκέλεν (που αργότερα συντάχθηκε με τους Αμερικανούς και εξελίχθηκε σε υψηλόβαθμο στέλεχος των δυτικογερμανικών μυστικών υπηρεσιών) τον υπερασπίστηκε μέχρι τέλους -για μια άποψη βλέπε Stephan R., *Stalin's Secret War. Soviet Counterintelligence Against the Nazis, 1941-1945*, University Press of Kansas, Lawrence / Kansas, 2004, κεφάλαιο 6, σ. 153-174

⁷⁰ FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques and Procedures*, ό. π., σ. 4-14 – 4-15111

πυροβολικού εμφανίζονται νοτίως, ε) υποτιθέμενες προετοιμασίες επιμελητείας μιας μεγάλης επιχείρησης λαμβάνουν χώρα πολύ μακριά από τα παράλια.⁷¹



Εικόνα 17: Γράφημα του εγχειρήματος. Άποψη του πεδίου με το άνω βέλος να αποτυπώνει τις πραγματικές συμμαχικές προθέσεις και το κάτω τους σχεδιασμούς εξαπάτησης. Η εικόνα έχει αντιγραφεί από το

https://www.google.gr/?gfe_rd=cr&ei=73H0U_78LiK0AWS8YDoAQ#q=operation+bertram+photos όπου ανατρέξαμε την 20^η Αυγούστου 2014

Το στρατήγημα της εξαπάτησης στέφτηκε με επιτυχία.⁷² Ο Ρόμμελ περιμένοντας επίθεση εντός του Νοέμβρη επιστρέφει στη Γερμανία. Οι σύμμαχοι κινούν την 23^η Οκτωβρίου κατά ενός στρατεύματος του οποίου: α) η κεφαλή απουσιάζει, β) μέρος των τεθωρακισμένων του αδρανεί στα νότια -όταν αποδεσμεύεται είναι αργά. Η «Επιχείρηση Μπέρτραμ» αποδεικνύει πως ένα μελετημένο σχέδιο παραπλάνησης δεν κωλύεται από την έλλειψη κάλυψης, αντιθέτως, δύναται να ενισχυθεί με ψευδείς επιδείξεις και ελιγμούς και με την απόκρυψη του χώρου / χρόνου διεξαγωγής της μάχης να δεικνύει ζητούμενο και απαραίτητο συστατικό του στρατηγήματος.⁷³

Είναι εφικτή η στρατηγική / τακτική αντιπαραπλάνηση;

Η ήττα συγχωρείται, ο αιφνιδιασμός ποτέ

Φρειδερίκος Β'⁷⁴

Το αμερικανικό DoD ορίζει ως *αντιπαραπλάνηση / counterdeception* κάθε προσπάθεια ακύρωσης, εξουδετέρωσης ή ελαχιστοποίησης των συνεπειών μιας

⁷¹ ...σε βάθος σαράντα και πλέον χιλιομέτρων. Εντυπωσιακό είναι ότι είχαν στρωθεί υποτιθέμενα δίκτυα μεταφοράς ύδατος με τους αγωγούς να διατρέχουν μία απόσταση τριάντα περίπου χιλιομέτρων από βορρά προς νότο -για περισσότερες λεπτομέρειες βλέπε Blanks Kenneth, *An Effectiveness Analysis of the Tactical Employment of Decoys*, μελέτη κατατεθειμένη στο U.S. Army Command and General Staff College, Κάνσας, 1994, σ. 32

⁷² Σε βαθμό που ο επικεφαλής των συμμαχικών αεροπορικών επιχειρήσεων στη Μέση Ανατολή Arthur Tedder αναφώνησε: «Πρόκειται για το πλέον ικανό εγχείρημα εξαπάτησης, για εγχείρημα που αποπροσανατόλισε ολοσχερώς τις εχθρικές Υπηρεσίες». Κατά τον Whaley, ο Μοντγκόμερι πέτυχε κάτι παραπάνω από έναν τακτικό αιφνιδιασμό. Ο μελετητής θεωρεί ότι η έκπληξη των Γερμανών δεν μπορεί παρά να ήταν απόλυτη όπως, άλλωστε, απόλυτη ήταν η σιγουριά τους περί του χρόνου έναρξης των μαχών· το τελευταίο αντικατοπτρίζεται στο γεγονός της επιστροφής του Ρόμμελ στο Βερολίνο, οπωσδήποτε, σε ακατάλληλη στιγμή -για όλα αυτά βλέπε Whaley B., *Stratagem: Deception and Surprise in War*, Artech House, Inc., Norwood / Massachusetts, 2007, σ. 332-334

⁷³ FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques and Procedures*, ό. π., σ. 4-15 – 4-16

⁷⁴ Brown A., *Bodyguard of Lies*, Harper and Row, New York, 1975, σ. 415

αλλότριας επιχείρησης παραπληροφόρησης.⁷⁵ Οι Michael Bennet και Edward Waltz γράφουν πως αντιπαραπλάνηση σημαίνει διαδικασία της οποίας ο σκοπός κατατείνει σε δύο αποσαφηνίσεις: α) περί των δυνατοτήτων και προθέσεων του εκτελών την παραπλάνηση και β) περί του πώς ακριβώς αυτός σκοπεύει να 'χειριστεί' τον στόχο ή, αλλιώς, περί του ερωτήματος ...*τι ακριβώς επιθυμεί* (ο θύτης) *να πράξει ο λήπτης / υποτιθέμενο θύμα της όλης επιχείρησης*.⁷⁶ Ωστόσο πριν φτάσει το όποιο επιτελείο στις απαντήσεις πρέπει να εντοπισθεί ο κίνδυνος. Είναι κάτι τέτοιο εφικτό και αν ναι σε ποιο βαθμό; Οι δύο ερευνητές προβαίνουν σε μια λεπτομερή καταγραφή απόψεων ξεκινώντας από τον R. V. Jones που γράφει περί το 1942 για να καταλήξουν σε ευρήματα / οδηγίες που η CIA απελευθέρωσε περί το 1997 γύρω από την αντιπαραπλάνηση. Το συμπέρασμα δεν είναι ιδιαίτερα αισιόδοξο. Αυτό που παρουσιάζεται είναι μια ποικίλη εικόνα βάσει της οποίας στην αποκάλυψη του παιγνίου δύναται, ενδεχομένως, να συμβάλλει: α) μια ικανή συλλογή / ορθή ανάλυση της πληροφορίας, β) η γνώση των ειδών και των μεθόδων της παραπληροφόρησης, γ) η γνώση ιστορικών παραδειγμάτων, δ) ένας επανασχεδιασμός των Υπηρεσιών σε λειτουργικό / γραφειοκρατικό επίπεδο, ασφαλώς η οξύνοια των επαγγελματιών κ. λ. Εντούτοις στεκόμαστε στους Robert Jervis και Michael Handel που μνημονεύονται στο έργο των Bennet και Waltz. Οι Jervis και Handel δεν μελετούν άμεσα την (αντι)παραπληροφόρηση. Ο πρώτος (με το *Perception and Misperception in International Politics* -1976) αναφέρεται στην κακή αποκρυπτογράφηση των καταστάσεων. Ο δεύτερος (με το *War, Strategy and Intelligence* -1989) ασχολείται με ζητήματα όπως η στρατηγική, η τεχνολογία και η πληροφορόρηση σε σχέση με τον πόλεμο συμβάλλοντας στη συζήτηση υπό μια διαφορετική σκοπιά. Κατ' αυτήν την έννοια, και όσον αφορά στον Jervis, η επιτυχία μιας επιχείρησης παραπλάνησης οφείλεται πολλές φορές στην κακή αντίληψη του περιβάλλοντος που οι αντίπαλοι policymakers διατηρούν, μια εμμένουσα αντίληψη που σχετίζεται με: α) προβλέψεις ή επιθυμίες που δεν καταπίπτουν ακόμα και υπό την παρουσία σοβαροτάτων ενδείξεων, β) τη μη ύπαρξη προσώπων που θα παρουσίαζαν τη μη «ελκυστική» άποψη (*devil's advocates*), γ) τη σύνδεση εικόνων και σκέψεων με συγκεκριμένες αναλλοίωτες θεωρήσεις και δ) τη μη συναίσθηση του γεγονότος ότι η παγίδα της προκατειλημμένης σκέψης ενδέχεται να βρίσκεται πολύ κοντά ⁷⁷ -αν γι' αυτά τα τέσσερα σημεία ληφθεί μέριμνα, τότε, ο αμυνόμενος αυξάνει τις πιθανότητές του. Από τη μεριά του ο Michael Handel αν και αγωνιά καταφανώς όσον αφορά στις πιθανότητες πρόληψης και αποφυγής ενός αιφνιδιασμού, και εμμέσως μιας δράσης παραπληροφόρησης, προτείνει έξι πιθανά αντίμετρα, ειδικότερα: α) αποφυγή εξάρτησης από μία και μόνη πηγή πληροφορόρησης, β) αποφυγή εξάρτησης από φραστικές πληροφορίες που δεν συνοδεύονται στον ίδιο χρόνο από χειροπιαστές αποδείξεις, γ) αποφυγή εξάρτησης από «αόρατους» πράκτορες, δ) έλεγχο και επανέλεγχο των πληροφοριακών αντιφάσεων, ε) μη απόρριψη εκ προοιμίου των αναλύσεων του κατωτέρου προσωπικού των Υπηρεσιών ακόμα και αν αυτές φαίνονται παράδοξες και στ) γνώση των δυνατοτήτων και τρωτοτήτων του αντιπάλου, τέλος, αξιοσημείωτη είναι η φράση του: «Υπό ορισμένων συνθηκών, όσο καλύτερα δένουν τα κομμάτια ενός αινίγματος, τόσο μεγαλύτερος είναι ο κίνδυνος παραπλάνησης. Αυτό πιθανολογείται πρωτίστως όταν η ληφθείσα πληροφορία

⁷⁵ Bennet M., Waltz E., *Counterdeception Principles and Applications for National Security*, ό. π., σ. 143

⁷⁶ *ibid*

⁷⁷ Jervis R., *Perception and Misperception in International Politics*, Princeton University Press, USA, 1976, σ. 409-424

εμφανίζεται εν τη απουσία 'θορύβου' και αντικρουόμενων εικόνων, όταν το συμπέρασμα ικανοποιεί ξεκάθαρα τις προσδοκίες κάποιου». ⁷⁸

Κατά τους Shulsky και Schmitt είναι σχεδόν αδύνατον για έναν πληροφοριακό οργανισμό να αντιληφθεί κάθε εκπορευόμενη προσπάθεια παραπληροφόρησης εκ μέρους μιας αντίπαλης Υπηρεσίας. Το πρώτο που οφείλει να ληφθεί υπόψη είναι η υπαρκτή πιθανότητα στοχοποίησης των οικείων διαύλων συλλογής δεδομένων, συνεπώς, σοφή είναι η διατήρηση του μεγαλύτερου δυνατού αριθμού αυτών -ένα δεύτερο πρόβλημα δεικνύει η ενδεχόμενη δράση κάποιου διπλού πράκτορα. Οι δύο ερευνητές γενικά δεν αφήνουν ιδιαίτερα περιθώρια αισιοδοξίας όσον αφορά στην επιτυχή αντιπαραπλάνηση τονίζοντας πως μόνο η τελική επιβεβαίωση των συλλεγομένων πληροφοριών θα αποδείξει την αλήθεια που φέρονται να κομίζουν. ⁷⁹

Ο Whaley εμφανίζεται ακόμα πιο απαισιόδοξος τονίζοντας πως αν ο αιφνιδιασμός αποτελεί κλειδί νίκης, η παραπλάνηση είναι η προϋπόθεσή του. Έχοντας καταγράψει πλήθος περιπτώσεων από το 1914 μέχρι το 1968 υποστηρίζει ότι σχεδόν τίποτα δεν καταφέρνει να ακυρώσει άμεσα τη συγκεκριμένη τακτική. Πάρα ταύτα ελλοχεύουν δύο κίνδυνοι για τον ασκών την εξαπάτηση. Ο πρώτος σχετίζεται με την πιθανότητα μη ξεκάθαρης ανατροφοδότησης / feedback και μια ακόλουθη «άσκηση υποθέσεων» εκ μέρους του. Ο δεύτερος έχει να κάνει με την εκ των προτέρων γνώση του πλάνου εκ μέρους του δεχόμενου την επίθεση. Ο ερευνητής υποστηρίζει ότι μια δράση παραπληροφόρησης συνηθέστατα επιτυγχάνει όσο και αν ο «δέκτης» είναι το ίδιο συνεπής (ή καλύτερος) σ' αυτήν την τέχνη από τον «πομπό». Το πώς θα αποφευχθεί η θυματοποίηση δεν μπορεί να απαντηθεί μέσα από σίγουρες λύσεις. Η προσεκτική ανάλυση της πληροφόρησης δεικνύει μια ελπίδα αποφυγής του κακόβουλου στρατηγήματος -κατά συνέπεια η οξύνοια μιας υπηρεσίας CI καλείται να αποδειχτεί. ⁸⁰

Η Grabo υποστηρίζει ότι δεν υπάρχει κράτος που να μην υπόκειται στον κίνδυνο της εξαπάτησης με τις δημοκρατίες να παρουσιάζονται πιο ευάλωτες από τα ολοκληρωτικά καθεστώτα. Επιπλέον, δεν διατηρεί ιδιαίτερες ελπίδες όσον αφορά στην αποτελεσματικότητα των όποιων προληπτικών μέτρων τονίζοντας ότι πρόκειται για μέσα διά των οποίων περισσότερο φαίνεται να επιχειρείται μια σπασμωδική προσπάθεια εισχώρησης στο αντίπαλο πληροφοριακό σύστημα χωρίς να αναφερόμαστε, όπως καταθέτει, στο χρονοβόρο ή ατελέσφορο σχεδιασμό τους. Μόλα ταύτα η ίδια στο ερώτημα «τι μπορούμε να κάνουμε προκειμένου να προστατευθούμε έναντι της εν λόγω πρακτικής;» προτείνει: α) τη σπουδή σχετικών ιστορικών περιπτώσεων, β) την αποδοχή της άποψης που φέρει τον φιλύποπτο και ρεαλιστή σε πλεονεκτικότερη θέση έναντι του εφησυχασμένου, γ) την απόρριψη προκαταλήψεων και τη μη εγκόλπωση άκαμπτων πολιτικών θεωριών που συσκοτίζουν τελικά την αληθή εικόνα, δ) την περαιτέρω ανάπτυξη της αναλυτικής λειτουργίας των Υπηρεσιών και, τελευταίο και σημαντικότερο, τη διατήρηση ικανών δυνάμεων ώστε ακόμα και αν υπάρξει παραπλάνηση και αρχικός αιφνιδιασμός να μην ακολουθήσει μια στρατιωτική ταπείνωση. ⁸¹

Η JP 3-13.4 του 2006 υποστηρίζει ότι η πετυχημένη αντιπαραπλάνηση συνεισφέρει στην προστασία του οικείου συστήματος C2W αλλά και του αντίστοιχου λήψεως αποφάσεων από πληροφοριακές επιθέσεις. Εντός των καθηκόντων της αντιπαραπλάνησης εντάσσεται η προσπάθεια αποκάλυψης της στάσεως και των προθέσεων του ανταγωνιστή γύρω από ένα ή περισσότερα φλέγοντα ζητήματα' κατ'

⁷⁸ Handel M., *War, Strategy, and Intelligence*, Frank Cass & Co. Ltd., Βρετανία, 1989, σ. 341, 396-397

⁷⁹ Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 121-126

⁸⁰ Whaley B., *Stratagem: Deception and Surprise in War*, ό. π., σ. 75-78, 138

⁸¹ Grabo C., *Anticipating Surprise. Analysis for Strategic Warning*, ό. π., σ. 129-133

αυτόν τον τρόπο πιθανολογείται η ταυτοποίηση ενδεχόμενης / μελλοντικής προσπάθειας παραπληροφόρησης εκ μέρους του. Η γνώση προηγούμενων σχετικών δράσεων του βοηθά αξιοσημείωτα. Οι αναλυτές οφείλουν να εκτιμήσουν δεόντως στοιχεία που εκ πρώτης όψης φαίνονται ασήμαντα. Η απόρριψη αυτών λόγω, π. χ., προκατάληψης ή αδιαφορίας ή «έλλειψης βαρύτητας» δεικνύει την ασφαλέστερη οδό επιτυχίας του αντιπάλου, άλλωστε, ωφελεί να μη μας διαφεύγει ότι ο τελευταίος χτίζει ακριβώς στα φαινομενικά επουσιώδη προσπαθώντας να μην κινήσει υποψίες. Τέλος, αν η αμυντική αντιπαραπλάνηση στοχεύει στην αποκάλυψη της παραπλάνησης, τότε, η επιθετική σκοπεύει στην επιμήκυνση της (αποκαλυφθείσας) τελευταίας, μέσω υποτιθέμενης άγνοιας, προς: α) σπατάλη πόρων του ανταγωνιστή και β) απόδοση ψευδούς εικόνας στο στρατόπεδό του ⁸² -γίνεται φανερό πως η επιθετική αντιπαραπλάνηση δεικνύει μορφή παραπλάνησης.

Ο J. B. Bell συντασσόμενος με τη JP 3-13.4 αποκρυπτογραφεί την αμυντική αντιπαραπλάνηση (που ο ίδιος ονομάζει *παθητική*) ως διαδικασία συνεχούς σκαναρίσματος της δοθείσης πραγματικότητας αποζητώντας λάθη και ανωμαλίες, κρυφές απειλές κ. λ. όπως ακριβώς κάνει ένα ραντάρ. Η επιθετική (*ενεργητική* κατά τον Bell) αντιπαραπλάνηση επιχειρεί να χειραγωγήσει το εχθρικό πλάνο -για να επιτευχθεί κάτι τέτοιο πρέπει είτε να ληφθεί πληροφόρηση μέσα από το ανταγωνιστικό επιτελείο, είτε να αποκαλυφθεί ο αντίπαλος σχεδιασμός στα αρχικά του στάδια. Μια κλασική στρατηγική αντιπαραπληροφόρησης δεικνύει η τακτική της άρνησης οποιασδήποτε γνώσης στον εχθρό -πρόκειται για μέθοδο που ακολούθησε κατά κόρον ο κομμουνιστικός κόσμος κατά τη διάρκεια του ψυχρού πολέμου. Κατ' αυτόν τον τρόπο μόνο εικασίες μπορούσαν να συντεθούν / εκφραστούν και μάλιστα μέσα από ελάχιστα δεδομένα. Όπως γίνεται κατανοητό ένα υποθετικό δυτικό πλάνο παραπληροφόρησης μόνο σε αδύναμα σενάρια μπορούσε να στηριχθεί, οπωσδήποτε, κάτι όχι θετικό -βέβαια αντιπαραπληροφόρηση δεν σημαίνει τόσο την απόκρυψη της πραγματικότητας (που άλλωστε δύσκολα επιτυγχάνεται στις μέρες μας, συμπληρώνουμε) αλλά την αποκάλυψη της εξαπάτησης. Από κει και πέρα, συμπληρώνει ο Bell, ανθρωπinoι και τεχνητοί πόροι παροχής πληροφοριών δύναται να βοηθήσουν στο ξεσκέπασμα ενός δόλιου παιγνίου, ωστόσο, το δύσκολο του εντοπισμού της όποιας παγίδας λειτουργεί υπέρ του επιτιθέμενου.⁸³

Οι Roy Godson και James Wirtz αντιμετωπίζουν το όλο ζήτημα υπό την έποψη της αμερικανικής μικρο και μακρο στρατηγικής. Το D&D δεν αφορά μόνο σε κρατικούς αλλά, επίσης, σε μη κρατικούς δρώντες, ακόμα ακόμα σε ομάδες που δραστηριοποιούμενες στο διεθνικό έγκλημα συνθέτουν κοινωνική απειλή. Όπως γίνεται αντιληπτό η αντιμετώπιση της πρόκλησης απαιτεί συντονισμένη δράση της πληροφοριακής κοινότητας, του DoD και άλλων κυβερνητικών υπηρεσιών, τη συμμετοχή περιφερειακών αξιωματούχων, των MME όπως και των πολιτών. Ό,τι πρέπει να γίνει σχετίζεται με μια: α) ανάπτυξη προγραμμάτων διαφώτισης των κυβερνητικών επιτελείων περί της χρήσης και των μεθόδων του D&D. Οι πολιτικοί άρχοντες οφείλουν να γνωρίζουν ότι ενδέχεται να γίνουν στόχοι παραπληροφόρησης ή ότι, ίσως, κληθούν να παραπληροφορήσουν, β) ενημέρωση των πολιτών και των ειδησεογραφικών δικτύων περί του κινδύνου παγίδευσής τους από μια επιχείρηση deception ή προπαγάνδας εκπορευομένης από κέντρα εκτός επικρατείας, γ) αποφυγή αποκάλυψης ευαίσθητων πληροφοριών σε τρίτους χωρίς την έγκριση των Υπηρεσιών -πρόκειται για σφάλμα στο οποίο υπόκεινται συχνά κρατικοί αξιωματούχοι διαφόρων βαθμίδων, δ) αναβάθμιση των Υπηρεσιών σε επίπεδο συλλογής / ανάλυσης

⁸² JP 3-13.4, *Military Deception*, 2006, ό. π., σ. II-1, II-2

⁸³ Bell B. J., "Toward a Theory of deception", ό. π., σ. 275-278

πληροφορίας, ε) μελέτη ιστορικών παραδειγμάτων με την ψυχροπολεμική περίοδο να δεικνύει πλούσια πηγή. Αν και κανείς από τους δύο μελετητές δεν τρέφει ελπίδες περί καθολικών λύσεων, εντούτοις, όπως δηλώνουν, η ελαχιστοποίηση ή, έστω, «σμίκρυνση» των συνεπειών μιας επιχείρησης εξαπάτησης καθόλου δεν είναι αδύνατη.⁸⁴

Οι Bennet και Waltz έχοντας αναλύσει τα ανωτέρω καταλήγουν στις τέσσερις κατ' αυτούς θεμελιώδεις αρχές αντιπαραπλάνησης, πιο συγκεκριμένα:

- *Γνώριζε τον εαυτό σου.* Αν για πράγματα που γνωρίζουμε υπάρχει ένα θεωρητικά στέρεο έδαφος, τότε, για το άγνωστο δεν υπάρχει τίποτα από ή δεδομένο. Ο Whaley τονίζει πως ...αν το θύμα δεν σκεφτεί την πιθανότητα μιας επικείμενης ή και εξελισσόμενης παραπλάνησης εις βάρος του, τότε, αναπόφευκτα θα παγιδευτεί.⁸⁵ Η προτροπή «γνώριζε τον εαυτό σου» ένα βαθύτερο στόχο έχει: να γίνει κατανοητή η αδυναμία επίγνωσης του κάθε τι, άρα, να καταστεί ευνόητη η ανάγκη συνεχούς επαγρύπνησης.⁸⁶
- *Γνώριζε τον αντίπαλό σου.* Έχοντας υπόψη τις πολιτικές, διπλωματικές, οικονομικές, στρατιωτικές δυνατότητες και προθέσεις του εχθρικού παράγοντα βρισκόμαστε ένα βήμα πιο κοντά στη σύλληψη της επόμενης σκέψης του και, ίσως, μιας ενέργειας εις βάρος μας. Βέβαια, όπως λέει ο M. Dewar, για να επιτευχθεί κάτι τέτοιο πρέπει να εισβάλουμε στον κόσμο και στην οπτική του -πρόκειται για το πλέον αποτελεσματικό και ίσως μοναδικό όπλο των αναλυτών έναντι του κινδύνου της εξαπάτησης.⁸⁷
- *Γνώριζε την κατάσταση.* Η προτροπή έχει να κάνει κυρίως με ενδεχόμενες αλλαγές στο διεθνές περιβάλλον. Πώς αυτές επηρεάζουν τους σχεδιασμούς μας; Πώς εισπράττονται από τους ανταγωνιστές μας; Τι ευκαιρίες δημιουργούν; Αξιίζουν το ρίσκο μιας επιχείρησης παραπληροφόρησης από τη μία ή την άλλη πλευρά; Αν ναι πώς μπορεί η τελευταία να εκδηλωθεί; Πώς να αποτραπεί;⁸⁸
- *Έλεγχε τους διαύλους των πληροφοριών σου.* Προκειμένου να πραγματοποιούν οι άνω επιταγές απαιτείται ένα σύστημα καναλιών πληροφόρησης. Αυτά τα κανάλια πρέπει κατά το δυνατό να ελέγχονται ως προς τη φερεγγυότητά τους -όπως γράφει ο R. V. Jones ...*know your channels*. Ένας τέτοιος έλεγχος καθίσταται απαραίτητος αν αναλογιστούμε ότι η πλειονότητα των πληροφοριών απορρέει από δεύτερες και τρίτες πηγές, συνεπώς, μια πληροφοριακή στρέβλωση είναι πιθανή.⁸⁹

⁸⁴ Godson R., Wirtz J., "Strategic Denial and Deception" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 432-435

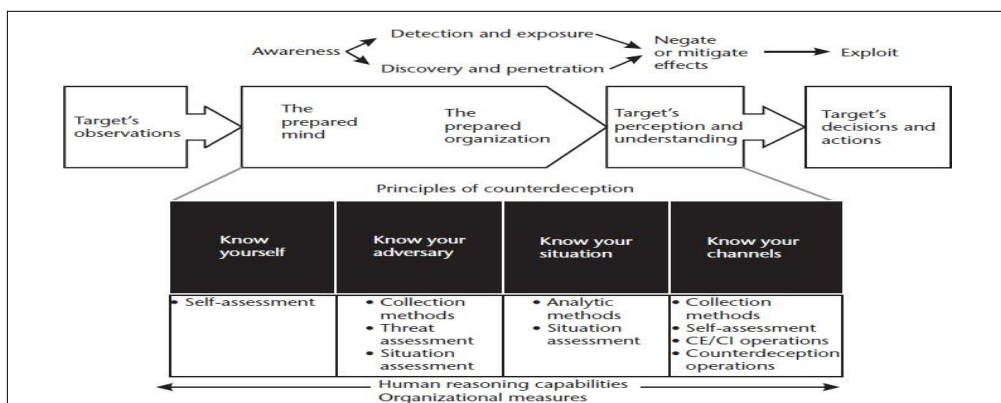
⁸⁵ Whaley B., *Stratagem: Deception and Surprise in War*, Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, USA, 1969, σ. 142

⁸⁶ Bennet M., Waltz E., *Counterdeception Principles and Applications for National Security*, ό. π., σ. 176-177

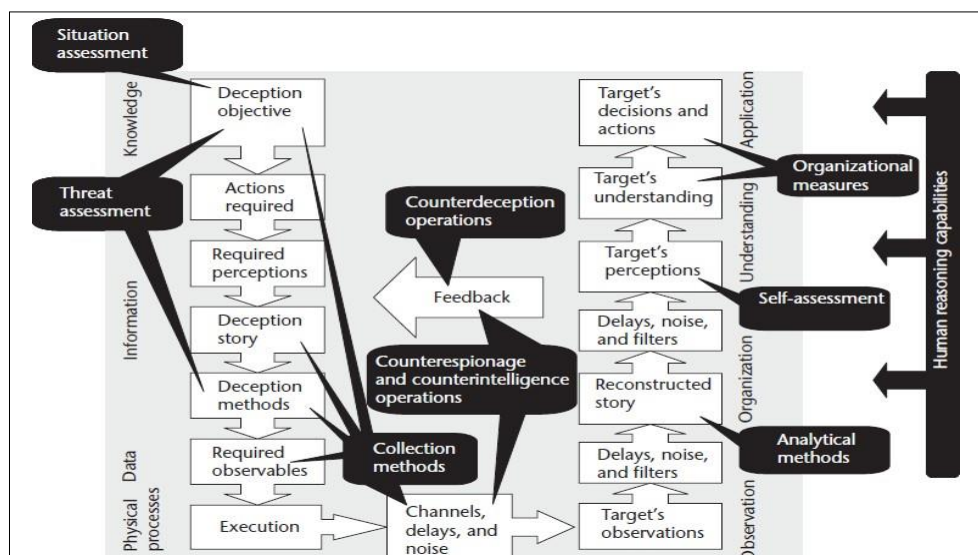
⁸⁷ ό. π., σ. 177-178

⁸⁸ ό. π., σ. 178-179

⁸⁹ ό. π., σ. 179-180. Τέλος, για μια ευρύτερη παρουσίαση μεθόδων, τύπων και πρακτικών counterdeception βλέπε στο ίδιο, σ. 143-175



Εικόνα 18: οι τέσσερις -κατά Bennet, Waltz- θεμελιώδεις αρχές της αντιπαραπλάνησης. Η εικόνα ελήφθη από τη σελίδα 174 του *Counterdeception Principles and Applications for National Security* των Bennet, Waltz



Εικόνα 19: ο κύκλος της παραπλάνησης σε δεκαπέντε βήματα από τη χάραξη των προσδοκιών του επιτιθέμενου μέχρι την αντίδραση του στόχου. Οι όποιες επιχειρήσεις αντιπαραπλάνησης του τελευταίου θα ενσωματωθούν, εφόσον λάβουν χώρα, στο λεγόμενο *feedback* ήτοι, στην αντίδρασή του. Η συγκεκριμένη αντίδραση θα επιστρέψει στον επιτιθέμενο. Το εάν με τη σειρά της αποτελέσει παγίδα εξαρτάται από τις Υπηρεσίες του στόχου. Η εικόνα ελήφθη από τη σελίδα 173 του *Counterdeception Principles and Applications for National Security* των Bennet, Waltz

Συμπεράσματα

Δεν υπάρχουν θεμελιώδεις διαφορές μεταξύ των ερευνητών τόσο για το τι σημαίνει και πώς λειτουργεί η τακτική της παραπλάνησης όσο και για αντίστοιχα ερωτήματα περί την αντιπαραπλάνηση με μόνη διαφορά τον ποικίλο βαθμό αισιοδοξίας / απαισιοδοξίας ως προς την επίτευξη της τελευταίας. Ό,τι οφείλουμε να τονίσουμε σχετίζεται με ένα εγγενές πλεονέκτημα, πρόκειται για τη γνώση, από τον ένα δρώντα, της εν εξελίξει πλεκτάνης τη στιγμή που το υποψήφιο θύμα πιθανότατα δεν διαθέτει σχετικές προσλαμβάνουσες. Θέτοντας προμετωπίδα της συζήτησης αυτήν ακριβώς την παρατήρηση κατανοούμε γιατί η τακτική παραπλάνηση έχει μελετηθεί

πληρέστερα και ποιες δυσκολίες αντιμετωπίζει η αντιπαραπλάνηση ως προς μια επιτυχή έκβαση.

Η αλλοίωση της αληθούς εικόνας δεν μπορεί, συνηθέστατα, παρά να επηρεάσει τη διαδικασία λήψεως αποφάσεων με αποτέλεσμα μια κακή εκτίμηση ή κίνηση, έναν λανθασμένο σχεδιασμό -στόχος ενός πλάνου εξαπάτησης δεν είναι παρά το αντίπαλο επιτελείο πολιτικό ή στρατιωτικό. Η γνώση του παρελθόντος / παρόντος, η αυξημένη επιφυλακή, η χρήση ανθρωπίνων και τεχνικών πόρων, η βελτίωση της αναλυτικής λειτουργίας του αντικατασκοπευτικού πλέγματος προτείνονται ως μερικές λύσεις στην αποκάλυψη του deception. Πάρα ταύτα οι δύο πλέον σίγουροι οδοί επιτυχούς counterdeception φαίνεται να αναγνωρίζονται εντός του συστήματος του επιτιθέμενου -πρόκειται για την έλλειψη ορθής ανατροφοδότησης του και, κυρίως, την ύπαρξη επιβουλών προσώπων εντός του δικτύου του.⁹⁰

Η δράση μιας υπηρεσίας Αντικατασκοπίας προς εξύφανση ενός σχεδίου παραπλάνησης είναι κατανοητή. Αυτό που προβληματίζει σχετίζεται με την αντιμετώπισή του. Μόλα ταύτα, όσο είναι δυσοίωνη η πρόβλεψη τόσο απαραίτητη είναι μια μέριμνα προς αποτροπή κακόβουλων εγχειρημάτων και μόνο αυτός που χρησιμοποιεί το δηλητήριο γνωρίζει το αντίδοτο: τα βήματα που δύναται να γίνουν σ' αυτήν την κατεύθυνση και πάλι μέσα από μια υπηρεσία Πληροφοριών και δη και Αντικατασκοπίας θα ενορχηστρωθούν.

⁹⁰ Κατά την FM 3-13 μια επιχείρηση παραπλάνησης ρισκάρει: α) μια αποτυχία, β) μια έκθεση πηγών, γ) μια πρόκληση παρενεργειών. Το ρίσκο της αποτυχίας σχετίζεται με μια μη αναμενόμενη αντίδραση του υποψηφίου θύματος, της έκθεσης πηγών με μια ορθή συναγωγή συμπερασμάτων εκ μέρους των αντιπάλων Υπηρεσιών σχετικά με τα πληροφοριοδοτικά assets του επιτιθέμενου και, τέλος, της πρόκλησης ανεπιθύμητων αποτελεσμάτων με μια απρόβλεπτη εμπλοκή τρίτων μερών κατά τον έναν ή άλλο τρόπο. Προκειμένου να μειωθούν οι συγκεκριμένοι κίνδυνοι απαιτείται, μεταξύ άλλων, μια συνεχής πληροφοριακή υποστήριξη γύρω από τις (αντι)δράσεις του δεχόμενου την παραπληροφόρηση και, δεύτερον, μια αδιαπέραστη ασπίδα προστατευτικών μέτρων γύρω από το εγχείρημα. Τα τελευταία έχοντας να κάνουν, πέραν της κλασικής απόκρυψης και επιβολής μυστικότητας, με υπολογισμό ρίσκων και ανάλυση απειλών απαιτούν πρόσληψη, επίσης, πληροφοριών. Όλα αυτά ανήκουν στο πεδίο καθηκόντων μιας υπηρεσίας CI όπως, ασφαλώς, σ' αυτήν ανήκει η επιλογή τού τι θα αποκρυφτεί και τι θα επιδειχθεί εντέχνως στα μάτια του αντιπάλου, άρα, η ασπίδα των προστατευτικών μέτρων δύναται, κατ' επιλογή, να παρουσιαστεί ημιπερατή -για περισσότερες πληροφορίες βλέπε FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques and Procedures*, ό. π., σ. 4-24 – 4-25

ΠΡΟΣΘΗΚΗ

Στρατιωτική αντικατασκοπία: Υπάρχει απάντηση στο πρόβλημα του στρατηγικού αιφνιδιασμού;

Ένα ζήτημα που επανέκαμψε μετά την 11^η Σεπτεμβρίου είναι αυτό της δυνατότητας εξουδετέρωσης, ή μη, μιας αιφνιδιαστικής επίθεσης μείζονος σημασίας.⁹¹ Η απάντηση του ερωτήματος ενδιαφέρει καθώς σε μεγάλο βαθμό αποτελεί δείκτη αξιολόγησης των Υπηρεσιών και δη και αυτών της Αντικατασκοπίας ενώ συνδέεται επίσης με το εγχείρημα της παραπλάνησης.

Ο Or Arthur Honig σημειώνει πως δύο σχολές καταπιάνονται με το θέμα. Πρόκειται για την Ορθόδοξη Σχολή (Orthodox School) και την αντίστοιχη Αναθεωρητική (Revisionist School). Η πρώτη υποστηρίζει πως ενδογενείς παθολογίες και εμπόδια που ενεδρεύουν εντός των μυστικών υπηρεσιών καθιστούν την πρόβλεψη ενός στρατηγικού αιφνιδιαστικού χτυπήματος πολύ δύσκολη έως αδύνατη. Η δεύτερη δηλώνει πως δεν υπάρχουν έμφυτοι ή αναπόδραστοι αρνητικοί παράγοντες που την αποκλείουν.⁹²

Η μέχρι το τέλος του 20^{ου} αιώνα βιβλιογραφία δίδει έμφαση στους παράγοντες που πριμοδοτούν μια αιφνιδιαστική επίθεση τείνοντας να θεωρήσει μια τέτοια ενέργεια σχεδόν μη αντιμετωπίσιμη.⁹³ Από τη μεριά του ο Honing υποστηρίζει πως ο

⁹¹ Ο Κωνσταντίνος Κολιόπουλος στις σελίδες 28-29 του *Στρατηγικός Αιφνιδιασμός. Υπηρεσίες Πληροφοριών και Αιφνιδιαστικές Επιθέσεις* αναφέρει πως η έννοια του στρατηγικού αιφνιδιασμού δεν γίνεται αντιληπτή με τον ίδιο τρόπο από όλους τους μελετητές. Π. χ. ο Ντέιβιντ Τουϊνγκ ορίζει ως τέτοια δράση την καταφυγή σε πολεμικές επιχειρήσεις υψηλής έντασης τις οποίες δεν αναμένει ο αντίπαλος και εκ των οποίων τίθεται σε απειλή η ύπαρξή του. Η Καταρίνα Μπροντίν μιλά για «μια επίθεση χωρίς καμιά ή με ελάχιστη προειδοποίηση» ή / και για «μια επίθεση που εξαπολύεται από θέση στάσης χωρίς μακρές προετοιμασίες» τη στιγμή που «ο αντίπαλος συλλαμβάνεται απροετοίμαστος σε σχέση με τα μέσα που διαθέτει και μπορεί να κινητοποιήσει σε περιπτώσεις αναμενόμενων δράσεων». Σε γενικές γραμμές μια αξιοσημείωτη πλειάδα μελετητών (Andrews, Knorr, Morgan) συμφωνεί πως ένας στρατηγικός στρατιωτικός αιφνιδιασμός αποπειράται να προξενήσει στον αντίπαλο μια συντριπτική ήττα, αντιπροσωπεύει, δε, μια έντονη και άμεση απειλή κατά των ζωτικών εθνικών συμφερόντων του. Ο Αριέλ Λεβίτε, συναθροίζοντας τα δεδομένα, ορίζει ως στρατηγικό αιφνιδιασμό την κατάσταση κατά την οποία ένα κράτος καταλαμβάνεται εξαπίνης από ένα άλλο σε στρατηγικό επίπεδο διαπιστώνοντας πως η αντίληψη απειλής, βάσει της οποίας λειτουργούσε, ήταν λανθασμένη -περί τούτων βλέπε Brian Greene, *Rethinking Strategic Surprise. Defence Planning Under "Bounded Uncertainty"*, Defence R&D Canada / Centre for Operational Research & Analysis, Canada, 2010, σ. 4. Σημειώνουμε πως ο όρος *στρατηγικός αιφνιδιασμός* δύναται να αντικατασταθεί από τον όρο *απόλυτος (στρατηγικός) αιφνιδιασμός* υπό την έποψη ενός συμβάντος που «ενσκήπτει από το πουθενά» -για περισσότερες λεπτομέρειες βλέπε στο *Intelligence Warning Terminology* (Οκτώβριος 2001, σ. 5-6) του Joint Military Intelligence College στη σελίδα <https://www.hsdl.org/?view&did=7443> όπου ανατρέξαμε τη 13^η Ιανουαρίου 2016

⁹² Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies" στο *International Journal of Intelligence and CounterIntelligence*, Volume 20, Issue 4, 2007, σ. 699-700. Αλλά πώς ορίζει την στρατηγική αιφνιδιαστική επίθεση ο Honing; Κατ' αυτόν μια τέτοια δράση οριοθετεί την από μεριάς επιτιθέμενου 'υπέρβαση' εις βάρος ζωτικών συμφερόντων του δέκτη της επίθεσης ...*a crossing of interstate lines against the victim's expectations*. Ο ερευνητής θεωρεί ότι η λύση πρέπει να αναζητηθεί στη βελτίωση της αναλυτικής διαδικασίας καθώς αυτή (η λύση) καθόλου δεν βρίσκεται, συνεχίζει, εντός του πλέγματος Υπηρεσιών και πολιτικής ηγεσίας (*decisionmaker-intelligence nexus*) τη στιγμή, μάλιστα, που η αποτυχία μάλλον δεν οφείλεται σε παρενέργειες του *Συνδρόμου Ψευδούς Συναγερμού (Cry Wolf Syndrome)* ή, αλλιώς, *Alert Fatigue Syndrome*

⁹³ Αυτό καταθέτει ο Stephen Marrin στη μονογραφία του "Preventing Intelligence Failures by Learning from the Past" θεωρώντας πως από το 1978 (έτος κατά το οποίο δημοσιεύθηκε το άρθρο "Analysis, War and Decision: Why Intelligence Failures Are Inevitable" του Richard Betts) και έπειτα ένα είδος ομοφωνίας έχει εμφανιστεί στους κόλπους των μελετητών του τομέα της πληροφόρησης. Σύμφωνα με αυτήν, η αποτυχία στην απόκρουση ενός αιφνιδιασμού πρέπει να θεωρείται, σχεδόν, δεδομένη με τις

τρόπος με τον οποίο προσεγγίζεται η πληροφορία από την επιστημονική κοινότητα δεν μπορεί να υποδείξει τι ακριβώς δικαιούμαστε να απαιτούμε από τις Υπηρεσίες. Ο ερευνητής πιστεύει πως ερωτήσεις τύπου «τι πήγε λάθος;» ή «ποιος φταίει;» συνθέτοντας το κύριο ενδιαφέρον των θεωρητικών του πεδίου το μόνο που προσφέρουν είναι να εμπλουτίζουν μια λίστα παθολογιών⁹⁴ και πολύ λιγότερο να συνεισφέρουν στη λύση του προβλήματος.⁹⁵

Σίγουρα υπάρχουν τρωτά ή ευαίσθητα σημεία, συνεχίζει ο Honing. Ζητούμενο δεν αποτελεί μόνο η καταγραφή τους αλλά, κυρίως, η θεραπεία τους. Όταν αυτό συμβεί μπορούμε να ορίσουμε φιλοδοξίες και προσδοκίες γύρω από τις Υπηρεσίες. Ο συγγραφέας ελέγχει τον τομέα της ανάλυσης της πληροφορίας πιστεύοντας πως το παραχθέν αποτέλεσμα έχει να κάνει με μια σειρά παραγόντων (ανθρώπινο δυναμικό, μεθοδολογικά εργαλεία). Σχετικά μ' αυτό, αντλώντας και αναφερόμενος στις δύο άνω Σχολές, γράφει:

- Η Ορθόδοξη Σχολή τονίζει τους περιορισμούς εντός των οποίων κινείται η διαδικασία ανάλυσης πληροφοριών. Πώς μπορεί να προσδιοριστεί επακριβώς ένας κίνδυνος αιφνιδιασμού όσον αφορά στο είδος και στον χρόνο εκδήλωσής του; Ο Richard Betts καταθέτει πως ακόμα και αν διαθέτουμε μια πρόωγη ενημέρωση δεν μπορούμε να ευελπιστούμε σε μια αρκούντως ικανή αντίδραση.⁹⁶ Κατ' αυτόν τον τρόπο μια αποτυχία δεν πρέπει να χρεωθεί τόσο στην ανικανότητα των Υπηρεσιών ή της πολιτικής ηγεσίας⁹⁷ αλλά, κυρίως, στο ευμετάβλητο και διαχειριστικά δύσκολο του προβλήματος ήτοι, στην ασάφεια ή / και πολυπλοκότητα των πληροφοριών, στον χρονικό περιορισμό, στη δυνατότητα παραπλάνησης εκ μέρους του αντιπάλου κ. λ.⁹⁸ -πρόκειται για

Υπηρεσίες ελάχιστα μόνο να μπορούν να προσφέρουν -για περισσότερες πληροφορίες βλέπε Marrin Stephen, "Preventing Intelligence Failures by Learning from the Past" στο *International Journal of Intelligence and CounterIntelligence*, Volume 17, Issue 4, 2004, σ. 661

⁹⁴ Ειδικότερα περί των παθολογιών των υπηρεσιών Πληροφοριών βλέπε Κολιόπουλος Κ., *Στρατηγικός Αιφνιδιασμός. Υπηρεσίες Πληροφοριών και Αιφνιδιαστικές Επιθέσεις*, Ελληνικά Γράμματα, Αθήνα, 2000, σ. 93-115

⁹⁵ Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 700

⁹⁶ Και αυτό γιατί η όλη αναλυτική διαδικασία στερείται κατάλληλων εργαλείων προκειμένου να συλληφθεί το νόημα μιας πρωτογενούς πληροφορίας. Ο Richard Betts θεωρεί πως πολύ λίγα μπορεί να γίνουν ώστε να βελτιωθεί η κατάσταση τη στιγμή που η διαδικασία της ανάλυσης πρέπει να αντισταθεί προσκομιμάτων όπως η ασάφεια των συλλεχθέντων στοιχείων (ambiguity of evidence) ή η αμφιβολία περί του ορθού της τελικής κρίσης (ambivalence of judgment) -περί αυτών βλέπε Betts Richard, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable" στο *World Politics*, Volume 31, Number 1, 1978, σ. 61-62, 69-72. Ο ίδιος μελετητής στη σελίδα 4 του *Surprise Attack: Lessons for Defense Planning* (Brookings Institution Press, Ουάσιγκτον, 1982) καταθέτει πως ...ένας στρατηγικός αιφνιδιασμός συνίσταται στο βαθμό που το θύμα δεν έχει εκτιμήσει την πιθανότητα εκδήλωσής του, το πότε, το που και το πώς ο αντίπαλος θα χτυπήσει -περί τούτων βλέπε Brian Greene, *Rethinking Strategic Surprise. Defence Planning Under "Bounded Uncertainty"*, ό. π., σ. 2

⁹⁷ Betts R., "Fixing Intelligence" στο *Foreign Affairs*, Volume 81, Number 1, 2002, σ. 57. Από την άλλη ο Betts δεν αθώνει ούτε τις Υπηρεσίες ούτε την πολιτική ηγεσία. Φέροντας ως παράδειγμα την 11^η Σεπτεμβρίου εγκαλεί και τους δύο θεσμικούς βραχίονες -για περισσότερες λεπτομέρειες βλέπε Morgan Trujillo "Are Intelligence Failures Inevitable?", Νοέμβριος 2012, στη δικτυακή τοποθεσία <http://www.e-ir.info/2012/11/08/are-intelligence-failures-inevitable/> εις την οποία ανατρέξαμε τη 13^η Ιανουαρίου 2016

⁹⁸ Ό,τι επισημαίνεται κατηγοριοποιείται, κατά βάσει, εντός του *Φαινομένου του Θορύβου* και της *Υπαρξης Δομικού Μειονεκτήματος*. Το πρώτο αναφέρεται στο γεγονός της εμφάνισης πολλαπλών σημάτων προειδοποίησης που αναγνωρίζονται ως ανταγωνιστικά, αντιφατικά, ενδεχομένως παραπλανητικά ή ανούσια δυσχεραίνοντας / συσκοτίζοντας το έργο των Υπηρεσιών. Το Δομικό Μειονέκτημα σχετίζεται με το γεγονός της ανάληψης πρωτοβουλιών από τον αντίπαλο σε άγνωστο χρόνο προσδίδοντας στον τελευταίο το αβαντάζ της λεγομένης «χρονικής διαφοράς» ή του λεγομένου «παραγόμενου αιφνιδιασμού» τη στιγμή που το κράτος-στόχος υπόκειται στο μειονέκτημα της

στοιχεία που δημιουργούν ένα πληροφοριακό / αναλυτικό χάντικαπ.⁹⁹ Από την πλευρά τους οι Αναθεωρητικοί βεβαιώνουν πως έχει δοθεί ιδιαίτερη προσοχή σε αποτυχίες τη στιγμή που παραγνωρίζονται επιτυχίες. Υπό αυτών των περιστάσεων θεωρητικές μελέτες τρόπων ανάλυσης πληροφοριακού υλικού, και κατ' επέκταση αποφυγής αιφνιδιαστικών επιθέσεων, ή, γενικότερα, προσπάθειες δόμησης μιας κεντρικής *normative-positive* θεωρίας πληροφόρησης¹⁰⁰ δεν έχουν ευδοκιμήσει. Για τους Αναθεωρητικούς τα λάθη δεν είναι αναπόφευκτα. Προκαλούνται από εσωτερικές αστοχίες, π. χ. έλλειψη προσοχής, των οποίων η ίαση καλείται και δύναται να επιτευχθεί.¹⁰¹

- Οι Ορθόδοξοι διατείνονται πως είναι φύσει αδύνατο να αποκρυπτογραφηθεί / αξιοποιηθεί καλώς ακόμα και μια ορθή πληροφορία. Πριν την αξιοποίηση, λένε, προηγείται η αξιολόγηση. Πέρα των δυσκολιών αποκωδικοποίησης, οι αναλυτικές διαδικασίες αυτές καθαυτές, συνεχίζουν, χωλαίνουν επιστημολογικά / μεθοδολογικά.¹⁰² Οι Αναθεωρητικοί επικεντρώνουν στην έλλειψη ικανοποιητικής πληροφόρησης όπως και ενός ευρύτερου σχεδιασμού που δεν θα σχετίζεται με το κομμάτι της ανάλυσης ή μόνο μ' αυτό. Το πρόβλημα πιστεύουν έγκειται περισσότερο στη συλλογή της πληροφορίας και λιγότερο στην ανάλυσή της.¹⁰³
- Οι Ορθόδοξοι υποστηρίζουν ότι οι αποτυχίες δεν δεικνύουν αμέλεια ή χαμηλό υπηρεσιακό πνεύμα αλλά οφείλονται σε ασαφή πληροφοριακά *analysis patterns* που επηρεάζουν την κρίση του προσωπικού. Η δυσλειτουργία σχετίζεται με το γεγονός της εγκαθίδρυση μοντέλων ανάλυσης που ικανοποιούν περισσότερο τη φύση του ανθρώπου παρά την «αντικειμενική πραγματικότητα», συνεπώς, δεν είναι εύκολο να απορριφθούν.¹⁰⁴, ¹⁰⁵ Από τη μεριά τους οι Αναθεωρητικοί βεβαιώνουν πως οι *ανθρωπογενείς γνωσιακές ευρετικές (human cognitive heuristics)* που χρησιμοποιούνται δεν είναι απαραίτητως κακές. Τα όποια σφάλματα δεν προέρχονται από αυτές αλλά από τον ειδικότερο τρόπο σκέψης

«χρονικής στέρξης» και της άμεσης ανάγκης «απορρόφησης της αιφνίδιας επίθεσης» -για περισσότερες λεπτομέρειες βλέπε Κολιόπουλος Κ., *Στρατηγικός Αιφνιδιασμός. Υπηρεσίες Πληροφοριών και Αιφνιδιαστικές Επιθέσεις*, ό. π., σ. 93-101

⁹⁹ Και δυστυχώς ...*not only is uncertainty ubiquitous, it is impossible to get rid of it by merely working hard to do so*, όπως ο αναλυτής Paul Davis σημειώνει -για μια άποψη βλέπε Brian Greene, *Rethinking Strategic Surprise. Defence Planning Under "Bounded Uncertainty"*, ό. π., σ. 2

¹⁰⁰ Υπονοώντας τη δημιουργία ενός 'χάρτη' που θα υποδεικνύει δρόμους μεταξύ αυτού που πρέπει και αυτού που δύναται να γίνει

¹⁰¹ Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 701

¹⁰² Στην ουσία οι Ορθόδοξοι χαρακτηρίζουν ως 'αντιεπιστημονικές' τις όποιες διαδικασίες ανάλυσης. Το ζητούμενο γι αυτούς είναι η εύρεση μοντέλων μέσω των οποίων θα φιλτράρονται 'επιστημονικά' οι πληροφορίες (*standards of evidence*)

¹⁰³ Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 701-702

¹⁰⁴ Ουσιαστικά αναφερόμαστε στο *Cognitive Bias* φαινόμενο -για περισσότερες λεπτομέρειες βλέπε στη σελίδα <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art12.html> από όπου αντλήσαμε υλικό την 23^η Οκτωβρίου 2016

¹⁰⁵ Η κριτική των οπαδών της Ορθόδοξης Σχολής έχει να κάνει με στοιχεία που ο Betts εντάσσει εντός του γκρουπ των «innocent enemies» και αυτού των «inherent enemies» -για περισσότερες πληροφορίες βλέπε Dujmovic Nicholas, "Intelligence in Recent Public Literature. Enemies of Intelligence: Knowledge and Power in American National Security" στο *Studies in Intelligence*, Volume 51, Number 4, 2007, σ. 40. Σ' αυτό το σημείο σημειώνουμε πως ο Betts με το πέρασμα του χρόνου άμβλυσε έστω ελάχιστα τις, από το 1978, θέσεις του παραδεχόμενος ορισμένες επιτυχίες των αμερικανικών υπηρεσιών Αντικατασκοπίας θεωρώντας πως μια μικρή βελτίωση στη λειτουργία και αποδοτικότητα των μυστικών υπηρεσιών μπορεί να λάβει χώρα -για περισσότερα βλέπε Richard Betts, "Fixing Intelligence", ό. π., σ. 59

και την ιδιαίτερη αντίληψη της κάθε μονάδας ατομικά ή ομάδας συλλογικά, άρα, η προσωπικότητα των «πρακτόρων» είναι αυτή που μετράει. Η πρώτη Σχολή δεν αποδίδει μια αποτυχία σε έλλειψη υπηρεσιακού επαγγελματισμού τη στιγμή που η δεύτερη θεωρεί την παρουσία του ή την έλλειψή του καίριο παράγοντα επιτυχίας ή αποτυχίας. Η Ορθόδοξη Σχολή διακηρύσσει μια εγγενή γνωσιακή / ψυχολογική αδυναμία του ανθρώπινου δυναμικού των Υπηρεσιών που αντικατοπτρίζεται στη διαδικασία της ανάλυσης της πληροφορίας όταν η Αναθεωρητική Σχολή επικεντρώνει στην έλλειψη στοιχείων και στον (αντι)επαγγελματισμό ορισμένων στελεχών.¹⁰⁶

- Όσον αφορά στο ζήτημα της *παραπληροφόρησης (disinformation)* και του *θορύβου (noise)* σημειώνουμε πως οι Ορθόδοξοι πιθανολογούν σε συντριπτικό ποσοστό την επιτυχία μιας προσεκτικά σχεδιασμένης επιχείρησης παραπληροφόρησης από τη στιγμή που το δυνητικό θύμα δεν βρίσκεται εντός των κέντρων αποφάσεων του δυνητικού θύτη ούτως ειπείν, δεν γνωρίζει. Οι Αναθεωρητικοί αντικρούουν λέγοντας πως μια ικανή υπηρεσία Αντικατασκοπίας δεν θα αργήσει να συλλέξει έστω και ένα ελάχιστο στοιχείο που θα καταδείξει τις αντίπαλες προθέσεις.¹⁰⁷ Συνεχίζοντας, και σύμφωνα με τους πρώτους, το φαινόμενο των αντιφατικών πληροφοριών / εικόνων, εξ αιτίας του πληροφοριακού θορύβου, δεν είναι δυνατόν να ξεπεραστεί μέσω κάποιου «φίλτρου αληθείας». Για την Roberta Wohlstetter μια *a priori* γνώση περί αξιοπιστων ή μη πληροφοριών δεν μπορεί να επιτευχθεί. Κατά παρόμοιο τρόπο η Janice Stein γράφει πως ...μόνον κατόπιν εορτής αντιλαμβανόμαστε την αλήθεια. Οι μελετητές της δεύτερης Σχολής υιοθετούν την άποψη ότι όπως ένας καταξιωμένος ιατρός ή ένας κορυφαίος σκακιστής προβλέπουν / επιλέγουν μέσα από έναν τεράστιο όγκο πιθανοτήτων / δεδομένων τη σωστή θεραπεία ή την ενδεδειγμένη επόμενη κίνηση, έτσι και ένας έμπειρος αναλυτής πληροφοριών θα πράξει. Σύμφωνα με την Deborah Larson ...τα μοντέλα (ανάλυσης) βασίζονται σε όγκο-ους ενδείξεων που συνδέονται / διαπλέκονται όπως ακριβώς τα ράμφη και τα φτερά ενός σμήνους πτηνών. Ένα κράτος που σχεδιάζει μια επίθεση θα μετακινήσει τα στρατεύματά του, θα συλλέξει προμήθειες, θα εκτοξεύσει απειλές κ. λ.^{108, 109}

¹⁰⁶ Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 702-703

¹⁰⁷ ό. π., σ. 704. Ο Michael Handel γράφει ότι ένας αιφνιδιασμός πολύ σπάνια λαμβάνει χώρα καταφέροντας ολοκληρωτικά να αποκρύψει στοιχεία ή προειδοποιητικά σινιάλα που αφορούν στο χώρο και χρόνο εκδήλωσής του. Μια επίθεση τέτοιου είδους (*attack out of the blue*) σχεδόν δεν δύναται να υπάρξει. Επίσης, σπάνια έχουν καταγραφεί αιφνιδιαστικές επιθέσεις των οποίων προηγούνται μόνο λίγα προειδοποιητικά σημάδια, συνήθως προηγείται ένα ικανό σώμα ενδείξεων -για μια εικόνα βλέπε Handel M., *War, Strategy, and Intelligence*, ό. π., σ. 349, υποσημείωση 32

¹⁰⁸ Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 705

¹⁰⁹ Για τους μελετητές που δεν αποκλείουν μια πετυχημένη αντιμετώπιση ενός στρατηγικού αιφνιδιασμού ισχύει η παραδοχή πως μια τέτοια πρόθεση συνοδεύεται από κάποιες ενδείξεις, πως υφίσταται μια *τυπολογία καταστάσεων στρατηγικής προειδοποίησης* -περί τούτου βλέπε Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 710-712. Από την άλλη μεριά πρέπει να σημειώσουμε πως κατά την Cynthia Grabo ένας στρατηγικός αιφνιδιασμός μπορεί μεν να προβλεφθεί αλλά δύσκολα να οριοθετηθεί εντός συγκεκριμένου χρόνου. Αυτό οφείλεται στο γεγονός των ανιχνεύσιμων αρχικών προετοιμασιών του δυνητικού θύτη τη στιγμή που δεν μπορεί να εντοπισθεί το πότε ο τελευταίος θα 'απασφαλίσει'. Αυτή τη δεδομένη στιγμή, και έχοντας ολοκληρώσει σε μέγιστο βαθμό τις προετοιμασίες, ελάχιστα (συνεπώς εύκολα προστατεύσιμα) απομένουν να τελεστούν πριν το 'readiness' στο οποίο βρίσκεται μετακυλήσει σε 'scramble'. Ιδιαίτερα αξιοσημείωτο είναι το γεγονός πως ο επιτιθέμενος αρκετές φορές, και για διάφορους λόγους, παραβιάζει ή αναγκάζεται να μην τηρήσει το προβλεπόμενο χρονοδιάγραμμα μεταθέτοντας την έναρξη των επιχειρήσεων σε κάποιο μελλοντικό σημείο που ενίοτε δεν γνωρίζει καν αυτός -περί τούτων βλέπε Grabo Cynthia, "Strategic Warning: The Problem of Timing" στο *Studies in Intelligence*, Volume 16, Number 2, 1972, σ. 80-82. Τέλος, ασχολούμενη με τα κύρια προσχώματα μιας έγκαιρης

Ο Honig καταλήγει στο συμπέρασμα πως οι απαντήσεις στα αίτια των αποτυχιών πρόβλεψης / αντιμετώπισης μιας αιφνιδιαστικής επίθεσης συνθέτουν έναν ανόμοιο όγκο. Εντούτοις πρέπει να γίνει αποδεκτό πως υπάρχουν περιθώρια βελτίωσης των αμυντικών (αντι)δράσεων τη στιγμή που κάποιες καταστάσεις δεν δύναται να αποφευχθούν. Οι δύο Σχολές αντιλαμβάνονται διαφορετικά το ζήτημα -για τους μεν το ποτήρι είναι μισοάδειο ή σχεδόν άδειο, για τους δε μισογεμάτο ή σχεδόν γεμάτο¹¹⁰, για ορισμένους ένας στρατηγικός αιφνιδιασμός είναι σχεδόν αδύνατο να αντιμετωπιστεί, για κάποιους άλλους δεν αποκλείεται μια ικανοποιητική αντίδραση από μεριάς αμυνομένου.¹¹¹

Το 2004 ο Stephen Marrin υποστήριξε πως η αποτυχία της πρόβλεψης του χτυπήματος το Σεπτέμβρη του 2001 δεν μπορεί να αποδοθεί με σιγουριά ούτε στις αμερικανικές υπηρεσίες Αντικατασκοπίας, ούτε στην πολιτική ηγεσία. Το πλεονέκτημα του επιτιθέμενου είναι ότι σχεδιάζει κάτω από απόλυτη μυστικότητα και δρα σε άγνωστο χρόνο, άρα, οι Υπηρεσίες πρέπει είτε να ανακαλύψουν, είτε να μαντέψουν κάτι που, σχεδόν, «δεν υπάρχει». Ο Marrin συνέχισε λέγοντας πως όσο και αν οι πράκτορες εξοπλίζονται με την τελευταία λέξη της τεχνολογίας, όσο και αν δρουν εν κρυπτώ και παραβύστω και υπό συνθήκες μέγιστης κρατικής κάλυψης, δεν έχουν κάτι εύκολο να αντιπαλέψουν. Περαιτέρω, η έννοια της αποτυχίας είναι σχετική. Αποτυχίες κάνουν την εμφάνισή τους καθημερινά. Άλλες είναι ασήμαντες, άλλες ηχηρές και αυτό δεν έχει να κάνει μόνο με το γεγονός καθαυτό αλλά και με το χρόνο εκδήλωσής του, τις πολιτικές συνθήκες, τις επιπτώσεις που, ενδεχομένως, ποικίλουν από χρόνο σε χρόνο κ. λ.¹¹²

προειδοποίησης αναφέρεται: α) στην ανεπαρκή κατανόηση των πληροφοριών, β) στην προσκόλληση στην τελευταία πριν την εκδήλωση ενός αιφνιδιασμού εικόνα. Συνηθέστατα πρόκειται για εικόνα ηρεμίας που καθησυχάζει το δυνητικό θύμα, γ) στην προσκόλληση / εμμονή σε ακλόνητες απόψεις, ιδέες κ. λ., δ) στη μη γνώση του χρόνου προσβολής, ε) στη διστακτικότητα αποδοχής δυσάρεστων πληροφοριών, στ) στη διστακτικότητα έναρξης συναγεμμού, ζ) στο φόβο, γενικότερα, της διάπραξης λάθους -για μια εικόνα βλέπε Grabo Cynthia, *Anticipating Surprise. Analysis for Strategic Warning*, Joint Military Intelligence College's Center for Strategic Intelligence Research, Washington, D.C., 2002, σ. 163-169

¹¹⁰ Honig Arthur Or, "A New Direction for Theory-Building in Intelligence Studies", ό. π., σ. 712-713

¹¹¹ Η αποστολή διευκολύνεται αν υπονιάζομαστε το δυνητικό δράστη. Κάτι τέτοιο είναι πολύ πιθανό καθώς, όπως φαίνεται, μια στρατηγική αιφνιδιαστική επίθεση έπεται μιας περιόδου αντεγκλήσεων ένθεν και εκείθεν. Συνεπώς, αν και είναι δύσκολο να γνωρίζουμε το χρόνο και το χώρο εκδήλωσής της, αυτό δεν ισχύει όσον αφορά στην ταυτότητα του πιθανού θύτη. Με λίγα λόγια, ό,τι παρουσιάζεται ως παντελώς ασαφές μπορεί τελικά να αποτελεί μια «περιορισμένη αβεβαιότητα» (bounded uncertainty) με τις πιθανότητες αντίδρασης να αυξάνονται -για περισσότερες λεπτομέρειες βλέπε Brian Greene, *Rethinking Strategic Surprise. Defence Planning Under "Bounded Uncertainty"*, ό. π., σ. 7-8 ¹¹² Marrin St., "Preventing Intelligence Failures by Learning from the Past" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 656-658

ΚΕΦΑΛΑΙΟ 6

Αντικατασκοπία και οικονομία

6.1

Οικονομική αντικατασκοπία

Εισαγωγή στην οικονομική αντικατασκοπία.

Ο ρόλος της οικονομικής αντικατασκοπίας έναντι της οικονομικής κατασκοπίας (Financial Intelligence -FININT) σχετίζεται: α) με εντοπισμό / εξουδετέρωση προσπαθειών ξένων Υπηρεσιών που στοχοποιούν μυστικά της εγχώριας ιδιωτικής / κρατικής οικονομικής δραστηριότητας και επιχειρηματικότητας (Kristen Michal, Samuel Porteous), β) με προσπάθεια κατάδειξης του αναποτελεσματικού μιας δράσης οικονομικής κατασκοπίας με απώτερο στόχο την αποτροπή σχετικών σκέψεων / πράξεων (Thompson Strong), γ) με άσκηση μιας, στην πραγματικότητα, παραδοσιακής δράσης προστασίας οικονομικών πόρων (Randal Fort).¹

Ο Michael Turner, αξιωματούχος της CIA, τονίζει τη σύνδεση οικονομικής αντικατασκοπίας και στρατιωτικής ασφαλείας καθώς δεν είναι μόνο οι στρατιωτικές διαβαθμισμένες πληροφορίες που αφορούν στην τελευταία αλλά και οι τεχνολογικές ανάλογες (στην ουσία κάνει λόγο για σχέση μεταξύ οικονομίας, ανταγωνιστικότητας, τεχνολογίας και στρατιωτικού πεδίου).²

Ο Ιωάννης Κωνσταντόπουλος διαχωρίζει την οικονομική αντικατασκοπία του 20^{ου} και 21^{ου} αιώνα σε δύο περιόδους, την ψυχροπολεμική και τη μεταψυχροπολεμική. Τα στοιχεία της πρώτης περιόδου δείχνουν ότι η άσκηση οικονομικής αντικατασκοπίας περνούσε μέσα από τα φίλτρα των διεθνών πολιτικών σκοπιμοτήτων. Ειδικότερα και όσον έχει να κάνει με τις ΗΠΑ ο κάματος κατά την περίοδο του ψυχρού πολέμου δεν αφορούσε στην αποκάλυψη των επιχειρήσεων οικονομικής κατασκοπίας των δυτικών συμμάχων εις βάρος της χώρας, αλλά, μάλλον, στη συγκάλυψη. Ο Peter Schweizer γράφει πως οι αμερικανικές Υπηρεσίες και η πολιτική ηγεσία επουδενί θα διακινδύνευαν τη διακρατική συνεργασία υπό το βάρος μιας αποκάλυψης «οικονομικών κατασκόπων» καθώς η συνοχή έναντι της σοβιετικής απειλής προείχε. Στο ίδιο μήκος κύματος ο Herb Meyer τονίζει το ζήλο των ΗΠΑ να κερδίσουν τον ψυχρό πόλεμο μέσα από μια κατάθεση οικονομικών πόρων και πνευματικής ενέργειας που, ωστόσο, δεν φαίνεται να συμμερίστηκαν οι σύμμαχοί τους. Οι τελευταίοι κατέφυγαν σε αμφιλεγόμενες πρακτικές προκειμένου να αποσπάσουν πληροφορίες, πάρα ταύτα, όπως ο Bob Inman δηλώνει, ο ψυχρός πόλεμος δεν επέτρεπε μια εμφανή αντίδραση εκ μέρους των Ηνωμένων Πολιτειών. Κάτι άλλο που «ακύρωνε» μια αντικατασκοπευτική πρόληψη / δράση, πέραν της αμερικανικής εκούσιας αβλεψίας, σχετίστηκε με την κείμενη νομοθεσία. Όπως καταθέτει ο

¹ Michal Kr., “Business counterintelligence and the role of the U.S. intelligence community” στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 4, 1994, σ. 417, Fort Randall, “Economic Espionage” στο *U.S. Intelligence at a Crossroad*, επιμ. Godson R., May E., et al., Brassey's UK Ltd, ΗΠΑ, 1995, σ. 182, Porteous S., “Economic & Commercial Interests and the World's Intelligence Services: A Canadian Perspective” στο *International Journal of Intelligence and CounterIntelligence*, Volume 8, Issue 3, 1995, σ. 288, Strong T., “Tilting with Machiavelli: Fighting Competitive Espionage in the 1990s” στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 2, 1995, σ. 170

² Turner M., “Understanding CIA's Role in Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 4, Issue 3, 1990, σ. 300

Maynard Anderson ακόμα και οι αυστηρότερες ποινές ...ήσαν πολύ περισσότερο επιεικείς από τις ανάλογες περί συμβατικής κατασκοπίας. Πρέπει να περιμένουμε το 1981 όταν η κυβέρνηση Reagan φάνηκε να αντιδρά. Βέβαια δεν επρόκειτο για κάποια δραματική μεταστροφή, αλλά, μάλλον, για ένα συγκρατημένο, ωστόσο, στοχευμένο πρόγραμμα παρακολούθησης φιλικών ή ουδέτερων κρατών. Τελικά με την πάροδο του χρόνου και αυτή η κίνηση εξέπεσε σε επίπεδο νουθεσιών προς τους «αδιόρθωτους συμμάχους».³

Είναι με την πτώση του Τείχους όταν ο πρέσβης Richard Walker δηλώνει ότι η οικονομική αντικατασκοπία ...θα αποκτήσει τώρα μεγαλύτερη σημαντικότητα. Η συμπεριφορά τύπου «πρέπει να είμαστε στην κορυφή των επιστημονικών και τεχνολογικών εξελίξεων με κάθε μέσο» άλλων οικονομικά ανεπτυγμένων κρατών, ακόμα και συμμάχων, υποδηλώνει διάθεση κατασκοπευτικής εμπλοκής.⁴ Την ξεκάθαρη τοποθέτηση / ρητορική του Walker ακολουθεί ο γερουσιαστής Boren του οποίου προτροπή δεικνύει η προστασία των εγχώριων επιχειρήσεων.⁵ Ο αξιωματούχος του FBI Raymond Wannal συμφωνεί υποστηρίζοντας πως στο παρελθόν η Υπηρεσία αφιέρωσε πόρους στον πόλεμο με τους Σοβιετικούς και τους συν αυτό αγνοώντας τη δράση «φίλων», η κατάσταση πρέπει να αλλάξει.⁶ Με τον τελευταίο συμπράττει ο πρώην αρχηγός της CIA, John Deutch. Ο Deutch ομιλεί ξεκάθαρα περί του ρόλου της αντικατασκοπίας ως προς την ενημέρωση εγχώριων επιχειρηματικών συμφερόντων όταν αυτά βρίσκονται σε κίνδυνο.⁷

Γενικά καθ' όλη τη δεκαετία του 1990 παρατηρείται μια μεταστροφή στην αμερικανική αντίληψη περί οικονομικής κατασκοπίας / αντικατασκοπίας. Είναι ο πρόεδρος Bush ο πρεσβύτερος που τάσσεται υπέρ της συλλογής πληροφοριών προκειμένου να αποτραπεί οποιοσδήποτε επιχειρών υποκλοπή εγχώριας τεχνολογίας, οποιοσδήποτε που μετέρχεται δόλια μέσα αρνούμενος να αποδεχτεί τους διεθνείς οικονομικούς κανόνες.⁸ Είναι ο αρχηγός της CIA Robert Gates που συνδέει τη δράση της Υπηρεσίας με την διατήρηση της υψηλής αμερικανικής οικονομικής

³ Περί τούτων βλέπε Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, Αθήνα, 2010, σ. 587-591 και Schweizer P., *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal our Secrets*, Atlantic Monthly Press, USA, 1993, σ. 6-9, 286-287, 420. Πάντως το FBI εγκαινιάζει το 1974 το Developing Espionage and Counterintelligence Awareness program (DECA) με σκοπό την επαγρύπνηση των εμπλεκόμενων φορέων στην αμυντική βιομηχανία. Η κυβέρνηση Clinton συνεχίζει το 1994 με το National Counterintelligence Center (NACIC), το, δε, State Department αποδέχεται το 1995 το ρόλο τού «διαφωτιστή» της επιχειρηματικής κοινότητας όταν «κάτι δεν πάει καλά» αλλά και τον αντίστοιχο τού φορέα επίδοσης διαβημάτων διαμαρτυρίας σε χώρες των οποίων οι μυστικές υπηρεσίες «παρεκτρέπονται» -για μια εικόνα διάβαζε Johnson L., *Secret Agencies Intelligence in a hostile world*, Yale University Press, ΗΠΑ, 1996, σ. 167-168 και Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 603-604

⁴ Schweizer P., *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal our Secrets*, ό. π., σ. 10, 32

⁵ Wright Jeffrey, "Intelligence and Economic Security" στο *International Journal of Intelligence and CounterIntelligence*, Volume 5, Issue 2, 1991, σ. 206

⁶ Schweizer P., *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal our Secrets*, ό. π., σ. 11

⁷ DCI John Deutch, "Remarks at CIA Town Meeting", 11 Μαΐου 1995 στη διαδικτυακή σελίδα https://www.cia.gov/news-information/speeches-testimony/1995/dci_speech_51195.html στην οποία ανατρέξαμε την 9^η Δεκεμβρίου 2016, επίσης βλέπε Kober Stanley, "Why Spy? The Uses and Misuses of Intelligence", 1996 στο http://www.cato.org/pubs/pas/pa-265.html#FOOTNOTE_11 με ημερομηνία εισόδου τη 10^η Δεκεμβρίου 2014

⁸ Galvan Robert, "The Role of American Intelligence in the Global Economy: Business and Industrial Spying" στο *International Journal of Intelligence and CounterIntelligence*, Volume 8, Issue 3, 1995, σ. 353

ανταγωνιστικότητας⁹, ο ομόλογός του Richard Helms που διακηρύσσει μια ανάγκη προστασίας των αμερικανικών μικροοικονομικών μυστικών ως προϋπόθεση επιβίωσης του οικείου οικονομικού συστήματος¹⁰, ο ναύαρχος Stansfield Turner, ο πρώην εκπρόσωπος των ΗΠΑ στη General Agreement on Tariffs and Trade (GATT) πρέσβης Michael Smith, οι μελετητές Diane Snyder και Sean Gregory που επιθυμούν μια ουσιαστική επαγρύπνηση των Υπηρεσιών και δη και των τμημάτων Αντικατασκοπίας προκειμένου να ανακουφιστεί ο κόσμος της ημεδαπής οικονομίας από την εναντίον του κατασκοπική δραστηριότητα. Πέρα τούτων καταγράφονται τα όποια ευαίσθητα τεχνολογικά και βιομηχανικά assets, αναδιοργανώνεται το αντικατασκοπευτικό τμήμα του FBI, δημιουργείται η National Security Threat List (NSTL) με πρώτιστο, αλλά όχι μοναδικό, σκοπό την αποτροπή διαρροής στοιχείων περί κρίσιμων τεχνολογιών οικονομικού και στρατιωτικού χαρακτήρα όπως αυτές καταχωρούνται στη National Critical Technologies List (NCTL) του Λευκού Οίκου και στη Military Critical Technologies List (MCTL) του αμερικανικού υπουργείου Αμύνης.¹¹ Αν ο Deutch μιλά έξω από τα δόντια το 1995, είναι ο Gates, ήδη από το 1992, που υπογραμμίζει το ρόλο της «the Agency». Η τελευταία αυξάνει το ενδιαφέρον της περί οικονομικών πληροφοριών δίδοντας έμφαση στην αντικατασκοπία ούτως ειπείν, στον εντοπισμό και αντιμετώπιση περιπτώσεων παγίδευσης αμερικανικών επιχειρήσεων στην αλλοδαπή εκ μέρους Υπηρεσιών / κυβερνήσεων.¹² Το 1993 ο οικονομολόγος Richard Neu εκπονεί ένα πλάνο αντικατασκοπευτικής δράσης ενώ ο Lawrence Summers, αξιωματούχος του αμερικανικού υπουργείου Οικονομικών, καταθέτει στην Intelligence Committee της Γερουσίας περί του καίριου των πληροφοριακών οργανισμών στην αντιμετώπιση επίβουλων ενεργειών αλλότριων Υπηρεσιών και κρατών.¹³ Το 1994 ο James Woolsey, διευθυντής της CIA μεταξύ Φεβρουαρίου 1993 και Ιανουαρίου 1995, δηλώνει: «We are in the business of understanding when other countries and foreign companies, some of these countries quite friendly to the United States otherwise, are engaged in bribery in order to take contracts away from American corporations. We spend a great deal of time and effort trying to help the Secretary of State and the Secretary of Commerce be able to level that playing field».¹⁴

⁹ Schweizer P., *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal our Secrets*, ό. π., σ. 290, Schweizer P., «The Growth of Economic Espionage: America Is Target Number One» στο *Foreign Affairs*, Volume 75, Number 1, 1996, σ. 11

¹⁰ Evans Joseph, «U.S. Business Competitiveness and the Intelligence Community» στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 3, 1994, σ. 355

¹¹ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 595-598

¹² Warner William, «International technology transfer and economic espionage» στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 2, 1994, σ. 153. Είναι χαρακτηριστικό ότι ο William Studeman, πρώην επικεφαλής της NSA κατά την περίοδο 1988-1992, δηλώνει ότι εφόσον υπάρχουν αποδείξεις περί στοχοποίησης μιας αμερικανικής εταιρίας, τότε, η πληροφοριακή κοινότητα θα ενημερώσει την επιχείρηση, πιθανόν θα τη συμβουλεύσει τόσο σε τεχνικό όσο και πολιτικό επίπεδο. Εντός αυτού του πνεύματος η CIA, το Μάιο του 1993, προειδοποιεί ορισμένες ημεδαπές εταιρίες αεροδιαστημικής ότι σχετική έκθεση που ανοίγει τις πύλες της στο Παρίσι πρόκειται να κατακλειστεί από πράκτορες της γαλλικής υπηρεσίας εξωτερικών Πληροφοριών DGSE· οι εν λόγω εταιρίες είτε ακυρώνουν τη συμμετοχή τους είτε λαμβάνουν κατάλληλα μέτρα προστασίας -για μια ιδέα διάβαζε Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 602-603. Οποσδήποτε η αμερικανική Υπηρεσία δεν αποτελεί το μόνο παράδειγμα, παρόμοιες, π. χ., ανησυχίες εκφράζουν οι γαλλικές SGDN, DST, SIAR και DPSD ή η καναδική SCSR -περί τούτων βλέπε Guisnel Jean, *Πόλεμοι στον Κυβερνοχώρο. Μυστικές Υπηρεσίες και Internet*, μτφρ. Ζακοπούλου Γεωργία, Στάχυ, Αθήνα, 1997, σ. 233-237

¹³ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 600-601

¹⁴ Porteous Samuel, «Economic Espionage II», *Commentary*, Number 46 στην ιστοσελίδα <http://www.datapacrat.com/True/INTEL/CSIS/COM46E.HTM> όπου ανατρέξαμε την 11^η Δεκεμβρίου

Το δεύτερο μισό της δεκαετίας του 1990 οι αντικατασκοπευτικές δράσεις των αμερικανικών πληροφοριακών οργανισμών εντείνονται. Το 1995 το FBI επιδίδει διαμαρτυρία στην κυβέρνηση του Παρισίου όταν αποκαλύπτεται επιχείρηση οικονομικής κατασκοπίας των γαλλικών Υπηρεσιών εις βάρος της IBM και της Texas Instruments. Το 1996 το NACIC διοργανώνει συζήτηση με θέμα την απειλή της οικονομικής κατασκοπίας. Την ίδια χρονιά το National Security Council προειδοποιεί για ζητήματα που αφορούν στο πεδίο των λεγομένων δικαιωμάτων πνευματικής ιδιοκτησίας, από κοντά δραστηριοποιείται και το FBI.¹⁵

Κατά τον Jeffrey Wright η δημιουργία μιας ικανής ομπρέλας προστασίας οικονομικών μυστικών απαιτεί τη συνεργασία Υπηρεσιών και κυβέρνησης. Αυτό σημαίνει επέκταση των υφιστάμενων προγραμμάτων, αύξηση προσωπικού και τεχνικών / οικονομικών πόρων. Επιπλέον απαιτείται επαύξηση του κόστους που θα καταβάλει ο όποιος συλληφθείς. Ο Michal Kristen είναι σαφής: η πάταξη του φαινομένου πρέπει να στηριχθεί και στην επιβολή ικανών προστίμων, μακροχρόνιων καθειρξεων, εμπορικών κυρώσεων έναντι εταιριών ή κρατών που επενδύουν στις συγκεκριμένες τακτικές. Ο Schweizer συμφωνεί τονίζοντας ότι ακόμα και το καλύτερο αντικατασκοπευτικό δίκτυο δεν μπορεί να αποδώσει αν δεν υπάρξουν αξιοσημείωτες κυρώσεις. Οι αλλαγές πρέπει να εντοπιστούν όχι μόνο στη νομοθεσία αλλά και στον τρόπο με τον οποίο χαράσσεται η διπλωματική και εξωτερική πολιτική.¹⁶ Με τις απόψεις Kristen / Schweizer συμφωνούν οι David Boren, Arlen Specter, Herbert Hohl, όλοι γνωστοί πολιτικοί με τον πρόεδρο Κλίντον να ξεχωρίζει. Ο τελευταίος υπογράφει την Economic Espionage Act of 1996. Κατά τον Larry Torrence, αξιωματούχο του FBI, η συγκεκριμένη Πράξη αποδεικνύεται πραγματικό όπλο στα χέρια των αρχών¹⁷ χαράσσοντας μια νέα δυναμική στην αντιμετώπιση οικονομικών εγκλημάτων κατά επιχειρήσεων υψηλής τεχνολογίας.¹⁸

Μάκρο και μικρο -οικονομική αντικατασκοπία. Η πράξη

Σ' αυτό το σημείο ας δούμε πώς αποτυπώνει την οικονομική αντικατασκοπία στην πράξη ο Lock Johnson. Για τον μελετητή κύριο καθήκον ενός πράκτορα δεικνύει η προστασία του εγχώριου οικονομικού χαρτοφυλακίου από ενέργειες ξένων Υπηρεσιών. Ο Johnson υπό του όρου *economic portfolio* υποδηλώνει κάθε τι που

2016. Πάρα ταύτα ο Woolsey αναφερόμενος στις αμερικανικές επιχειρήσεις παρουσιάζεται δυσαρεστημένος καθώς ...δεν συνειδητοποιούν ποτέ ότι έχουν λάβει τη βοήθειά μας δηλώνοντας ακόμα και δημοσίως ότι δεν την έχουν ανάγκη. Ο ίδιος μιλά για χώρες ή trust που επιβουλεύονται την αμερικανική θέση καθώς και για προοπτικές επανορθώσεων / αποζημιώσεων δισεκατομμυρίων δολαρίων που καθίστανται, ενδεχομένως, απαιτητές υπό τη σοβαρότητα των στοιχείων που η CIA (θα) φέρει στο φως. Τέλος δεν αποφεύγει, σε ομιλία του στο Center for Strategic and International Studies (CSIS) στην Ουάσιγκτον τον Ιούλιο του 1994, να αγγίξει το ευαίσθητο θέμα χρηματισμού και δωροδοκιών προκειμένου ξένες επιχειρήσεις να λάβουν ευνοϊκότερη θέση στην κούρσα σύναψης υψηλών εμπορικών και συναφών διεθνών συμβολαίων -για μια καλύτερη εικόνα βλέπε Michal Kristen, "Business Counterintelligence and the Role of the U.S. Intelligence Community" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 417 και Kober Stanley, "Why Spy? The Uses and Misuses of Intelligence", 1996 στο http://www.cato.org/pubs/pas/pa-265.html#FOOTNOTE_11 με ημερομηνία ανάκτησης την 11^η Δεκεμβρίου 2014

¹⁵ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 604

¹⁶ ό. π., σ. 605

¹⁷ ό. π., σ. 606-607, βλέπε επίσης "Cybercrime, Transnational Crime and Intellectual Property Theft", (κατάθεση του Larry E. Torrence στη Joint Economic Committee του αμερ. Κογκρέσου στις 24 / 3 / 1998) στο <http://www.iwar.org.uk/ecoespionage/resources/senate/echearingmarch98/torrence.htm> όπου ανατρέξαμε τη 12^η Δεκεμβρίου 2014

¹⁸ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 607-608, επίσης βλέπε "Cybercrime, Transnational Crime and Intellectual Property Theft", ό. π.

σχετίζεται με την κρατική οικονομία, έτσι, ακόμα και ένα ταξίδι ενός κυβερνητικού παράγοντα προς εξυπηρέτηση σχετικών αναγκών ή διακρατικών διαμοιβών και συμβάσεων πρέπει να τσεκαριστεί ως προς την ασφάλειά του ή, αλλιώς, ως προς τον αποκλεισμό διαρροών που ενδέχεται να προκύψουν. Ωστόσο, δεν εξετάζεται μόνο η περίπτωση της επίθεσης ενός αλλότριου πληροφοριακού οργανισμού αλλά και αυτή μιας εθελούσιας συνεργασίας προσώπου ή προσώπων εκ των έσω.

Για τον Johnson κάθε κλασικό μέσο που σχετίζεται με προστασία «σκληρών περιοχών / στόχων» δύναται να χρησιμοποιηθεί προς κάλυψη κρατικών οικονομικών assets' τα εν χρήσει tricks-of-the-trade εμφανίζουν ομοιότητες. Ο καθηγητής δεν αρνείται τη σχέση μακροοικονομικής και μικροοικονομικής κατασκοπίας και κατ' επέκταση την εμπλοκή της αντικατασκοπίας και στις δύο διακριτές περιοχές. Κατ' αυτήν την έννοια οι αμερικανικές Υπηρεσίες «θα βρουν τρόπο να ενημερώσουν τον εγχώριο επιχειρηματικό κόσμο για τις όποιες αόρατες επικινδυνότητες με σκοπό την καίρια αντίδρασή του».¹⁹ Η έκφραση «θα βρουν τρόπο» δεν είναι τυχαία. Μέχρι τα μέσα της δεκαετίας του 1990 θεσμικό πλαίσιο συνεργασίας Υπηρεσιών και κόσμου της οικονομίας δεν υπήρξε, πιθανότατα δεν υπάρχει μέχρι και τα μέσα της δεκαετίας του 2010. Οι όποιες ανταλλαγές ακολουθούν υπόγειες διαδρομές, επαφίενται, δε, στην καλή διάθεση / διακριτική ευχέρεια των πληροφοριακών οργανισμών και στη δεκτικότητα του βιομηχανικού / επιχειρηματικού δικτύου. Όπως δήλωσε αξιωματούχος της CIA διατηρώντας την ανωνυμία του *...δεν επιχειρούμε αντικατασκοπευτική δράση όταν μια αντίστοιχη κατασκοπευτική διεξάγεται εις βάρος αμερικανικών εταιριών από ομόλογες αλλοδαπές. Επικεντρώνουμε σε ενέργειες κυβερνήσεων. Ωστόσο όταν ένας από εμάς πληροφορηθεί περί κατασκοπίας μιας ξένης φίρμας, τότε, αυτή η πληροφόρηση περνά στο σχετικό "policy department" της κυβέρνησης.* Από τη μεριά του ο Warren Christopher δεν διστάζει να υποστηρίξει το Νοέμβριο του 1993 μπροστά στην Επιτροπή Εξωτερικών Σχέσεων της Γερουσίας ότι «η εθνική ασφάλεια καθίσταται αχώριστη από την ανάλογη οικονομική» αφήνοντας να καταγραφεί μια αναγκαιότητα ύπαρξης αντικατασκοπευτικών οικονομικών πλάνων.²⁰ Ο Robert N. Galvan σε άρθρο του το 1995 υποστηρίζει πως η (αμερικανική) πληροφοριακή κοινότητα μπορεί να συμβάλει στην προστασία αλλά και στη μεγέθυνση της εγχώριας οικονομίας μέσω τριών εργαλείων: α) της οικονομικής ανάλυσης, β) των αμυντικών επιχειρήσεων και γ) των επιθετικών εγχειρημάτων που αφορούν στη βιομηχανική κατασκοπία. Συνοπτικά σημειώνουμε πως η οικονομική ανάλυση έχει να κάνει με απόδοση στοιχείων / μελετών σε πολιτικούς και οικονομικούς παράγοντες τη στιγμή που τα άλλα εγχειρήματα δεν απολαμβάνουν εκτίμησης εκ μέρους, τουλάχιστον, του εταιρικού κόσμου λόγω κουλτούρας επιχειρείν -προφανώς από το 1995 μέχρι σήμερα κάποια πράγματα, λίγα ή πολλά, έχουν διαφοροποιηθεί. Ωστόσο, αυτό που απασχολεί είναι η αντικατασκοπευτική οικονομική δράση. Ο Galvan σημειώνει πως: α) η συγκεκριμένη δράση είναι ίσως η πλέον συμβατή ως προς το προφίλ και τον χαρακτήρα των

¹⁹ Καταθέτοντας στο αμερικανικό Κογκρέσο ο, κατά την περίοδο Νοεμβρίου 1991-Ιανουαρίου 1993, Director of Central Intelligence (DCI) και επικεφαλής της CIA Robert Gates υποστήριξε πως σε ακραίες περιπτώσεις η δράση της αντικατασκοπίας «προκειμένου να προστατευτεί η [αμερικανική] οικονομία από πρόσωπα που δεν παίζουν σύμφωνα με τους κανόνες» καθίσταται απαραίτητη. Επιπλέον, συνέχισε λέγοντας ότι CIA και FBI πληροφορούν τον εταιρικό κόσμο για επίβουλες κινήσεις ξένων συμφερόντων αφού προηγουμένως ληφθεί μέριμνα προστασίας «μεθόδων και πηγών» -περί τούτων βλέπε στην κατάθεση του Robert Gates στην υποεπιτροπή Οικονομικής και Εμπορικής Νομοθεσίας του αμερικανικού Κογκρέσου τον Απρίλιο και Μάιο του 1992 και ειδικότερα στο *The Threat of Foreign Economic Espionage to U.S. Corporations*, U.S. Government Printing Office, Washington, D.C., 1992, σ. 53-54

²⁰ Johnson L., *Secret Agencies U.S. Intelligence in a hostile world*, ό. π., σ. 166-168, 173

Υπηρεσιών και β) με την πάροδο του χρόνου οι αμυντικοί οικονομικοί σχεδιασμοί γίνονται όλο και πιο αποδεκτοί.²¹ Σχετικά με το τελευταίο ο John F. Hayden, αντιπρόεδρος της Boeing Corporation, καταθέτει, εν έτει μάλιστα 1993, ενώπιον του αμερικανικού Κογκρέσου πως η εταιρία του προκρίνει την παροχή κυβερνητικής προστασίας όσον αφορά στην αποσόβηση φαινομένων διαρροής τεχνολογικών και λοιπών συναφών μυστικών προς όφελος αλλοδαπών ανταγωνιστών όταν μια ανάλογη κυβερνητική «επιθετική βοήθεια» δεν ενδιαφέρει.²²

Μάκρο και μικρό -οικονομική αντικατασκοπία. Προβληματισμοί σε επιχειρησιακό επίπεδο

Ό, τι δυσκολεύει τη δράση της οικονομικής αντικατασκοπίας έχει να κάνει με: α) την, για πολλούς, αναγκαιότητα εμπλοκής στο παίγνιο μιας ξένης κυβέρνησης. Κατ' αυτόν τον τρόπο το αντικατασκοπευτικό κίνητρο ακυρώνεται όταν αναφερόμαστε σε βιομηχανική κατασκοπία. Βέβαια υπάρχουν φωνές που υποστηρίζουν ότι η εμπλοκή μιας κυβέρνησης έτσι κι αλλιώς δεν είναι ευδιάκριτη ή πως το συγκεκριμένο επιχείρημα καταπίπτει εάν σκεφτούμε ότι οι Υπηρεσίες καταδιώκουν, π. χ., την τρομοκρατία ανεξαρτήτως του αν προέρχεται από επίσημους ή μη δρώντες, β) τη χρήση της υψηλής τεχνολογίας εκ μέρους του επιτιθέμενου, γ) την εγγενή δυσκολία διαφύλαξης πληροφοριών / προϊόντων οικονομικού, βιομηχανικού, τεχνολογικού και λοιπού παρόμοιου χαρακτήρα σε σχέση, τουλάχιστον, με τη δυνατότητα διαφύλαξης ανάλογων στρατιωτικού ενδιαφέροντος. Είναι χαρακτηριστικό ότι έρευνα που εκπονήθηκε το 1993 υπολόγισε πως μόνο μία στις δώδεκα περιπτώσεις υφαρπαγής οικονομικών δεδομένων εντοπίζεται από τις αμερικανικές υπηρεσίες Αντικατασκοπίας.²³

Ο Ιωάννης Κωνσταντόπουλος υποστηρίζει ότι μια υπόθεση πλήρους επιτυχίας των αμερικανικών υπηρεσιών CI στον πόλεμο κατά της οικονομικής κατασκοπίας δεν αποτελεί άλλο από χίμαιρα, προφανώς, αυτό ισχύει για τις Υπηρεσίες κάθε χώρας. Από τη μεριά του ο William Warner καταδεικνύει τις δυσκολίες του εγχειρήματος υπογραμμίζοντας ότι: α) η οικονομική κατασκοπία υπάρχει, αναπτύσσεται και θα εξακολουθήσει να απειλεί ίσως, μάλιστα, με αυξητικούς ρυθμούς, β) το διεθνές κλίμα απαλλαγμένο από τα άγχη της προ του 1990 εποχής ευνοεί τις οικονομικές κατασκοπικές δράσεις, γ) τα όποια κρατικά και ιδιωτικά αμυντικά πλάνα δεν δεικνύουν μια ικανοποιητική θεραπεία, η νομοθετική θωράκιση το ίδιο. Η φύση της οικονομικής δραστηριότητας δεν επιτρέπει υψηλές φιλοδοξίες ως προς τη λύση του προβλήματος, δ) η οικονομική αντικατασκοπευτική δράση αν και θεσμικά αναβαθμισμένη έπεται της αντίστοιχης που ασχολείται με παραδοσιακές αλλά και νέες πολιτικοστρατιωτικές απειλές.²⁴ Από κει και πέρα πρέπει να δοθεί απάντηση στα εξής ερωτήματα: α) είναι απαραίτητη η εμπλοκή μιας ξένης Υπηρεσίας / κυβέρνησης στο όλο παίγνιο προκειμένου να δραστηριοποιηθούν οι εγχώριοι αντιπληροφοριακοί οργανισμοί; β) κατά πόσο είναι εύκολο να αναγνωριστεί η δράση μιας αλλότριας Υπηρεσίας / κυβέρνησης; γ) γιατί πρέπει να υποβαθμίζεται μια επίβουλη ενέργεια

²¹ Galvan N. R., "The Role of American Intelligence in the Global Economy" στο *International Journal of Intelligence and CounterIntelligence*, ό. π., σ. 353-357

²² Hayden F. J. "Economic Intelligence" στην Select Committee on Intelligence, U.S. Senate, 103rd Congress, Συνεδρία 1^η, 5 Αυγούστου 1993, σ. 5

²³ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπία. Θεωρία και Πράξη*, ό. π., σ. 582, 615-621 αλλά και Nasheri H., *Economic Espionage and Industrial Spying*, Cambridge University Press, N. York, ΗΠΑ, 2005, σ. 52-53

²⁴ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπία. Θεωρία και Πράξη*, ό. π., σ. 608-611 αλλά και Warner William, "International technology transfer and economic espionage", ό. π., σ. 157

εκπορευόμενη από μια ξένη εταιρία; δ) πότε πρόκειται για ζήτημα εθνικής οικονομικής ασφαλείας; Τέλος, πρέπει να ληφθεί υπόψη: α) η ύπαρξη χιλιάδων, ανέργων πολλές φορές, ειδικών επί υπολογιστικών συστημάτων. Οι τελευταίοι μη αντιμετωπίζοντας τους εξαιρετικούς κινδύνους που ένας θηρευτής πολιτικών ή στρατιωτικών μυστικών οφείλει να αναλογιστεί, ίσως υποκύψουν ευκολότερα σε πειρασμούς και β) η ευκολία μετακίνησης ατόμων εντός μιας παγκοσμιοποιημένης κοινωνίας με ό,τι αυτό συνεπάγεται για τον οικονομικό τομέα.

Συμπεράσματα

Ό,τι έχει αναφερθεί μέχρι τώρα ωθεί να υποθέσουμε ότι πριν το 1990: α) ο οικονομικός πολιτικός σχεδιασμός απετέλεσε τμήμα των λεγόμενων χαμηλών κρατικών προτεραιοτήτων, β) η οικονομική αντικατασκοπία δεν αντιμετωπίστηκε ως ίσης βαρύτητας με την ανάλογη πολιτικοστρατιωτική, γ) η οικονομική αντικατασκοπία συνάντησε προσκόμματα ως προς την ορθή εκτέλεσή της, δ) η οικονομική αντικατασκοπία δεν εκλήφθηκε ως εργαλείο προστασίας εθνικών οικονομικών συμφερόντων, ε) η οικονομική αντικατασκοπία σχετίστηκε με αντιμετώπιση αλλότριων δράσεων που εντάσσονταν σε μια προσπάθεια κτισίματος μορφών ήπιας ισχύος σε αντίθεση με τη στρατιωτική ανάλογη που δρούσε ως ανάχωμα έναντι βλέψεων κατάκτησης ισχύος σκληρού αποτυπώματος.

Μετά το 1990 ισχύει ότι: α) οι μεταψυχροπολεμικές συνθήκες, η παγκοσμιοποίηση της οικονομίας όπως και η αναβάθμιση της αξίας των οικονομικών δεικτών επιβάλλουν μια νέα αποτίμηση σχετικά με την ανάγκη για οικονομική αντικατασκοπευτική δραστηριότητα, β) αν και ο αντικατασκοπευτικός οικονομικός σχεδιασμός ξέφυγε από τις ψυχροπολεμικές τροχοπέδες εξακολουθεί να αντιμετωπίζει δυσκολίες ως προς την εκπόνηση / υλοποίησή του, γ) η επίλυση του προβλήματος της οικονομικής κατασκοπίας δεν εγκιβωτίζεται αποκλειστικά εντός του περιγράμματος των Υπηρεσιών, δ) η φύση του παγνίου δεν επιτρέπει υπεραισιοδοξία ως προς την πάταξη των οικονομικών εγκληματιών. Πρόκειται για πραγματικότητα που έχει διαγνώσει, ήδη από το 1994, ο William Warner. Σύμφωνα με τον ερευνητή η φυσική ασφάλεια είναι αποτελεσματική αλλά πολυδάπανη και σαφώς πέρα των δυνατοτήτων μη μεγάλων επιχειρήσεων. Επιπλέον, η νέα τεχνολογία και ό,τι άυλο φέρει αυτή δεν μπορεί να προστατευθεί από αδιάκριτα μάτια όπως μπορεί ένα, π. χ., τανκ ή κάποιο hardware.²⁵

Υπάρχει μια πρόταση «οικονομικής ασφαλείας»; Ό,τι μπορούμε να σκεφτούμε, αντλώντας από το αμερικανικό παράδειγμα, συνοψίζεται στα εξής: α) οι δράσεις της οικονομικής αντικατασκοπίας καλούνται να ενισχυθούν, β) οι υπηρεσίες Αντικατασκοπίας πρέπει να συνεργαστούν με αυτές του law enforcement, γ) οι πληροφοριακοί οργανισμοί, κατά την άποψή μας, νομιμοποιούνται να σταθμίσουν τη συνεργασία τους με την επιχειρηματική κοινότητα ακόμα και αν αυτή η συνεργασία αναφέρεται σε περιπτώσεις βιομηχανικού πολέμου, δ) οι μεγάλες επιχειρήσεις οφείλουν να υιοθετήσουν προγράμματα προστασίας των ευαίσθητων δεδομένων τους.²⁶

²⁵ Warner William, "International Technology Transfer and Economic Espionage", ό. π., σ. 152

²⁶ Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, ό. π., σ. 608-615

Οικονομική / βιομηχανική αντικατασκοπία στο κυβερνοδιάστημα και στον εταιρικό κόσμο

Οικονομικός / βιομηχανικός αντιπληροφοριακός κυβερνοπόλεμος

Στο ετήσιο οικονομικού ενδιαφέροντος δελτίο προς το αμερικανικό Κογκρέσο με τίτλο *Foreign Economic Collection and Industrial Espionage, 2005* αναφέρεται το εξής: «Η CI Κοινότητα πιστεύει ότι το διαδίκτυο αποτελεί όλο και περισσότερο όχημα εκμείωσης ευαίσθητων τεχνολογικών πληροφοριών αμερικανικής πατρίδας. Οι κίνδυνοι προέρχονται από κρατικούς και μη κρατικούς παράγοντες. Γεγονός που μεγεθύνει την ανησυχία δεικνύει η διαπίστωση ότι κράτη με αυξημένες ικανότητες χρήσης κυβερνοεργαλείων είναι κράτη που παραδοσιακά προβαίνουν σε επιθετική συλλογή πληροφοριών εκ των Ηνωμένων Πολιτειών».²⁷

Αν και το ανωτέρω paper δεν κάμει λόγο για οικονομικό πληροφοριακό πόλεμο μπορούμε να εντάξουμε σ' αυτόν (κυβερνο)τακτικές με σκοπό την απόσπαση οικονομικών μυστικών. Αλήθεια είναι ότι το ύψος της συγκεκριμένης κυβερνοκλοπής δεν μπορεί να υπολογιστεί με βεβαιότητα· σ' αυτό συντρέχει κυρίως το γεγονός της απροθυμίας των ιδιωτικών επιχειρήσεων να προβούν σε σχετικές ανακοινώσεις / καταγγελίες φοβούμενες τη δυσφήμιση.²⁸ Μελέτη του FBI περί τα μέσα της πρώτης δεκαετίας του 2000 καταλήγει στο συμπέρασμα ότι το 90% αυτών υπέστη δικτυακή επίθεση παρά τη λήψη μέσων προστασίας. Η ανίχνευση των πηγών ή των κινητηρίων μοχλών τέτοιων συμβάντων δεν αποτελεί καθόλου εύκολο εγχείρημα καθώς η σχετική έρευνα χάνεται εντός των καναλιών της κυβερνοσφαίρας, εντός διαδρομών που διέρχονται ηλεκτρονικών κόμβων εγκατεστημένων στη μία ή στην άλλη χώρα με τα όποια νομικά ή και διπλωματικά προβλήματα να εγείρονται. Πρόκληση τελικά για τις αμερικανικές υπηρεσίες Αντικατασκοπίας δεικνύει ο αριθμός των μη αντιληπτών επιθέσεων και όχι μια απάντηση στην ερώτηση «ποιοι προβαίνουν σε δικτυακή οικονομική κατασκοπία;» ή μια απάντηση στην ερώτηση «ποιοι οι δυνητικοί διαπράττοντες οικονομικού πληροφοριακού πολέμου;» -αυτοί που ενοχοποιούνται συνθέτουν συνήθως, αλλά καθόλου αποκλειστικά, ξένες κυβερνήσεις και αλλοδαπές υπηρεσίες Πληροφοριών.²⁹

Τον Ιανουάριο του 2001 το Bureau αναγγέλλει ένα πρόγραμμα συνεργασίας με αριθμό ιδιωτικών εταιριών. Σκοπός του προγράμματος η ανταλλαγή πληροφοριών περίξ του δικτυακού εγκλήματος και τρόποι αναχαίτισής του. Ο Luis J. Freeh, τότε διευθυντής της Υπηρεσίας, σημειώνει ότι «το κυβερνοέγκλημα αποτελεί ένα από τα μεγαλύτερα και πλέον δυναμικά αναπτυσσόμενα προβλήματα που αντιμετωπίζει το FBI». Συνεχίζει τονίζοντας πως το πρόγραμμα InfraGard ανοίγει δρόμους επικοινωνίας μεταξύ δημοσίου και ιδιωτικού τομέα με τη συμμετοχή του law enforcement -μέχρι τότε μια αμοιβαία καχυποψία χαρακτήριζε τις σχέσεις μεταξύ των ιδιωτών επιχειρηματιών και των αρχών ασφαλείας. Κατά τη λογική του προγράμματος InfraGard τρεις κατηγορίες απειλών χρωματίζουν τον οικονομικό κυβερνοπόλεμο: α) η κατηγορία των μη δομικών απειλών (unstructured threats).

²⁷ *Foreign Economic Collection and Industrial Espionage, 2005*, NCIX, Αύγουστος 2006, σ. 10, διαθέσιμο και στην τοποθεσία http://www.ncsc.gov/publications/reports/fecie_all/FECIE_2005.pdf όπου ανατρέξαμε την 4^η Σεπτεμβρίου 2015

²⁸ Sulick Michael, *American spies: espionage against the United States from the Cold War to the present*, Georgetown University Press, USA, 2013, σ. 292-293

²⁹ *Foreign Economic Collection and Industrial Espionage, 2005*, NCIX, Αύγουστος 2006, σ. 10

Πρόκειται για απειλές / επιθέσεις προερχόμενες από μεμονωμένους / ανεξάρτητους hackers, β) η κατηγορία των δομικών απειλών (structured threats). Πρόκειται για απειλές / επιθέσεις προερχόμενες από το οργανωμένο έγκλημα, εμπορικούς ανταγωνιστές ή τρομοκρατικές ομάδες, γ) η κατηγορία των απειλών εθνικής ασφαλείας (national security threats). Πρόκειται για απειλές / επιθέσεις προερχόμενες από αλλοδαπές Υπηρεσίες και ξένα κράτη. Τα μέλη του προγράμματος ελάμβαναν ειδοποιήσεις τριών επιπέδων ήτοι, του συναγερμού (alert), της γνωμοδότησης (advisory) και της εκτίμησης (assessment) κατόπιν επιβεβαίωσης του National Threat Warning System του FBI.³⁰

Οι προσπάθειες οικονομικής διαδικτυακής κλοπής με στόχο ειδικότερα την υψηλή τεχνολογία συνδέονται και με την στρατιωτική τεχνολογική εξέλιξη και ισχύ. Το άνω δελτίο (*Foreign Economic Collection and Industrial Espionage*, 2005) αποκαλύπτει ότι κατά το οικονομικό έτος 2005 το σύνολο της αμερικανικής Λίστας Κρισίμων Στρατιωτικών Τεχνολογιών (MCTL) ευρέθη στο στόχαστρο με Κίνα και Ρωσία να δεικνύουν τους πλέον επικίνδυνους κυνηγούς πληροφοριών. Κατά τον έναν ή άλλο τρόπο τόσο το DSS όσο και τα Air Force Office of Special Investigations -AFOSI, Army Counterintelligence Center -ACIC και National Reconnaissance Office -NRO συναινούν στο ότι αυτό που συμβαίνει μεγεθύνεται καθημερινά· όλο και περισσότεροι κρατικοί και μη κρατικοί δρώντες δείχνουν ενδιαφέρον κτήσης πληροφοριών περίξ της διαστημικής τεχνολογίας. Η αμερικανική αντικατασκοπευτική κοινότητα πιστεύει πως στις αρχές του 21^{ου} αιώνα άνω των τριάντα χωρών επιχειρούν να αποσπάσουν σχετικά στοιχεία και δεδομένα από τις ΗΠΑ αν και για το 75% των περιπτώσεων ενοχοποιείται ένας μικρός πυρήνας κρατών με την Κίνα να κατέχει τα πρωτεία.³¹

Εν κατακλείδι, αυτό που ενδιαφέρει σχετίζεται με τρόπους αντιμετώπισης του φαινομένου. Κατ' αυτήν την έννοια ο Αμερικανός ταξίαρχος Gregory J. Touhill ορίζει την εταιρική κυβερνοασφάλεια ως ...*συνεργασία τεχνολογιών, διαδικασιών και πρακτικών με σκοπό την προστασία πληροφοριών και networks, υπολογιστικών συστημάτων και εφαρμογών, προγραμμάτων συλλογής, ανάλυσης, διαβάθμισης και διανομής δεδομένων από επίθεση, φθορά ή μη εγκεκριμένη πρόσβαση*³² -δεν υφίσταται ιδιαίτερη απόκλιση στόχων / τοποθετήσεων μεταξύ εταιρικών και μη εταιρικών προγραμμάτων / στρατηγικών κυβερνοασφαλείας. Οι αμερικανικές Υπηρεσίες και ιδιαίτερα αυτές των Αντιπληροφοριών λαμβάνοντας μέριμνα προσανατολίζονται στη(ν): α) βελτίωση της συνεργασίας μεταξύ κρατικών οργανισμών και ομάδων εργασίας που μάχονται την απειλή της κυβερνοκατασκοπίας. Το National Cyber Counterintelligence Working Group, δημιουργήμα των δεκαέξι ομοσπονδιακών Υπηρεσιών όπως και άλλων κρατικών ιδρυμάτων, δεικνύει ένα παράδειγμα. Άλλο παράδειγμα αποτελεί το επίσης εκ του FBI καθοδηγούμενο National Cyber Investigative Joint Task Force σκοπός του οποίου είναι η ανταλλαγή πληροφοριών μεταξύ δομών που επιφορτίζονται την άμυνα έναντι δικτυακών προσβολών κατά των αμερικανικών συστημάτων, β) βελτίωση των συλλεκτικών και αναλυτικών μεθόδων. Αν και οι αμερικανικές Υπηρεσίες κάνουν βήματα στην αναγνώριση κυβερνοαπειλών έναντι κυβερνητικών συστημάτων φαίνεται πως καταγράφεται, παρά τις προσπάθειες, ένα έλλειμμα αντίστοιχης «κυβερνογνώσης» όταν η συζήτηση μεταφέρεται στο πεδίο του οικονομικού τομέα, κυρίως, του ιδιωτικού, γ) βελτίωση των επιχειρησιακών

³⁰ Fink Steven, *Sticky Fingers. Managing the Global Risk of Economic Espionage*, Dearborn Trade Publishing, USA, 2002, σ. 125-126

³¹ *Foreign Economic Collection and Industrial Espionage*, 2005, NCIX, Αύγουστος 2006 σ. 10-12

³² Touhill J. G., Touhill J. C., *Cybersecurity for Executives. A Practical Guide*, John Wiley & Sons, Inc., Hoboken / New Jersey, 2014, σ. 2

μεθόδων ανίχνευσης, αποτροπής ή διακοπής / αποσυντονισμού επίβουλων κυβερνοενεργειών, δ) επίρρωση μιας κουλτούρας διαρκούς εκπαίδευσης και σπουδής για επίγνωση της κατάστασης, μιας κουλτούρας που τόσο ο κρατικός όσο και ο ιδιωτικός οικονομικός τομέας οφείλουν να κτίσουν.³³

Εντούτοις η συνεργασία μεταξύ της κυριότερης αμυντικής πολιτικής δομής, αυτής του DoD, και πολλών αποκλειστικών αναδόχων αμυντικών συμβάσεων (cleared defense contractors -CDCs) παρουσιάζει κωλύματα ως προς την εκτέλεση ενός υποθετικά συμφωνηθέντος πλάνου βάσει του οποίου η πληροφοριακή κοινότητα θα βελτιώσει τη γνώση της γύρω από κυβερνοαπειλές εκ της αλλοδαπής. Παρά το ότι οι CDCs οφείλουν να αναφέρουν τις όποιες ύποπτες προσπάθειες προσέγγισης μέσω δικτυακών ή άλλων οδών εκ μέρους ξένων συμφερόντων, μόνο το 10% αυτών υποβάλει τη σχετική ετήσια αναφορά. Μια άλλη ανεπάρκεια ελαύνεται εκ της τάσεως των CDCs να αποκρύπτουν, στο βαθμό που είναι ικανοί, περιστατικά κλοπών ευαίσθητων δεδομένων που κατέχουν και δεδομένων που σχετίζονται με το αμερικανικό Πεντάγωνο. Από τη μεριά τους τα τμήματα ασφαλείας των εταιριών συνηθέστατα διαμαρτύρονται για βραδείες ή και περιττές διαδικασίες που οφείλουν να ακολουθηθούν τη στιγμή που καλούνται να αποδώσουν τη ίδια πληροφόρηση, π. χ. στο DSS και στο FBI, υπό διαφορετική μορφή ή τύπο αρχείων. Πάντως, σύμφωνα με έρευνα του 2010 μόνο ένα 5% των εταιρικών στελεχών ενδιαφέρονται για ζητήματα προστασίας δικτύων ενώ ένα μικρό 13% των εταιριών απασχολεί ειδικευμένο περί κυβερνοαπειλών προσωπικό.³⁴

Βάσει των αναφερομένων κατανοείται η σύζευξη οικονομίας, τεχνολογίας, (κυβερνο)διαστήματος, πληροφορίας, στρατιωτικής εξέλιξης και οικονομικού πληροφοριακού πολέμου. Οι δυσκολίες που αντιμετωπίζουν οι Υπηρεσίες ως προς την εξουδετέρωση επίδοξων κυβερνοκλεπτών οικονομικών μυστικών εθνικού ενδιαφέροντος σχετίζονται με ό,τι έχουμε ήδη αποτυπώσει περί των μετά το 1990 προκλήσεων. Από κει και έπειτα η ανάπτυξη των τεχνολογικών assets ευνοεί όσο, κυρίως, δυσχεραίνει το έργο των οργανισμών Ασφαλείας και Αντικατασκοπίας. Έμμεση απόδειξη του τελευταίου η αναζήτηση από τον Michael Erbschloe τακτικών αντιμετώπισης του φαινομένου και εντός του επιχειρηματικού κόσμου όσον αφορά, τουλάχιστον, το κομμάτι του private economic information warfare που στα ανεπτυγμένα κράτη συχνά συνδέεται με εθνικές πολιτικές.³⁵

³³ US Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Οκτώβριος 2011, σ. A-1 – A-2. Σ' αυτό το σημείο σημειώνουμε ότι εκτός των DSS, AFOCI, ACIC, NRO και FBI πέντε ακόμα δομές [ONCIX, DIA (Defense Intelligence Agency), DoE (Department of Energy), NGA (National Geospatial-Intelligence Agency), DNI Open Source Center] πλέκουν το ευρύτερο οικονομικό αντικατασκοπευτικό δίκτυο των ΗΠΑ με το ONCIX να δεικνύει την κεφαλή και το DoD να συνεργάζεται. Το συγκεκριμένο δίκτυο επιλαμβάνεται κάθε είδους οικονομικών απειλών είτε αυτές κάνουν την παρουσία τους στον κυβερνοχώρο είτε όχι επιχειρώντας, ειδικότερα, μία έρευνα περί: α) της υφής των ξένων οικονομικών επενδύσεων, β) των οικονομικών ενδιαφερόντων των αλλοδαπών επενδυτών, γ) των οικονομικών ενδιαφερόντων ξένων κρατών, δ) των οικονομικών ενδιαφερόντων ξένων Υπηρεσιών, ε) τρόπων διαφύλαξης της πυρηνικής τεχνολογίας. Περαιτέρω ελέγχεται η συμπεριφορά των αποκλειστικών αναδόχων αμυντικών συμβάσεων του DoD όπως διώκεται, μέσω FBI, κάθε αντιληπτή έκνομη ενέργεια -για περισσότερα βλέπε *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008*, ONCIX, Ιούλιος 2009, σ. 5-7

³⁴ US Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Οκτώβριος 2011, σ. A-1 – A-2

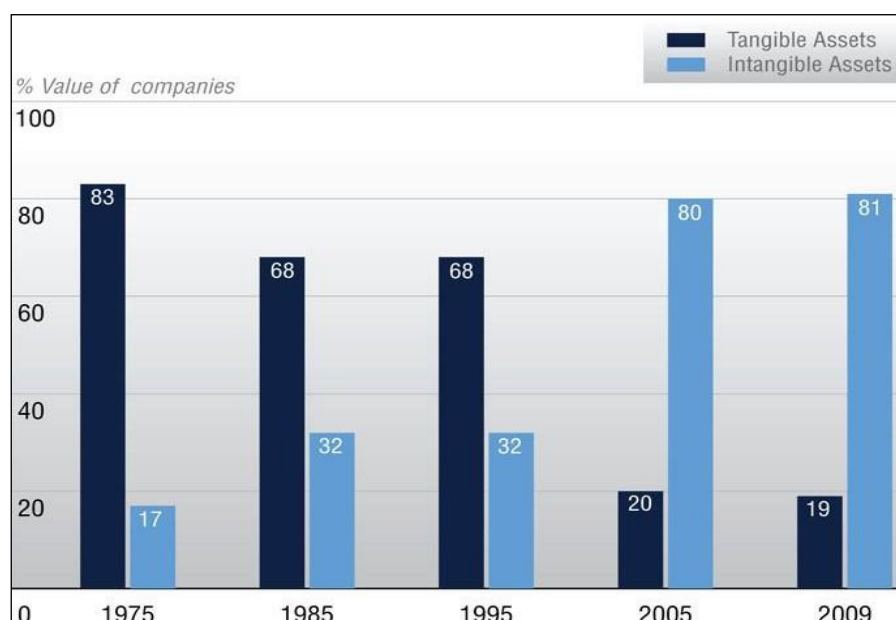
³⁵ Erbschloe M, *Information Warfare. How to Survive Cyber Attacks*, The McGraw-Hill Companies, USA, 2001, σ. 64. Περί εταιρικών στρατηγικών αντιμετώπισης κυβερνοαπειλών βλέπε, μεταξύ

Στρατηγικές εταιρικής αντικατασκοπίας. Η διάχυση της έννοιας

Ευαίσθητες αμερικανικές οικονομικές και τεχνολογικές πληροφορίες βρίσκονται στο στόχαστρο μυστικών υπηρεσιών, ιδιωτικών εταιριών, ακαδημαϊκών και ερευνητικών ινστιτούτων αλλά και μεμονωμένων πολιτών δεκάδων χωρών

ONCIX³⁶

Η στροφή της παγκόσμιας οικονομίας, ειδικότερα της αμερικανικής, από μια παραδοσιακή τάση κατοχής φυσικών (tangible) αξιών σε μια αντίστοιχη κατοχής πνευματικών (intangible) κεφαλαίων ωθεί στα ύψη τις ευκαιρίες, τη δυνατότητα αλλά και τη θέληση για οικονομική / βιομηχανική κατασκοπία. Ο Simon Hunt, αντιπρόεδρος της McAfee, γράφει, εν έτει 2011, ότι πλέον ...υφίσταται πολύ υψηλότερη αξία [κέρδος] στην πώληση εταιρικών ιδιοκτησιακών πληροφοριών σε ανταγωνιστές και ξένες κυβερνήσεις ... η υπόγεια δικτυακή οικονομία έχει επικεντρώσει στην κλοπή επιχειρηματικών πνευματικών κεφαλαίων.³⁷



Εικόνα 20: Γράφημα της εταιρικής ανοδικής τάσης κατοχής άυλων αξιών από το 1975 μέχρι και το 2009. Η εικόνα ελήφθη από το *Protecting Key Assets: A Corporate Counterintelligence Guide*

Με δεδομένη την άνω εικόνα το ODCIX επισημαίνει πως: α) κάθε αμερικανική επιχείρηση χρήζει σχεδιασμών φυσικής προστασίας με άξονα αναφοράς το προσωπικό, τις εγκαταστάσεις και τα πληροφορι(α)κά συστήματα, β) ένα αντικατασκοπευτικό πλάνο χαρακτηρίζεται από μια αμυντική όσο και μια «δυναμική» υφή. Ενσωματώνει διαδικασίες έρευνας και ανάλυσης σχεδιασμένες να

πολλών, Jalil Sh., *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, SANS Institute, 2003

³⁶ *Protecting Key Assets: A Corporate Counterintelligence Guide*, ONCIX, 2012, σ. 1, διαθέσιμο στο http://www.ncsc.gov/publications/reports/fecie_all/ProtectingKeyAssets_CorporateCIGuide.pdf όπου ανατρέξαμε την 3^η Δεκεμβρίου 2016

³⁷ *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, McAfee, 2011, σ. 3, διαθέσιμο και στη διαδικτυακή τοποθεσία <http://www.ndia.org/Divisions/Divisions/Cyber/Documents/tp-underground-economies.pdf> στην οποία καταφύγαμε την 3^η Δεκεμβρίου 2015

προβλέπουν, να αντιπαρατίθενται και να αποτρέπουν αντίπαλες δράσεις προστατεύοντας τους εταιρικούς πόρους και νεωτερισμούς, γ) ένα πρόγραμμα κλασικής ασφαλείας (υλικοί πόροι) συνδεδεμένο με ένα αντίστοιχο αντικατασκοπευτικής μέριμνας (ανθρώπινοι πόροι) συνιστά την πληρέστερη προστασία για μια επιχείρηση.

Το ODCIX βασισμένο στην τεχνογνωσία που έχει κατακτήσει δομεί / προτείνει έναν εταιρικό αντικατασκοπευτικό σχεδιασμό τεσσάρων σταδίων, ειδικότερα:

- Στάδιο 1 (Counterintelligence Risk Assessment). Το συγκεκριμένο στάδιο εκτιμά εταιρικές απειλές θέτοντας προτεραιότητες ασφαλείας, αναλύοντας διαθέσιμες πληροφορίες, αναγνωρίζοντας εσωτερικές τρωτότητες, υπολογίζοντας συνέπειες από απώλειες κρίσιμων δεδομένων αλλά και κόστη προστασίας. Η τελική εκτίμηση ρίσκου επιβοηθά στον καταμερισμό των απαιτούμενων πόρων ώστε να τρέξει ένα αποτελεσματικό Corporate CI πρόγραμμα.



Εικόνα 21: Τα τέσσερα τμήματα του Σταδίου 1. Η εικόνα έχει αντιγραφεί από το *Protecting Key Assets: A Corporate Counterintelligence Guide*, ONCIX, 2012, σ. 3

- Στάδιο 2 (Groundwork Corporate CI Program). Αν η ανάλυση ρίσκου (στάδιο 1) αποδίδει το εύρος και τη φύση των απειλών, η προετοιμασία αντιμετώπισης συνθέτει το επόμενο βήμα. Η εύρεση ειδικευμένων σε θέματα ασφαλείας προσώπων, τα οργανωτικά του πλάνου, η ανάπτυξη σχέσεων μεταξύ της επιχείρησης και εκπροσώπων των κοινοτήτων law enforcement και Πληροφοριών προς όφελος τόσο ιδιωτικών όσο και κρατικών συμφερόντων, η εναρμόνιση δράσεων με το ισχύον νομικό πλαίσιο δεικνύουν κάποιους από τους στόχους αυτού του σταδίου.
- Στάδιο 3 (Capabilities Needed). Τι απαιτείται για την εφαρμογή ενός Corporate CI Program; Το ONCIX προϋποθέτει έξι στοιχεία ήτοι, α) επίγνωση κινδύνων / εκπαίδευση προσωπικού (threat awareness / training), β) διαδικασία ανάλυσης στοιχείων, αναφοράς απειλών και απόκρισης (analysis, reporting, response), γ) διαδικασία αναφοράς υπόπτων δραστηριοτήτων ως σύστημα εγκαίρου προειδοποίησης (suspicious activity reporting), δ) έλεγχο χρηστών δικτυακών συστημάτων (CI audit), ε) εκτέλεση και κατάθεση αναφορών ασφαλείας και σύννομων οιονεί «αντικατασκοπευτικών ερευνών» (CI investigations), στ) καλλιέργεια επαφών / επίρρωση κλίματος εμπιστοσύνης / συνεργασίας με τις κρατικές αρχές (liaison).
- Στάδιο 4 (Corporate CI Program Implementation). Με την πλήρωση των τριών άνω σταδίων ξεκινά η εφαρμογή ενός εταιρικού πλάνου αντικατασκοπίας. Το τελευταίο εντάσσεται είτε στο βασικό (basic / essential), είτε στο διευρυμένο

(expanded), είτε στο πλήρες (full scope) αναλόγως της έκτασης και της φύσεώς του.³⁸

Οι Herbert D. Clough και Robert A. Margulies σε άρθρο τους στο *Competitive Intelligence Review* αναφέρονται στα κύρια συστατικά ενός αντικατασκοπευτικού εταιρικού μηχανισμού. Σύμφωνα με τους δύο ερευνητές, αυτά σχετίζονται με: α) την *κριτική πληροφοριακή ανάλυση* (critical information analysis), πρόκειται για διαδικασία αναγνώρισης πληροφοριών που απαιτείται να βρίσκονται υπό καθεστώς προστασίας, β) την *ανάλυση κινδύνου* (threat analysis), πρόκειται για διαδικασία ταυτοποίησης απειλών κατά κρίσιμων πληροφοριών, γ) την *ανάλυση τρωτοτήτων* (vulnerability analysis), αφορά σε αναγνώριση αδυναμιών / τρωτοτήτων των συστημάτων προστασίας πληροφοριών, δ) την *εκτίμηση ρίσκου* (risk assessments), αφορά στην αναγνώριση των πληροφοριών που χρήζουν ιδιαίτερης προστασίας, των ειδών των απειλών, των πηγών των τρωτοτήτων, στην κατηγοριοποίηση των ρίσκων επί τη βάσει της σοβαρότητά τους κ. λ., ε) την πολιτική αντιμέτρων (countermeasures), αφορά σε ελέγχους ασφαλείας, εκτίμηση κόστους εφαρμογής αντιμέτρων κ. λ., στ) την μέτρηση αποτελεσματικότητας των μέτρων ασφαλείας, πρόκειται για περιοδική διαδικασία μέτρησης αποτελεσματικότητας των συστημάτων ασφαλείας.³⁹

Ο ερευνητής Donald Krause είναι λιτότερος. Υποστηρίζει πως οι νίκες στον οικονομικό στίβο κερδίζονται από στελέχη που γνωρίζουν εκ των προτέρων τις κινήσεις των ανταγωνιστών. Δεν πρόκειται για πληροφόρηση που σχετίζεται με τη μελέτη του παρελθόντος ή παρέχεται μέσω μετρήσεων, αναλύσεων και εκτιμήσεων αγοράς ή δημογραφικών δεδομένων και τάσεων· οι πραγματικά «χρήσιμες ειδήσεις» προέρχονται από ανθρώπους που διαθέτουν εσωτερική πρόσβαση. Εφόσον οι τελευταίοι ανήκουν στο επίβουλο κατασκοπευτικό στοιχείο, τότε, το αντικατασκοπευτικό ανάλογο οφείλει να: α) προστατεύει τα πληροφοριακά / ηλεκτρονικά εταιρικά δίκτυα (ασφάλεια), β) ελέγχει την αξιοπιστία των εισερχομένων πληροφοριών (αμυντική αντικατασκοπία), γ) εκτιμά την αποδοτικότητα των παραπλανητικών πληροφοριών που η οικεία επιχείρηση διέσπειρε (επιθετική αντικατασκοπία + παραπλάνηση / εκτίμηση παραπλάνησης), δ) στρατολογεί ανθρώπους των ανταγωνιστών (επιθετική αντικατασκοπία).

Τα δύο πρώτα καθήκοντα εντάσσονται στο αμυντικό σκέλος του σχεδιασμού, τα δύο επόμενα στο επιθετικό. Ασφαλώς ο πληροφοριακός κύκλος από τη συλλογή μέχρι την απόδοση του τελικού προϊόντος δεν αλλάζει, τέλος, κατά τον Krause το πλέον σημαντικό asset στον πόλεμο του οικονομικού / εμπορικού ανταγωνισμού είναι ακριβώς αυτό για το οποίο κάνουμε λόγο ήτοι, η αντικατασκοπευτική δραστηριότητα.⁴⁰

Ο Daniel J. Benny στο κεφάλαιο 8 του *Industrial Espionage. Developing a Counterespionage Program* επικεντρώνοντας στο ανθρώπινο εταιρικό δυναμικό καταγράφει τη διαδικασία μέσω της οποίας δύναται να ελεγχθεί το ποιόν κάποιου εν ενεργεία ή υπό πρόσληψη υπαλλήλου / στελέχους. Σημειώνουμε ότι το συγκεκριμένο

³⁸ *Protecting Key Assets: A Corporate Counterintelligence Guide*, ONCIX, 2012, σ. 3-8, Benny J. Daniel, *Industrial Espionage. Developing a Counterespionage Program*, CRC Press, 2014, σ. 51-68, Wimmer Bruce, *Business Espionage. Risks, Threats, and Countermeasures*, Elsevier Inc., 2015, σ. 116-119 (Business Espionage Security Awareness Training + Employee Counterespionage Education and Awareness Program), σ. 146 (περί συνεργασίας μεταξύ εταιριών και Υπηρεσιών)

³⁹ Clough D. H., Margulies A. R., “The Corporate Competitive Intelligence / Counterintelligence Team: A Symbiotic Design for the Future” στο *Competitive Intelligence Review*, Volume 5, Number 3, 1994, σ. 48

⁴⁰ Krause D., *Η Τέχνη του Πολέμου για Στελέχη Επιχειρήσεων*, μτφρ. Ναθανάηλ Ν., Κριτική, Αθήνα, 1998, σ. 155-160

τσεκάρισμα επιδέχεται κριτικής καθώς πρακτικές συνεντεύξεων με τη μεσολάβηση πολυγράφου συχνά δεν υιοθετούνται καν σε πολιτείες της Αμερικής.⁴¹

Ο Steven Fink καταθέτει τρία βήματα εταιρικής οικονομικής / βιομηχανικής αντικατασκοπίας. Σύμφωνα μ' αυτά μια επιχείρηση οφείλει: α) να 'αναγνωρίζει' τα εμπορικά και λοιπά μυστικά του χώρου, β) να λαμβάνει μέτρα προστασίας αυτών ακριβώς των μυστικών, γ) να επιμορφώνει το προσωπικό περί των ανωτέρω μέτρων.⁴²

Τέλος, ο καθηγητής Eugene Spafford του Purdue University αναφερόμενος στην έννοια της εταιρικής ασφάλειας και κυβερνοασφάλειας επισημαίνει ότι:

- Μια ικανή εταιρική στρατηγική ασφαλείας βοηθά στην καλύτερη διαδικασία λήψεως εταιρικών αποφάσεων.
- Μια ικανή εταιρική στρατηγική κυβερνοασφάλειας: α) μειώνει τις πιθανότητες κλοπής ψηφιακών δεδομένων / αρχείων, β) πριμοδοτεί μια ανάληψη οικείων επιχειρηματικών ρίσκων και γ) επιβοηθά στο κτίσιμο ενός αναγνωρισμένου trademark, κάτι σημαντικότατο για την κατάληψη αξιόλογου μεριδίου αγοράς.⁴³

Συμπεράσματα

Βάσει των όσων έχουν κατατεθεί συμπεραίνουμε πως: α) η ψηφιακή έκρηξη και η εκτίναξη χρήσης του παγκοσμίου ιστού όλο και αυξάνει τις πιθανότητες οικονομικής / βιομηχανικής κλοπής καθώς ικανοποιητικές δικτυακές ασφαλιστικές δικλίδες δεν υπάρχουν⁴⁴, β) η ταυτοποίηση των κυβερνοδραστών αποτελεί πολύ δύσκολο εγχείρημα, γ) η πλειοψηφία των μεγάλων αμερικανικών εταιριών έχει πέσει θύμα δικτυακής επίθεσης είτε αυτή έγινε αντιληπτή είτε όχι, δ) η σύνδεση του βιομηχανικού / τεχνολογικού τομέα με τον αντίστοιχο κρατικό οικονομικό αλλά και στρατιωτικό οξύνει το πρόβλημα, ε) η δράση των Υπηρεσιών και δη και αυτών της Αντικατασκοπίας δεν αρκεί ως προς την επίλυση του ζητήματος, στ) απαιτείται η

⁴¹ Benny J. Daniel, *Industrial Espionage. Developing a Counterespionage Program*, ό. π., κ. 8, σ. 153-167

⁴² Fink Steven, *Sticky Fingers: Managing the Global Risk of Economic Espionage*, ό. π., σ. 224. Για περισσότερες πληροφορίες βλέπε στο ίδιο, κεφάλαιο 22, σ. 223-236, επίσης Douglas Bernhardt, *Competitive Intelligence. How to acquire and use corporate intelligence and counter-intelligence*, Pearson Education Limited, UK, 2003, σ. 85-90, 91-92, 95-96

⁴³ *Unsecured Economies: Protecting Vital Information*, McAfee, Inc., σ. 29 διαθέσιμο στη δικτυακή τοποθεσία https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf εις την οποία ανατρέξαμε την 1^η Μαΐου 2016

⁴⁴ Ο Kevjn Lim σημειώνει πως το έτος 2000 μόνο το 25% των αποθηκευμένων πληροφοριών παγκοσμίως ευρίσκοντο σε ψηφιακή μορφή. Το έτος 2013 το ποσοστό ξεπερνά το 98% πλησιάζοντας έναν όγκο 1175 exabytes όταν 1 exabyte ισούται με 1 δις gigabytes -περί τούτου βλέπε Lim K., "Big Data and Strategic Intelligence" στο *Intelligence and National Security*, Volume 31, Volume 4, 2016, σ. 622, επίσης ανάτρεξε στο Cukier Neil Kenneth, Mayer-Schoenberger Viktor, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, Boston, 2013, σ. 9. Για περισσότερες λεπτομέρειες βλέπε Rosenau James, "The Information Revolution: Both Powerful and Neutral" στο *The Information Revolution and National Security*, επιμ. Copeland Th., Strategic Studies Institute / US Army War College, Pennsylvania, 2000, σ. 9-29, Williams Phil, Dunlevy Casey, Shimeal Tim, "Intelligence Analysis for Internet Security" στο *Contemporary Security Policy*, Volume 23, Issue 2, 2002, σ. 1-38, Maniscalco M. Luisa, "Living in the Cyber Era: Reflections on Security in a Hybrid World" στο *Mediterranean Council for Intelligence Studies Yearbook*, 2012, σ. 13-8, Degaut Marcos, "Spies and Policymakers: Intelligence in the Information Age" στο *Intelligence and National Security*, Volume 31, Number 4, 2016, σ. 512, επίσης στις διαδικτυακές τοποθεσίες <http://www.factshunt.com/2014/01/world-wide-internet-usage-facts-and.html>, <http://worldwidewebsite.com/> και <http://foreignpolicy.com/2009/10/26/web-of-influence/> στις οποίες καταφύγαμε τη 13^η Φεβρουαρίου 2017

ανάπτυξη μιας, γενικότερα, κουλτούρας ασφαλείας και, ειδικότερα, μιας δικτυακής ανάλογης εκ μέρους του επιχειρηματικού κόσμου, ζ) απαιτείται η παραδοχή του γεγονότος της σύνδεσης του κυβερνοχώρου με τον κρατικό / ιδιωτικό οικονομικό αλλά και τον στρατιωτικό τομέα, άρα, με την έννοια της εθνικής ασφαλείας και άμυνας, η) οι αντικατασκοπευτικές αρχές, τακτικές κ. λ. του εταιρικού χώρου δεν είναι, όπως σημειώνει ο Lawrence Sulk, άλλο από παραλλαγές αντικατασκοπευτικών αρχών και τακτικών που εφαρμόζονται στο χώρο των πολιτικών, στρατιωτικών και law enforcement αντιπληροφοριακών οργανισμών.⁴⁵

⁴⁵ Sulc L., *Law Enforcement Counterintelligence*, Varro Press, Kansas / USA, 1996, σ. 187

ΚΕΦΑΛΑΙΟ 7

Αντικατασκοπία και τρομοκρατία

Οι πρακτικοί σκοποί αντικατασκοπίας και αντιτρομοκρατίας είναι όμοιοι

Paul J. Redmond¹

Η επιτυχής διαχείριση πολεμικών ενεργειών με σκοπό την καταστολή εξεγέρσεων στηρίζεται στην οργανωμένη πληροφοριακή αρχιτεκτονική όπως και στην ανάλογη αντιπληροφοριακή που συχνά παραμελείται

Keshav Mazumadar²

...the word “counterintelligence” does not have a single, agreed-upon meaning; and the definitional difficulty turns out to have practical and not merely semantic significance. At its broadest, “counterintelligence” refers to efforts to prevent any covert activities inimical to our national security, not only espionage by foreign powers but also penetration of the nation by sleeper cells that might someday be awakened to engage in sabotage or terrorist attacks. At that level of generality “counterintelligence” includes counterterrorism intelligence; and indeed until recently (approximately the 1990s) counterterrorism intelligence was a more or less undifferentiated part of counterintelligence³

Κρατικές Υπηρεσίες και τρομοκρατία

Ειδικά μετά το 2001 το τρομοκρατικό φαινόμενο απασχολεί ως προς την αντιμετώπισή του το σύνολο των δυτικών Υπηρεσιών και όχι μόνο. Σχετικά με τις Ηνωμένες Πολιτείες η συγκεκριμένη έγνοια καταγράφεται μέσω πλήθους κρατικών εγγράφων, εκδόσεων και εγχειριδίων. Έτσι: α) η *Executive Order 12333--United States Intelligence Activities* ήδη από το 1981 τονίζει το ρόλο των πληροφοριακών οργανισμών στην προστασία του αμερικανικού έθνους έναντι τρομοκρατικών σχεδιασμών⁴, β) η *Executive Order 12292 “Further Amendment to Executive Order 12958, as Amended, Classified National Security Information”* του 2003 εφιστά προσοχή στον τρόπο διαχείρισης / ταξινόμησης πληροφοριών περίξ τρομοκρατικών σχεδιασμών⁵, γ) στη *National Security Act of 1947*, (Chapter 343; 61 Stat. 496; approved July 26, 1947), [As Amended Through P.L. 110–53, Enacted August 3, 2007], καταγράφεται το καθήκον των αμερικανικών μυστικών υπηρεσιών ως προς τη δίωξη της τρομοκρατίας⁶, δ) στο *National Intelligence. A Consumer’s Guide* του 2009 γίνεται αναφορά στην προσπάθεια καταδίωξης του εγχωρίου και διεθνούς τρομοκρατικού φαινομένου εκ μέρους των αμερικανικών οργανισμών και Υπηρεσιών, μεταξύ αυτών βλέπε το Counterterrorism Division (CTD) και το

¹ Redmond J. Paul, “The Challenges of Counterintelligence” στο *The Oxford Handbook of National Security Counterintelligence*, επιμ. Johnson Loch, Oxford University Press, New York, 2010, σ. 552

² Mazumadar Keshav, *Actionable Intelligence*, RIEAS, RIEAS e-Book No 5, Αθήνα, Σεπτέμβριος 2013, σ. 32

³ Posner Richard, “Counterintelligence, Counterterrorism, Civil Liberties, and the Domestic Intelligence Controversy” στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, USA, 2009, σ. 261-262

⁴ *Executive Order 12333--United States Intelligence Activities*, Δεκέμβριος 1981, παράγραφος 1.4

⁵ *Executive Order 12292 “Further Amendment to Executive Order 12958, as Amended, Classified National Security Information”*, Μάρτιος 2003

⁶ *National Security Act of 1947*, (Chapter 343; 61 Stat. 496; approved July 26, 1947), [As Amended Through P.L. 110–53, Enacted August 3, 2007], διαθέσιμο και στην διαδικτυακή τοποθεσία <https://www.ncsc.gov/training/resources/nsaact1947.pdf> εις την οποία ανατρέξαμε την 8^η Ιουλίου 2016

Terrorist Screening Center (TSC) του FBI, το Department of Homeland Security (DHS), το National Counterterrorism Center (NCTC), το Defense Intelligence Agency (DIA), το Drug Enforcement Administration (DEA), το Office of Naval Intelligence (ONI) κ. λ.⁷, ε) η FM 2-0, *Intelligence*, του 2010 επιβεβαιώνει το *National Intelligence. A Consumer's Guide* κάνοντας ειδικότερη μνεία στο ρόλο της κοινότητας της αντικατασκοπίας στην καταδίωξη των τρομοκρατικών οργανώσεων⁸, στ) το *U.S. National Intelligence. An Overview* του 2013 ουσιαστικά ανανεώνει το *National Intelligence. A Consumer's Guide*⁹, ζ) στο *The National Intelligence Strategy of the United States of America* του 2014 τονίζεται η ανάγκη συμμετοχής της πληροφοριακής κοινότητας σε αντιτρομοκρατικές επιχειρήσεις.¹⁰

Στα βρετανικά *National Intelligence Machinery* (2000) και *Security Service Act* 1989 καταγράφονται οι έργοι της Joint Intelligence Committee (JIC) όπως και η εμπλοκή της Security Service (SS / MI5) στον πόλεμο κατά της τρομοκρατίας.¹¹ Στην παράγραφο 65 του *HM Government. Countering International Terrorism: The United Kingdom's Strategy* του 2006 αναφέρεται ότι η μυστική φύση της τρομοκρατίας επιβάλλει την αξιοποίηση των μυστικών υπηρεσιών στον αγώνα κατά της πρώτης. Οι σχετικές επιχειρήσεις βασίζονται στη συλλογή και ανάλυση της πληροφορίας με τη συμμετοχή των MI5 / Joint Terrorism Analysis Center, MI6, Government Communications Headquarters (GCHQ) και τμημάτων της βρετανικής αστυνομίας να αποτελεί προϋπόθεση επιτυχίας.¹² Από τη μεριά του το *HM Government. Pursue, Prevent, Protect, Prepare. The United Kingdom's Strategy for Countering International Terrorism* του 2009¹³ επιβεβαιώνει το αμέσως προηγούμενο έγγραφο τη στιγμή που σε 'επιχειρηματικό / ιδιωτικό' επίπεδο η MI5 προτείνει μέσω του *Protecting Against Terrorism* τρόπους προστασίας έναντι εξτρεμιστικών ενεργειών.¹⁴

⁷ *National Intelligence. A Consumer's Guide*, ODNI, 2009

⁸ FM 2-0, *Intelligence*, Headquarters. Department of the Army, Μάρτιος 2010

⁹ *U.S. National Intelligence. An Overview*, ODNI, 2013

¹⁰ *The National Intelligence Strategy of the United States of America*, ODNI, 2014, σ. 4

¹¹ *National Intelligence Machinery*, The Stationary Office, Απρίλιος 2000 και *Security Service Act* 1989, The Stationary Office, Chapter 5, 1989, σ. 1

¹² *HM Government. Countering International Terrorism: The United Kingdom's Strategy*, The Stationary Office, Ιούλιος 2006, παράγραφος 65, σ. 17

¹³ Όπου *pursue* (καταδίωξη) ίσον καταδίωξη / αποσόβηση τρομοκρατικών επιθέσεων, *prevent* (αποτροπή) ίσον αποτροπή στρατολόγησης νέων προσώπων στην τρομοκρατία, *protect* (προστασία) ίσον ενίσχυση μέτρων έναντι τρομοδράσεων και *prepare* (προετοιμασία) ίσον προετοιμασία προς ελάφρυνση αντικτύπου όταν ένα δυνητικό εξτρεμιστικό κτύπημα θεωρηθεί 'αναπότρεπτο'. Το συγκεκριμένο δόγμα των Τεσσάρων P στηρίζει τη βρετανική αντιτρομοκρατική στρατηγική γνωστή ως Counter-Terrorism Strategy (CONTEST) -περί τούτων βλέπε *HM Government. Pursue, Prevent, Protect, Prepare. The United Kingdom's Strategy for Countering International Terrorism*, The Stationary Office, Μάρτιος 2009, παράγραφος 8.03, σ. 64, Nicander Lars, "Understanding Intelligence Community Innovation in the Post 9-11 World" στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 3, 2011, σ. 554. Σχετικά με το ελάχιστο ερευνηθέν ζήτημα της αντιπροπαγάνδας έναντι της (τρομοκρατικής) προπαγάνδας (counternarratives vs narratives) ήτοι, της αποτροπής στρατολόγησης νέων προσώπων στην τρομοκρατία (*prevent*) βλέπε Braddock Kurt, "Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism" στο *Studies in Conflict and Terrorism*, Volume 39, Issue 5, 2016, σ. 381-404, επίσης, Abdullah bin Khaled al-Saud, "The Tranquillity Campaign: A Beacon of Light in the Dark World Wide Web" στο *Perspectives on Terrorism*, Volume 11, Issue 2, 2017, σ. 58-63

¹⁴ Security Service MI5, *Protecting Against Terrorism*, διαθέσιμο στη διαδικτυακή τοποθεσία [http://www.lancsresilience.org.uk/Documents/Bcm/Protecting Against Terrorism.pdf](http://www.lancsresilience.org.uk/Documents/Bcm/Protecting%20Against%20Terrorism.pdf) εις την οποία καταφύγαμε την 1^η Σεπτέμβρη 2016

Τέλος, στην αυστραλιανή έκδοση *Report of the Inquiry into Australian Intelligence Agencies* του 2004 τονίζεται η πρωταγωνιστική θέση της πληροφόρησης και των Υπηρεσιών στο άρμα της κυβερνητικής αντιτρομοκρατικής εκστρατείας.¹⁵

Οι Graeme C. S. Steven και Rohan Gunaratna εξαίρουν το ρόλο των πληροφοριακών οργανισμών στη μάχη κατά της τρομοκρατίας. Γράφουν: μια πληροφορία με προοπτική μετατροπής σε πληροφόρηση δύναται να συλλεχθεί μέσω μεθόδων SIGINT, ELINT, HUMINT, μέσω ανοικτών / κλειστών πηγών, μέσω, τελικά, ποικιλίας τρόπων. Αν και οι Ηνωμένες Πολιτείες έχουν επενδύσει εκατομμύρια δολάρια σε μια προσπάθεια τεχνικής / τεχνολογικής υπεροχής, φαίνεται ότι αυτό που κάνει τη διαφορά σχετίζεται με τον ανθρώπινο παράγοντα. Οι Υπηρεσίες πρέπει να χαρακτηρίζονται από επάρκεια ανθρώπινου δυναμικού και μάλιστα διαφόρων ειδικοτήτων. Πράκτορες και αναλυτές οφείλουν να διαθέτουν πολιτισμικές, γλωσσικές και άλλες γνώσεις / δεξιότητες με αντικειμενικό σκοπό τη διείσδυση εντός τρομοκρατικών πυρήνων, τη στρατολόγηση ατόμων, τη συγκέντρωση πληροφοριών, την κατανόηση της φύσης των εξτρεμιστικών σχεδιασμών, την κατανόηση των πολιτικών κινήτρων των τρομοκρατών, της επιμελητείας, την αποκάλυψη των οικονομικών πόρων, των συνδέσμων, των σχέσεων τους με το οργανωμένο έγκλημα κ. λ.¹⁶

Οι Neal Pollard και John Sullivan γράφουν ότι οι πληροφοριακοί οργανισμοί παίζουν κεντρικό ρόλο στην αντιμετώπιση της τρομοκρατίας διά τους εξής τέσσερις, τουλάχιστον, λόγους: α) παράγουν πληροφόρηση με σκοπό την κατανόηση του κινδύνου, β) προειδοποιούν περί προθέσεων και δυνατοτήτων εξτρεμιστικών ομάδων, γ) ανευρίσκουν και εξουδετερώνουν εξτρεμιστικές ομάδες, δ) αξιολογούν την αποτελεσματικότητα ή μη της αντιτρομοκρατικής πολιτικής και στρατηγικής όπως και των σχετικών επιχειρήσεων.¹⁷ Οι ίδιοι σημειώνουν τα τρία επίπεδα της πληροφοριακής αντιτρομοκρατικής προσέγγισης ήτοι, το στρατηγικό, το επιχειρησιακό και το τακτικό όπως και την αμυντική και επιθετική πλευρά των αντιτρομοκρατικών δράσεων. Συνοπτικά αναφέρουμε πως: α) η αμυντική στρατηγική όψη αφορά στην απομείωση οικείων δομικών τρωτοτήτων, β) η αμυντική επιχειρησιακή όψη αφορά στην αναγνώριση / αποκάλυψη του οργανωτικού και επιχειρησιακού κομματιού των τρομοκρατικών ομάδων, γ) η αμυντική τακτική όψη προειδοποιεί περί κινήσεων ή και προετοιμασιών επίθεσης εκ μέρους τρομοκρατικών γκρουπ, δ) η επιθετική στρατηγική όψη αφορά στην καταπολέμηση της τρομοκρατικής ιδεολογίας, ε) η επιθετική επιχειρησιακή όψη αφορά πρωτίστως στην εξουδετέρωση των διεθνικών χρηματοδοτικών δικτύων της τρομοκρατίας, στ) η επιθετική τακτική όψη αφορά στη σύλληψη ή στην καθ' οιονδήποτε τρόπο εξουδετέρωση τρομοκρατών ηγετικού κυρίως προφίλ.¹⁸

Λαμβάνοντας υπόψη τα αμερικανικά *National Military Strategic Plan for the War on Terrorism (NMSP-WOT)* του 2006 και JP 3-26, *Counterterrorism*, του 2009 διαπιστώνουμε ότι ο πληροφοριακός σχεδιασμός και η αγωνία των υπηρεσιών Ασφαλείας / Αντικατασκοπίας γύρω από το φαινόμενο της τρομοκρατίας (αλλά και

¹⁵ *Report of the Inquiry into Australian Intelligence Agencies*, Australian Government, Ιούλιος 2004

¹⁶ Steven Graeme, Gunaratna Rohan, *Counterterrorism. A Reference Handbook*, ABC-CLIO, Inc., Santa Barbara / California, 2004, σ. 111-113. Μαζί τους συμφωνούν οι Max Manwaring και Σπυρίδων Πλακούδας με τα *Internal Wars: Rethinking Problem and Response*, Strategic Studies Institute / U.S. Army War College, Pennsylvania, 2001, σ. 18 και “Strategy in Counter-Insurgency: A Distilled Approach” στο *Studies in Conflict and Terrorism*, Volume 38, Issue 2, 2015, σ. 137, αντιστοίχως

¹⁷ Pollard Neal, Sullivan John, “Counterterrorism and Intelligence” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014, σ. 245

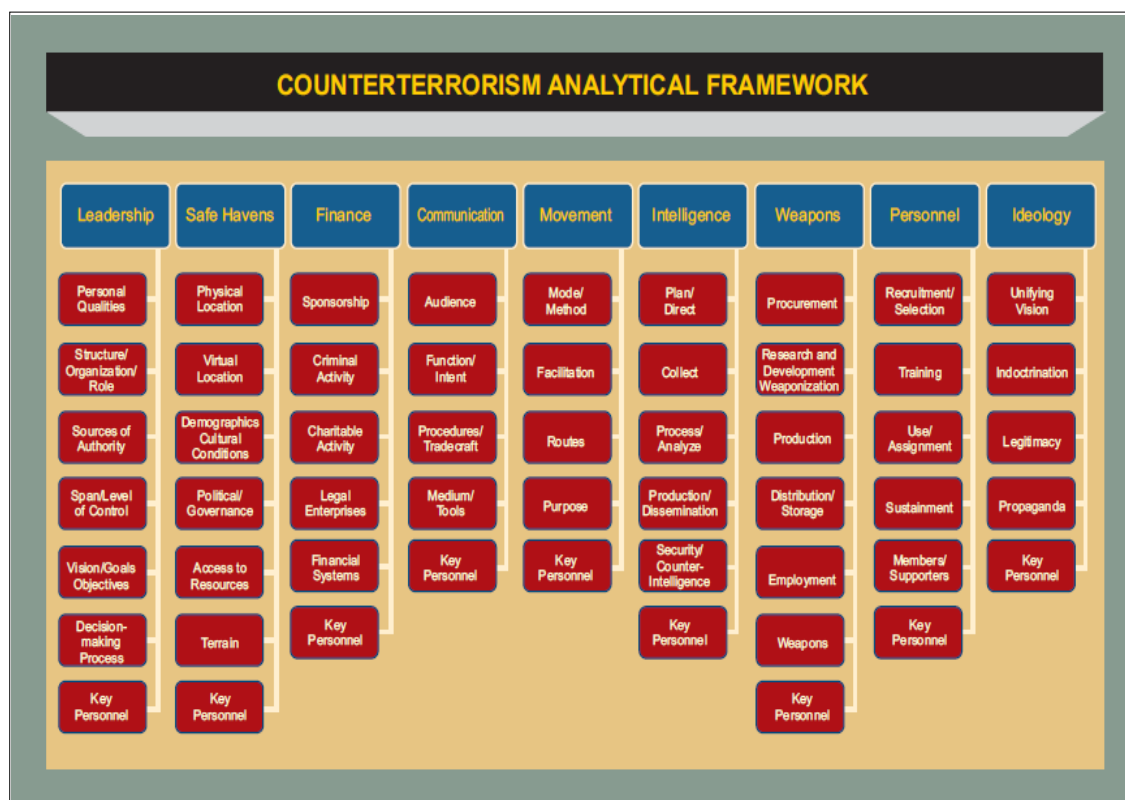
¹⁸ ό. π., σ. 247-148

στάσεων / εξεγέρσεων) κατατείνει / ευελπιστεί στην αποκάλυψη / αποδιάρθρωση των εξής εννέα συστατικών του μερών: α) της ηγεσίας. Οι περισσότερες τρομοκρατικές οργανώσεις διακρίνονται για την παρουσία ενός κεντρικού προσώπου και κάποιων, ή αρκετών, περιφερειακών / επιχειρησιακών υπαρχηγών που συνδέονται με το πρώτο, β) των καταφυγίων. Ένα ασφαλές καταφύγιο παρέχει δυνατότητα απομόνωσης / απόκρυψης, επιχειρησιακών σχεδιασμών, ενδεχομένως εκπαίδευσης κ. λ., γ) των πόρων χρηματοδότησης. Τέτοιοι μπορεί να σχετίζονται με ανεπίσημα τραπεζικά δίκτυα, νομότυπες επιχειρήσεις, εταιρίες-βιτρίνες, πρόσωπα υψηλής οικονομικής επιφανείας, κρατικούς ή μη κρατικούς οργανισμούς, εγκληματικές οργανώσεις κ. λ.¹⁹, δ) των επικοινωνιακών δικτύων. Στην ουσία αναφερόμαστε στην ικανότητα λήψης, αποθήκευσης, ελέγχου, απόδοσης πληροφοριών υπό την μία ή άλλη μορφή, μέθοδο κ. λ. ε) των κινήσεων / μετακινήσεων προσώπων και εξοπλισμού, στ) των ειδικών πληροφοριακών δικτύων. Οι εξτρεμιστικές οργανώσεις προβαίνουν σε δράσεις κατασκοπίας, αντικατασκοπίας, ελέγχου οικείου ανθρώπινου δυναμικού, εφαρμογής μέτρων επιχειρησιακής ασφαλείας, άρνησης πληροφοριών, παραπλάνησης κ. λ., ζ) των οπλικών δυνατοτήτων, η) των δυνατοτήτων στρατολόγησης προσωπικού. Ένα μέλος τρομοκρατικής ή άλλης ακραίας οργάνωσης στρατολογείται, εκπαιδεύεται, καθυποτάσσεται ιδεολογικά. Μέρος ή και όλη η διαδικασία ενδέχεται να εξελιχθεί εντός εκπαιδευτικών, θρησκευτικών, μη κυβερνητικών οργανισμών κ. λ., θ) του ιδεολογικού οικοδομήματος.²⁰ Κύριο όπλο επίρρωσης μιας σχετικής ιδεολογίας δεικνύει η προπαγάνδα, άρα, οι επιχειρήσεις αντιπροπαγάνδας εμπίπτουν εντός των υποχρεώσεων των Υπηρεσιών.²¹

¹⁹ Για μια εικόνα περί τη σχέση εταιριών, rogue states, μη κρατικών δρώντων, εγκληματικών ή τρομοκρατικών οργάνωσεων βλέπε Sloan Stephen, "Terrorism: How Vulnerable is the United States?" στο *Terrorism: National Security Policy and the Home Front*, επιμ. Pelletiere Stephen, Strategic Studies Institute, USA, 1995, σ. 53 και Lemieux Frédéric, "Financing Terrorism: Entrepreneurship, Business Strategies, and Moral Issues" στο *Protecting the Homeland from International and Domestic Terrorism Threats: Current Multi-Disciplinary Perspectives on Root Causes, the Role of Ideology, and Programs for Counter radicalization and Disengagement*, επιμ. Fenstermacher Laurie, Rieger Tom, κ. ά., 2010, σ. 208-217

²⁰ "Al-Qaeda is not a state nor a great power but a transnational network and more importantly an idea around which resistance is organised globally and locally" -για μια άποψη βλέπε Barkawi Tarak, Laffey Mark, "The Post-Colonial Moment in Security Studies" στο *Review of International Studies*, Volume 32, Issue 2, 2006, σ. 329. Στη γαλλική *Le Monde* της 29^{ης} Οκτωβρίου 2001 κάνει την εμφάνισή του κείμενο που εικάζεται πως συντρόφευσε τους τρομοκράτες της 11^{ης} Σεπτεμβρίου ως την τελευταία στιγμή. Το συγκεκριμένο κείμενο αποδίδει την ηθικοθρησκευτική διάσταση του ευρύτερου ψυχοκοινωνικού και ιδεολογικού προφίλ του 'μάρτυρα - μαχητή' του Ισλάμ -για περισσότερα βλέπε Καφφές Γιώργος, *Κοινωνιολογία της Τρομοκρατίας*, Παπαζήσης, Αθήνα, 2010, σ. 74-83

²¹ Για τα εννέα συστατικά μέρη μιας εξτρεμιστικής οργάνωσης βλέπε *National Military Strategic Plan for the War on Terrorism*, Chairman of the Joint Chiefs' of Staff, Washington, D.C., 2006, σ. 14-19, επίσης ανέτρεξε στο JP 3-26, *Counterterrorism*, Joint Chiefs of Staff, Νοέμβριος 2009, σ. V-6



Εικόνα 22: τα εννιά συστατικά μέρη μιας εξτρεμιστικής οργάνωσης. Η εικόνα ελήφθη από τη σελίδα V-4 της JP 3-26, *Counterterrorism*, 2009

Αναφορικά με τα τμήματα ανάλυσης πληροφοριών, η εργασία τους σχετίζεται με: α) την ακτινογράφιση του επιχειρησιακού περιβάλλοντος ήτοι, του φυσικού χώρου εντός του οποίου θα δράσουν οι έννομες δυνάμεις προκειμένου να αποπλιστούν οι τρομοκράτες. Σ' αυτή τη φάση αναζητούνται τα κύρια χαρακτηριστικά του συγκεκριμένου χώρου, β) την αξιολόγηση του επιχειρησιακού περιβάλλοντος. Σε δεύτερη φάση εκτιμώνται τα πλεονεκτήματα και τα μειονεκτήματα του συγκεκριμένου περιβάλλοντος ως προς τις δυνητικές επιχειρήσεις φίλων και μη δυνάμεων, γ) την εκτίμηση της τρομοκρατικής απειλής, δ) την εκτίμηση της απειλής κατά την πορεία των επιχειρήσεων -πρακτικά γίνεται λόγος περί των τεσσάρων στοιχείων της πληροφοριακής προετοιμασίας μάχης.²²

Ο Carl Wellman στο κεφάλαιο 5 του *Terrorism and Counterterrorism. A Moral Assessment* καταγράφει τις δυνητικές απαντήσεις ενός κρατικού παράγοντα έναντι του τρομοφαινομένου. Οι δράσεις που δύνανται να συνδέονται με τις υπηρεσίες

²² Larson Eric, Eaton Derek, κ. ά., *Assessing Irregular Warfare. A Framework for Intelligence Analysis*, RAND Corporation, Santa Monica, 2008, σ. 41. Η εκτίμηση της απειλής κατά την πορεία της επιχείρησης (threat's likely future Course of Action -COA) συνυφαίνεται άμεσα με την Πληροφοριακή Προετοιμασία Μάχης (Intelligence Preparation of the Battlefield -IPB) περί της οποίας ο ενδιαφερόμενος μπορεί να ανατρέξει στο FM 34-130, *Intelligence Preparation of the Battlefield*, Headquarters, Department of the Army, USA, July 1994 ή στο FM 3-24 / FMFM 3-24, *Counterinsurgency*, Headquarters, Department of the Army, Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., June 2006, σ. 3-2 – 3-14. Ειδικότερα περί του IPB και των τεσσάρων στοιχείων του σε σχέση με αντεπαναστατικές επιχειρήσεις [counterinsurgency (COIN) operations] βλέπε FM 3-24 / MCWP 3-33.5, *Counterinsurgency*, Headquarters, Department of the Army, Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., December 2006, σ. 3-2 – 3-24

Πληροφοριών είναι οι εξής: α) παρατήρηση / παρακολούθηση (surveillance). Ένα κράτος, στην προσπάθεια καταπολέμησης της τρομοκρατίας, οφείλει να εντοπίσει τους δυνητικούς δράστες, να μάθει περί των σχεδίων τους, να λάβει μέτρα· όλα αυτά απαιτούν εκτεταμένη και επίμονη παρακολούθηση. Ο Wellman παραπέμπει στο *American Heritage Dictionary* ορίζοντας το «surveillance» ως ...στενή παρακολούθηση ατόμου ή ομάδας για το οποίο / την οποία υπάρχουν [οι όποιες] υποψίες. Σημειώνουμε ότι μια επιχείρηση παρακολούθησης συνεπάγεται καθήκοντα συλλογής, ταξινόμησης και ανάλυσης πληροφορίας²³, β) στοχευμένες εκτελέσεις (targeted killing). Πρόκειται για τακτική που εφαρμόζεται τόσο από το Ισραήλ όσο και τις ΗΠΑ. Ο Michael L. Gross γράφει πως ...αντιμέτωποι με όλο και συχνότερες επιθέσεις κατά πολιτών, με ένα όλο και πιο ευρύ [παλαιστινιακό] δίκτυο πολιτοφυλακής, οι 'επιλεκτικές' εκτελέσεις / δράσεις συμβάλουν στη μείωση των παράπλευρων απωλειών την ίδια στιγμή που πλήττουν την ηγεσία της πολιτοφυλακής και αυτούς που ευθύνονται για την τρομοκρατία. Οι συγκεκριμένες ενέργειες συνάδουν με τη φιλοδοξία επίρρωσης αισθήματος εθνικής ασφαλείας, ελαχιστοποίησης των θυμάτων και επιστροφής των Παλαιστινίων στο τραπέζι των διαπραγματεύσεων²⁴, γ) διείσδυση (intrusion). Αν και τα όποια τοπικά τρομοκρατικά γκρουπ δεν λείπουν, στις μέρες μας ο πλέον σοβαρός κίνδυνος αντιπροσωπεύεται από διεθνείς εξτρεμιστικές ομάδες. Κατά την έννοια τούτη η αποτελεσματική αντιμετώπιση της τρομοκρατίας φαίνεται να συνδέεται (και) με προληπτική κρατική δράση εκτός συνόρων με όποιες παρενέργειες ίσως προκληθούν. Παράδειγμα αποτελούν οι επιθέσεις, με χρήση drones, των ΗΠΑ²⁵ σε περιοχές τρομοκρατών εντός της επικράτειας του Πακιστάν, η εκτέλεση του bin Laden από τα US Navy SEALs, οι στοχευμένες αμερικανικές επιχειρήσεις κατά ηγετικών φυσιογνωμιών της ακραίας ιδεολογίας εντός της επικράτειας της Υεμένης κ. λ.²⁶, δ) εισβολή (invasion). Τρανταχτό παράδειγμα στη

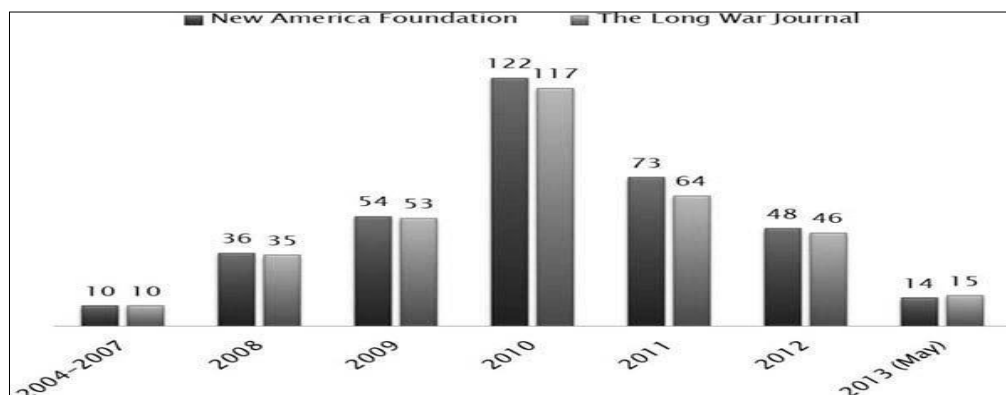
²³ Wellman Carl, *Terrorism and Counterterrorism. A Moral Assessment*, Springer, 2013, σ. 80

²⁴ Gross L. M., "Fighting by Other Means in the Mideast: a Critical Analysis of Israel's Assassination Policy", *Political Studies*, Volume 51, Issue 2, 2003, σ. 351, επίσης Schulze, K. E., "Camp David and the Al-Aqsa intifada: an assessment of the state of the Israeli-Palestinian peace process July-December 2000", *Studies in Conflict and Terrorism*, Volume 24, Issue 3, 2001, σ. 223-225. Από την άλλη μεριά οι Steven και Gunaratna σημειώνουν ότι οι εκτελέσεις τρομοκρατών συχνά αποδεικνύονται αντιπαραγωγικές καθώς δημιουργούν μάρτυρες, αντιστασιακά πρότυπα και ευκαιρία για προπαγάνδα -για μια άποψη βλέπε Steven Graeme, Gunaratna Rohan, *Counterterrorism. A Reference Handbook*, ABC-CLIO, Inc, Santa Barbara / California, 2004, σ. 112, επίσης, McIntosh Christopher, "Counterterrorism as War: Identifying the Dangers, Risks, and Opportunity Costs of U.S. Strategy Toward L Qaeda and Its Affiliates" στο *Studies in Conflict and Terrorism*, Volume 38, Issue 1, 2015, σ. 32

²⁵ Περί τούτου βλέπε Jordan Javier, "The Effectiveness of the Drone Campaign against Al Qaeda Central: A Case Study" στο *Journal of Strategic Studies*, Volume 37, Number 1, 2014, σ. 4-29, Hazelton L. Jacqueline, "Drone Strikes and Grand Strategy: Toward a Political Understanding of the Uses of Unmanned Aerial Vehicle Attacks in US Security Policy" στο *Journal of Strategic Studies*, Volume 40, Number 1-2, 2017, σ. 68-91, "US forces deploy deadly new drone: Images reveal how Al Qaeda leader was killed with deadly accurate strike -which didn't even break his car's windows", *Mail Online*, 27 Φεβρουαρίου 2017 στο <http://www.dailymail.co.uk/news/article-4265870/Images-Syrian-strike-new-kind-drone-exist.html> όπου καταφύγαμε την 1^η Απριλίου 2017, Helmore Edward, "US retires Predator Drones after 15 years that changed 'the war on terror'", *The Guardian*, 13 Μαρτίου 2017 στην ιστοσελίδα <https://www.theguardian.com/world/2017/mar/13/predator-drone-retire-reaper-us-military-obama> όπου ανατρέξαμε επίσης την ανωτέρω ημερομηνία. Συγκριτικά βλέπε "Game of 'Drones': the uses of UAVs by militant groups in Iraq and Syria", *HIS Markit*, 6 Μαρτίου 2017 στο <http://blog.ihs.com/game-of-drones-the-uses-of-uavs-by-militant-groups-in-iraq-and-syria> εις το οποίο προσφύγαμε την 3^η Απριλίου 2017

²⁶ Wellman Carl, *Terrorism and Counterterrorism. A Moral Assessment*, Springer, 2013, σ. 103, επίσης βλέπε Larsdotter Kersti, "Regional Support for Afghan Insurgents: Challenges for Counterinsurgency Theory and Doctrine" στο *Journal of Strategic Studies*, Volume 37, Number 1, 2014, σ. 135-162

δεκαετία του 2000 η εκ μέρους των ΗΠΑ και των συμμάχων τους αντιτρομοκρατική εκστρατεία / εισβολή τόσο στο Αφγανιστάν (2001) όσο και στο Ιράκ (2003)²⁷ με τις υπηρεσίες Πληροφοριών να διαδραματίζουν καίριο ρόλο στην προετοιμασία / εκτέλεση των εγχειρημάτων.



Εικόνα 23: Γράφημα των αμερικανικών κτυπημάτων μεταξύ 2004 και Μαΐου 2013 με χρήση drones στο Πακιστάν σύμφωνα με το New America Foundation και τη *The Long War Journal*. Κορύφωση παρατηρείται το 2010, ακριβώς πριν την εξολόθρευση του Bin Laden. Η εικόνα ελήφθη από το “The Effectiveness of the Drone Campaign against Al Qaeda Central: A Case Study” του Javier Jordan στο *Journal of Strategic Studies*, Volume 37, Number 1, 2014, σ. 12

Παρόμοιοι στρατηγισμοί κατατίθενται στο *The End of Intelligence* του David Tucker. Ομαδοποιώντας καταγράφουμε τις τακτικές: α) της εξόντωσης όλων ανεξαιρέτως των εμπλεκόμενων σε ανταρτικές / τρομοκρατικές οργανώσεις (killing insurgents), β) των επιλεκτικών στοχοποιήσεων προσώπων / assets των άνω οργανώσεων (selective targeting), γ) της αποψίλωσης των άνω οργανώσεων μέσω πρακτικών τρώσης εμπιστοσύνης μεταξύ μελών ή συνδεδετικών κρίκων, μέσω παραπληροφόρησης, χειραγώγησης κ. ο. κ. (attacking organization).²⁸

²⁷ Wellman Carl, *Terrorism and Counterterrorism. A Moral Assessment* ό. π., σ.106

²⁸ Tucker David, *The End of Intelligence. Espionage and State Power in the Information Age*, Stanford University Press, USA, 2014, σ. 143-151, επίσης, Mottram Richard, “Protecting the Citizen in the Twenty-first Century: Issues and Challenges” στο *The New Protective State. Government, Intelligence and Terrorism*, επιμ. Hennessy Peter, Continuum Books, Mile End Institute, New York, 2007, σ. 49-51, Wilner Alex, “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism” στο *Journal of Strategic Studies*, Volume 34, Number 1, 2011, σ. 3-37 και Searle Nicholas, “To defeat terrorists we have to get inside their minds”, *The Guardian*, 17 Μαρτίου 2017, στο <https://www.theguardian.com/commentisfree/2017/mar/17/defeat-terrorists-terrorism> εις το οποίο προσφύγαμε την 3^η Απριλίου 2017. Οπωσδήποτε δεν ξεχνάμε το αντεπαναστατικό δόγμα της προσέγγισης του τοπικού πληθυσμού (population-centric COIN) με έμφαση στην «καρδιά και στο μυαλό / hearts and minds» των ντόπιων κοινωνιών και με τις Υπηρεσίες να συμμετέχουν στο κτίσιμο των λεγόμενων *trusted networks* -για μια εικόνα βλέπε FM 3-24 / MCWP 3-33.5, *Counterinsurgency*, ό. π., σ. A-5, επίσης, Rid Thomas, “The Nineteenth Century Origins of Counterinsurgency Doctrine” στο *Journal of Strategic Studies*, Volume 33, Number 5, 2010, σ. 727-758 αλλά και Šmíd Tomáš, Mareš Miroslav, “Kadyrovtsy’: Russia’s Counterinsurgency Strategy and the Wars of Paramilitary Clans” στο *Journal of Strategic Studies*, Volume 38, Number 5, 2015, σ. 650-677. Με τη σειρά τους τα *trusted networks* θα χρησιμοποιήσουν την προπαγάνδα / αντιπροπαγάνδα, τις επικοινωνίες και τα social media -περί τούτων βλέπε και στο Bouzis Kathleen, “Countering the Islamic State: US Counterterrorism Measures” στο *Studies in Conflict and Terrorism*, Volume 38, Issue 10, 2015, σ. 888-891. Επισημαίνουμε τέλος ότι εφόσον η όποια αντεπαναστατική κίνηση έχει αναληφθεί από το όποιο απολυταρχικό καθεστώς, τότε, οι Υπηρεσίες και οι οργανισμοί Ασφαλείας θα κινηθούν πρώτα και κύρια στη γραμμή της σκληρής καταστολής -περί τούτου βλέπε Ucko David, “The People are

Παρά το ότι η αντικατασκοπία ως πεδίο ενσωματώνει, κατά τον Loch Johnson, την αντιτρομοκρατία,²⁹ παρά τον κοινό σκοπό όσον αφορά στην εξουδετέρωση του τρομοκινδύνου και τις εν πολλοίς κοινές πρακτικές, υπάρχουν αντικειμενικοί περιορισμοί και διαφοροποιήσεις. Π. χ. ο John Buckley διαπιστώνει ότι συχνά οι περί επικείμενων κτυπημάτων πληροφορίες διακρίνονται από έλλειψη ακρίβειας τη στιγμή που τις χαρακτηρίζει η γενικότητα. Πώς θα μπορούσε να χρησιμοποιηθεί μια τέτοια πληροφορία; Που θα μπορούσε να βρεθεί μια ισορροπία μεταξύ γενικότητας και ακρίβειας; Ο Buckley δίδει το εξής παράδειγμα: ας υποθέσουμε ότι έρχεται σε κάποιον law enforcement σταθμό μια πληροφορία από αξιόπιστη πηγή περί σχεδιασμού τρομοκρατικού κτυπήματος σε κάποιο νυκτερινό κλαμπ στη Ν. Υόρκη εντός εβδομάδας. Τι δύναται να πράξουν οι Υπηρεσίες; Οι επιλογές ποικίλουν από: α) μια προειδοποίηση του κοινού, β) μια προειδοποίηση των επιχειρηματιών νυκτερινών κλαμπ αφού πρώτα οριστεί τι σημαίνει ‘νυκτερινό κλαμπ’, γ) μια αστυνομική εκστρατεία με την προοπτική αποτροπής της επίθεσης με όποιο κόστος, και όχι μόνο οικονομικό, αυτή η εκστρατεία επιφέρει, δ) μια στάση αδρανείας, κάτι μάλλον όχι αποδεκτό. Από κει και έπειτα τι προβλέπεται εάν περάσει η εβδομάδα χωρίς κάποια εξέλιξη; Ίσως η επίθεση ακυρώθηκε για κάποιον λόγο. Ίσως αναβλήθηκε. Τα όποια μέτρα ασφαλείας θα διατηρηθούν; Ας μην ξεχνάμε, συνεχίζει ο μελετητής, ότι η τρομοκρατία επιβάλλει τον φόβο όχι μόνο μέσα από θύματα αλλά και μέσα από αλλαγή συμπεριφοράς της κοινωνίας. Το πρόβλημα εντοπίζεται στη διαχείριση της πληροφορίας και όχι σ’ αυτήν καθαυτή. Οι επιτελικοί καλούνται να αποφασίσουν άμεσα βασισμένοι στο διαθέσιμο στοιχείο της στιγμής.³⁰ Αυτό κατά τον Michael Sulick αποτελεί ίσως το μεγαλύτερο πρόβλημα αναδεικνύοντας την κύρια επιχειρησιακή διαφορά μεταξύ αντιτρομοκρατίας και αντικατασκοπίας: Η πρώτη απαιτεί στιγμιαία κινητοποίηση πόρων / προσωπικού, άμεση τακτική αντίδραση, κεραυνοβόλες επιχειρήσεις. Η δεύτερη δύναται να απλωθεί εις μακρόν, να μελετήσει διεξοδικά τον στόχο, να συσχετίσει υπομονετικά δεδομένα και λεπτομέρειες, να ξεδιαλύνει διαδοχικά τις σκιές. Ασφαλώς, κλείνει ο Sulick, κατά την εμπλοκή ενός συνόλου Υπηρεσιών ενσκήπτει ενδεχομένως το πρόβλημα των διαρροών, της ανεπαρκούς συνεργασίας, των όποιων γραφειοκρατικών αγκυλώσεων κ. λ.³¹

Revolting’: An Anatomy of Authoritarian Counterinsurgency” στο *Journal of Strategic Studies*, Volume 39, Number 1, 2016, σ. 29-61

²⁹ Johnson K. L., “National Security Intelligence in the United States: A Performance Checklist”, *Studies in Intelligence*, Volume 26, Number 5, 2011, σ. 614

³⁰ Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, CRC Press, Florida, 2014, σ. 449-450

³¹ Sulick J. Michael, “Counterintelligence in the War Against Terrorism”, *Studies in Intelligence*, Volume 48, Number 4, 2004, σ. 31-33. Οι προβληματισμοί που αναπτύσσει ο Sulick μεγεθύνονται όταν το όποιο αντιτρομοκρατικό πλάνο αναφέρεται σε πολιτικές ασφαλείας ευρύτερων σχηματισμών όπως, π. χ., της Ευρωπαϊκής Ένωσης -για μια ιδέα περί των αντιτρομοκρατικών κινήσεων της τελευταίας βλέπε Argomaniz Javier, Bures Oldrich, Kaunert Christian, “A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment”, Bures Oldrich, “Ten Years of EU’s Fight against Terrorist Financing: A Critical Assessment”, Monar Jörg, “The EU as an International Counterterrorism Actor: Progress and Constraints” και Den Boer, Monica, “Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis” στο *Intelligence and National Security*, Volume 30, Number 2-3, 2015, σ. 191-206, 207-233, 333-356 και 402-419 αντιστοίχως, επίσης, Fägersten Björn, “Bureaucratic Resistance to International Intelligence Cooperation: The Case of Europol” στο *Intelligence and National Security*, Volume 25, Number 4, 2010, σ. 500-520 και *The European Union’s Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness*, European Parliament, Brussels, Ιανουάριος 2017, στη διαδικτυακή τοποθεσία [http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU\(2017\)583124_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf) εις την οποία ανατρέξαμε την 3^η Απριλίου 2017

Σ' αυτό το σημείο ας επιχειρήσουμε μια εν τάχει καταγραφή της πολιτικής του Ισραήλ σχετικά με την αντιμετώπιση επιθέσεων παλαιστινιακών ομάδων εντός της ισραηλινής περιμέτρου. Από πληροφοριακής απόψεως οι κρατικές ισραηλινές Υπηρεσίες επικεντρώνουν: α) στην αναγνώριση δυνητικών κινδύνων προερχομένων από ομάδες ή μεμονωμένα άτομα, β) στην αποκάλυψη πηγών / μεθόδων χρηματοδότησης των αναφερομένων ομάδων ή ατόμων, γ) στην αποκάλυψη των εξοπλιστικών πηγών των αναφερομένων ομάδων ή ατόμων, δ) στην αποκάλυψη ενδεχομένων συνεργασιών μεταξύ υπόπτων ομάδων / ατόμων και αλλοδαπών μυστικών υπηρεσιών.³²

Με το ξέσπασμα της δεύτερης παλαιστινιακής ιντιφάντα (2000) η ισραηλινή υπηρεσία εσωτερικών Πληροφοριών ISA (Israel Security Agency, γνωστή ως Shin Bet ή Shabak) αναπτύσσει σε συνεργασία με τις ισραηλινές ένοπλες δυνάμεις (Israel Defense Force / IDF) και το πληροφοριακό τους τμήμα (Intelligence Branch / IB, γνωστό ως AMAN) ένα σύστημα οριζόντιας διανομής πληροφοριών σε πραγματικό χρόνο με σκοπό την ανταλλαγή δεδομένων μεταξύ των τακτικών επιχειρησιακών μονάδων προς επίσπευση της «πληροφοριακής χρήσης». Η συγκεκριμένη μέθοδος διανομής τακτικού επιπέδου πληροφοριών προσδίδει σημαντικά κέρδη τόσο στην προσπάθεια σύλληψης υπόπτων τρομοκρατίας όσο στην αποδιοργάνωση σχετικών δικτύων. Ασφαλώς, είναι οι ένοπλες δυνάμεις που εφοδιάζουν με προσωπικό προκειμένου το τελευταίο να προβεί σε συλλήψεις, καταστροφές τούνελ ή άλλων χρησίμων στις παλαιστινιακές ανταρτικές δυνάμεις υποδομών. Περαιτέρω, ο στρατός παρέχει τον κύριο όγκο πληροφοριών SIGINT τη στιγμή που η ISA επικεντρώνει στο κομμάτι του HUMINT στρατολογώντας / ελέγχοντας άτομα παλαιστινιακής καταγωγής.³³

Αν και η ανταλλαγή τακτικών πληροφοριών μεταξύ AMAN και ISA αντιμετώπισε κάποιες δυσκολίες σε περιπτώσεις ευρύτερων επιχειρήσεων³⁴, το αληθινό πρόβλημα εντοπίζεται στην αποτυχία μακροστρατηγικών προβλέψεων ή, αλλιώς, στην παραγωγή στρατηγικής πληροφόρησης. Η ισραηλινές Υπηρεσίες απέτυχαν να διαβλέψουν το ξέσπασμα των δύο παλαιστινιακών ιντιφάντα (1987, 2000)³⁵ όπως και την πορεία των επακόλουθων γεγονότων με αποτέλεσμα τη μη εκπόνηση καταλλήλων πολιτικών, τη μη ορθή διανομή πόρων, τη μη λήψη προληπτικών μέτρων.³⁶ Κατά τον Efraim Halevy οι βελτιώσεις στην αντιτρομοκρατική πρακτική του Ισραήλ στηρίζονται σε lessons learned τακτικού επιπέδου παρά σε μια προσπάθεια κατανόησης / πρόληψης πιθανών γεγονότων· μαζί του συμφωνεί ο Daniel Byman μιλώντας για εφαρμογή ad hoc αντιτρομοκρατικών τακτικών.³⁷ Με την πάροδο των ετών, συνεχίζει ο Halevy, οι Υπηρεσίες προσπάθησαν να επηρεάσουν τις

³² Morag Nadav, "Foreign Intelligence and Counterterrorism: An Israeli Perspective" στο *Homeland Security and Intelligence*, επιμ. Logan G. Keith, Praeger, Santa Barbara / California, 2010, σ. 157

³³ ό. π., σ. 157-158

³⁴ Π. χ. στην περίπτωση του δευτέρου πολέμου στο Λίβανο το 2006 -για περισσότερες πληροφορίες βλέπε Harel Amos, Issacharoff Avi, *34 Days: Israel, Hezbollah, and the War in Lebanon*, Palgrave Macmillan, New York, 2008, σ.133

³⁵ Ο Eyal Pascovich διαφωνεί θεωρώντας ότι η δεύτερη ιντιφάντα (Al-Aqsa Intifanta) δεν συνέλαβε εξαπίνης τις ισραηλινές Υπηρεσίες καθώς οι τελευταίες, συνεχίζει, είχαν διαβλέψει την αναζωπύρωση των συγκρούσεων μετά την αποτυχία των συνομιλιών στο Camp David τον Ιούλιο του 2000, εντούτοις ο ίδιος δηλώνει ότι υπάρχουν και αντίθετες απόψεις -περί τούτων βλέπε Pascovich Eyal, "Military Intelligence and Controversial Political Issues: The Unique Case of the Israeli Military Intelligence" στο *Intelligence and National Security*, Volume 29, Number 2, 2014, σ. 20

³⁶ Morag Nadav, "Foreign Intelligence and Counterterrorism: An Israeli Perspective" στο *Homeland Security and Intelligence*, ό. π., σ. 158, επίσης βλέπε Bar-Joseph Uri, "Israel's Military Intelligence Performance in the Second Lebanon War" στο *International Journal of Intelligence and CounterIntelligence*, Volume 20, Issue 4, 2007, σ. 583-601

³⁷ Halevy Efraim, *Man in the Shadows: Inside the Middle East Crisis with a Man Who Led the Mossad*, St. Martin's Press, New York, 2006, σ. 231, Byman Daniel, *A High Price: The Triumphs and Failures of Israeli Counterterrorism*, Oxford University Press, Oxford, 2011, σ. 5-6, 344-346, επίσης βλέπε Freilich D. Charles, "Israel Counter-Terrorism Policy: How Effective?" στο *Terrorism and Political Violence*, Volume 29, Issue 2, 2017, σ. 363, 371

κρατικές πολιτικές όπως και να αναλάβουν πρωτοβουλίες.³⁸ Αυτό, σύμφωνα με τον Amos Gilboa, κάποιες φορές οδηγεί σε φτωχά αποτελέσματα καθώς έμφαση δίδεται περισσότερο στην ‘απόκρουση’ παρά στην ‘αναζήτηση ευκαιριών’. Ας μην ξεχνάμε, συνεχίζει ο ερευνητής, πως η AMAN δεν είναι άλλο από στρατιωτικός οργανισμός του οποίου βασική αποστολή δεν αποτελεί η διπλωματία αλλά η αναγνώριση / καταπολέμηση απειλών εθνικής ασφαλείας.³⁹

Σε κάθε περίπτωση μετά τη συλλογή πληροφοριών ακολουθεί η προσπάθεια της πρόληψης / παρεμπόδισης. Η ισραηλινή αντιτρομοκρατική προσέγγιση στηρίζεται στην υπόθεση πως αν ο υποψήφιος τρομοκράτης δεν εξουδετερωθεί προτού εκκινήσει την αποστολή του, τότε, κάποιος θα πληρώσει με αίμα, συνεπώς, το δόγμα της πρόληψης / παρεμπόδισης λαμβάνει ακόμα μεγαλύτερες διαστάσεις. Παρά το ότι οφείλουμε να συνυπολογίζουμε την πραγματικότητα της στενής γεωγραφίας, ισχύει το εξής: εφόσον κάποιος βομβιστής αυτοκτονίας βγει από τη βάση του και εντός ολίγων λεπτών βρεθεί μέσα σε αστική εβραϊκή περιοχή, τότε, και με την οιαδήποτε, έστω αναίμακτη, κατάληξη, το σύστημα ασφαλείας έχει αποτύχει.⁴⁰ Σχετικά με το πληροφοριακό τμήμα των law enforcement αρχών σημειώνουμε πως αυτό δεν συμμετέχει στο σύστημα πληροφοριών εθνικής ασφαλείας παρά μόνο κατόπιν κλήσεως και εφόσον εγερθούν υπόνοιες σύνδεσης μεταξύ εγκληματικών δραστηριοτήτων και τρομοκρατίας.⁴¹ Πάρα ταύτα εάν κάποιο ύποπτο στοιχείο υπερκεράσει τα σημεία ελέγχου και σημανθεί, είναι οι αστυνομικές αρχές που εντέλλονται ως προς την ταυτοποίησή του.⁴²

Στο Ισραήλ, τονίζει ο Morag, δεν διαχωρίζουν, όπως π. χ. στις ΗΠΑ, μεταξύ εθνικής (national) και εγχώριας (homeland) ασφαλείας.⁴³ Αν και οι δύο έννοιες συνθέτουν ουσιαστικά κοινό τόπο, το γεγονός δεικνύει το μέγεθος του προβλήματος -εθνική ασφάλεια στο Ισραήλ σημαίνει, κυρίως και κατά το δυνατόν, αποσόβηση τρομοκρατικών κινδύνων / κτυπημάτων. Η ισραηλινή αντιτρομοκρατική στρατηγική περιστρέφεται γύρω από τους πυλώνες της πρόληψης / αποτροπής, συνεργασίας με τον πληθυσμό, καταδίωξης και, τέλος, συλλογής / ανάλυσης πληροφοριών.⁴⁴ Η εμπειρία, συνεχίζει ο μελετητής, καταδεικνύει ότι η έμφαση στην πληροφοριακή διαδικασία (πολιτικών / στρατιωτικών Υπηρεσιών) συν την επιβολή αυστηρών αποτρεπτικών μέτρων «στο δρόμο» δύναται, αν όχι να εξαλείψει το τρομοκρατικό φαινόμενο, να το περιορίσει σε διαχειρίσιμα επίπεδα.⁴⁵

Αντικατασκοπευτικές πρακτικές στην υπηρεσία τρομοκρατικών ομάδων

Ο Μ. Η. Schiattareggia σε άρθρο του το καλοκαίρι του 1962 γράφει / ρωτά: «Ποιες οι πληροφοριακές ανάγκες (essential elements of information -EEI) των στασιαστικών συσσωματώσεων;». Ο ίδιος απαντά λέγοντας πως οι πληροφοριακές τους ανάγκες σχετίζονται με τη γνώση των κινήσεων των διωκτών τους, το επιχειρησιακό χρονοδιάγραμμα και τις διαδρομές που οι τελευταίοι ακολουθούν ώστε να επιλεγούν

³⁸ Halevy Efraim, *Man in the Shadows: Inside the Middle East Crisis with a Man Who Led the Mossad*, ό. π., σ. 231-232

³⁹ Morag Nadav, “Foreign Intelligence and Counterterrorism: An Israeli Perspective”, ό. π., σ. 158. Επικουρικά βλέπε Pascovich Eyal, “Military Intelligence and Controversial Political Issues: The Unique Case of the Israeli Military Intelligence” στο *Intelligence and National Security*, Volume 29, Number 2, 2014, σ. 227-261

⁴⁰ ό. π., σ. 159. Βέβαια, πλήρης αποκλεισμός παλαιστινιακών θυλάκων δεν μπορεί να επιτευχθεί. Η άρνηση πρόσβασης σε χώρους πέριξ ‘σκληρών στόχων’ και η εκτέλεση αντιποίνων αποτελούν επίσης προληπτικές / αποτρεπτικές μεθόδους -περί τούτου βλέπε Kirchofer P. Charles, “Managing Non-State Threats with Cumulative Deterrence-by-Denial” στο *Perspectives on Terrorism*, Volume 11, Issue 2, 2017, σ. 23

⁴¹ Morag Nadav, “Foreign Intelligence and Counterterrorism: An Israeli Perspective”, ό. π., σ. 156

⁴² ό. π., σ. 160

⁴³ ό. π., σ. 155

⁴⁴ ό. π., σ. 77

⁴⁵ ό. π., σ. 165-166

εκ μέρους των ανταρτών σημεία κατάλληλα για ενέδρες όπως και να αναγνωριστούν δίοδοι διαφυγής. Ασφαλώς, επιθυμητή είναι η γνώση της ισχύος των διωκτικών ομάδων, των σημείων συγκεντρώσεών τους, των σημείων εφοδιασμού τους, των τακτικών μάχης που ακολουθούν. Οι πληροφορίες αντλούνται από διάφορες πηγές και με διάφορα μέσα, βλέπε: α) τον τοπικό πληθυσμό που θα συνταχθεί με τους αντάρτες στον όποιο βαθμό, που θα τους προσφέρει κάλυψη και οδούς διαφυγής, είτε λόγω ιδεολογικής συγγενείας, είτε λόγω επιτυχούς εκ μέρους των ανταρτών προπαγάνδας, είτε λόγω εκβιασμού / εκφοβισμού⁴⁶, β) αντάρτικες περιπόλους, γ) ομάδες παρακολούθησης, δ) σημεία κατόπτευσης, ε) ανακρίσεις αιχμαλώτων, στ) διείσδυση εντός των διωκτικών αρχών και υπηρεσιών, ζ) technical intelligence σε περίπτωση διαθέσεως σχετικών δυνατοτήτων / πόρων.⁴⁷

Ο Carlos Revillo Arango της CIA αναφερόμενος εν έτει 1968 σε λατινοαμερικανικές ανταρτικές ομάδες γράφει ότι αντιπληροφοριακές πρακτικές χρησιμοποιούνται προκειμένου να αντιπαρέλθουν κίνδυνοι που σχετίζονται με: α) δράση κυβερνητικών δυνάμεων ασφαλείας, β) επίβουλες πράξεις εκ μέρους αντιπάλων εξτρεμιστικών ομάδων, γ) φαινόμενα συνεργασίας με / αυτομόλησης στον εχθρό, δ) τυχαίες καταστάσεις που ενδέχεται να κάνουν με απροσεξία κινήσεων, απροσδόκητες αλλαγές στον κυβερνητικό σχεδιασμό ασφαλείας, φυσικές καταστροφές κ. λ.⁴⁸

Ο Βραζιλιάνος θεωρητικός, και όχι μόνο, του αστικού αντάρτικου Carlos Marighella στο *Minimanual of the Urban Guerrilla / Minimanual do Guerriheiro Urbano* (1969) τονίζει την ανάγκη λήψεως μέτρων ασφαλείας εκ μέρους της όποιας σχετικής οργάνωσης προκειμένου να: α) διασφαλιστεί η μυστική διαδικασία στρατολόγησης, β) εμποδιστεί η αχρείαστη διασπορά πληροφοριών μεταξύ των μελών της οργάνωσης, γ) αποφευχθούν κρούσματα απειθαρχίας, περιστατικά αβλεψίας κ. λ., δ) διαφυλαχθούν ντοκουμέντα, ονόματα, διευθύνσεις, χάρτες, σχέδια / σχεδιαγράμματα παντός τύπου επιπέδου «εμπιστευτικών» και άνω, ε) διασφαλιστούν κρίσιμες πληροφορίες, στ) συμμορφωθούν με τους κανόνες σύντροφοι που περιέπεσαν σε σφάλμα-τα, ζ) αποφευχθούν 'συναντήσεις' με τις αρχές Ασφαλείας, η) ληφθούν πληροφορίες σχετικές με τις αρχές Ασφαλείας, θ) διασφαλιστεί η

⁴⁶ Για μια τυπολογία υποστήριξης αντάρτικων κινημάτων εκ μέρους του τοπικού πληθυσμού βλέπε Boylan Brandon "Sponsoring Violence: A Typology of Constituent Support for Terrorist Organizations" στο *Studies in Conflict and Terrorism*, Volume 38, Issue 8, 2015, σ. 652-670

⁴⁷ Schiattareggia H. M., "Counterintelligence in Counter guerrilla Operations", *Studies in Intelligence*, Volume 6, Number 3, 1962, σ. 40-43. Σημειώνουμε σε αδρές γραμμές πως οι τακτικές που δύναται να ακολουθήσουν οι αρχές προκειμένου να απομειώσουν τις πληροφοριακές / αντιπληροφοριακές δυνατότητες των ανταρτών ποικίλουν από: α) απομάκρυνση του πληθυσμού από την εύφλεκτη περιοχή, β) ανάπτυξη αστυνομικών μέτρων (παρακολούθηση, συλλήψεις / ανακρίσεις υπόπτων στοιχείων), γ) ανάπτυξη αντικατασκοπευτικών πρακτικών παρακολούθησης και προστασίας, δ) ανάπτυξη επιθετικών αντικατασκοπευτικών μεθόδων (παρακολούθηση, διείσδυση, χρήση διπλών πρακτόρων, παραπλάνηση) -για περισσότερες λεπτομέρειες βλέπε Schiattareggia H. M., "Counterintelligence in Counter guerrilla Operations", ό. π., σ. 43-52, επίσης βλέπε Arango R. Carlos, "Counterintelligence vs. Insurgency", *Studies in Intelligence*, Volume 12, Number 2, 1968, σ. 65-81, Steinmeyer Walter, "The Intelligence Role in Counterinsurgency", *Studies in Intelligence*, Volume 9, Number 4, 1965, σ. 57-63, Harber Justin, "Unconventional Spies: The Counterintelligence Threat from Non-State Actors" στο *International Journal of Intelligence and Counter Intelligence*, Volume 22, Issue 2, 2009, σ. 226-227, Mazumadar Keshav, *Actionable Intelligence*, RIEAS, RIEAS e-Book No 5, Αθήνα, Σεπτέμβριος 2013, σ. 63-66

⁴⁸ Arango R. Carlos, "Insurgent Counterintelligence", *Studies in Intelligence*, Volume 12, Number 1, 1968, σ. 39-40, επικουρικά βλέπε Gentry J., Spencer D., "Colombia's FARC: A Portrait of Insurgent Intelligence" στο *Intelligence and National Security*, Volume 25, Number 4, 2010, σ. 468-471, Wege A. Carl, "Hizballah's Counterintelligence Apparatus" στο *International Journal of Intelligence and Counter Intelligence*, Volume 25, Issue 4, 2012, σ. 771-785

αποσιώπηση στοιχείων κατόπιν συλλήψεων φίλιων προσώπων, ι) διαφυλαχτεί η απαράβατη και αυστηρή λειτουργία των όποιων μέτρων / συστημάτων ελέγχου και προστασίας.⁴⁹

Ωστόσο, των τριών προηγείται ο πατέρας του εξωαστικού ανταρτικού κινήματος, Κουβανός Alberto Bayo y Giroud. Στο έργο του *150 Questions for a Guerrilla* (Αβάνα, 1959) γίνεται, μεταξύ άλλων, λόγος για αντικατασκοπευτικές πρακτικές που έλαβαν χώρα κατά τη διάρκεια του *Δεύτερου Μαροκινού Πολέμου* ή *Πολέμου του Rif* ανάμεσα στους γηγενείς Βερβέρους και στις ισπανικές και γαλλικές δυνάμεις στη δεκαετία του 1920 -στο συγκεκριμένο πόλεμο κατεγράφησαν πλήθος παραπλανητικών / αντιπληροφοριακών εγχειρημάτων. Τα κάτωθι σημεία συμπεριλαμβάνονται στη σχετική, κατά Bayo, «ανταρτική αντικατασκοπευτική θεματολογία»:

- Το πληροφοριακό κλιμάκιο μιας ανταρτικής ομάδας καθοδηγούμενο από τον *second-in-command chief* οφείλει να χειρίζεται πληροφοριακές / αντιπληροφοριακές υποθέσεις. Είναι συνετό να αποτελείται από μικρούς πυρήνες ώστε να μειώνεται η πιθανότητα υπονόμησης. Συλλέγει πληροφορήση, καταγράφει τη συμπεριφορά των μελών, καταγράφει συμπαθούντες και μη, διατηρεί κέντρο κωδικοποίησης / αποκωδικοποίησης μηνυμάτων, διεξάγει έρευνες πέριξ υπόπτων για μεταφορά πληροφοριών εκτός ομάδας κ. λ.
- Πληροφόρηση / αντιπληροφόρηση διεξάγεται ουσιαστικά από κάθε μέλος. Ωστόσο η δεύτερη εν καιρώ μάλιστα πολέμου, για την εκτέλεση της οποίας τα γυναικεία μέλη θεωρούνται απαραίτητα, απολαμβάνει ιδιαίτερης εκτίμησης.⁵⁰
- Τα οφέλη που προέρχονται από κάποιον πληροφοριοδότη που δρα εντός των γραμμών του εχθρού είναι ανεκτίμητα καθώς προάγεται τόσο η οικεία πληροφόρηση όσο, επίσης, αυξάνονται οι πιθανότητες παραπληροφόρησης του τελευταίου.
- Η αξία της πληροφόρησης / αντιπληροφόρησης για ένα επαναστατικό γκρουπ συμπυκνώνεται στο «περισσότεροι πόλεμοι κερδήθηκαν μέσω τεχνασμάτων παρά μέσω μαχών».

⁴⁹ Turbiville Graham, Jr., *Guerrilla Counterinsurgency. Insurgent Approaches to Neutralizing Adversary Intelligence Operations*, Joint Special Operations University Press, Florida, 2009, σ. 20-21, επίσης βλέπε Marighella Carlos, *Minimanual of the Urban Guerrilla*, 1969, διαθέσιμο στην ιστοσελίδα [http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Insurgent%20Principles%20and%20Practices/MiniManual%20of%20the%20Urban%20Guerrilla%20%20Carlos%20Marighella%20\(1969\).pdf](http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Insurgent%20Principles%20and%20Practices/MiniManual%20of%20the%20Urban%20Guerrilla%20%20Carlos%20Marighella%20(1969).pdf) εις την οποία ανατρέξαμε την 30^η Αυγούστου 2016 αλλά και στην ελληνική έκδοση του Μαρικέλα Κάρλος, *Το Εγχειρίδιο του Αντάρτη των Πόλεων*, μτφρ. Σύρρου Κατερίνα, Ελεύθερος Τύπος, Αθήνα, σ. 47-50 όπως και στο Bonanate Luigi, *Διεθνής Τρομοκρατία*, μτφρ. Σιδέρη Ντίνα, Κέδρος, Αθήνα, 2009, σ. 134 (τίτλος πρωτοτύπου *Terrorismo Internazionale*, 1994, 2001)

⁵⁰ Το γιατί καθίσταται κατανοητό. Η αποτελεσματικότητα της αντικατασκοπίας παίζει, όπως καταγράφει ο John Gentry, αποφασιστικό ρόλο στην επιβίωση των *επιθετικών μη κρατικών δρώντων* (*violent non-state actors / VNA*). Είναι χαρακτηριστικό πως το CI τμήμα ενός VNA δύναται σε πολλές περιπτώσεις να μπλοκάρει την εκτέλεση ενός ριψοκίνδυνου σχεδιασμού, άρα, να παρέμβει σε επίπεδο decisionmaking πολύ εμφαντικότερα από ό,τι ένα ανάλογο πληροφοριακό τμήμα ευρισκόμενο στην υπηρεσία ενός κρατικού δρώντα -για μια εικόνα βλέπε Gentry John, "Toward a Theory of Non-State Actors' Intelligence" στο *Intelligence and National Security*, Volume 31, Number 4, 2016, σ. 473, 485-486, επίσης, Bowyer Bell, J., "The armed struggle and underground intelligence: An overview" στο *Studies in Conflict and Terrorism*, Volume 17, Issue 2, 1994, σ. 129-130, Charters A. D., "Eyes of the Underground: Jewish Insurgent Intelligence in Palestine, 1945-47" στο *Intelligence and National Security*, Volume 13, Number 4, 1998, σ. 170-172, Murphy Jr., J. F., "Michael Collins and the Craft of Intelligence" στο *International Journal of Intelligence and CounterIntelligence*, Volume 17, Issue 2, 2004, σ. 333-355

- Η διαδικασία στρατολόγησης νέων μελών οφείλει να λαμβάνει υπόψη με ιδιαίτερη προσοχή το «βιογραφικό» των υποψηφίων καθώς ενδέχεται να μετατραπεί (η στρατολόγηση) σε εσωτερική τρωτότητα.
- Η τιμωρία ενός εσωτερικού καταδότη δεν μπορεί να είναι άλλη από θάνατος.
- Η ομάδα οφείλει να βρίσκεται σε μόνιμη επαγρύπνηση. Η μεταμφίεση του εχθρού πιθανολογείται σφόδρα.
- Μίας επίθεσης σε αστικό κέντρο προηγείται η καταλογογράφηση ατόμων που ενδέχεται να παίζουν ρόλο χαφιέ ή διώκτη.
- Το μέγιστο μέγεθος μιας υποομάδας ανταρτών δεν πρέπει να υπερβαίνει τα τρία άτομα διά λόγους ασφαλείας.
- Οι εκτελέσεις των προδοτών πρέπει να τελούνται άμεσα, σε δημόσιο χώρο και με το λόγο της καταδίκης πλήρως διασαφηνισμένο.
- Εφόδια και εξοπλισμός πρέπει να βρίσκονται υπό συνεχή επίβλεψη. Πρέπει να διατηρούνται μακριά από ξένα βλέμματα. Η ομοιομορφία στις τακτικές απόκρυψης πρέπει να αποφεύγεται.
- Αν η αμείλικτη τιμωρία ταιριάζει στους καταδότες, η επιείκεια έναντι δεδομένων εκ προοιμίου αντιπάλων και εχθρών δεν αποκλείεται για διαφόρους λόγους.⁵¹

Αναφορικά με την Al-Qaeda⁵² ο Gaetano Joe Ilardi σημειώνει ότι ...στην καρδιά του αντικατασκοπευτικού σχεδιασμού της Qaeda επικάθεται η απλούστερη, πάρα ταύτα, βασική αρχή: κάθε δράση οφείλει να τελεί υπό συνθήκες πλήρους ασφαλείας.⁵³ Με άλλα λόγια, η άμυνα προηγείται της επίθεσης με σκοπό την ασφαλή εκτέλεση του όποιου πλάνου.⁵⁴ Μυστικότητα και αιφνιδιασμός συνθέτουν κύρια ατού επίλυσης του προβλήματος της ασυμμετρίας ισχύος.⁵⁵

Ο Desmond Ball γράφει πώς: α) η παγκόσμια κινητοποίηση κατά του φαινομένου, β) η ασυμμετρία πόρων και γ) η διεθνής συνεργασία καθιστούν το επιχειρησιακό περιβάλλον εντός του οποίου δρα η Qaeda καταφανώς επικίνδυνο γι' αυτήν.⁵⁶ Τα πράγματα επιβαρύνονται περαιτέρω λόγω της φιλόδοξης και σύνθετης φύσης των επιχειρημάτων της. Τα τελευταία συνηθέστατα λαμβάνουν χώρα κάτω από εξαιρετικά αντίξοες συνθήκες, σε απομακρυσμένες από τις βάσεις της περιοχές, εντός εχθρικών

⁵¹ Turbiville Graham, Jr., *Guerrilla Counterintelligence. Insurgent Approaches to Neutralizing Adversary Intelligence Operations*, ό. π., σ. 12-15, επίσης βλέπε Giroud Alberto, *One Hundred Fifty Questions for a Guerrilla*, διαθέσιμο στην ιστοσελίδα <http://www.latinamericanstudies.org/bayo.htm> όπου ανατρέξαμε την 31^η Αυγούστου 2016 και Stime Britta, "Counterinsurgency Agent Networks and Noncombatant-Targeted Violence" στο *Intelligence and National Security*, Volume 32, Number 1, 2017, σ. 116-119

⁵² Για μια πολύ καλή μελέτη σχετικά με τα πληροφοριακά δίκτυα της Qaeda βλέπε Gunaratna Rohan, *Inside Al Qaeda: Global Network of Terror*, Berkeley Books, New York, 2003

⁵³ Π. χ. βλέπε ...μη μιλάς ποτέ και σε κανέναν, ούτε καν σε άλλο μέλος [volunteer] περί στρατιωτικών επιχειρήσεων. Ίσως πρόκειται για πράκτορα ή για κάποιον που δεν κρατά το στόμα του κλειστό, που θα μπορούσε αθέλητα να περάσει πληροφορίες στον εχθρό, που θα μπορούσε να συλληφθεί και να «σπάσει» στην ανάκριση... στο Ilardi Gaetano, "Irish Republican Army Counterintelligence", *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 1, 2010, σ. 9

⁵⁴ Π. χ. βλέπε ...πριν ξεκινήσουμε μια επιθετική πολιτική ή στρατιωτική επιχείρηση λαμβάνουμε τα αυστηρότερα μέτρα ασφαλείας ... δεν εκκινούμε πριν σιγουρέψουμε τις αμυντικές προετοιμασίες, την πληροφόρηση, την προστασία, τη λειτουργικότητα του οπλισμού, την επάρκεια πολεμοφοδίων κ. λ. και, ασφαλώς, ότι η επιχείρηση θα αυξήσει τους υποστηρικτές μας χωρίς τον κίνδυνο της απομόνωσης από τον πληθυσμό... στο Ilardi Gaetano, "Irish Republican Army Counterintelligence", ό. π., σ. 10

⁵⁵ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control" στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 2, 2009, σ. 247

⁵⁶ Ball Desmond, "Desperately Seeking Bin Laden: The Intelligence Dimension of the War Against Terrorism" στο *Worlds in Collision: Terror and the Future of Global Order*, επιμ. Booth Ken, Dunne Tim, Palgrave, New York, 2002, σ. 60-73

πληθυσμιακών συγκεντρώσεων, συνεπώς, τα όποια λάθη στα πρωτόκολλα ασφαλείας / αντικατασκοπίας πιθανότατα οδηγήσουν σε αποτυχία.⁵⁷ Ο Bin Laden αναγνωρίζοντας τις ιδιαιτερότητες τονίζει σε φετβά του το 1996 ότι ...εξ αιτίας της ανισορροπίας ισχύος μεταξύ των ενόπλων τμημάτων μας και των αντιστοίχων εχθρικών ωφελεί να υιοθετηθεί ένας κατάλληλος τρόπος μάχης, π. χ., η αξιοποίηση ελαφρών δυνάμεων που επιχειρούν κάτω από απόλυτη μυστικότητα.⁵⁸

Η εκτεταμένη χρήση του αντιπληροφοριακού tradecraft εκ μέρους της Al-Qaeda σκοπό έχει τη δημιουργία μιας αδιαπέραστης ομπρέλας που θα καλύψει κάθε είδους, μικρή ή μεγάλη, επιχείρηση. Στο *Declaration of Jihad Against the Country's Tyrants* της οργάνωσης εξηγείται πως κάθε εγχείρημα απαιτεί ...ένα συστηματικό, προσεκτικό και συμπαγές πλάνο ασφαλείας που θα αποκρύψει τις προθέσεις μέχρι το χρόνο υλοποίησής τους.⁵⁹ Καθοδηγητές όπως ο Sayf Al-Adl επαναλαμβάνουν την οδηγία δίδοντας έμφαση στην υιοθέτηση διεξοδικών μέτρων ασφαλείας που πρέπει να βρίσκονται εν ισχύ μέχρι και την έναρξη των όποιων κινήσεων.⁶⁰ Ένα πλάνο ασφαλείας, κατά το *Declaration of Jihad Against the Country's Tyrants*, ορίζεται ως ...οργανωμένο, συνεκτικό και ενοποιημένο σύνολο μέτρων συνδεδεμένων με συγκεκριμένες δραστηριότητες. Απότοκο αυτών των μέτρων [και της μυστικότητας] δεικνύει η σύγχυση [του εχθρού] και ο αιφνιδιασμός. Αν οι αναφερόμενες δραστηριότητες αποκαλυφθούν, η λήψη των άνω μέτρων θα οδηγήσει, τουλάχιστον, στον περιορισμό των απωλειών. Όσο πιο αυστηρό είναι το πλάνο ασφαλείας τόσο πιο επιτυχής θα καταστεί η επιχείρηση περί της οποίας εκπονείται. Όσο πιο χαλαρός αποδεικνύεται ένας σχεδιασμός προστασίας τόσο μειώνονται οι πιθανότητες επιτυχίας του εγχειρήματος τη στιγμή που οι απώλειες αυξάνονται. Κατά συνέπεια, κλείνει το συγκεκριμένο τμήμα του *Declaration*, κάθε δραστηριότητα που βρίσκεται στο στόχαστρο του εχθρού πρέπει να καλύπτεται από ένα σχέδιο ασφαλείας.⁶¹ Τα πρακτικά και ψυχολογικά οφέλη ενός τέτοιου πλάνου περιγράφονται από τον Al-Adl, ειδικότερα: α) αυξάνονται οι πιθανότητες επιτυχίας ενός επιδιωκόμενου αιφνιδιασμού κατά του αντιπάλου, β) η a priori ύπαρξη ενός τέτοιου πλάνου αποτελεί έτσι και αλλιώς μία από τις αρχές του πολέμου, γ) η επιτυχής ενεργοποίηση ενός σχετικού σχεδιασμού δύναται να ενημερώσει τη Jemaah [ομάδα] περί του τι σχεδιάζει ο αντίπαλος, άρα, να βοηθήσει στην αμυντική προετοιμασία έναντι του τελευταίου, δ) προστατεύεται η Jemaah από ενδεχόμενες εχθρικές προσπάθειες παρείσδυσης εντός των γραμμών της, ε) ελαχιστοποιούνται τόσο οι απώλειες όσο και ο κίνδυνος απομείωσης της επιχειρησιακής ετοιμότητας της Jemaah, στ) αποφεύγεται η πτώση ηθικού έπειτα από επανειλημμένες επιχειρησιακές αποτυχίες, αποτυχίες που οφείλονται σε έλλειψη πλάνων ασφαλείας.⁶²

⁵⁷ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 247-248

⁵⁸ Osama bin Laden, *A Declaration of War Against the Americans Occupying the Land of the Two Holy Places: A Message from Osama bin Muhammad bin Laden unto his Muslim brethren all over the world generally, and toward the Muslims of the Arabian Peninsula specifically*, διαθέσιμο στο <http://www.outpost-of-freedom.com/opf980830a.htm> εις το οποίο ανατρέξαμε τη 17^η Αυγούστου 2016

⁵⁹ Al-Qaeda, *Declaration of Jihad against the Country's Tyrants, Military Series*, (Ninth Lesson, "Security Plan"), διαθέσιμο και στην διαδικτυακή τοποθεσία http://www.au.af.mil/au/awc/awcgate/terrorism/alqaida_manual/manualpart1_3.pdf εις την οποία ανατρέξαμε 17^η Αυγούστου 2016

⁶⁰ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 247

⁶¹ Al-Qaeda, *Declaration of Jihad against the Country's Tyrants, Military Series*, ό. π.

⁶² Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 249

Το ζήτημα της επιχειρησιακής ασφαλείας παραμένει ένα εκ των πλέον συζητήσιμων εντός της βιβλιογραφίας της Qaeda: περιοδικές εκδόσεις, εγκυκλοπαίδειες και εγχειρίδια ασχολούνται μ' αυτό. Π. χ. το *Al Battar Training Camp* μέχρι τα τέλη της δεκαετίας του 2010 καταπιάνεται με την προστασία των πληροφοριών, την επιχειρησιακή ανωνυμία, με τεχνικές απόκρυψης, με κώδικες και κρυπτογραφήματα. Ασφαλώς η Qaeda ενθαρρύνει τη χρήση πλέον εκλεπτυσμένων μορφών αντικατασκοπίας όπως αυτών της παραπληροφόρησης, των διπλών πρακτόρων, της αντιπαρακολούθησης (countersurveillance): είναι φανερό πως η οργάνωση priμοδοτεί τόσο την αμυντική όσο και την επιθετική αντιπληροφόρηση.⁶³

Η ουσία του αντιπληροφοριακού δόγματος της Qaeda αντανακλά τη φιλοσοφία της: αλόγιστο ρίσκο και τυχειότητα δεν έχουν θέση στη διεξαγωγή της όποιας επιχείρησης. Η ακριβής κατανόηση του περιβάλλοντος μάχης όπως και της φύσεως των απειλών ελαχιστοποιεί τις πιθανότητες μιας κακώς προετοιμασμένης δράσης.⁶⁴

Η προσοχή στη λεπτομέρεια αποτελεί ακρογωνιαίο λίθο. Η βήμα προς βήμα εκτέλεση των σχεδιασμών ασφαλείας παραπέμπει σε μια σχεδόν μηχανιστική προσέγγιση / λατρεία. Οι επιχειρησιακοί της Qaeda επιτηρώντας το παραμικρό που ενδέχεται να προκαλέσει, εφοδιάζονται με οδηγίες για το είδος της αμφίεσης που πρέπει να τους περιβάλει, καλούνται να εξαφανίσουν ύποπτες γενειάδες, επίσης, να ακούνε μουσική κατά τη διάρκεια ενός ταξιδιού, να συμπεριφέρονται με τρόπο απολύτως δυτικό.⁶⁵ Παρόμοιες προτροπές εμφανίζονται στο *The Declaration, Al-Battar Training Camp* και αλλού αποδεικνύοντας την πίστη της οργάνωσης περί ενός σφικτού και σχολαστικού «αντικατασκοπευτικού καθεστώτος -counterintelligence regime» του οποίου το δημιούργημα, ο προστατευτικός μανδύας, δύσκολα διαρρηγνύεται.⁶⁶

Άλλο σημαντικό ατού δεικνύει η γνώση περίξ του αντιπάλου. Η Qaeda γνωρίζει ότι το δόγμα ασφαλείας που υιοθετεί βρίσκεται σε αναπόδραστη σύνδεση με τις εναντίον της δράσεις.⁶⁷ Στη σελίδα 1 του *Encyclopedia of the Afghan Jihad* διαβάζουμε: «...η μάχη μεταξύ ημών και εχθρών είναι πρώτα απ' όλα μάχη πίστεως και πεποιθήσεων και κατόπιν μάχη ασφαλείας και πληροφοριών», συνεπώς, η γνώση των «πιστεύω» του αντιπάλου αποτελεί όπλο.⁶⁸ Κατά τα ανωτέρω, πλήθος αντικατασκοπευτικών πρακτικών της Qaeda βασίζονται στη μελέτη των αντιπάλων δυνάμεων και στην ικανότητα διασποράς των συμπερασμάτων αυτής ακριβώς της μελέτης σε συμπαθόντες ομάδες. Σ' αυτή τη βάση φορμάρονται τα όποια αντιπληροφοριακά εξτρεμιστικά παραδείγματα. Ο Paul Wolfowitz, πρώην αναπληρωτής υπουργός του DoD, δηλώνει ότι:

...δεν πρέπει να υποτιμήσουμε την ικανότητα όπως και την αποφασιστικότητα του αντιπάλου να αποκρύψει τις δραστηριότητές του, να μας παραπλανήσει. Γνωρίζουν πώς συλλέγουμε πληροφορίες, τον τρόπο οργάνωσής μας, τον τρόπο με τον οποίο αναλύουμε στοιχεία. Ακριβώς

⁶³ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 250

⁶⁴ ό. π., σ. 251

⁶⁵ Glasser Susan, "A Terrorist's Guide to Infiltrate West" στο *The Washington Post*, 9 Δεκεμβρίου 2001, διαθέσιμο και στην ιστοσελίδα <https://www.washingtonpost.com/archive/politics/2001/12/09/a-terrorists-guide-to-infiltrate-west/2bb6d717-d9a0-4cdf-ba8c-9ab13710eb37/> όπου καταφύγαμε τη 18^η Αυγούστου 2016, επίσης, Cullison Allan, "Inside Al-Qaeda's Hard Drive" στο *The Atlantic Monthly*, Σεπτέμβριος 2004, σ. 61

⁶⁶ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 252

⁶⁷ *ibid*

⁶⁸ *ibid*

όπως αυτοί, οφείλουμε να αναπροσαρμόζουμε διαρκώς τις Υπηρεσίες μας, να καινοτομούμε. Προσπαθούμε επίμονα να εφεύρουμε τρόπους που θα διαχωρίζουν το 'σήμα' του τρομοκράτη από τον 'θόρυβο' της όλης εικόνας, οφείλουμε, δε, να αναγνωρίσουμε ότι κάθε εχθρός προσπαθεί να δημιουργήσει τέτοιο θόρυβο στο σύστημα ώστε να αποκρύψει τα πραγματικά σημάδια.⁶⁹

Το αντιπληροφοριακό παράδειγμα της Qaeda δηλώνει πως η σπουδή του εχθρού, των μεθόδων, τακτικών και «υποθέσεων» του συνθέτει αποφασιστικό βήμα στη δημιουργία μιας τζιχαντιστικής πρακτικής ασφαλείας. Η αντιπληροφόρηση συνδεδεμένη με την πληροφόρηση υπαγορεύει ότι η γνώση προηγείται της δράσης. Στο *Encyclopedia of the Afghan Jihad* τονίζεται ότι ...αυτός που επιτυγχάνει, είναι αυτός που διαθέτει περισσότερα δεδομένα [information], έτσι, τόσο η πληροφόρηση [intelligence] όσο και η ασφάλεια [security] που δομείται είναι η δυνατόν πληρέστερη. Η Qaeda μέσω των αντιπληροφοριακών της δικτύων προσομοιώνει / περιγράφει πιθανές μελλοντικές καταστάσεις υιοθετώντας ανάλογα αντίμετρα.⁷⁰ Χαρακτηριστικό είναι το παράδειγμα που ανασύρουμε από το *Declaration of Jihad against the Country's Tyrants* -πρόκειται για φυλλάδιο με ερωτήσεις που πιθανόν απευθυνθούν σε τζιχαντιστές που ταξιδεύουν εκτός της βάσης τους.

Η Qaeda χαρακτηρίζεται από μια πραγματικά αξιοσημείωτη ικανότητα. Έχει αναπτύξει χαρακτηριστικά ενός οργανισμού «που συνεχώς μαθαίνει, ενός *learning organization*». Ο Peter Senge ορίζει ως τέτοιον έναν οργανισμό που ...εκτείνει αδιάκοπα τη δυνατότητα «δημιουργίας μέλλοντος». Δεν ενδιαφέρεται απλώς να επιβιώσει. Θέλει να φτιάξει [μέσω μάθησης / γνώσης] την τύχη του.⁷¹ Κατά την έννοια τούτη ο αντικατασκοπευτικός της σχεδιασμός δεν είναι στατικός. Εισπράττει από τις εμπειρίες άλλων ανεξαρτήτως πολιτικών ή θρησκευτικών πεποιθήσεων. Οι υποστηρικτές της ενθαρρύνονται να μελετούν τόσο το σωστό όσο και το λάθος ειδικά αν αυτό ή αυτά προέρχονται από «αδελφούς» που βρέθηκαν αντιμέτωποι με αλλοδαπές υπηρεσίες Ασφαλείας. Οι τελευταίοι δύνανται να μεταφέρουν γνώση περί των εχθρικών μεθόδων όπως και να συμβάλουν μέσω της σπουδής των επιχειρησιακών τους λαθών.⁷² Ο Al-Adl σε τεύχος του *Al-Battar Training Camp* γράφει:

⁶⁹ Wolfowitz P., "Prepared Testimony of Deputy Secretary of Defense Paul Wolfowitz for the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence: Joint Inquiry Hearing on Counterterrorist Center Customer Perspective", 19 Σεπτεμβρίου 2002, διαθέσιμο και στο https://fas.org/irp/congress/2002_hr/091902wolfowitz.pdf όπου ανατρέξαμε τη 18η Ιουλίου 2016

⁷⁰ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 253

⁷¹ Senge Peter, *The Fifth Discipline: The Art and Practice of the Learning Organization*, Random House, Sydney, 1992, σ. 14. Ο Sergio E. Sanchez γράφει πως οι πληροφοριακές / αντιπληροφοριακές δεξιότητες της Qaeda όπως και άλλων μη κρατικών δρώντων θεωρούνται πολλάκις μη άξιες αναφοράς. Κάτι τέτοιο, συνεχίζει, είναι λάθος. Η συγκεκριμένη οργάνωση διακρίνεται από μια εξαιρετική ικανότητα απορρόφησης / ενσωμάτωσης πληροφοριακών τακτικών, τεχνικών και διαδικασιών που εργαλειοποιούνται από μεγάλες κρατικές δυνάμεις και που μεταφέρονται από αυτές σ' αυτήν μέσω ενός ευρέος δικτύου (spider web) σχέσεων και επαφών (relationships and links). Όποιοι δεν αντιλαμβάνονται την πραγματικότητα είναι είτε αφελείς, είτε προκατειλημμένοι. Οι αξιωματούχοι της κατασκοπίας / αντικατασκοπίας οφείλουν να κατανοήσουν πως οι πληροφοριακές δυνατότητες της Qaeda είναι αξιοθαύμαστες, καταλήγει -για περισσότερα βλέπε Sanchez E. S., "Spider Web: Al-Qaeda's Link to the Intelligence Agencies of the Major Powers" στο *International Journal of Intelligence and CounterIntelligence*, Volume 28, Issue 3, 2015, σ. 442

⁷² Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 255

Ένας μουσουλμάνος οφείλει πάντα να βρίσκεται σε επαγρύπνηση, πάντα να στερεί το στοιχείο του αιφνιδιασμού από τον εχθρό. Πρέπει να αποκτά τη χρήσιμη πληροφορία. Πρέπει να μελετά, να φροντίζει για την εκπαίδευσή του στο πεδίο [της ασφαλείας]. Επιβεβαιώνουμε την ανάγκη ανταλλαγής πληροφορήσης μεταξύ των αδελφών μας ... Πώς συλληφθήκανε; Ποια τα λάθη τους; Πώς αποκαλύφθηκαν τα μέρη που κρύβονταν; Ποιες πληροφορίες διαθέτουν για τον εχθρό; Ποιες οι εμπειρίες αδελφών που αποφυλακίστηκαν; Για όλα αυτά μάθε από την πράξη, επεξέτεινε τους ορίζοντές σου, μείνε σε εγρήγορση.⁷³

Αμυντική αντικατασκοπία

Η μυστικότητα με την οποία οφείλει να δράσει η Al-Qaeda δεν αφορά μόνο σε τρομοκρατικές δράσεις. Πλήθος ενεργειών όπως εύρεση κεφαλαίων, στρατολόγηση μελών, εκπαίδευση προσωπικού κ. λ. πρέπει να εκτελεστούν μακριά από τα φώτα. Γι' αυτόν ακριβώς το λόγο η αντικατασκοπευτική στρατηγική της οργάνωσης ευελπιστεί στο κτίσιμο μιας περιμέτρου που θα αποκρύπτει, θα παραλλάσει / καμουφλάρει κάθε δραστηριότητα. Ο Ilardi σημειώνει ότι η αναφορά όλων των σχετικών τακτικών θα απαιτούσε πλήθος σελίδων, ωστόσο, η καταγραφή των πιο σημαντικών λύνει απορίες περίξ του τρόπου σκέψης της Qaeda.⁷⁴ Ειδικότερα:

- Στρατολόγηση και εκπαίδευση: από τη στιγμή της στρατολόγησης, περιλαμβανομένης της διαδικασίας διά της οποίας αυτή επιτεύχθη, μέχρι την εμπλοκή σε επιχειρησιακό στάδιο προτεραιότητα αποτελεί η απόκρυψη των ταυτοτήτων των νέων μελών. Ο νεοεισερχόμενος στην οργάνωση αποκτά ψευδώνυμο τη στιγμή που κάθε προσωπικό έγγραφο απομακρύνεται.⁷⁵ Συνήθως προκρίνεται η δημιουργία πυρήνων με πρόσωπα που διακρίνονται για την κοινή καταγωγή με σκοπό τη σφυρηλάτηση υψηλού αισθήματος ομαδικότητας.⁷⁶ Για νεοεισελθόντες «ιδιαίτερης αξίας» λαμβάνεται ως πρόσθετο μέτρο η απομάκρυνσή τους από τους υπολοίπους όπως και η απόκρυψη του τόπου καταγωγής τους. Η ενεχυρίαση παραποιημένων διαβατηρίων, αδειών οδήγησης κ. λ. με το υποτιθέμενο όνομα των κατόχων προσδίδει μια αίσθηση νομιμότητας και αληθοφάνειας.⁷⁷ Το «γνωρίζω ό,τι χρειάζεται και μόνο αυτό» αποτελεί απαράβατο όρο. Ο Ahmed Ressam θυμάται την εξής αρχή ...*όταν ένα άτομο λειτουργεί εντός ομάδας γνωρίζει ό,τι πρέπει να γνωρίζει, όχι περισσότερα, προκειμένου να προστατευθούν τα μυστικά...*⁷⁸ Η Qaeda ακολουθώντας πρακτικές κρατικών μυστικών υπηρεσιών αποδίδει την αμυντική αντικατασκοπευτική λειτουργία στον ευρύτερο πληροφοριακό μηχανισμό· ουσιαστικά την ταυτίζει με την ασφάλεια προκειμένου να αναληφθεί με αξιοπιστία η επίβλεψη νεοσύλλεκτων ή και «ιδιόμορφων» μελών μέσω πραγμάτωσης συνεντεύξεων, επίδοσης ερωτηματολογίων κ. λ.⁷⁹
- Επικοινωνίες: στο *Declaration of Jihad against the Country's Tyrants, Military Series* αναφέρεται ότι ...*στις κρυφές επιχειρήσεις οι επικοινωνίες αποτελούν το*

⁷³ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 255

⁷⁴ ό. π., σ. 259-260

⁷⁵ ό. π., σ. 260

⁷⁶ ό. π.

⁷⁷ ό. π.

⁷⁸ ό. π., σ. 260-261, επίσης, United States District Court, *United States of America v. Mokhtar Haouari*, Southern District of New York, 3 Ιουλίου 2001, σ. 642

⁷⁹ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 261, επίσης, United States District Court, *United States of America v. Osama bin Laden, et al.*, 6 Φεβρουαρίου 2001, σ. 236-237

άλφα και το ωμέγα της επιτυχίας. Αποτελούν επίσης δίκωπο μαχαίρι: αν αξιοποιηθούν σωστά αποδίδουν πλεονέκτημα, αν εκτελεστούν δίχως λήψη μέτρων ασφαλείας μετατρέπονται σε σιλέτο που μπήγεται στην πλάτη του κατόχου του.⁸⁰ Ο Ramzi Binalshidh, εκ των εγκεφάλων του κτυπήματος της 11^{ης} Σεπτεμβρίου, παρατηρεί: «κάθε επιχειρησιακή φάση χαρακτηρίζεται από τη δική της ‘γλώσσα επικοινωνίας’ που διαφέρει από την επόμενη. Πριν την εκτέλεση ενός σχεδίου λαμβάνει χώρα μια συνάντηση κατά την οποία συμφωνείται αυτή η ‘γλώσσα’».⁸¹

- Κάλυψη: υψηλή θέση στο αντικατασκοπευτικό πρωτόκολλο της Qaeda απολαμβάνει το θέμα της κάλυψης υπό την έννοια / προοπτική της μη κίνησης υποψιών. Η *Encyclopedia of the Afghan Jihad* προτείνει όπως η εξωτερική εμφάνιση / περιβολή ατόμου ή ομάδας ατόμων επιβοηθά στην απόκρυψη της φύσης της μυστικής αποστολής, στην απόκρυψη των δραστηριοτήτων [του ατόμου ή της ομάδας] από τις εχθρικές υπηρεσίες Ασφαλείας.⁸² Ο Al-Adl περιγράφει την κάλυψη ως ...πέπλο πίσω από το οποίο κρύπτονται μυστικές πράξεις ατόμων, οργανώσεων, ομάδων κ. λ. Αυτό ακριβώς το πέπλο δικαιολογεί την παρουσία [του ατόμου, της ομάδας] στο σωστό μέρος, την κατάλληλη ώρα, προκειμένου να εκτελεστεί το εγχείρημα.⁸³

Επιθετική αντικατασκοπία

Η Al-Qaeda, κατά τον Ilardi, στον τομέα της επιθετικής αντικατασκοπίας έχει επιδείξει ποιότητα προσομοιάζουσα αυτής των κορυφαίων παγκοσμίως μυστικών υπηρεσιών. Η ικανότητα διείσδυσης εντός οργανισμών Ασφαλείας και Πληροφοριών αποτελεί δείκτη της επιθυμίας της για συλλογή δεδομένων, επιπλέον, έναν θρίαμβο γι' αυτήν, μια παταγώδη αποτυχία για τον αντίπαλο. Η παρουσία διπλών πρακτόρων στις γραμμές του εχθρού δεικνύει τη θέλησή της να περιορίσει το επιχειρησιακό ρίσκο γνωρίζοντας τις δυνατότητες και επηρεάζοντας τις προθέσεις του αντιπάλων Υπηρεσιών.⁸⁴ Οι εξτρεμιστές της οργάνωσης αντιλαμβάνονται το χρόνο που απαιτεί η εκπλήρωση του τελικού τους οράματος εκτιμούν ιδιαίτερος την τακτική της επιθετικής αντικατασκοπίας. Ο Abu Bakr Naji, ηγετική τζιχαντιστική φυσιογνωμία στη μετά 2001 εποχή,⁸⁵ παρατηρεί σε κείμενό του πως η εισχώρηση εντός πληροφοριακών οργανισμών πρέπει να συνεχιστεί με σκοπό τη βελτίωση των πρωτοκόλλων ασφαλείας του κινήματος.⁸⁶ Σύμφωνα με τον Naji:

⁸⁰ Al-Qaeda, *Declaration of Jihad against the Country's Tyrants, Military Series*, (Fifth Lesson, "Means of Communication and Transportation"), διαθέσιμο στη διαδικτυακή τοποθεσία http://www.au.af.mil/au/awc/awcgate/terrorism/alqaida_manual/manualpart1_2.pdf εις την οποία ανατρέξαμε την 22^η Ιουλίου 2016

⁸¹ Mowbray Joel, "How They Did It: An 'Evil One' Confesses, and Boasts" στο *National Review*, Volume 54, Number 24, 2002, σ. 37, επίσης κατέφυγε στην διαδικτυακή τοποθεσία <http://www.freerepublic.com/focus/news/807903/posts?page=3> όπου ανατρέξαμε την 22^η Ιουλίου 2016

⁸² Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 262

⁸³ ό. π., σ. 273, υποσημείωση 73

⁸⁴ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 264

⁸⁵ Ulph Stephen, "New Online Book Lays out al-Qaeda's Military Strategy" στο *Terrorism Focus*, Volume 2, Issue 6, 2005, επίσης στη διαδικτυακή τοποθεσία του *The Jamestown Foundation* http://www.jamestown.org/programs/tm/single/?tx_ttnews%5Btt_news%5D=27713&tx_ttnews%5Bba#V7suZKIRPZ4 εις την οποία ανατρέξαμε την 21^η Αυγούστου 2016

⁸⁶ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 264

*Η μάχη μας είναι μακρά και βρίσκεται ακόμα στην αρχή. Η διάρκειά της μας δίδει χρόνο και ευκαιρία για διείσδυση εντός των τάξεων του εχθρού και των συμμάχων του με σκοπό την εγκαθίδρυση ενός μηχανισμού ασφαλείας για την προάσπιση του κινήματος και, αργότερα, του κράτους. Πρέπει να διεισδύσουμε στις γραμμές / τάξεις αστυνομικών και ενόπλων δυνάμεων, πολιτικών κομμάτων, εντύπων ενημέρωσης, ισλαμικών ομάδων, πετρελαϊκών εταιριών, εταιριών ιδιωτικής ασφαλείας, ευαίσθητων δημοσίων οργανισμών / ινστιτούτων κ. λ. Αν και η προσπάθεια έχει ξεκινήσει πριν δεκαετίες οφείλει να ενισχυθεί υπό την πίεση των νέων συνθηκών.*⁸⁷

Κατά τον ίδιο, η σπουδαιότητα παρείσφρησης εντός αλλοδαπών Υπηρεσιών προσδίδει στο πρόσωπο που τη διεκπεραιώνει κύρος ίσο με αυτό που απολαμβάνει ένας μάρτυρας της οργάνωσης. Παραδέχεται ότι αυτή η τόσο μοναδική αποστολή απαιτεί ειδική εκπαίδευση και αφοσίωση. Για παράδειγμα, εξ αιτίας της απαιτούμενης περιόδου που το μέλος χρειάζεται προκειμένου να εκπαιδευτεί στο ρόλο που καλείται να παίξει, ακριβώς αυτό το μέλος, και επίδοξος διπλός πράκτορας-τζίχαντιστής, οφείλει να παρακολουθεί επιμορφωτικά προγράμματα με σκοπό τη διατήρηση μιας πίστης που δεν πρέπει να αλλοιωθεί ή αποκαλυφθεί εξ αιτίας των συνθηκών εντός των οποίων καλείται να κινηθεί.⁸⁸ Τέτοιου είδους επιθετικές (αντι)πληροφοριακές ενέργειες έχουν καταγραφεί από τα τέλη της δεκαετίας του 1980 αν όχι παλαιότερα. Πιο συγκεκριμένα:

- Περίπτωση Ali Mohammed: ήδη από τις αρχές της δεκαετίας του 1980, ο Ali Mohammed δραστηριοποιείται εντός της τρομοκρατικής ομάδας Egyptian Islamic Jihad διατηρώντας παράλληλα πόστα στην Qaeda, πόστα όπως αυτό του καθοδηγητή, του προϊσταμένου ασφαλείας, του αξιωματούχου πληροφοριών.⁸⁹ Ο Mohammed, έχοντας υπηρετήσει ως αξιωματικός πληροφοριών στον αιγυπτιακό στρατό, κατατάσσεται στις αμερικανικές ένοπλες δυνάμεις θητεύοντας ως λοχίας εφοδιασμού στα Special Forces στο Fort Bragg πριν απολυθεί το 1989. Μέσω της θέσης του αποκτά διαβαθμισμένα στρατιωτικά έγγραφα που τελικά ανευρίσκονται στην οικία ενός εκ των καταδικασμένων για την βομβιστική ενέργεια στο World Trade Center το 1993.⁹⁰ Λέγεται ότι ο Mohammed αιτήθηκε θέσης μεταφραστή αραβικών στο FBI, θέση που θα του έδιδε πρόσβαση σε κάποια εκ των πλέον ευαίσθητων περίξ αντιτρομοκρατικών επιχειρήσεων εγγράφων.⁹¹

Ο Sulick θεωρεί ότι η περίπτωση Mohammed ίσως δεικνύει το πλέον αντιπροσωπευτικό δείγμα διείσδυσης τρομοκράτη εντός των αμερικανικών Υπηρεσιών. Κατόρθωσε, αφού παντρεύτηκε μια ημεδαπή το 1985, να λάβει την υπηκοότητα και να βρεθεί εν έτει 1986 στον στρατό των Ηνωμένων Πολιτειών. Βοήθησε την ομάδα που επιτέθηκε στο WTC να βρει τις κατάλληλες εκρηκτικές ύλες και να εκπαιδευτεί σ' αυτές. Μετά την αποστρατεία του, με εύφημο μάλιστα μνεία, βρέθηκε στο προσκήνιο των επιχειρήσεων της Qaeda. Επιμελήθηκε των

⁸⁷ Naji Abu, *The Management of Savagery: The Most Critical Stage Through Which the Umma Will Pass*, μετάφραση στην αμερικανική γλώσσα από τον William McCants υπό τη χορηγία του John M. Olin Institute for Strategic Studies / Harvard University, 2006, σ. 52, διαθέσιμο και στην διαδικτυακή τοποθεσία <https://azelin.files.wordpress.com/2010/08/abu-bakr-naji-the-management-of-savagery-the-most-critical-stage-through-which-the-umma-will-pass.pdf> όπου ανατρέξαμε την 21^η Ιουλίου 2016

⁸⁸ ό. π.

⁸⁹ United States District Court, *United States of America v. Ali Mohamed*, Southern District of New York, 20 Οκτωβρίου 2000, σ. 15

⁹⁰ Lance Peter, *1000 Years for Revenge: International Terrorism and the FBI-The Untold Story*, Regan Books, New York, 2003, σ. 31-35

⁹¹ Ilardi Gaetano, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control", ό. π., σ. 265

κινήσεων του Laden σε Σουδάν και Αφγανιστάν όπως και της εκπαίδευσης των σωματοφυλάκων των κυριοτέρων προσώπων της οργάνωσης. Ετοίμασε στρατιωτικά τόσο τα σώματα της Qaeda στο Αφγανιστάν όσο και Σομαλούς αντάρτες πριν την τραγική *Gothic Serpent* επιχείρηση του Οκτωβρίου του 1993 στο Μογκαντίσου. Το 1998 βρίσκει τον Mohammed ακόμα υψηλότερα στην κλίμακα της οργάνωσης διαδραματίζοντας κεντρικό ρόλο στην ενορχήστρωση των κτυπημάτων των πρεσβειών σε Κένυα και Τανζανία.⁹²

Ο Ali Mohammed συνελήφθη το 1998. Καταδικάστηκε σε ισόβια. Η όλη ιστορία καταδεικνύει την απειλή που άτομα συνδεδεμένα με την τρομοκρατία αντιπροσωπεύουν ειδικά όταν καταφέρουν να εισδύσουν εντός κρατικών στρατιωτικών οργανισμών και οργανισμών πληροφόρησης.

- Περίπτωση Mohammed Hamdi al-Ahdal: ο Mohammed Hamdi al-Ahdal ή Abu Assem al-Makky συνελήφθη από τις αρχές ασφαλείας της Υεμένης το 2003 αποτελώντας μέλος της Qaeda και έχοντας κατηγορηθεί ως κεντρικό πρόσωπο στην οργάνωση της επίθεσης κατά του USS Cole το 2000 και του γαλλικού πετρελαιοφόρου Limbourg το 2002. Λίγο πριν τη σύλληψή του επιχειρούσε το σχηματισμό μικρών ανεξάρτητων ομάδων προς διείσδυση στις Υπηρεσίες της Υεμένης με σκοπό τη συλλογή πληροφοριών περί κυβερνητικών προσπαθειών εξουδετέρωσης ανταρτών.⁹³
- Περίπτωση Willie Brigitte: ο γαλλικής υπηκοότητας Willie Brigitte συλλαμβάνεται από τις αυστραλιανές αρχές τον Οκτώβριο του 2003 με την κατηγορία της προτιθέμενης επίθεσης κατά στρατιωτικής βάσης στο Σύνδνεϊ. Πιστεύεται ότι πρόκειται για μέλος της LeT (Lashkar-e-Taiba / Army of the Good) με διασυνδέσεις στην Qaeda. Ο Brigitte είχε παντρευτεί τη Melanie Brown, πρώην μέλος του αυστραλιανού στρατού, προσηλυτισμένη στο Ισλάμ. Δεν είναι ξεκάθαρο αν ο γάμος είχε σχέση με το επαγγελματικό παρελθόν της Brown, ωστόσο ο Brigitte δείχνει ιδιαίτερο ενδιαφέρον για τις παλαιές δραστηριότητες της συζύγου του ζητώντας μάλιστα από την τελευταία να τις καταγράψει εξηγώντας πως «ο Θεός και οι μουσουλμάνοι χρειάζονται αυτές τις πληροφορίες». Η Brown, φοβούμενη, καταστρέφει τρία σχετικά ημερολόγια με τον Brigitte να της απαγορεύει να προβεί στο εξής σε παρόμοιες πράξεις χωρίς να τον ενημερώσει.⁹⁴

Ο Rickard Clarke σημειώνει ότι η παρουσία διπλών πρακτόρων, ή απλώς συμπαθούντων τους εξτρεμιστές, εντός οργανισμών ασφαλείας και πληροφόρησης προσδίδει ένα ακόμα προστατευτικό κάλυμμα στην Qaeda καθιστώντας την ικανή γνώσης επικείμενων αντιτρομοκρατικών επιχειρήσεων. Για παράδειγμα, η χαμένη ευκαιρία σύλληψης του Khalid Sheikh Mohammed το 1997 στο Κατάρ εικάζεται πως οφείλεται σε διαρροή των καταριανών Υπηρεσιών ή σε διαρροή προερχόμενη από

⁹² Sulick Michael, *American Spies: Espionage Against the United States from the Cold War to the Present*, Georgetown University Press, USA, 2013, σ. 285-286

⁹³ “Al-Qaeda Plot to Bomb Embassy in Yemen Foiled” στο *World News*, 13 Δεκεμβρίου 2003, διαθέσιμο στο δικτυακό τόπο <https://www.theguardian.com/world/2003/dec/13/politics.alqaida> εις τον οποίο ανατρέξαμε την 25^η Αυγούστου 2016, περαιτέρω, “Al-Qaeda Plot to Blow Up British Embassy” στο *The Scotsman*, 14 Δεκεμβρίου 2003, διαθέσιμο στο <http://www.scotsman.com/news/world/al-qaeda-plot-to-blow-up-british-embassy-1-1297039> όπου ανατρέξαμε επίσης την άνω ημερομηνία

⁹⁴ Ilardi Gaetano, “Al-Qaeda’s Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control”, ό. π., σ. 265-266, επίσης βλέπε “Testimony: Melanie Brown”, *Four Corners*, 9 Φεβρουαρίου 2004 στο <http://www.abc.net.au/4corners/content/2004/s1132151.htm> όπου καταφέγαμε την 25^η Αυγούστου 2016. Για παρόμοιες δράσεις της Qaeda εντός της ισραηλινής περιφέρειας ανέτρεξε στο Shpiro Shlomo, “Israeli Intelligence and al-Qaeda” στο *International Journal of Intelligence and CounterIntelligence*, Volume 25, Issue 2, 2012, σ. 244-248

τον άμεσο κύκλο του εμίρη της χώρας.⁹⁵ Αν και ουσιαστικά πρόκειται για αμυντική δράση, ωφελεί να μη λησμονάμε την πιθανότητα παραπληροφόρησης ή και άμεσης επιθετικής εκδήλωσης. Μια τέτοια απειράπη στο Μπίρμινχαμ της Βρετανίας το 2007. Αντικειμενικός σκοπός η τρώση του ηθικού των βρετανικών ενόπλων δυνάμεων διά της απαγωγής και εκτέλεσης διά αποκεφαλισμού κάποιου ή κάποιων Βρετανών στρατιωτών μουσουλμανικού θρησκευματος από ομάδα ισλαμιστών που, μάλιστα, σχεδίαζε να αξιοποιήσει τη δικτυακή τεχνολογία προς εντυπωσιασμό και διασπορά πανικού. Ρεπορτάζ της περιόδου αναφέρουν ότι στα χέρια των συλληφθέντων ευρέθη λίστα με ονόματα και διευθύνσεις εικοσιπέντε υπηρετούντων. Αν και η πηγή της διαρροής δεν εντοπίστηκε πιστεύεται ότι ταυτίζεται με άτομο εντός του βρετανικού Ministry of Defence.⁹⁶

Καταληκτικά, κλείνουμε το κεφάλαιο με μια ελάχιστη αναφορά στο διαβόητο Ισλαμικό Κράτος και στον πληροφοριακό του μηχανισμό. Κατά τον Ahmet Yayla και την Anne Speckhard τα καθήκοντα της *Emni*⁹⁷ περιλαμβάνουν μεταξύ άλλων: α) συλλογή πληροφοριών για μάχες στη Συρία, στο Ιράκ και αλλού, β) συλλογή πληροφοριών για κάθε πρόσωπο που ζει εντός Ισλαμικού Κράτους, γ) συλλογή πληροφοριών που αφορούν σε περιοχές οι οποίες ενδιαφέρουν το Ισλαμικό Κράτος, δ) συλλογή πληροφοριών που αφορούν σε νεοσύλλεκτους ειδικά αν αυτοί δεν κομίζουν κάποια ‘συστατική επιστολή’, ε) συλλογή και ανάλυση πληροφοριών περί πιθανών επιθέσεων κατά του Ισλαμικού Κράτους, στ) διασπορά προπαγανδιστικών μηνυμάτων εντός και εκτός επικρατείας Ισλαμικού Κράτους, ζ) στρατολόγηση και ανάπτυξη αλλοδαπών μαχητών προς συλλογή πληροφοριών και εκτέλεση επιθέσεων εντός των χωρών των τελευταίων, η) αποστολή και ανάπτυξη πρακτόρων και υπεύθυνων στρατολόγησης εντός της Τουρκίας αλλά και άλλων χωρών, περιλαμβανομένης της κατασκοπίας Συρίων προσφύγων, θ) παρακολούθηση της εντός της Τουρκίας επιμελητείας του Ισλαμικού Κράτους με σκοπό την αποτροπή τόσο διακοπών της τελευταίας όσο και πληροφοριακών διαρροών, ι) επικοινωνία με πράκτορες από άλλα τρομοκρατικά γκρουπ αλλά και με πράκτορες της κυβέρνησης Άσσαντ, ια) εκτέλεση ‘βρώμικων επιχειρήσεων’ όπως διεξαγωγή δουλεμπορίου, λαθρεμπορίου πετρελαίου, λαθρεμπορίου αρχαιοτήτων, επίσης, δολοφονίες, απαγωγές, παζάρεμα λύτρων κ. λ.⁹⁸

⁹⁵ Clarke Richard, *Against All Enemies: Inside America's War on Terror*, Free Press, New York, 2004, σ. 152-153. Επίσης, φέρεται ότι το 2006 η Qaeda διείσδυσε εντός της κυβέρνησης των Ηνωμένων Αραβικών Εμιράτων ως είχε ήδη κάνει, σύμφωνα με τον ερευνητή Lorenzo Vidino, σε Σαουδική Αραβία, Πακιστάν και Κουβέιτ -περί τούτου βλέπε Latham Niles, “Qaeda Claim: We ‘Infiltrated’ UAE Gov’t”, 25 Φεβρουαρίου 2006 στην σελίδα <http://nypost.com/2006/02/25/qaeda-claim-we-infiltrated-uae-govt/> του *The New York Post* με ημερομηνία εισόδου την 11^η Φεβρουαρίου 2017

⁹⁶ McGrory Daniel, Jenkins Russell, “Fears of Terror Mole in UK Defence” στο *The Weekend Australian*, 3 Φεβρουαρίου 2007, επίσης βλέπε “UK officials suspect jihadist mole in Ministry of Defence”, 4 Φεβρουαρίου 2007 στο <https://bsimmons.wordpress.com/2007/02/04/uk-officials-suspect-jihadist-mole-in-ministry-of-defense/> εις το οποίο ανατρέξαμε την 25^η Αυγούστου 2016. Για μια περαιτέρω ματιά σχετική με αντικατασκοπευτικές πρακτικές ανταρτικών ή εξτρεμιστικών οργανώσεων βλέπε Ilardi Gaetano, “Irish Republican Army Counterintelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 1, 2010, σ. 1-21 και Wege Anthony Carl, “Hizballah's Counterintelligence Apparatus”, ό. π., σ. 771-785

⁹⁷ Η λέξη *Emni* προέρχεται από τη λέξη *Amn* της οποίας η ηχητική απόδοση στα αυτιά ενός Άραβα μεταφράζεται ως ‘εμπιστοσύνη’, ‘προστασία’ ή ‘ασφάλεια’. *Emni* για το Ισλαμικό Κράτος σημαίνει ‘πληροφόρηση’ -περί τούτου βλέπε Speckhard A., Yayla A., “The ISIS Emni: Origins and Inner Working s of ISIS's Intelligence Apparatus” στο *Perspectives on Terrorism*, Volume 11, Issue 1, 2017, σ. 3

⁹⁸ Speckhard A., Yayla A., *ISIS Defectors: Inside Stories of the Terrorist Caliphate*, Advances Press / LLC, McLean / Virginia, 2016, επίσης, Speckhard A., Yayla A., “The ISIS Emni: Origins and Inner Working s of ISIS's Intelligence Apparatus”, ό. π.

Τα άνω καθήκοντα / δράσεις εμπλέκοντας τόσο τεχνικές / τακτικές κατασκοπίας όσο και αντικατασκοπίας καταδεικνύουν τη σημαντικότητα της πληροφορίας στο στήσιμο ενός εξτρεμιστικού οργανισμού με φιλοδοξίες που ξεπερνούν τη δημιουργία εντυπώσεων ή χάους και φτάνουν μέχρι την εγκαθίδρυση κράτους / καθεστώτος.⁹⁹

⁹⁹ Το “The ISIS Emni: Origins and Inner Working s of ISIS’s Intelligence Apparatus” των Speckhard και Yayla στηρίχτηκε: α) στις μαρτυρίες, μεταξύ Οκτωβρίου 2015 και Φεβρουαρίου 2017, τεσσαράκοντα δύο (42) αποσκιρτησάντων από τις τάξεις του Ισλαμικού Κράτους, β) στην εργασία του ρεπόρτερ Rukmini Callimachi των *New York Times* και γ) στην έρευνα του δημοσιογράφου Christoph Reuter του *Der Spiegel*. Ο τελευταίος έφερε στο φως την ιστορία του Haji Bakr, αξιωματούχου των ιρακινών μυστικών υπηρεσιών και ενός εκ των οργανωτών του πληροφοριακού δικτύου του Ισλαμικού Κράτους -περί τούτου βλέπε Speckhard A., Yayla A., “The ISIS Emni: Origins and Inner Working s of ISIS’s Intelligence Apparatus”, ό. π., σ. 2

ΚΕΦΑΛΑΙΟ 8

Αντικατασκοπία και κυβερνοχώρος

Η κυβερνοκατασκοπία αποτελεί τη μεγαλύτερη πληροφοριακή καταστροφή από την εποχή της διαρροής των πυρηνικών μας μυστικών

Jim Lewis, Διευθυντής του Centre for Strategic and International Studies¹

...κυβερνοαπειλή ... το νέο σύνορο της αντικατασκοπίας

Paul J. Redmond²

Διευκρινήσεις

Δεν χρειάζεται να μας συνδέει κάποια επαγγελματική σχέση με τον τομέα των επιστημών του κυβερνοδιαστήματος προκειμένου να αντιληφθούμε ότι τεχνικές παραπλάνησης / αντιπαραπλάνησης, προπαγάνδας, ασύμμετρες απειλές, γενικότερα επιχειρήσεις Information Operations (IO) / Information Warfare (IW), οικονομικές επιθέσεις αλλά και επιθέσεις κλασικότερων μορφών περνούν πλέον σε μέγιστο βαθμό μέσα από τον έλεγχο του κυβερνοχώρου. Αν αυτό δεικνύει τη μία πλευρά του παιγνίου, κατά κύριο λόγο την επιθετική, η αμυντική συνθέτει την άλλη.³

Το παρόν κεφάλαιο δεν καταπιάνεται με ζητήματα που άπτονται των ειδικών των hardware / software εφαρμογών / συστημάτων. Η επίβλεψη της κυβερνοσφαίρας αντιμετωπίζεται ως ανάγκη που αφορά το σύνολο των εντός αυτής σύννομων δρώντων είτε ομιλούμε για κρατικούς ή διεθνείς οργανισμούς, για τεχνολογικά ιδρύματα, για πολιτειακούς φορείς, για τις ένοπλες δυνάμεις, για τις υπηρεσίες Ασφαλείας / Πληροφοριών κ. λ. Οποσδήποτε, ζητούμενο αποτελεί η διασφάλιση της απρόσκοπτης λειτουργίας καίριων κρατικών ή υπερεθνικών υπηρεσιών, κρίσιμων εθνικών υποδομών, του αδιάβλητου των διαβαθμισμένων ηλεκτρονικών πληροφοριών, της συνέχισης της ομαλότητας της οικονομικής / κοινωνικής ζωής κ. ο. κ. Οι Υπηρεσίες εντός αυτού του πλαισίου οφείλουν να προστατεύσουν πρωταρχικά τα οικεία πληροφοριακά / υπολογιστικά συστήματα / δίκτυα από τις κατά καιρούς κυβερνοεπιθέσεις⁴ συνεισφέροντας, παράλληλα, σε ανάλογα προγράμματα εάν και

¹ “War in the fifth domain”, *The Economist*, 1 Ιουλίου 2010, διαθέσιμο και στην ιστοσελίδα <http://www.economist.com/node/16478792> όπου ανατρέξαμε την 25^η Οκτωβρίου

² Redmond J. Paul, “The Challenges of Counterintelligence” στο *The Oxford Handbook of National Security Counterintelligence*, επιμ. Johnson Loch, Oxford University Press, New York, 2010, σ. 552

³ Για τη σχέση / σύνδεση μεταξύ εθνικής ασφαλείας και (εθνικής) κυβερνοασφαλείας όπως και για τις πέντε συνιστώσες της τελευταίας (στρατιωτική, πληροφοριακή, πολιτική, προστασίας κρίσιμων υποδομών, καταπολέμησης κυβερνοεγκλήματος) βλέπε Hathaway E. Melissa, Klimburg Alexander, “Preliminary Considerations: On National Cyber Security” στο *National Cyber Security. Framework Manual*, επιμ. Klimburg Alexander, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2012, σ. 20-27, 31-34

⁴ RAND Organization Research Review, *Information Warfare: A Two-Edged Sword*, διαθέσιμο στον ιστότοπο http://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/infor_war.html όπου καταφύγαμε την 1^η Οκτωβρίου 2015. Κατανοώντας τη σημασία της εσωτερικής ασφαλείας τονίζουμε ότι η αμερικανική Federal Information Security Management Act (FISMA) του 2002 μεριμνά ορίζοντας τρόπους προστασίας των εσωτερικών πληροφοριακών συστημάτων των ομοσπονδιακών υπηρεσιών και οργανισμών έναντι κυβερνοεπιθέσεων -για περισσότερες λεπτομέρειες ανέτρεξε στον ιστότοπο <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> εις τον οποίο καταφύγαμε την 27^η Αυγούστου 2015, επίσης βλέπε GAO (2005b), *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, (GAO Publication No. GAO-05-231), Government Printing Office, Washington, D.C., 2005, εναλλακτικά, Reddick Christopher,

εφόσον το απαιτήσουν οι κρατικοί σχεδιασμοί ...*cyber-counterintelligence* (CCI) *ίσον στρατηγική προς αναγνώριση / εξουδετέρωση αλλοδαπών πληροφοριακών επιχειρήσεων (ή προς διείσδυση εντός αυτών) των οποίων βασική μεθοδολογία δράσης δεικνύει η χρήση κυβερνοεργαλείων / κυβερνομεθόδων*⁵ -καθίσταται κατανοητό ότι αν η έννοια του κλασικού counterintelligence εμπεριέχει την αμυντική και την επιθετική όψη το ίδιο ισχύει στην περίπτωση του CCI.⁶ Ουσιαστικά η έννοια του CCI αναπτύχθηκε *de facto* στην Αμερική με την είσοδο της πληροφοριακής τεχνολογίας στο πεδίο της εθνικής αμύνης και της ασφαλείας. Κάπου μεταξύ τελών δεκαετίας 1990 και αρχών πρώτης δεκαετίας του 21^{ου} αιώνα η αμερικανική κοινότητα CI αναγνώρισε ένα νέο αντικατασκοπευτικό υποπεδίο, το υποπεδίο της κυβερνοαντικατασκοπίας με σκοπό τη μελέτη τρωτοτήτων / δυνατοτήτων υπολογιστικών / πληροφοριακών δικτύων. Με άλλα λόγια η κυβερνοαντικατασκοπία περιστρέφεται γύρω από τα συγκεκριμένα δίκτυα είτε αυτά αποτελούν 'στόχο' κατασκοπίας, είτε 'μέσο' κατασκοπίας⁷, π. χ., το αμερικανικό DoD σχετίζει τις δράσεις CCI με αναγνώριση / εξουδετέρωση αλλοδαπών επιχειρήσεων, επίσης, με διείσδυση εντός αυτών.⁸ Σημειώνουμε ότι ο ανώνυμος, αόρατος, αχανής και άναρχος κόσμος της κυβερνοσφαίρας, η έλλειψη επαρκούς προϋστορίας, άρα εμπειρίας και συνακόλουθης νομοθεσίας, η ευκολία χρήσης της δοθείσης τεχνολογίας από κάθε ενδιαφερόμενο, τα μη σύνορα του χώρου, η μη ανάληψη εκ μέρους του επιτιθέμενου υψηλού οικονομικού κόστους αλλά και φυσικού ρίσκου όσον αφορά στην πράξη του καθαυτή, η ευχέρεια εμπλοκής, εισβολής, διασύνδεσης του ενός network με το άλλο κ. λ. καθιστούν την *κυβερνοπροστασία / κυβερνοασφάλεια και κυβερνοαντικατασκοπία* κάθε άλλο παρά μια άκοπη υπόθεση.^{9, 10}

Προκλήσεις και παραδείγματα

Η ψηφιακή κατασκοπία ανάγει χρονικά τις ρίζες της τουλάχιστον στο 1982. Φημολογείται πως εκείνη τη χρονιά η KGB υπεξάιρεσε λογισμικό από καναδική φίρμα το οποίο εμπεριείχε κακόβουλο κώδικα τύπου *logic bomb* τοποθετημένο κρυφά

Homeland Security Preparedness and Information Systems. Strategies for Managing Public Policy, IGI Global, USA, 2010, σ. 175-176

⁵ Winterfeldt Steve, Andress Jason, *The Basics of Cyber Warfare. Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Elsevier, Inc., USA, 2013, σ. 92. Επίσης βλέπε σελίδες 21-23 περί αρμοδιοτήτων κρατικών και ιδιωτικών φορέων ως προς την αντιμετώπιση πληροφοριακών συμβάντων ή απειλών επί τη βάση της τυπολογίας αυτών

⁶ Lee M. Robert, "Cyber Counterintelligence: From Theory to Practice", *The State of Security*, 5 Μαΐου 2014, διαθέσιμο στη σελίδα <http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/> όπου καταφύγαμε την 29^η Νοεμβρίου 2015

⁷ French Geoffrey, Kim Jin, "Acknowledging the Revolution: The Urgent Need for Cyber Counterintelligence" στο *National Intelligence Journal*, Volume 1, Number 1, 2009, σ. 72

⁸ JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 Απριλίου 2001 (as amended through 17 October 2007), σ. 139

⁹ Σημειώνεται ότι οι σχετικοί κίνδυνοι έχουν επισημανθεί, έστω σε πρωτόλεια μορφή, ήδη από τη δεκαετία του 1960 -για μια εικόνα βλέπε Warner M., "Cybersecurity: A Pre-History" στο *Intelligence and National Security*, Volume 27, Number 5, 2012, σ. 782

¹⁰ Για μια πληρέστερη άποψη βλέπε Weimann Gabriel, "Cyberterrorism: The Sum of All Fears?" στο *Studies in Conflict & Terrorism*, Volume 28, Issue 2, 2005, σ. 137. Για πολύ περισσότερες λεπτομέρειες περί του γιατί καθίσταται ελκυστικός ο κυβερνοπόλεμος ως επιθετικό εργαλείο τη στιγμή που δεικνύει σχεδόν άλυτο πρόβλημα για τον αμυνόμενο βλέπε Schreier Fred, *On Cyberwarfare*, DCAF Horizon 2015, Working Paper No 7, σ. 27-28

από τη CIA.¹¹ Ελάχιστα αργότερα Γερμανοί hackers εισδύουν σε αμερικανικά κυβερνητικά και στρατιωτικά πληροφοριακά συστήματα υφαρπάζοντας μυστικές πληροφορίες που πωλούνται, τελικά, σε πράκτορες τρίτης χώρας.¹² Μόλα ταύτα είναι ο 21^{ος} αιώνας που χαρακτηρίζει την απογείωση της κυβερνοκατασκοπίας καθώς, τουλάχιστον για τους Singer και Friedman, κάθε ανά τον κόσμο υπηρεσία Πληροφοριών δραστηριοποιείται στο πεδίο¹³, κάθε χώρα βρίσκεται στο στόχαστρο. Μάλιστα η εταιρία McAfee ήδη από το 2007 έχει προειδοποιήσει πως υφίσταται μια «εικονική κούρσα εξοπλισμών» στον κυβερνοχώρο. Πλήθος χωρών αναπτύσσουν κυβερνοόπλα με προεξέχουσες τις Ηνωμένες Πολιτείες, τη Ρωσία, την Κίνα, το Ισραήλ και τη Γαλλία.¹⁴ Κατά τον Jeff Carr, CEO της Grey Logic Company, πολλές κυβερνήσεις κτίζουν οπλοστάσιο προς διεξαγωγή κυβερνοπολέμων¹⁵ τη στιγμή που νατοϊκά ρεπορτάζ ισχυρίζονται πως σχεδόν εκατόν είκοσι χώρες αναπτύσσουν στρατιωτικές κυβερνοδυνατότητες. Οι τελευταίες δύναται να χαρακτηριστούν είτε «επιχειρησιακές», είτε «στρατηγικές» με τις δεύτερες να αναφέρονται αποκλειστικά στο κυβερνοδιάστημα μη εμπλεκόμενες σε φυσικές (kinetic) επιχειρήσεις.¹⁶ Μια άλλη κατηγοριοποίηση ακολουθεί το U.S. Air Force Scientific Advisory Board (AF-SAB). Κατά τον συγκεκριμένο οργανισμό τρία είναι τα επίπεδα κυβερνοεπιθέσεων. Το πρώτο (I) καλείται *network war* ή *system administrator versus system administrator* αναφερόμενο σε κάθε είδους μικροεπιθέσεις που θεωρητικά αντιμετωπίζονται στην πλειοψηφία τους μέσω συμβατικών δικτυακών μέτρων ασφαλείας. Το δεύτερο (II) καλείται *cyber-adjunct to kinetic combat* αναφερόμενο στη σύνδεση των επιστημών του κυβερνοδιαστήματος με τον επιχειρησιακό αγώνα (βλέπε ρωσογεωργιανό πόλεμο 2008). Το τρίτο (III) ονοματοδοτείται ως *malicious manipulation* δεικνύοντας το πλέον επικίνδυνο επίπεδο με τον επιτιθέμενο να επιδιώκει μεγίστης ισχύος κτύπημα του οποίου το αποτέλεσμα δύναται να γίνει άμεσα αντιληπτό ή να λανθάνει επί μακρόν ως συνέβη στην υπόθεση Stuxnet -τέτοιου είδους εγχειρήματα δεν μπορούν, μάλλον και προς το παρόν, να υποστηριχτούν από non-state actors (NSAs).¹⁷ Επιστρέφοντας στο επίπεδο (I) παρατηρούμε, πάντα σύμφωνα με το AF-SAB, την εντός αυτού συμπερίληψη της κυβερνοκατασκοπίας ή, αλλιώς, Computer Network Espionage (CNE) -κάποιοι ερευνητές μη συμφωνώντας με την κατηγοριοποίηση θεωρούν το CNE ως τη σοβαρότερη απειλή.¹⁸

¹¹ Pufeng Wang, "The challenge of information warfare" στο *China Military Science* (Ανοιξη 1995), διαθέσιμο και στο http://fas.org/irp/world/china/docs/iw_mg_wang.htm όπου καταφύγαμε την 11^η Νοέμβρη 2015

¹² Stoll Clifford, "Stalking the Willy Hacker", *Communication of the ACM*, Volume 31, Number 5, 1988, σ. 484-500, επίσης, Stoll Clifford, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, Doubleday, New York, 1989

¹³ ...προκειμένου επίτευξης πληροφοριακής υπεροχής (information superiority) με απώτερο σκοπό «μεγάλες νίκες με μικρά κόστη» όπως γράφει ο στρατηγός Wang Pufeng στο "The challenge of information warfare" στο *China Military Science* (Ανοιξη 1995)

¹⁴ *US, China, Russia have 'cyber weapons': McAfee*, 18 Νοεμβρίου 2009, διαθέσιμο στην τοποθεσία <http://zeenews.india.com/news/world/us-china-russia-have-cyber-weapons-mcafee-579965.html> όπου ανατρέξαμε τη 19^η Νοεμβρίου 2015

¹⁵ *What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare*, 2 Μαρτίου 2010, διαθέσιμο στη δικτυακή σελίδα <http://blog.executivebiz.com/2010/03/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/> όπου καταφύγαμε τη 19^η Νοεμβρίου 2015

¹⁶ Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, European Parliament, Belgium, 2011, σ. 11-12

¹⁷ ό. π., σ. 7-8

¹⁸ ό. π., σ. 51

Επανερχόμενοι σε πραγματικά περιστατικά διαφόρων διαβαθμίσεων σημειώνουμε ότι μεταξύ Απριλίου 1990 και Μαΐου 1991 παρατηρείται πλήθος κυβερνοεπιθέσεων κατά τριάντα τεσσάρων δικτυακών τοποθεσιών του DoD.¹⁹ Την περίοδο 1998-2000 υποκλέπτονται από το εν λόγω Department, το Department of Energy, τη NASA, από πανεπιστήμια και εταιρίες αμυντικής τεχνολογίας πληροφορίες εμπιστευτικού χαρακτήρα. Σύμφωνα με αναφορές οι επιθέσεις (κωδική ονομασία Moonlight Maze) σχετίζονται με server συνδεδεμένο με τη Ρωσική Ακαδημία Επιστημών, εκτελούνται, δε, από τη ρωσική Ομοσπονδιακή Υπηρεσία Ασφαλείας (FSB) και συνεργαζόμενους ανεξάρτητους κυβερνοπειρατές.²⁰ Το Νοέμβριο του 2002 η αμερικανική δικαιοσύνη στρέφεται κατά του Gary McKinnon αφού προηγουμένως αποκαλύπτεται ηλεκτρονική πειρατεία εις βάρος των U.S. Army, U.S. Navy, U.S. Air Force, του Πενταγώνου και της NASA.²¹ Το έτος 2003 αποτελεί αφετηρία ακόμα μιας περίπτωσης cyberespionage (κωδική ονομασία Titan Raid) καταλήγοντας στην παραβίαση αμερικανικών στρατιωτικών υπολογιστικών συστημάτων και στην εκμείωση 10 έως 20 terabytes σχετικών πληροφοριών. Σ' αυτή την περίπτωση η ομάδα των κυβερνοκατασκόπων ανακαλύπτεται κάπου στην επαρχία Guangdong της Κίνας με τη δράση να εκτείνεται τουλάχιστον έως το 2007, επίσης, όπως και στο προηγούμενο συμβάν, φέρεται να υπάρχει συνεργασία μεταξύ κρατικών Υπηρεσιών και ανεξάρτητων hackers.²² Το 2008 το αμερικανικό στρατιωτικό πληροφοριακό δίκτυο πέφτει θύμα κυβερνοπειρατείας αλλοδαπής Υπηρεσίας.²³ Το Μάρτιο του 2011 αξιωματούχοι της αμερικανικής κυβέρνησης ανακοινώνουν τη διεξαγωγή έρευνας περί προτιθέμενου hacking από τους Anonymous κατά του Marine Corps (Quantico (πρώην Potomac) / Βιρτζίνια) με αφορμή υποτιθέμενη κράτηση πληροφοριοδότη των WikiLeaks.²⁴ Παρόμοιες επιθέσεις σημειώνονται έναντι θεσμών / οργανισμών και κυβερνητικών δικτυακών συστημάτων χωρών-μελών της Ευρωπαϊκής Ένωσης χωρίς, ωστόσο, να αποκαλύπτονται λεπτομέρειες ή να γίνεται λόγος περί ζημιών και υπόπτων. Δύο φαίνονται ως πλέον εξηγητικές αιτίες αυτής της στάσης. Η πρώτη έχει να κάνει με το γεγονός της πολύ δύσκολης -αν όχι αδύνατης- επίσημης σύνδεσης της

¹⁹ GAO, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, Μάιος 1996, διαθέσιμο στην τοποθεσία <http://fas.org/irp/gao/aim96084.htm> όπου ανατρέξαμε την 8^η Οκτωβρίου 2015

²⁰ Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, ό. π., σ. 51, επίσης, *Information Operations: The Hard Reality of Soft Power*, σ. 45-46, διαθέσιμο στην διαδικτυακή τοποθεσία <http://www.iwar.org.uk/iwar/resources/jioprc/io-textbook.pdf> όπου καταφύγαμε τη 19^η Οκτωβρίου 2015

²¹ Department of Justice, U.S. District Court for the Eastern District of Virginia, Alexandria Division, Indictment, *United States of America v. Gary McKinnon*, (Alexandria, VA, November 2002), διαθέσιμο στο https://en.wikisource.org/wiki/US_v_Gary_McKinnon_Indictment όπου καταφύγαμε τη 13^η Οκτωβρίου 2015

²² Περί της υποθέσεως βλέπε Thornburgh Nathan, "Inside the Chinese hack Attack", *Time*, 25 Αυγούστου 2005 στο <http://content.time.com/time/nation/article/0,8599,1098371,00.html>, Arthur Charles, "Google the latest victim of Chinese 'state-sponsored' cyberwar", *The Guardian*, 14 Ιανουαρίου 2010 στο <http://www.theguardian.com/technology/2010/jan/14/google-hacking-china-cyberwar>, Winkler Ira, "Guard against Titan Rain hackers", *Computerworld*, 20 Οκτωβρίου 2005 στο <http://www.computerworld.com/article/2559195/security0/guard-against-titan-rain-hackers.html>, (κοινή ημερομηνία ανάκτησης των άρθρων η 19^η Νοεμβρίου 2015)

²³ Mick Jason, "USB Stick Led to Worst Cyber Attack on U.S. Military; Russia Suspected", *Daily Tech*, 26 Αυγούστου 2010, διαθέσιμο στη διαδικτυακή τοποθεσία <http://www.dailytech.com/USB+Stick+Led+to+Worst+Cyber+Attack+on+US+Military+Russia+Suspected/article19458.htm> όπου καταφύγαμε την 25^η Νοεμβρίου 2015

²⁴ Menn Joseph, "US probes Anonymous plans for attack on marines", *FT. com*, 8 Μαρτίου 2011, στο <http://www.ft.com/cms/s/0/82343fba-491a-11e0-af8c-00144feab49a.html#axzz3sdXtN2G5> όπου ανατρέξαμε την 25^η Νοεμβρίου 2015

όποιας επίβουλης δράσης με κάποια Υπηρεσία ή κρατική πολιτική παρά τη θεωρούμενη βέβαιη ύπαρξη υπόγειων διαδρομών μεταξύ πληροφοριακών οργανισμών και κυβερνοπειρατών. Η δεύτερη, που αφορά σε μη αποκάλυψη επιθέσεων οικονομικής υφής έναντι ιδιωτικών συμφερόντων, αφορά στην επιβίωση μιας επιχείρησης: η τελευταία δεν θα παραδεχτεί την παραβίαση των συστημάτων ασφαλείας της.²⁵

Αν και το DoD από την έναρξη των περιστατικών αποδέχεται την πραγματικότητα των κυβερνοαπειλών -άρα πολύ πριν την είσοδο του 21^{ου} αιώνα- είναι μόλις το 1998 όταν επισήμως «τρέχει» το επονομαζόμενο Joint Task Force-Computer Network Defense (JTF-CND), πρόγραμμα με σκοπό την προάσπιση των οικείων υπολογιστικών συστημάτων.²⁶ Δύο υπήρξαν οι λόγοι καθιέρωσής του. Ο πρώτος σχετίζεται με τα αποτελέσματα της άσκησης Eligible Receiver (1997) κατά την οποία η NSA προκαλεί αποδιοργάνωση πλήθους δικτυακών πληροφοριακών συστημάτων του DoD, μεταξύ αυτών, του National Military Command Center του Πενταγώνου, της U.S. Pacific Command -USPACOM, της U.S. Space Command -USSPACECOM, της U.S. Transportation Command -USTRANSCOM και της U.S. Special Operations Command -USSOCOM²⁷ καταδεικνύοντας τρύπες ασφαλείας που ενδέχεται να αποτελέσουν κερκόπορτα για ξένες Υπηρεσίες, αδιαφανείς οργανώσεις, τρίτα πρόσωπα κ. α. Ο δεύτερος αφορά σε συμβάντα κυβερνοεπιθέσεων τον Φεβρουάριο του 1998 κατά αμερικανικών στρατιωτικών πληροφοριακών συστημάτων. Το γεωγραφικό στίγμα εκπόρευσης των συγκεκριμένων κυβερνοενεργειών τοποθετείται κάπου στη Μέση Ανατολή με υποτιθέμενο εντολοδότη το κράτος του Ιράκ. Αν και δεν υπήρξε προσβολή διαβαθμισμένων assets, το έλλειμμα δικτυακής ασφαλείας θα μπορούσε να οδηγήσει στη διακοπή των ροών μεταξύ DoD και αμερικανικών στρατιωτικών διοικήσεων σταθμευμένων στην ανωτέρω περιοχή. Επιπλέον ανησυχητικό στοιχείο, η κατοπινή αποκάλυψη της ταυτότητας των δραστών -επρόκειτο για τρεις εφήβους (δύο Αμερικανούς, έναν Ισραηλινό), στοιχείο που υποδηλώνει την ευκολία με την οποία μπορεί κάποιος να παρεισδύσει εντός εθνικής σημασίας πόρων όσο και την άγνοια που περιβάλλει ακόμα και ειδικούς.²⁸ Τον Οκτώβριο του 2002 το JTF-CND μετονομάζεται σε Joint Task Force-Computer Network Operations (JTF-CNO) αποδιδόμενο, ειδικότερα, στη U.S. Strategic Command του DoD. Περιλαμβάνει προσωπικό από τους τέσσερις κλάδους των αμερικανικών Ενόπλων Δυνάμεων και από το Defense Information System Agency's Computer Emergency Response Team. Η αποστολή του JTF-CNO έχει διττό σκοπό: πρώτον, τη διασφάλιση, μέσω δράσεων Computer Network Defense (CND), των υπολογιστικών / πληροφοριακών δικτύων και συστημάτων του DoD από επίβουλες κυβερνοενέργειες και δεύτερον, το συντονισμό, την υποστήριξη και τη

²⁵ Sawyer Patrick, "Top Chinese officials ordered attack on Google, Wikileaks cables claim", *The Telegraph*, 4 Δεκεμβρίου 2010, διαθέσιμο στη διαδικτυακή τοποθεσία <http://www.telegraph.co.uk/news/worldnews/wikileaks/8181619/Top-Chinese-officials-ordered-attack-on-Google-Wikileaks-cables-claim.html>, Allan Darren, "Cyber-crime costs UK economy £27 billion per year", *Techwatch*, 17 Φεβρουαρίου 2011, διαθέσιμο και στον ιστότοπο <http://www.techwatch.co.uk/2011/02/17/cyber-crime-costs-uk-economy-27-billion-per-year/> (κοινή ημερομηνία ανάκτησης των άρθρων η 19^η Νοεμβρίου 2015)

²⁶ Fact File U.S. Strategic Command Public Affairs, 901 SAC Blvd, Suite 1A1, Offutt AFB NE 68113-6020, *Joint Task Force Computer Network Operations*, έγγραφο διαθέσιμο στη διαδικτυακή τοποθεσία <http://www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm> όπου καταφύγαμε τη 14^η Οκτωβρίου 2015

²⁷ Global Security.org, "Eligible Receiver" στο <http://www.globalsecurity.org/military/ops/eligible-receiver.htm> όπου καταφύγαμε τη 14^η Οκτωβρίου 2015

²⁸ Robinson Colin, *Military and Cyber-Defense: Reactions to the Threat*, Center for Defense Information Terrorism Project, Washington, D.C., 2002, σ. 1-2

διεξαγωγή κυβερνοεπιχειρήσεων υπό την εντολή του Λευκού Οίκου, μέσω δράσεων Computer Network Attack (CNA), προς διεκπεραίωση εθνικών αλλά και περιφερειακών διεθνών σχεδιασμών.²⁹

Ασφάλεια και αντικατασκοπία στον κυβερνοχώρο

Κατά τους Bilge Karabacak και Ünal Tatar οι κυβερνοεπιθέσεις κατατάσσονται εντός τεσσάρων κύριων κατηγοριών ήτοι, *hacktivism*, *cybercrime*, *cyberwar* και *cyberespionage* χωρίς να υπάρχει πάντα ξεκάθαρη διάκριση μεταξύ τους. Αν ό,τι κατά βάσει μας ενδιαφέρει περιστρέφεται γύρω από την προάσπιση εθνικών συμφερόντων και την ομαλή λειτουργία κρίσιμων υποδομών³⁰, τότε, αυτό που πρέπει να αντιμετωπιστεί αφορά πρωτίστως σε εκδηλώσεις κυβερνοκατασκοπίας και κυβερνοπολέμου.³¹ Ο Karabacak σε συνεργασία με τον Mert Uneri δημιουργεί έναν ‘χάρτη προστασίας’ υπολογιστικών συστημάτων / δικτύων κατά τον οποίο προτείνονται τρία στάδια ενεργειών, ειδικότερα: α) το στάδιο της *αναλυτικής φάσης* (*analysis phase*), β) το στάδιο της *φάσης σχεδιασμού* (*design phase*), γ) το *επιχειρησιακό* στάδιο (*operation phase*). Αυτό που συγκεκριλώνει την πρότασή τους έχει να κάνει με: α) ανάλυση ρίσκου λειτουργίας των networks (αναλυτική φάση), β) την κατάθεση ενός σχεδίου πολιτικής προστασίας γύρω από τα τελευταία (φάση σχεδιασμού), γ) την επιτήρηση / έλεγχο των networks και τη δημιουργία μιας ομάδας χειρισμού τέτοιου είδους θεμάτων / κρίσεων -Computer Emergency Response Team / CERN (επιχειρησιακό στάδιο).³²

Ο υποστράτηγος Luigi Vellone γράφοντας περί τρομοκρατίας σημειώνει τόσο την ικανότητά της να μένει στην αφάνεια όσο και τον, μέρα με τη μέρα, αποκεντρωμένο χαρακτήρα της. Οι συγκεκριμένες ποιότητες απαιτούν (αλλά και προσδίδουν) ευχέρεια επικοινωνιών, ταχύτητα κινήσεων, ευελιξία μεταφοράς πόρων (κεφαλαίων, οπλισμού, πληροφόρησης). Η εξάρθρωση του αρχικού πυρήνα της al Qaeda και η κατοπινή έρευνα κατέδειξε τις δυνατότητές της στη χρήση δικτυακών υπηρεσιών

²⁹ *Space, Missile Defense and Computer Network Operations Challenges: Computer Network Operations: A Critical Element of Current and Future Military Operations in Combating the Asymmetrical Threat* στο AUSA Background Brief, Number 96, Νοέμβριος 2002, διαθέσιμο και στο <https://www.ousa.org/SiteCollectionDocuments/ILW%20WebExclusivePubs/Background%20Briefs/bb96.pdf> όπου ανατρέξαμε τη 15^η Οκτωβρίου 2015. Ουσιαστικά η έννοια ‘Computer Network Operations’ αναφέρεται στο στρατιωτικό cyberwar / cyberattack τη στιγμή που μια πετυχημένη επιθετική δράση (CNA) απαιτεί μια πετυχημένη κατασκοπευτική (Computer Network Espionage -CNE) -για μια εικόνα βλέπε Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, ό. π., σ. 7

³⁰ Κατά τον David Powner μια υποδομή (π. χ. ένα φράγμα ύδατος) χαρακτηρίζεται καίρια όταν η υπολειτουργία ή, ακόμα χειρότερα, η καταστροφή της ενδέχεται να οδηγήσει ένα έθνος σε περιπέτειες ακόμα και γύρω από τη βιολογική του συνέχεια, τις οικονομικές του προοπτικές, την κοινωνική ειρήνη και συνοχή κ. ο. κ. -περί τούτων αλλά και για τους δεκαοκτώ κρίσιμους τομείς / υποδομές των ΗΠΑ βλέπε “Cyberwar. War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?”, *The Economist*, 1 Ιουλίου 2010, διαθέσιμο και στην διαδικτυακή τοποθεσία <http://www.economist.com/node/16478792> όπου ανατρέξαμε την 25^η Οκτωβρίου 2015, επίσης, Powner D., “Critical Infrastructure Protection. DHS Needs to Better Address its Cybersecurity Responsibilities” στο *Cybersecurity, Cyberanalysis and Warning*, επιμ. Norwood Kerry, Catwell Sandra, Nova Science Publishers, Inc, New York, 2009, σ. 72

³¹ Karabacak Bilge, Tatar Ünal, “Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection” στο *Critical Infrastructure Protection*, επιμ. Edwards Matthew, Ios Press, Amsterdam, 2014, σ. 63-68

³² Uneri Mert, Karabacak Bilge, “Securing Networks in the Information Age” στο *Cyberwar-Netwar. Security in the Information Age*, επιμ. Carvalho Fernando, daSilva Eduardo, Ios Press, Amsterdam, 2006, σ. 61-74

προς ικανοποίηση των ανωτέρω αναγκών. Ο Vellone αν και δεν αναφέρεται άμεσα στις Υπηρεσίες σημειώνει ότι η βελτίωση της διαδικασίας ανάλυσης της πληροφορίας, η αποκάθαρση του τελικού προϊόντος από ασάφειες / λάθη όπως και η πρόσβαση σε περισσότερες, κατά το δυνατό, βάσεις δεδομένων επικουρεί το έργο των δικτύων εθνικής ασφαλείας.³³

Ο ταγματάρχης J. P. I. A. G. Charvat τονίζει ότι η κυβερνοσφαίρα αποτελεί χώρο ρίζοσπαστικοποίησης, στρατολόγησης, προπαγάνδας, δημοσιότητας, επικοινωνίας, έρευνας και εύρεσης κεφαλαίων υπέρ της τρομοκρατίας προσφέροντας, επιπλέον, ευκολίες στους τομείς διοίκησης και ελέγχου.³⁴ Παρά την ύπαρξη συστημάτων τηλεμετρίας και αυτόματης επιτήρησης (Supervisory Control And Data Acquisition -SCADA) λειτουργίας καίριων υποδομών, ο κίνδυνος δολιοφθοράς καθόλου δεν απομακρύνεται ίσως διότι, συνεχίζει ο ταγματάρχης, οι σύγχρονες κοινωνίες στηρίζονται όλο και περισσότερο στην εξ αποστάσεως επίβλεψη και στα διασυνδεδεμένα ηλεκτρονικά συστήματα.³⁵ Παρά το ότι ο Charvat δεν κάμει λόγο για δράση των υπηρεσιών Ασφαλείας έναντι εξτρεμιστικών ομάδων, η εμπλοκή τους λόγω εμπειρίας, εξοπλισμού και τεχνογνωσίας θεωρείται εκ των ων ουκ άνευ.³⁶

³³ Vellone Luigi, "From Data to Knowledge: How Intelligence and Security Tools Can Help" στο *Cyberwar-Netwar. Security in the Information Age*, ό. π., σ. 115-122

³⁴ Βλέπε παραδείγματα στα Rogan Hanna, *Jihadism Online: A Study of How al-Qaeda and Radical Islam Groups Use the Internet for Terrorist Purposes*, Norwegian Defence Research Establishment, Norway, 2006, Sageman Marc, "The Next Generation of Terror" στο *Foreign Policy*, Μάρτιος / Απρίλιος 2008, σ. 41, Ishengoma Frederick, "Online Social Networks and Terrorism 2.0 in Developing Countries" στο *International Journal of Computer Science & Network Solutions*, Volume 1, Number 4, 2013, σ. 57-66, Bertram Stewart, Ellison Keith, "Sub Saharan African Terrorist Groups' use of the Internet" στο *Journal of Terrorism Research*, Volume 5, Issue 1, 2014, σ. 5-21, Campana Aurélie, Ducol Benjamin, "Voices of the 'Caucasus Emirate': Mapping and Analyzing North Caucasus Insurgency Websites" στο *Terrorism and Political Violence*, Volume 27, Issue 4, 2015, σ. 679-700, Aly Anne, "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization" και Conway Maura, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research" στο *Studies in Conflict and Terrorism*, Volume 40, Issue 1, 2017, σ. 1-9 και 77-98 αντιστοίχως, τέλος, στο Burke Jason, "Al-Shabab's Tweets Won't Boost its Cause", 16 Δεκεμβρίου 2011, στη σελίδα <https://www.theguardian.com/commentisfree/2011/dec/16/al-shabab-tweets-terrorism-twitter> του *The Guardian* με ημερομηνία εισόδου την 11^η Φεβρουαρίου 2017

³⁵ Charvat J., "Cyber Terrorism: A New Dimension in Battlespace" στο *The Virtual Battlefield: Perspectives on Cyber Warfare*, επιμ. Czosseck Christian, Geers Kenneth, Ios Press, Amsterdam, 2009, σ. 77-86

³⁶ ...παρότι η Myriam Dunn Cavelty, εν έτει 2007, υποστηρίζει ότι δεν υφίσταται κανένας κίνδυνος εθνικής ασφαλείας εξ αιτίας της κυβερνοτρομοκρατίας. Σύμφωνα με την ερευνητρια μελέτες έχουν δείξει ότι μια στρατηγική απειλή αυτού του είδους δεν δύναται να ευοδωθεί λόγω μη επαρκών υλικοτεχνικών πόρων εκ μέρους ακραίων οργανώσεων. Μαζί της συμφωνούν κατά τον έναν ή άλλο τρόπο οι Joris Evers και Gabriel Weimann τη στιγμή που οι Stephen Walt, Glenn Greenwald και Kevin Poulson τηρούν μια μέση στάση -περί τούτων βλέπε Cavelty Myriam, "Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics*, Volume 4, Issue 1, 2007, σ. 19-31, Evers Joris, "Does Cyberterrorism Pose a True Threat?", *PC World*, Μάρτιος 2003 και "Cyberterror threat overblown, say experts", *Computerworld*, Μάρτιος 2003 αντιστοίχως στα <http://www.pcworld.com/article/109819/article.html> και <http://www.computerworld.com/article/2581635/security0/cyberterror-threat-overblown--say-experts.html> όπου καταφύγαμε την 5^η Οκτωβρίου 2015, Weimann Gabriel, *Special Report-Counterterrorism: How Real is the Threat?*, United States Institute of Peace, Washington, D.C., Μάιος 2004 διαθέσιμο και στο <http://www.usip.org/sites/default/files/sr119.pdf> όπου καταφύγαμε επίσης την 5^η Οκτωβρίου 2015, Walt St., "Is the cyber threat overblown?", *Foreign Policy*, τεύχος 178, Μάρτιος / Απρίλιος 2010 στο <http://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/> εις το οποίο ανατρέξαμε την 6^η Οκτωβρίου 2015. Πάρα ταύτα, ως ήδη αναφέραμε, η άσκηση Eligible Receiver κατέδειξε σημαντικές αδυναμίες ορισμένων, τουλάχιστον, κρατικών / πολιτικών υποδομών όπως και κάποιων αμερικανικών στρατιωτικών υπολογιστικών / πληροφοριακών συστημάτων, τρωτότητες που ευνοούν μια μεγάλης κλίμακας κυβερνοεπίθεση -για μια καλύτερη εικόνα βλέπε Denning Dorothy,

Οι Eric Luijff και Jason Healey τονίζουν πως μια ξεκάθαρη διαχωριστική γραμμή μεταξύ κυβερνοεγκλήματος / κυβερνοκατασκοπίας και κυβερνοκατασκοπίας / στρατιωτικών κυβερνοδράσεων δεν υφίσταται. Η συμμετοχή των υπηρεσιών Αντικατασκοπίας σε κάθε περίπτωση καθίσταται απαραίτητη ειδικά όταν εγείρονται ζητήματα προστασίας κυβερνητικών συστημάτων από προηγμένες κυβερνοαπειλές κρατικών ή μη οντοτήτων. Ωστόσο, δεν είναι μόνο το αμυντικό καθήκον που απασχολεί, όπως αφήνουν να εννοηθεί ...είναι επίσης πιθανόν να μην αποκαλυφθεί μια συγκεκριμένη τρωτότητα με σκοπό την εξυπηρέτηση μιας συγκεκριμένης πληροφοριακής ανάγκης. Συνολικά, οι Υπηρεσίες παρά το ότι επικεντρώνουν στο επιχειρησιακό / τακτικό στοιχείο παίζουν σημαίνοντα ρόλο και σε στρατηγικό επίπεδο προβαίνοντας κυρίως σε εκτιμήσεις / αναλύσεις απειλών. Από κει και πέρα η διατήρηση του γνωστού πληροφοριακού κύκλου κυριαρχεί: συλλογή δεδομένων, ανάλυση, διασπορά τελικού προϊόντος στους θεσμικούς αποδέκτες.³⁷

Οι Johan Sigholm και Martin Bang μελετώντας την πράξη του cyber-counterintelligence υποστηρίζουν πως αυτή πάσχει λόγω της τάσης ταύτισης που τη διακρίνει με την αντίστοιχη του κλασικού CI. Δεύτερη κατ' επέκταση τροχοπέδη αποτελεί η αυστηρή ιεραρχική δομή του συστήματος που καθυστερεί την άμεση απάντηση προς αντιμετώπιση απειλών του κυβερνοχώρου. Αυτό που προτείνουν σχετίζεται με μια αυξημένη συνεργατικότητα μεταξύ των επιχειρησιακών (agents) και των άμεσα θιγομένων / ενδιαφερομένων (stakeholders). Πάρα ταύτα κατανοούν το δύσκολο του εγχειρήματος: πολλές φορές στο περιβάλλον του άπειρου κυβερνοχώρου δεν γνωρίζουμε καν ότι δεχόμαστε επίθεση τη στιγμή που ακόμα και αν το αντιληφθούμε ο δράστης παραμένει ανώνυμος.³⁸

Ο Robert Lee κάνοντας λόγο για αμυντικό και επιθετικό cyber CI γράφει πως το πρώτο εκτελεί εργασίες: α) εκτίμησης οικείων τρωτοτήτων (vulnerability assessment), β) ανάλυσης απειλών (threat analysis), γ) προσομοίωσης απειλών μέσω ομάδων Red Team. Το επιθετικό CCI σκοπό έχει: α) την παρείσδυση στο αντίπαλο κυβερνοδίκτυο προς συλλογή πληροφοριών σχετικών, μάλιστα, με ανταγωνιστικές

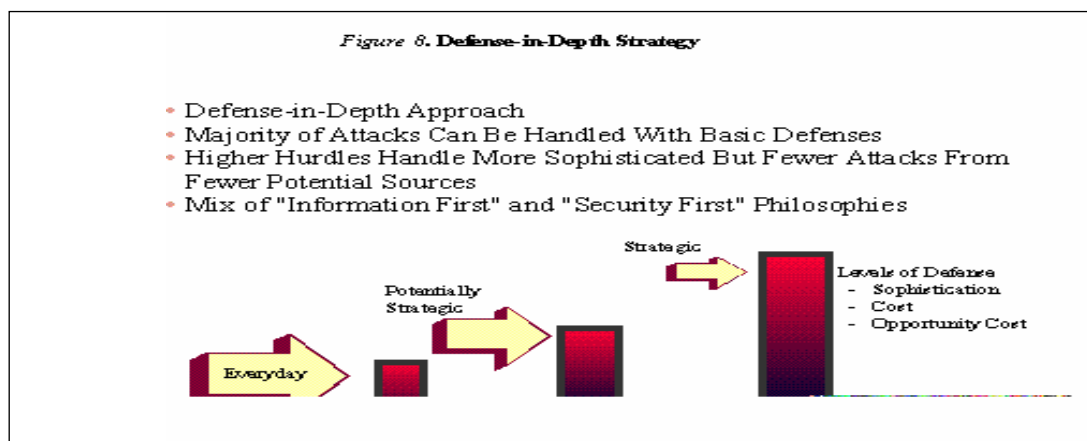
“Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” στο *Networks and Netwars: The Future of Terror, Crime, and Militancy*, επιμ. Arquilla John, Ronfeldt David, RAND, Santa Monica, 2001, σ. 286-287, επίσης Kenedli Tamás, Béres János, “Is the cyberterror exaggerated?” στο *AARMS*, Volume 7, Number 1, 2008, σ. 19-20. Από τη μεριά του το U.S. Government Accountability Office καταγράφοντας σειρά «κυβερνοσυμβάντων» δεν φαίνεται να συμμερίζεται την αισιοδοξία της Cavelti ασχέτως αποφυγής χρήσης της λέξης «κυβερνοτρομοκρατία» -για μια άποψη βλέπε U.S. Government Accountability Office, “Cyber Analysis and Warning. DHS Faces Challenges in Establishing a Comprehensive National Capability” στο *Cybersecurity, Cyberanalysis and Warning* στο *Cybersecurity, Cyberanalysis and Warning*, ό. π., σ. 10. Σ’ αυτό το σημείο τίθεται το ερώτημα της σχέσης κυβερνοτρομοκρατίας και Υπηρεσιών. Σε μια τέτοια περίπτωση ομιλούμε για κυβερνοπόλεμο; Κατά πόσο αυξάνουν οι πιθανότητες επιτυχούς κτυπήματος; Αν πάντως με τη λέξη «cyberterrorism» σημάζουμε την εμπλοκή αποκλειστικά τρομοκρατικών ομάδων, τότε, οφείλουμε να καταγράψουμε τα λόγια του πρώην DNI John “Mike” McConnell (στο Singer W. P., Friedman Allan, *Cybersecurity and Cyberwar. What Everyone Needs To Know*, Oxford University Press, USA, USA, 2014, σ. 99) σύμφωνα με τα οποία ...[τα τρομοκρατικά γκρουπ] *βρίσκονται σήμερα [αρχές δεύτερης δεκαετίας του 21^{ου} αιώνα] στο κάτω σημείο της κλίμακας ικανότητας αξιοποίησης δυνατοτήτων κυβερνοπολέμου [αλλά] αργά ή γρήγορα θα αποκτήσουν την απαιτούμενη τεχνογνωσία*

³⁷ Luijff Eric, Healey Jason, “Organisational Structures & Considerations” στο *National Cyber Security. Framework Manual*, ό. π., σ. 123-124

³⁸ Sigholm Johan, Bang Martin, “Toward Offensive Cyber Counterintelligence. Adopting a Target-Centric View on Advanced Persistent Threats”, 2013 European Intelligence and Security Informatics Conference, διαθέσιμο στο https://www.ida.liu.se/~johsi32/docs/EISIC2013_Sigholm_Bang.pdf εις το οποίο καταφύγαμε την 28^η Σεπτεμβρίου 2016

επιχειρήσεις συλλογής δεδομένων, β) την παραπλάνηση αυτών των επιχειρήσεων.³⁹ Πάντως η περίπτωση Snowden κατέδειξε ότι διαρροές πληροφοριών λαμβάνουν χώρα όχι λόγω μόνο εξωτερικών (outsiders) αλλά και εσωτερικών (insiders) παραγόντων. Προς αντιμετώπιση των δευτέρων προκρίνονται κλασικές πρακτικές εσωτερικής ασφαλείας όπως έλεγχος προσωπικού, αυστηρή αδειοδότηση προκειμένου πρόσβασης σε διαβαθμισμένες πληροφορίες, περιορισμός στη διακίνηση πληροφορίας κ. λ.⁴⁰

Ο David Alberts προτείνει τη λεγόμενη Defense-in-Depth στρατηγική προς αντιμετώπιση σχεδιασμών / συμβάντων πληροφοριακού πολέμου. Πρόκειται για τακτική ενσωμάτωσης τριών διαδοχικών επιπέδων αμύνης με το δεύτερο να επιχειρεί την αναχαίτιση «δυνητικά στρατηγικών» απειλών και το τρίτο την αναχαίτιση «στρατηγικών». Τα δύο τελευταία είδη απειλής, αν όχι μόνο το τελευταίο, είναι αυτά που ενδιαφέρουν τις κρατικές Υπηρεσίες και οργανισμούς με τον αριθμό να περιορίζεται σημαντικά σε σχέση με αυτόν των απειλών «καθημερινού τύπου». Οι δυνητικά στρατηγικές / στρατηγικές απειλές «τρέχουν» από άτομα που διατηρούν υψηλή γνώση του αντικειμένου «κυβερνοχώρος», συνεπώς, εκπορεύονται από μικρούς πυρήνες -πρόκειται για επισήμανση που θεωρητικά βοηθά τις αρχές να επικεντρώσουν κατά την έρευνα προσδιορισμού αυτών των κύκλων.



Εικόνα 24: Τα τρία κατά David Alberts επίπεδα κυβερνοάμυνας έναντι κυβερνοαπειλών. Η εικόνα ελήφθη από το *Defensive Information Warfare*, NDU Press Book, Washington, D.C., 1996, σ. 15, έργο του ίδιου

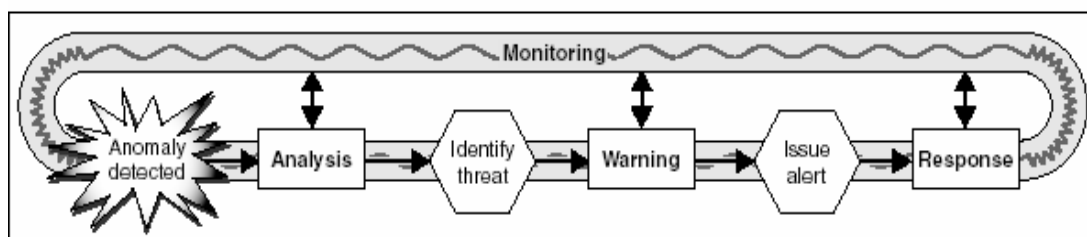
Ασφαλώς, συνεχίζει ο Alberts, μια συνεργασία μεταξύ κρατικών φορέων και ανάλογων του ιδιωτικού πεδίου ενδέχεται να παράξει αποτελέσματα όταν η ζητούμενη λύση αφορά σε στρατηγικές προκλήσεις των οποίων η περιοχή καλείται χαρακτηριστικά “zone of collaboration”. Δοθέντος της φύσεως του πληροφοριακού πολέμου δεν πρέπει να αποκλεισθεί το γεγονός εμπλοκής του κρατικού με τον ιδιωτικό τομέα· μια επίθεση σε μια εταιρία που ελέγχει μια καίρια υπηρεσία

³⁹ Lee M. Robert, “Cyber Counterintelligence. From Theory to Practice”, στη διαδικτυακή τοποθεσία <http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/> στην οποία καταφύγαμε την 27^η Οκτωβρίου 2016

⁴⁰ Elisan C. C., *Malware, Rootkits and Botnets: A Beginning Guide*, McGraw Hill, New York, 2013, σ. 290-293. Για τεχνικές λεπτομέρειες και πρακτικές αντιμετώπισης επίβουλων κυβερνοενεργειών βλέπε μεταξύ άλλων στον εξαιρετικό τόμο των Skoudis E., Liston T., *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Pearson Education, Inc., New Jersey, 2006²

κοινοφελούς σκοπού ίσως επηρεάσει, λιγότερο ή περισσότερο, αυτό που καλούμε «εθνική ασφάλεια».⁴¹

Το U.S. GAO μελετώντας μεταξύ 2007 και 2008 συγκεκριμένες ομοσπονδιακές και μη ομοσπονδιακές δομές και υπηρεσίες κατέληξε στο συμπέρασμα ότι ένα ικανό πρόγραμμα ανάλυσης και έγκαιρης προειδοποίησης κυβερνοαπειλών (cyber analysis and warning program) οφείλει να πληροί τις εξής τέσσερις προϋποθέσεις: α) *ελέγχου / επιτήρησης (monitoring)*: πρόκειται για διαδικασία ανίχνευσης κυβερνοαπειλών / κυβερνοεπιθέσεων και εσωτερικών τρωτοτήτων όσον αφορά σε οικεία συστήματα και στην απρόσκοπτη ροή της κυκλοφορίας / ανταλλαγής δεδομένων, β) *ανάλυσης (analysis)*: αναφερόμαστε στην κλασική διαδικασία ανάλυσης πληροφοριών συλλεγομένων μέσω του προηγούμενου σταδίου με σκοπό την αναγνώριση του είδους της όποιας απειλής, των ενδεχομένων επιπτώσεων, τη μελέτη ενδεδεδειγμένων κινήσεων κ. λ., γ) *προειδοποίησης (warning)*: αναφερόμαστε στην κρούση του κώδωνα περί πιθανών, επικείμενων ή τρεχουσών κυβερνοαπειλών / κυβερνοεπιθέσεων, δ) *απόκρισης / αντίδρασης (response)*: πρόκειται για στάδιο ανάληψης δράσεως προκειμένου να αναχαιτιστεί ένα επαπειλούμενο γεγονός, να εξασφαλισθεί η προστασία των *networks operations*, να ανακουφιστεί / αναρρώσει το σύστημα κατόπιν επίθεσης. Περαιτέρω επιζητείται μια καταχώρηση συμπερασμάτων ως *lessons learned* όπως και στοιχείων / δεδομένων σχετικών με κυβερνοαπειλές προκειμένου να βελτιωθεί η όλη σειρά ενεργειών με την προτεραιότητα, πάντως, να δίδεται στην ανάλυση / προειδοποίηση.⁴²



Εικόνα 25: ο διευρυμένος κύκλος ανάλυσης / προειδοποίησης κυβερνοαπειλών κατά το U.S. GAO [GAO (2008b), *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, (GAO Publication No. GAO-08-588), Government Printing Office, Washington, D.C., 2008]. Η εικόνα έχει ληφθεί από το *Cybersecurity, Cyberanalysis and Warning*, επιμ. Norwood Kerry, Catwell Sandra, Nova Science Publishers, Inc, New York, 2009, σ. 1

⁴¹ Alberts D., *Defensive Information Warfare*, NDU Press Book, Washington, D.C., 1996, σ. 15-17. Από τη μεριά τους οι Richard O. Hundley και Robert H. Anderson κάνουν λόγο για κυβερνοαπειλές τεσσάρων ειδών των οποίων τα ενδεχόμενα αποτελέσματα κατηγοριοποιούνται από «μικρής σημασίας» μέχρι «καταστροφικών επιπτώσεων» -για περισσότερα βλέπε Hundley O. R., Anderson H. R., "Emerging Challenge: Security and Safety in Cyberspace" στο *In Athena's Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997, σ. 232-235. Όσον αφορά στο DHS και προκειμένου αποφυγής περιστατικών σε καίριες πολιτικές υποδομές προτείνεται μια αντίστοιχη Defense-in-Depth στρατηγική καταδεικνύοντας την συγγένεια πολιτικών και στρατιωτικών πλάνων αμυντικής φύσεως -για περισσότερα βλέπε Lee Newton, *Counterterrorism and Cybersecurity. Total Information Awareness*, Springer, USA, 2013, σ. 106

⁴² U.S. Government Accountability Office, "Cyber Analysis and Warning. DHS Faces Challenges in Establishing a Comprehensive National Capability" στο *Cybersecurity, Cyberanalysis and Warning* στο *Cybersecurity, Cyberanalysis and Warning*, ό. π., σ. 15-17. Για περισσότερες λεπτομέρειες βλέπε επίσης σ. 17-25. Περί του πρωτοτύπου ανέτρεξε στη σελίδα <http://www.gao.gov/new.items/d08588.pdf> από όπου συλλέξαμε πληροφορίες την 23^η Αυγούστου 2015

Η μελέτη του GAO μας βοηθά να συναγάγουμε ότι: α) τα αναφερόμενα στάδια συνάδουν σε ικανό βαθμό με αυτά του κλασικού πληροφοριακού κύκλου χωρίς να ταυτίζονται. Η συλλογή, η ανάλυση, η διασπορά πληροφορίας δεικνύουν κοινό τόπο. Από την άλλη μεριά φαίνεται ότι μια παροχή κατευθύνσεων ως προς το τι επιζητάμε δεν αποδίδεται στο βαθμό, τουλάχιστον, που αυτό οφείλει να συμβεί κατά τη συμβατή πληροφοριακή διαδικασία καθώς το όλο πεδίο τελεί υπό «μη συμβατών συνθηκών», β) η όλη λειτουργία / φιλοσοφία ταιριάζοντας στο πνεύμα των Υπηρεσιών και δη και σ' αυτών της Αντικατασκοπίας δεν αφήνει περιθώρια μη εμπλοκής των τελευταίων ή, ίσως, η εμπλοκή τους οδηγεί στη συγκεκριμένη λειτουργία / φιλοσοφία, γ) αν και η ανάλυση του GAO δεν κάνει λόγο για επιθετικές τακτικές, κάτι τέτοιο αποτελεί αναπόσπαστο τμήμα των σχεδιασμών καθώς οι τρωτότητες του κυβερνοχώρου προσφέρουν αυτή την ευκαιρία.

Εξετάζοντας την αποστολή και το ρόλο του U.S. Department of Homeland Security εντός του αμερικανικού ιστού ασφαλείας διαπιστώνουμε ότι ο συγκεκριμένος θεσμός εκτελεί, μεταξύ άλλων, χρέη που σχετίζονται (και) με την αντικατασκοπία. Κατά τον τρόπο τούτο θεωρούμε πως μια παράθεση αρμοδιοτήτων, καθηκόντων και ζητουμένων του DHS όπως μεταφέρονται στο Παράρτημα Ι⁴³ του “Critical Infrastructure Protection. DHS Needs to Better Address its Cybersecurity Responsibilities” του David Powner, στο *Cybersecurity, Cyberanalysis and Warning* -2009, σε σχέση με μια ανάγκη ασφαλείας στην κυβερνοσφαίρα δεν απάδει δεικνύοντας, στον ίδιο χρόνο, σχέδιο αντιμετώπισης του προβλήματος. Ειδικότερα τονίζονται τα προαπαιτούμενα: α) της ανάπτυξης ενός εθνικού πλάνου προστασίας κρίσιμων υποδομών συμπεριλαμβανομένης και της προστασίας του κυβερνοχώρου, β) της ανάπτυξης συνεργατικών σχέσεων μεταξύ των ομοσπονδιακών Υπηρεσιών, των πολιτειακών και των τοπικών δομών με το κύριο καθήκον προστασίας της κυβερνοσφαίρας να βαραίνει το DHS, γ) της αύξησης των ανταλλασσόμενων πληροφοριών μεταξύ ομοσπονδιακών Υπηρεσιών, διακυβερνητικών δομών, ιδιωτικών φορέων, δ) του σχεδιασμού διαχείρισης απειλών περίξ της λειτουργίας κρίσιμων πληροφοριακών συστημάτων. Κάτι τέτοιο μεταξύ άλλων επιβάλλει μια ανάγκη συντονισμού εκτάκτων δράσεων των Υπηρεσιών καθώς και την κατάρτιση επανορθωτικών πλάνων αναλόγως συμβάντων, ε) της αναγνώρισης / εκτίμησης των κυβερνοαπειλών, στ) μιας προσπάθειας απομείωσης των τρωτοτήτων του κυβερνοϊστού σε επίπεδα software, επίσης, μιας προσπάθειας απομείωσης των κυβερνοαπειλών με τη συνεργασία της κοινότητας του law enforcement, ζ) μιας ενθάρρυνσης του τομέα έρευνας / ανάπτυξης τεχνικών κυβερνοπροστασίας, η) μιας υιοθέτησης επιμορφωτικών / εκπαιδευτικών περίξ του αντικειμένου προγραμμάτων, θ) μιας ενδυνάμωσης συνεργατικών τάσεων μεταξύ Υπηρεσιών ανά τον κόσμο, οργανισμών, βιομηχανικών συμπλεγμάτων κ. λ. με σκοπό την επίρρωση της έννοιας «κυβερνοασφάλεια» σε παγκόσμια βάση, ι) μιας ενσωμάτωσης της έννοιας «κυβερνοασφάλεια» εντός της ευρύτερης της «εθνικής ασφαλείας».⁴⁴

⁴³ ...που ουσιαστικά αποτελεί ανάλυση και σύνθεση της Homeland Security Act του 2002, της Homeland Security Presidential Directive -7 και της National Strategy to Secure Cyberspace του 2003 -περί των συγκεκριμένων κειμένων ανέτρεξε αντιστοίχως στους ιστοτόπους http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf> και https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf εις τους οποίους καταφύγαμε την 25^η Αυγούστου 2015

⁴⁴ Powner D., “Critical Infrastructure Protection. DHS Needs to Better Address its Cybersecurity Responsibilities” στο *Cybersecurity, Cyberanalysis and Warning*, ό. π., σ. 70-71. Επικουρικά βλέπε U.S. GAO (2005a), *Critical Infrastructure Protection. Department of Homeland Security Faces*

Τον Ιούνιο του 2003 το DHS λαμβάνοντας υπόψη το *National Strategy to Secure Cyberspace* (Φεβρουάριος 2003) και την *Homeland Security Act* του 2002 ⁴⁵ δημιουργεί το National Cyber Security Division -NCSA. Εντός των αρμοδιοτήτων / υποχρεώσεων του NCSA περιλαμβάνεται ο έλεγχος / ανάλυση του κυβερνοχώρου, η περί σχετικών απειλών προειδοποίηση, η βελτίωση της πληροφοριακής συνεργασίας, η έγκαιρη αντίδραση σε περιπτώσεις συμβάντων, η επικουρία στην αποκατάσταση επισφαλειών εθνικού κόστους τη στιγμή που συνεισφέρει, επιπλέον, στην επικοινωνία και συνεργασία μεταξύ οργάνων της ομοσπονδιακής κυβέρνησης των ΗΠΑ και του βιομηχανικού συμπλέγματος. Το NCSA κατά τους John W. Rittinghouse και William M. Hancock εντέλλεται αναγνώρισης, ανάλυσης, απομείωσης κυβερνοαπειλών, διανομής πληροφόρησης επικείμενων συμβάντων, συντονισμού ως προς την αντιμετώπιση αυτών, παροχής τεχνικής υποστήριξης και σχεδιασμού ανάρρωσης κατόπιν κυβερνοεπιθέσεων. Κατ' ουσία το Division οργανώνεται γύρω από τρία τμήματα με σκοπό: α) την αναγνώριση κινδύνων, την απομείωση τρωτοτήτων κυβερνητικών cyber assets, την ενημέρωση κρατικών και ιδιωτικών φορέων, β) την επιτήρηση του Cyber Security Tracking, Analysis, and Response Center -CSTARC αποστολή του οποίου δεικνύει η ανίχνευση / αντίδραση έναντι δικτυακών περιστατικών και κυβερνοαπειλών, ο συντονισμός μεταξύ ομοσπονδιακών, πολιτειακών, τοπικών, ιδιωτικών αλλά και διεθνών φορέων, γ) την εκπόνηση, σε συνεργασία με συναφείς Υπηρεσίες, επιμορφωτικών προγραμμάτων περί την κυβερνοπροστασία όπως και την επίρρωση της συνεργασίας μεταξύ κυβερνητικών, επιχειρηματικών, ακαδημαϊκών και λοιπών παραγόντων.⁴⁶

Περαιτέρω, το DHS είναι υπεύθυνο για τη λειτουργία του National Cyberspace Security Response System (NCSRS) προκειμένου ανάλυσης δεδομένων / προειδοποίησης απειλών, διαχείρισης περιστατικών εθνικής σπουδαιότητας, προστασίας κυβερνητικών συστημάτων και κρίσιμων υποδομών, ροής και διασποράς πληροφοριών μεταξύ οργάνων που εντέλλονται στην ασφάλεια του κυβερνοχώρου. Το NCSRS αφορά / επικουρεί τόσο κυβερνητικούς όσο μη κυβερνητικούς οργανισμούς / τομείς όπως, π. χ., τα Private Sector Information Sharing and Analysis Centers (ISAC's). Αν η λειτουργία του NCSRS συνθέτει την πρώτη (I) από τις πέντε προτεραιότητες / στοχεύσεις του *The National Strategy to Secure*



Εικόνα 26: Ανάλυση (analysis) και διασπορά (warning) πληροφόρησης εντός του επιχειρησιακού κύκλου του NCSRS -οι ομοιότητες με τον παραδοσιακό κύκλο της πληροφόρησης είναι φανερές. Η φωτογραφία ελήφθη από το *The National Strategy to Secure Cyberspace* του 2003, σ. 21

Challenges in Fulfilling Cybersecurity Responsibilities, May 2005 στη διαδικτυακή τοποθεσία <http://www.gao.gov/new.items/d05434.pdf> όπου καταφύγαμε την 26^η Αυγούστου 2015

⁴⁵ *The Homeland Security Act of 2002*, έγγραφο διαθέσιμο και στη διαδικτυακή τοποθεσία http://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf στην οποία καταφύγαμε τη 13^η Νοεμβρίου 2015

⁴⁶ Rittinghouse W., John, Hancock M., William, *Cybersecurity Operations Handbook*, Elsevier, Inc., USA, 2003, σ. 602-603

Cyberspace (2003), υπάρχουν άλλες τέσσερες, όλες υπό το συντονισμό του DHS. Κοινός τόπος αυτών δεν είναι κάτι διάφορο από τη διευθέτηση ζητημάτων εθνικής (II, III, IV) αλλά και διεθνούς κυβερνοασφαλείας (V) με την τελευταία να επαφίεται σε μια προοπτική συνεργασίας και ανταλλαγής πληροφοριών.⁴⁷

Το 2002 η αμερικανική νομοθεσία εμπλουτίζεται με τη Federal Information Security Management Act -FISMA. Η συγκεκριμένη Πράξη απευθυνόμενη σε ομοσπονδιακούς οργανισμούς και σε εξωτερικούς συνεργάτες επιχειρεί να εισάγει: α) ένα πλαίσιο ελέγχου αποτελεσματικότητας των μέτρων πληροφοριακής ασφαλείας ειδικά όταν αυτά σχετίζονται με ομοσπονδιακές επιχειρήσεις, β) ένα πλαίσιο προστασίας των ομοσπονδιακών πληροφοριών και των πληροφοριακών συστημάτων, γ) έναν μηχανισμό επίβλεψης των πληροφοριακών προγραμμάτων ασφαλείας των κυβερνητικών Υπηρεσιών, δ) έναν μηχανισμό αναγνώρισης / απελευθέρωσης συστημάτων πληροφοριακής ασφαλείας με σκοπό την εμπορική τους χρήση.⁴⁸ Σημειώνουμε πως το DHS ανταποκρινόμενο στις απαιτήσεις της νομοθεσίας αναλαμβάνει: α) την επίβλεψη των πολιτικών κυβερνοασφαλείας σε ομοσπονδιακό επίπεδο, β) την δυνητική επικουρία στην εφαρμογή αυτών των πολιτικών, γ) την επίβλεψη κυβερνητικών οργανισμών ως προς τη συμμόρφωσή τους σε επιμέρους απαιτούμενα της FISMA, δ) την καταγραφή της ανταπόκρισης αυτών των οργανισμών έναντι κυβερνοσυμβάντων όπως και την επίβλεψη των σχετικών επιχειρήσεων κυβερνοασφαλείας, ε) την επικουρία των τελευταίων.⁴⁹

Το αμερικανικό National Research Council ενσωματώνοντας προτάσεις του Defense Science Board και της President's Commission on Critical Infrastructure Protection ευελπιστεί όπως το φαινόμενο των κυβερνοαπειλών αντιμετωπιστεί μέσω δεκατριών δράσεων, ήτοι: α) συλλογή, ανάλυση και διασπορά πληροφοριών σχετικών με στρατηγικές απειλές κατά υπολογιστικών / πληροφοριακών συστημάτων, β) καταγραφή υπόπτων κινήσεων στον κυβερνοχώρο και απόδοση ειδοποίησης στους εν δυνάμει θιγομένους, γ) αναγνώριση εισβολέων, δ) έλεγχο αδυναμιών κυβερνοασφαλείας, ε) κλιμακούμενο, σε σχέση με την ένταση και την ποιότητα, πλάνο αντιμετώπισης κυβερνοαπειλών, στ) συντονισμένη αμυντική ενδοοργανική διαδικασία, ζ) συνεργασία μεταξύ κρατικών οργανισμών (civilian authorities) και εξωτερικών προμηθευτών (commercial providers), η) παρουσία από την πρώτη στιγμή ειδικών στα συστήματα προστασίας networks των οργανισμών που επιθυμούν να τα εντάξουν στην υπηρεσία τους, θ) παρακολούθηση, εκτίμηση και κατανόηση λειτουργίας των αμυντικών και επιθετικών πληροφοριακών τεχνολογιών, ι) συνεχή έρευνα περί αμυντικών πληροφοριακών τεχνολογιών, ια) αναβάθμιση ασφαλείας πληροφοριακών συστημάτων, ιβ) υιοθέτηση αυστηρών τεχνικών και

⁴⁷ Πρόκειται για πέντε projects ήτοι, το National Cyberspace Security Response System (I), το National Cyberspace Security Threat and Vulnerability Reduction Program (II), το National Cyberspace Security Awareness and Training Program (III), το Securing Governments' Cyberspace (IV) και το National Security and International Cyberspace Security Cooperation (V) -περί τούτων βλέπε U.S. President, *The National Strategy to Secure Cyberspace*, Φεβρουάριος 2003, σ. 19-52, διαθέσιμο στο https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf όπου καταφύγαμε τη 13^η Νοεμβρίου 2015

⁴⁸ Kostopoulos K. George, *Cyberspace and Cybersecurity*, Taylor and Francis Group, LLC, USA, 2013, σ. 161

⁴⁹ Βλέπε στο δικτυακό τόπο <http://www.dhs.gov/federal-information-security-management-act-fisma> όπου καταφύγαμε την 20^η Σεπτεμβρίου 2015

διαδικαστικών standards, ιγ) ανάπτυξη / αξιοποίηση εργαλείων / κριτηρίων εκτίμησης επιπέδου ασφαλείας.⁵⁰

Τα ίδια λίγο έως πολύ προτείνονται στην επανεπιβεβαιωμένη από τον πρόεδρο Barack Obama *Comprehensive National Cybersecurity Initiative -CNCI* του 2009. Αυτά που, μεταξύ άλλων, επισημαίνονται σχετίζονται με προτροπή ανάπτυξης: α) ενός mega-κυβερνητικού πλάνου κυβερνο-αντικατασκοπίας, β) ενός σχεδιασμού ασφαλείας διαβαθμισμένων δικτύων εθνικού ενδιαφέροντος, γ) ενός εκτεταμένου προγράμματος κυβερνο-εκπαίδευσης στον δημόσιο και ιδιωτικό φορέα, δ) μιας διεθνούς διαδικασίας ανάλυσης ρίσκου οικονομικών / εμπορικών συναλλαγών μέσω networks και ε) ενός κυβερνητικού ρόλου προς επίρρωση / επέκταση της έννοιας της κυβερνοασφαλείας εντός κρίσιμων κρατικών και μη κρατικών υποδομών και πόρων (critical infrastructures and key resources -CIKR).⁵¹ Ο ίδιος στα *National Security Strategy* των ετών 2010 και 2015 τονίζει πως η κυβερνοασφάλεια αντιπροσωπεύει κομμάτι της εθνικής ασφαλείας και απαιτούμενο αγαθό δημόσιας και οικονομικής ευταξίας. Οι κίνδυνοι εκπορεύονται τόσο από μεμονωμένους hackers όσο από οργανωμένα εγκληματικά κυκλώματα, από τρομοκρατικά δίκτυα ή προηγμένα κράτη.⁵² Η ανίχνευση, η αποτροπή / παρεμπόδιση, η επαναφορά συστημάτων έπειτα από επίθεση απαιτούν επενδύσεις σε έμψυχους και υλικοτεχνικούς πόρους, τη συνεργασία κυβερνητικού και ιδιωτικού φορέα εντός και εκτός χώρας, την εναρμόνιση εθνικής και διεθνούς νομικής πρακτικής.⁵³

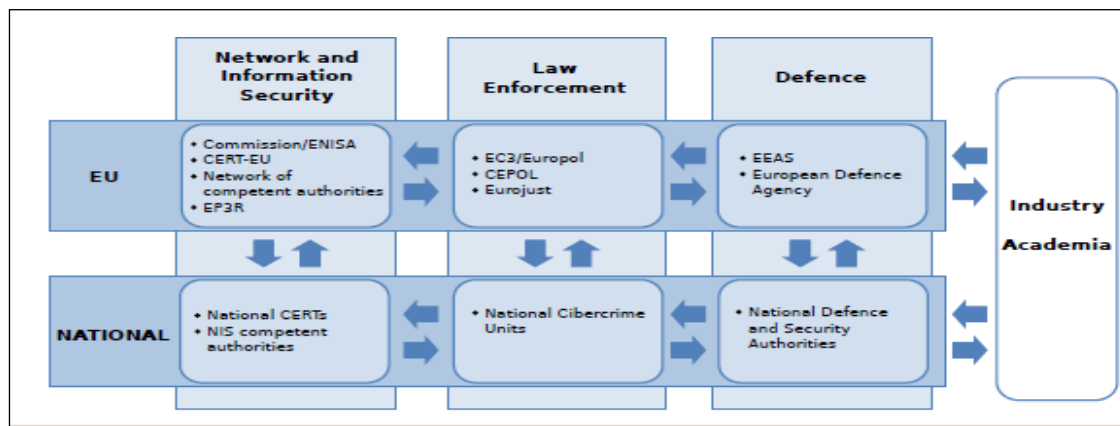
Από τη μεριά της η Ευρωπαϊκή Ένωση προσπαθεί να συμπλήξει τομείς με διαφορετικές υπευθυνότητες / δικαιοδοσίες τόσο σε εθνικό όσο σε υπερεθνικό επίπεδο με στόχο μια ικανή στρατηγική / δράση κυβερνοασφαλείας· κάτι τέτοιο συχνά δεν είναι εφικτό. Το βάρος πέφτει στους πυλώνες: α) της δικτυακής και πληροφοριακής ασφαλείας (Network and Information Security -NIS), β) των law enforcement υπηρεσιών και γ) της άμυνας (defence). Ο πρώτος πυλώνας εξυπηρετείται (και) από το European Network and Information Security Agency -ENISA και το ευρωπαϊκό Computer Emergency Response Team -CERT, ο δεύτερος από τη Europol και το European Police College ή, αλλιώς, Collège Européen de Police -CEPOL, ο δε τρίτος από το European External Action Service -EEAS και τη European Defence Agency -EDA.

⁵⁰ Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council, *Cybersecurity. Today and Tomorrow. Pay Now or Pay Later*, National Academy Press, Washington, D.C., 2002, σ. 25-31

⁵¹ Executive Office of the President of The U.S., *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, Executive Office of the President of The U.S., *The Comprehensive National Cybersecurity Initiative*, 2009, έγγραφα διαθέσιμα αντιστοίχως στους ιστοτόπους https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf και <https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf> στους οποίους μεταβήκαμε την 23^η Σεπτεμβρίου 2015. Βλέπε επίσης στο <http://acqnotes.com/acqnote/careerfields/cyberspace> όπου ανατρέξαμε την 27^η Σεπτεμβρίου 2015, ειδικότερα, δε, στο *Strategy for Operating in Cyberspace*, DoD, Ιούλιος 2011

⁵² Π. χ., τον Αύγουστο του 2003 ο ιός Blaster μολύνοντας περισσότερους από 500.000 υπολογιστές υποχρεώνει κάποια στιγμή την CSX Corporation να προβεί σε αναστολή των δρομολογίων των τρενών της. Προβλήματα επίσης προκαλούνται σε αρκετές αεροπορικές εταιρείες. Ελάχιστα αργότερα κτυπά ο ιός SoBig με «θύματα» 570.000 υπολογιστές -για περισσότερες πληροφορίες βλέπε *Strategic Survey 2003 / 2004. An Evaluation and Forecast of World Affairs*, International Institute for Strategic Studies / Oxford University Press, Oxford, 2004, σ. 51

⁵³ U.S. President, *National Security Strategy*, Washington, D.C., Μάιος 2010, σ. 27, U.S. President, *National Security Strategy*, Washington, D.C., Φεβρουάριος 2015, σ. 12-13



Εικόνα 27: Οι τρεις ευρωπαϊκοί πυλώνες αντιμετώπισης κυβερνοαπειλών. Η εικόνα έχει αντιγραφεί από το *Critical Infrastructure Protection: Threats, Attacks and Countermeasures*, σ. 8

Παρά το ότι μνεία σε Υπηρεσίες δεν γίνεται, η πληροφόρηση αποτελεί στοιχείο και σ' αυτήν την περίπτωση. Ανατρέχοντας στις επίσημες ιστοσελίδες πολλών εκ των ανωτέρω δομών διαπιστώνουμε ότι μεταξύ των αρμοδιοτήτων περίοπτη θέση κατέχει η συλλογή πληροφοριών. Η βέλτιστη διανομή των τελευταίων στους κατάλληλους δέκτες δεικνύει επίσης ζητούμενο. Η πληροφοριακή κουλτούρα συμπληρώνεται το 2013 όταν εντός της Europol δημιουργείται το European Cyber Crime Center -EC3 με σκοπό τη συλλογή, ανάλυση και διασπορά πληροφορίας προς καταπολέμηση του κυβερνοεγκλήματος. Εν κατακλείδι, η ευρωπαϊκή στρατηγική κυβερνοασφαλείας υιοθετεί τη συνεργασία σε επίπεδο πληροφοριών, πρωτίστως μεταξύ του ENISA, της Europol / EC3 και της EDA όπως μεταξύ αυτών και αντιστοίχων οργανισμών σε περιφερειακό επίπεδο, μάλιστα, το ENISA διατηρεί λίστα παρουσίας εθνικών στρατηγικών διαδικτυακής ασφαλείας.⁵⁴

Αναφορικά με την επιμέρους στρατηγική των ευρωπαϊκών κρατών σημειώνουμε πως μάλλον δεν αλλάζει κάτι ιδιαιτέρως σε σχέση με την στρατηγική της Ένωσης. Εξαιρώντας τις προσπάθειες ανάπτυξης τεχνικών αντιμέτρων, την ειδική ή μη επιμόρφωση, τις κοινές ή μη ασκήσεις ετοιμότητας, τη συνεργατική πολιτική, τη νομοθεσία κ. λ., κράτη-μέλη όπως η Γερμανία, η Γαλλία, η Βρετανία και η Ιταλία επενδύουν στην αξιοποίηση της κρυφής πληροφορίας αφού αυτή περάσει μέσα από

⁵⁴ *Critical Infrastructure Protection: Threats, Attacks and Countermeasures*, επιμ. Montarani Luca, Querzoni Leonardo, Tenace Prin Project, Italian Ministry of Education, University and Research, Μάρτιος 2014, σ. 8-9, επίσης, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, European Commission, 2013, διαθέσιμο και στο http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf όπου ανατρέξαμε την 26^η Νοεμβρίου 2015. Από και πέρα προσπάθειες όπως αυτή του 2001 Council of Europe Convention on Cybercrime (βλέπε στο http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf εις το οποίο καταφύγαμε την 28^η Οκτωβρίου 2016) ή οργανισμών όπως ο The Organization of Economic Cooperation and Development (OECD) / Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ή ο The Organization for Security and Cooperation in Europe (OSCE) / Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ) συμβάλλουν στην αντιμετώπιση του προβλήματος -για μια εικόνα βλέπε αντιστοίχως στις ιστοσελίδες <http://www.oecd.org/internet/ieconomy/40761118.pdf> και <http://www.osce.org/fsc/49775> εις τις οποίες ανατρέξαμε επίσης την άνω ημερομηνία. Για περισσότερες λεπτομέρειες περί της σχετικής ευρωπαϊκής πολιτικής / στρατηγικής βλέπε Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, ό. π., σ. 29-36

τα φίλτρα είτε των αρχών επιβολής νόμου και των συνακόλουθων αρχών ασφαλείας, είτε των μυστικών υπηρεσιών.⁵⁵

Από κει και πέρα υπάρχουν διαπιστώσεις που πρέπει να ληφθούν υπόψη, ειδικότερα: α) το επίπεδο προστασίας των ευρωπαϊκών οργανισμών από επιθέσεις κυβερνοπειρατών θεωρείται σχετικά χαμηλό, β) η ευρωπαϊκή πολιτική κυβερνοασφαλείας ερείδεται στην ύπαρξη πλήθους οργανισμών με την απουσία, εντούτοις, ενός κέντρου συντονισμού / αποφάσεων να καθίσταται φανερό, γ) η ευρωπαϊκή Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας / ΚΕΠΠΑ (Common Foreign and Security Policy -CFSP) φαίνεται να αγνοεί ζητήματα κυβερνοασφαλείας όπως και χρήσης κυβερνοϊσχύος, δ) οι ευρωπαϊκές πρωτοβουλίες κυβερνοπροστασίας σχεδόν αγνοούν τη δράση μη κρατικών φορέων, ε) η ευρωπαϊκή νομοθεσία περί κυβερνοχώρου πάσχει, στ) όλοι οι ευρωπαϊκοί οργανισμοί οφείλουν να αυξήσουν τα επίπεδα της πληροφοριακής ασφάλειάς τους (information assurance -IA), ζ) πρέπει να διασαφηνιστούν οι ρόλοι οργάνων όπως το Political and Security Committee -PSC, το Committee on Operational Cooperation on Internal Security -COSI, το Council Security Committee -CSC κ. λ., η) οι ευρωπαϊκοί θεσμοί οφείλουν να κατανοήσουν τη σημαντικότητα της ανταλλαγής πληροφοριών και της συνεργασίας κρατικών και ιδιωτικών φορέων (Public-Private Partnerships -PPP) σε μια κίνηση επίρρωσης κυβερνοασφαλείας, θ) το Ευρωπαϊκό Κοινοβούλιο οφείλει να εμπλακεί ενεργητικότερα στο όλο θέμα.⁵⁶

Το 2009 ο τότε DNI, Dennis C. Blair, καταθέτει ενώπιον του Κογκρέσου ότι «η όλο και πιο φανερό σχέση / σύνδεση μεταξύ πληροφοριακών συστημάτων, διαδικτύου και διαφόρων κρίσιμων υποδομών δίδει ευκαιρία στους όποιους επιτιθέμενους να αποδιοργανώσουν τη λειτουργία υπηρεσιών παροχής τηλεπικοινωνιών, ηλεκτρικής ενέργειας, χρηματοοικονομικών διεκπεραιώσεων κ. λ.». Προσθέτοντας σ' αυτές τις υπηρεσίες / οργανισμούς τις ένοπλες δυνάμεις και τις πολιτικές δομές μιας χώρας κατανοούμε το ενδιαφέρον των ανά τον κόσμο κρατών στην ανάπτυξη αμυντικών / επιθετικών κυβερνοεργαλείων όπως κατανοούμε και τη συμμετοχή των 'πρακτόρων' στο πεδίο.⁵⁷ Από την Presidential Decision Directive 63 (PDD 63), *Critical Infrastructure Protection* του Μαΐου του 1998⁵⁸, το *The National Strategy to Secure Cyberspace* του 2003, την Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization and Protection* του 2003⁵⁹ μέχρι την CNCI του 2009, η έγνοια είναι συγκεκριμένη αφορώντας στο συντονισμό κρατικών δομών, Υπηρεσιών και ιδιωτικού τομέα προκειμένου «να εξαλειφθεί κάθε σημαντική τρωτότητα που ανακινεί φιλοδοξίες φυσικών και δικτυακών επιθέσεων κατά κρίσιμων υποδομών και οικείων κυβερνοσυστημάτων». ⁶⁰ Ειδικότερα η CNCI επιχειρεί μια σύγκληση / συνεργασία

⁵⁵ *Critical Infrastructure Protection: Threats, Attacks and Countermeasures*, ό. π., σ. 9-23, επίσης, Ariely Ad Gil, "Adaptive Responses to Cyberterrorism" στο *Cyberterrorism. Understanding, Assessment, and Response*, επιμ. Chen Tomas, Jarvis Lee, Macdonald Stuart, Springer, New York, 2014, σ. 180-181. Για περισσότερες λεπτομέρειες περί σχετικών κρατικών στρατηγικών βλέπε Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, ό. π., σ. 36-40

⁵⁶ Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, ό. π., σ. 41-47

⁵⁷ Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, 10 Μαρτίου 2009, σ. 39-40

⁵⁸ Βλέπε στο <http://fas.org/irp/offdocs/pdd/pdd-63.htm> εις το οποίο καταφύγαμε την 1^η Νοεμβρίου 2016

⁵⁹ Βλέπε στο <https://www.hsdl.org/?abstract&did=441950> εις το οποίο καταφύγαμε την 1^η Νοεμβρίου 2016

⁶⁰ Presidential Decision Directive 63, *Critical Infrastructure Protection*, Μάιος 1998, τμήμα II

μεταξύ των αμυντικών κυβερνοαποστολών, του law enforcement, της πληροφόρησης / αντιπληροφόρησης και των στρατιωτικών δομών προς απάντηση σε κάθε είδος κυβερνοαπειλών.⁶¹

Βάσει των άνω γραμμών καταφαίνεται η αναγκαιότητα συμμετοχής των υπηρεσιών Πληροφόρησης στο πόλεμο της κυβερνόσφαιρας παρά το αμφίβολο του αποτελέσματος. Αιτία δεν είναι άλλη από το αχανές και άγνωστο του περιβάλλοντος. Η ίδια αιτία καλεί προς εγρήγορση ετερόκλητους φορείς / τομείς από το κρατικό law enforcement και τις Υπηρεσίες μέχρι την ιδιωτική επιχειρηματικότητα υπό το πρίσμα της πολιτικής ασφαλείας. Πάρα ταύτα η έννοια της τελευταίας στον κυβερνοχώρο είναι μια πολύ σχετική, αόριστη, άπιαστη, ίσως, έννοια.

Ειδικότερα περί Ενόπλων Δυνάμεων και κυβερνοασφαλείας

Ο Michael Erbschloe συνδέοντας το κυβερνοδιάστημα με τον πληροφοριακό πόλεμο καταγράφει τις ενδεδειγμένες δράσεις των στρατιωτικών δομών σε περίπτωση πληροφοριακής επίθεσης. Σύμφωνα με τον συγγραφέα: α) η προστασία και η αδιατάρακτη λειτουργικότητα των σχετικών στρατιωτικών συστημάτων αποτελεί πρωταρχικό σκοπό των Υπηρεσιών, β) δεύτερη προτεραιότητα δεικνύει η ανάπτυξη αντιμέτρων πληροφοριακού χαρακτήρα, γ) τρίτη αποστολή συνθέτει η επιβολή των πολιτικών αρχών και των αρχών επιβολής νόμου με σκοπό την προστασία πληροφοριακών υποδομών κυβερνητικών και άλλων οργανισμών.⁶²

Ο Erbschloe σημειώνει ότι οι ένοπλες δυνάμεις, τουλάχιστον στις ΗΠΑ, ανταποκρίνονται κατά το μάλλον ή ήττον στα δύο πρώτα ζητούμενα χωρίς, ωστόσο, κάτι τέτοιο να φαίνεται για το τρίτο. Εάν αυτές, συνεχίζει, θελήσουν την εμπλοκή τους με το τελευταίο, τότε, οφείλουν να αναπτύξουν νέες οργανωτικές και μεθοδολογικές προσεγγίσεις⁶³ -οι συγκεκριμένες αποτυπώσεις κατά κύριο λόγο αφορούν στην στρατιωτική αντικατασκοπευτική οργάνωση και σχεδιασμό. Επιπλέον ο ερευνητής μη παραλείποντας να ασχοληθεί με το διεθνές περιβάλλον τονίζει τις δυσκολίες συνεργασίας έναντι συμβάντων πληροφοριακής επίθεσης ακόμα και εντός συμμαχιών όπως, π. χ., αυτής του NATO. Παρά το ότι εντοπίζει το δυσεπίλυτο του προβλήματος στην φύση του φαινομένου προτείνει: α) μια ενεργητικότερη συμμετοχή των ενδιαφερομένων σε διεθνή προγράμματα αντιμετώπισης συμβάντων πληροφοριακού πολέμου, β) την άμεση ενημέρωση κρατών-ών εκ μέρους κρατών-ών που δέχτηκε-αν επίθεση, γ) την εκπαίδευση αξιωματούχων των ενόπλων δυνάμεων και του law enforcement γύρω από συναφείς τεχνολογίες / υποδομές.⁶⁴ Ο μελετητής συγκεφαλαιώνοντας καταθέτει, αλήθεια είναι εντός ευρύτερης οπτικής και με αφορμή την αντιμετώπιση του παράνομου εμπορίου όπλων και της τρομοκρατίας, την ακόλουθη ατζέντα κινήσεων: α) οι στρατιωτικοί οργανισμοί οφείλουν να ορίσουν το είδος υποστήριξης που χρειάζονται από τη βιομηχανία πληροφοριακών, υπολογιστικών, ηλεκτρονικών και λοιπών παρεμφερών τεχνολογιών και συστημάτων -η σχετική βιομηχανία σχετίζεται με τον τομέα της εθνικής ασφάλειας παρά το γεγονός της διαμοιβής της με το ελεύθερο εμπόριο, β) πρέπει να βεβαιούται πως

⁶¹ *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, Μάρτιος 2009, σ. 4-5, διαθέσιμο στη δικτυακή τοποθεσία https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf εις την οποία καταφύγαμε την 1^η Νοεμβρίου 2016

⁶² Erbschloe M, *Information Warfare. How to Survive Cyber Attacks*, The McGraw-Hill Companies, USA, 2001, σ. 11

⁶³ ό. π., σ. 11-12

⁶⁴ ό. π., σ. 15

άτομα με ειδικευση στα στρατιωτικά πληροφοριακά συστήματα (ειδικότερα άτομα που πλέον ιδιωτεύουν) απέχουν υπόπτων δραστηριοτήτων, γ) οι φάκελοι / αρχεία εκπαίδευσης των ανωτέρω ατόμων πρέπει να διατηρούνται και να έρχονται σε γνώση των αρμοδίων αρχών σε περιπτώσεις εγκλημάτων στον κυβερνοχώρο, δ) σεσημασμένοι εγκληματίες / τρομοκράτες πρέπει να ελέγχονται κατά το δυνατό για ικανότητα χρήσης κυβερνοεργαλείων, ε) πολιτικές υπηρεσίες αλλά και ιδιωτικές εταιρίες οφείλουν τήρησης αυστηρού πρωτοκόλλου πρόσληψης ατόμων των οποίων τα καθήκοντα προβλέπουν πρόσβαση σε κυβερνητικά πληροφοριακά / υπολογιστικά συστήματα, διαβαθμισμένα αρχεία, προηγμένη τεχνολογία, στ) πολιτικοί / στρατιωτικοί οργανισμοί αλλά και ιδιωτικοί φορείς οφείλουν τήρησης υψηλών επιπέδων εμπιστευτικότητας ως προς τις δραστηριότητες που εμπλέκουν / απαιτούν χρήση πληροφοριακών / υπολογιστικών συστημάτων ώστε να μειωθούν οι πιθανότητες διαρροής πληροφοριών⁶⁵, ζ) ο (αμερικανικός) στρατός και οι law enforcement υπηρεσίες πρέπει να προετοιμασθούν προς αντιμετώπιση ενός ολοένα αυξανόμενου αριθμού ατόμων, ομάδων και κρατών που ενδεχομένως θελήσουν να δραστηριοποιηθούν στον κυβερνοχώρο με επίβουλο τρόπο, η) απαιτείται η χαρτογράφηση μεθόδων πληροφοριακού πολέμου επί μονίμου βάσεως. Ο (αμερικανικός) στρατός, οι υπηρεσίες Πληροφοριών όπως και οι law enforcement αρχές οφείλουν να παρακολουθούν τόσο τις κοινωνικές όσο και τεχνολογικές εξελίξεις σε χώρες με διάθεση επέκτασης του ευρύτερου high tech τομέα τους.⁶⁶

Από τη μεριά του ο Martin Libicki τονίζοντας τη συγγένεια των τεχνικών μεθόδων προστασίας στρατιωτικών και πολιτικών networks και αναφερόμενος στα πρώτα, μεταξύ άλλων, ελπίζει στην αποκάλυψη του σκοπού της όποιας επίθεσης προτείνοντας ταυτόχρονα τη χρήση της τακτικής της παραπλάνησης και την αξιοποίηση των Red Teams σε ασκήσεις ετοιμότητας.⁶⁷

Αν ο Libicki υποδεικνύει έμμεσα την αντικατασκοπία ως εργαλείο κυβερνοάμυνας, το *The National Military Strategy for Cyberspace Operations* του 2006 την ορίζει ως μια από τις πέντε οδούς επίτευξης των κυβερνοσκοπών του DoD με κύριο τη διατήρηση της στρατιωτικής στρατηγικής υπεροπλίας στον κυβερνοχώρο (military strategic superiority in cyberspace).⁶⁸ Σύμφωνα με το έγγραφο ο συντονισμός των αντικατασκοπευτικών υπηρεσιών του Department με άλλους

⁶⁵ Το γεγονός της σε ικανό βαθμό λειτουργικής εξάρτησης του Global Information Grid του αμερικανικού DoD από 'εργαλεία' που το τελευταίο δεν ελέγχει άμεσα επιφέρει μέγιστο πονοκέφαλο στις στρατιωτικές διοικήσεις των ΗΠΑ. Παραδείγματος χάριν, η συνεργαζόμενη με το DoD τηλεπικοινωνιακή εταιρία Sprint εμπορεύεται, μεταξύ άλλων, λογισμικά των οποίων κάποιες φορές, αν και υποστηρίζουν τη μεταφορά δεδομένων του DoD, δεν γνωρίζει την ταυτότητα των δημιουργών. Το Σεπτέμβριο του 2003 η Sprint ανακοινώνει την απόδοση δημιουργίας λογισμικών, κωδικών και σχετικών προϊόντων υποστήριξης υπολογιστικών / πληροφοριακών δικτύων στις εταιρίες EDS και IBM. Ωστόσο ρεπορτάζ του *Business Week online* το Μάρτιο του 2004 αποκαλύπτει πως οι δύο εταιρίες απασχολούν προγραμματιστές εκτός χώρας με ερωτήσεις τύπου «ποιοι πραγματικά αναπτύσσουν τα λογισμικά;» ή «ποια τα μέτρα διασφάλισης ως προς τις προθέσεις των offshore μισθοδοτούμενων προσώπων;» να ζητούν απαντήσεις -για μια άποψη βλέπε "Sprint Inks Outsourcing Pacts with EDS, IBM", *Dallas Business Journal*, 16 Σεπτεμβρίου 2003, "Programming Jobs are Heading Overseas by the Thousands. Is there a Way for the U.S. to Stay on Top?" αντιστοίχως στις διαδικτυακές τοποθεσίες <http://www.bizjournals.com/dallas/stories/2003/09/15/daily21.html> και <http://www.tatvasoft.com/outsourcing/2005/05/programming-jobs-are-heading-overseas.html> στις οποίες μεταφερθήκαμε την 6^η Νοεμβρίου 2015

⁶⁶ Erbschloe M, *Information Warfare. How to Survive Cyber Attacks*, ό. π., σ. 227-228, 266

⁶⁷ Libicki M., *Cyberdeterrence and Cyberwar*, RAND, Santa Monica, 2009, σ. 160-174

⁶⁸ Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, DoD, Washington, D.C., Δεκέμβριος 2006, σ. ix, διαθέσιμο επίσης στη διαδικτυακή τοποθεσία <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf> εις την οποία καταφύγαμε την 3^η Νοεμβρίου 2015

αντίστοιχους κυβερνητικούς όπως και με οργανισμούς law enforcement αποτελεί πολλαπλασιαστική ισχύς στη μάχη του κυβερνοδιαστήματος και, ειδικότερα, σ' αυτήν της κυβερνοασφάλειας.⁶⁹ Το *The Department of Defense Strategy for Counterintelligence in Cyberspace* (2009) επιχειρηματολογώντας υπέρ: α) μιας ενότητας προσπαθειών μέσω συγχρονισμού επιχειρήσεων (synchronize and deconflict) και τυποποίησης τακτικών, τεχνικών και διαδικασιών (tactics, techniques, procedures -TTP), β) μιας επαύξησης / βελτίωσης της αντικατασκοπευτικής ετοιμότητας στον κυβερνοχώρο μέσω υπηρεσιακών επιλογών / σχεδιασμών (κατάλληλο προσωπικό, εκπαίδευση) και γ) μιας αντικατασκοπευτικής στρατηγικής μέσω προκαθορισμένων πόρων αντιμετώπισης απειλών και αξιοποίησης πεδίων ερεύνης και τεχνολογίας,⁷⁰ ευελπιστεί όπως: α) ανιχνεύονται, αναγνωρίζονται, αποτρέπονται, εξουδετερώνονται, εκτιμώνται ή και αντιστρέφονται / αξιοποιούνται εκ μέρους του DoD απειλές ενυπάρχουσες στο κυβερνοδιάστημα⁷¹, β) προστατεύεται το πεδίο της πληροφορίας και της τεχνολογίας⁷², γ) προστατεύεται η ακεραιότητα των πληροφοριακών και αντιπληροφοριακών συστημάτων του DoD⁷³, δ) αποτρέπονται ξένες κυβερνήσεις από εκτέλεση επίβουλων κυβερνοσχεδιασμών κατά των ΗΠΑ⁷⁴, ε) επιτευχθεί μια περαιτέρω συνεργασία μεταξύ ΗΠΑ και συμμάχων προς μια αποδοτικότερη αντικατασκοπευτική δράση στον κυβερνοχώρο.⁷⁵

Το 2010 εμφανίζεται ένας νέος αμερικανικός στρατιωτικός οργανισμός υπό την ονομασία U.S. Cyber Command -USCYBERCOM με αποστολή την εκπόνηση, το συντονισμό και την εκτέλεση δράσεων προστασίας και διασφάλισης της λειτουργικότητας κάποιων ιδιαίτερος ευαίσθητων πληροφοριακών δικτύων του DoD. Ακολουθεί η διεξαγωγή στρατιωτικών επιχειρήσεων ολικού φάσματος (full spectrum) στον κυβερνοχώρο με σκοπό την επικουρία ενόπλων σχεδιασμών σε ξηρά, θάλασσα και αέρα όπως επίσης «τη διασφάλιση ελευθερίας κινήσεων, υπέρ των ΗΠΑ και των συμμάχων τους, στην κυβερνοσφαίρα και την ταυτόχρονη άρνηση μιας ανάλογης στους όποιους ανταγωνιστές» -ο εντυπωμένος αλγόριθμος (Message-Digest algorithm 5 MD5) 9ec4c12949a4f31474f299058ce2b22a στο έμβλημα της Υπηρεσίας δηλώνει ακριβώς αυτό. Η CYBERCOM φέρει σε επαφή τμήματα που επιλαμβάνονται κυβερνοϋποθέσεων από την Ενάτη Στρατιωτική Διοίκηση Διαχείρισης Σημάτων (Army's Ninth Signal Command) μέχρι τον Δέκατο Στόλο (Navy's Tenth Fleet). Η έδρα της CYBERCOM βρίσκεται δίπλα σ' αυτήν της NSA καταδεικνύοντας και σημειολογικά μια στενή σχέση, άλλωστε, κατά την περίοδο Μαΐου 2010 - Μαρτίου 2014 κοινή διοίκηση ασκούσε ο στρατηγός Keith Alexander⁷⁶ προτού τελικά αποπεμφθεί εξ αιτίας του σκανδάλου Snowden.

Το *Strategy for Operating in Cyberspace* του 2011 ορίζει πέντε βήματα επίτευξης κυβερνοασφαλείας με την έννοια της αντικατασκοπίας να κάνει εμφανή την παρουσία της σε τακτικό και στρατηγικό επίπεδο στο δεύτερο, τρίτο και τέταρτο στάδιο / βήμα. Εντός αυτών ανακαλύπτουμε κλασικές προκλήσεις (εντοπισμό, ανάλυση, αντιμετώπιση απειλών -βήμα 2), συνεργατικές δράσεις εθνικού χαρακτήρα

⁶⁹ Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, DoD, ό. π., σ. 15

⁷⁰ *The Department of Defense Strategy for Counterintelligence in Cyberspace*, DoD, Αύγουστος 2009, σ. vi

⁷¹ *ibid*

⁷² *ibid*

⁷³ *ibid*

⁷⁴ *ibid*

⁷⁵ *ibid*

⁷⁶ Singer W. P., Friedman Allan, *Cybersecurity and Cyberwar. What Everyone Needs To Know*, ό. π., σ. 133-134, επίσης, DoD, *Quadrennial Defense Review Report*, Φεβρουάριος 2010, σ. 38

(π. χ. του DoD με το DHS -βήμα 3), όπως και ανάλογες διεθνούς (μεταξύ DoD / ΗΠΑ και συμμάχων -βήμα 4).⁷⁷

The U.S. Cybersecurity Strategy

Strategic Initiative	Strategy	Outcome
Step 1	Treat cyberspace as an operational domain	Organize, train, and equip DoD can take full advantage of cyberspace's potential
Step 2	Employ new defense operating concepts	Protect DoD networks and systems
Step 3	Partner with other U.S. government departments and agencies and the private sector	Enable a whole-of-government cybersecurity
Step 4	Build robust relationships with U.S. allies and international partners	Strengthen collective cybersecurity
Step 5	Leverage the nation's ingenuity	Encourage an exceptional cyber workforce and rapid technological innovation

Εικόνα 28: Τα πέντε βήματα της αμερικανικής στρατηγικής κυβερνοασφαλείας. Η εικόνα ελήφθη από το *U.S. Security Strategy toward North Korea's Cyber Terrorism* του Sunny Lee, σ. 21⁷⁸

Τον Ιανουάριο του 2013 το DoD επανέρχεται μέσω του Defense Science Board και του *Resilient Military Systems and the Advanced Cyber Threat*. Πρόκειται για δεκαοκτάμηνη μελέτη που συμπεραίνει τόσο τη σοβαρότητα των κυβερνοαπειλών όσο τη μη βεβαιότητα επιτυχούς αντιμετώπισης κυβερνοεπίθεσης κατά κρίσιμων πληροφοριακών συστημάτων όταν αυτή εκπορεύεται από κάποιον επιδέξιο αντίπαλο που εκμεταλλεύεται τις πληροφοριακές δυνατότητές του.⁷⁹ Η ομάδα εργασίας έλαβε σε ενάμιση χρόνο πλήθος συνοπτικών ενημερώσεων / briefings από το DoD, την πληροφοριακή κοινότητα, την ακαδημαϊκή και επιστημονική ανάλογη, τον πολιτικό και οικονομικό χώρο καταλήγοντας, μεταξύ άλλων, στα εξής: α) η έννοια «κυβερνοαπειλή» καθίσταται ορισμένες φορές τόσο σοβαρή όσο η έννοια της «πυρηνικής απειλής», β) μέσω του κυβερνοχώρου ανοίγονται κανάλια εκμείωσης πληροφοριών σχετικών με κρίσιμες στρατιωτικές, βιομηχανικές / τεχνολογικές υποδομές που στηρίζουν την οικονομική και την ευρύτερη εθνική ασφάλεια, γ) η στρατηγική του DoD λόγω κερματισμού δράσεων καθίσταται επισφαλής ως προς την ικανότητα αντιμετώπισης της απειλής, δ) η αμερικανική πληροφοριακή κοινότητα

⁷⁷ *Strategy for Operating in Cyberspace*, DoD, Washington, D.C., Ιούλιος 2011, σ. 5-13, διαθέσιμο και στην διαδικτυακή σελίδα <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-050.pdf> όπου ανατρέξαμε την 3^η Νοεμβρίου 2015

⁷⁸ Lee Sunny, *U.S. Security Strategy toward North Korea's Cyber Terrorism*, έγγραφο παρουσιασθέν στο Dupont Summit (Science, Technology & Environmental Policy: Pressing Issues, Little Time) του Carnegie Institution for Science, Washington, D.C., Δεκέμβριος 2011 καθώς και στο 2012 MPSA Annual Conference, Σικάγο, Απρίλιος 2012

⁷⁹ Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, DoD, Washington, D.C., Ιανουάριος 2013, σ. ii

δεικνύει σχετική ανεπάρκεια στην αντιμετώπιση κυβερνοαπειλών κατά του DoD εκπορευομένων από ξένες μυστικές υπηρεσίες.⁸⁰

Προτάσεις / δράσεις έναντι δυνητικών κυβερνοαπειλών

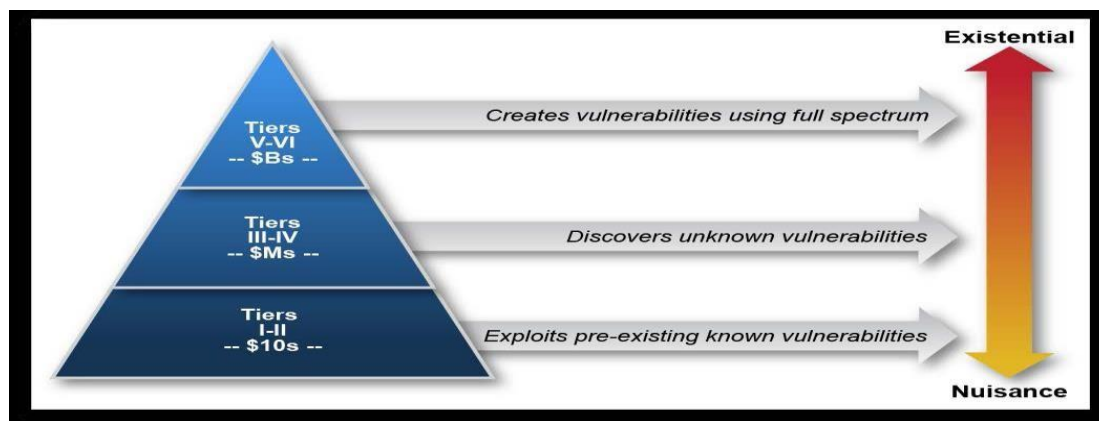
1 & 2	Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack). Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.
3	Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.
4	Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).
5	Enhance Defenses to Protect Against Low and Mid-Tier Threats.
6	Change DoD's Culture Regarding Cyber and Cyber Security.
7	Build a Cyber Resilient Force.

Εικόνα 29: Η εικόνα (τμήμα μεγαλύτερης) αντιγράφηκε από το *Resilient Military Systems and the Advanced Cyber Threat*, DoD, 2003, σ. 12

Ασφαλώς οι προτάσεις του ερευνητικού τμήματος, που συνοψίζονται στην άνω εικόνα, ως προς μια δυνητική λύση χαρακτηρίζονται από το στοιχείο της πληροφόρησης του οποίου εντονότερη αντανάκλαση εμπεριέχεται στην πρόταση 3. Κατά την ομάδα, είναι το DoD που σε συνεργασία με το DHS, το FBI και τη CIA οφείλει να πιέσει τον DNI προκειμένου αναβάθμισης των εργαλείων συλλογής και ανάλυσης πληροφοριών σχετικών με προηγμένες (high-end) κυβερνοαπειλές. Η πληροφόρηση (βλέπε Υπηρεσίες) οφείλει να συνεισφέρει στην αναγνώριση και κατανόηση των αντίπαλων προσπαθειών ανάπτυξης κυβερνοόπλων, των εργαλείων αυτών των προσπαθειών, της αντίπαλης ηγεσίας και των προθέσεων της. Πέραν τούτου οι πληροφοριακοί οργανισμοί καλούνται να αποδώσουν πληροφόρηση που θα συμβάλει στην αντιμετώπιση των δράσεων του ανταγωνιστή προκειμένου να εξοπλιστεί στο χώρο του κυβερνοδιαστήματος (counter cyber weaponization) βοηθώντας παράλληλα στην εκτίμηση εχθρικών πλάνων και δυνατοτήτων -σύμφωνα με τα ερευνητικά πορίσματα η άμυνα κατά απειλών επιπέδου tier V-VI (βλέπε παρακάτω) δεν μπορεί να τελεσφορήσει δίχως την καταλυτική παρουσία των Υπηρεσιών και ειδικά αυτών της Αντικατασκοπίας.⁸¹

⁸⁰ Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, DoD, Washington, D.C., Ιανουάριος 2013, σ. 1

⁸¹ ό. π., σ. 7-11, 47



Εικόνα 30: Τα τρία επίπεδα κυβερνοαπειλών κατά το *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, DoD, 2013, σ. 21

Στο *The DoD Cyber Strategy* του Απριλίου του 2015 επαναβεβαιώνεται η αποστολή του Department ως προς την προστασία των αμερικανικών συμφερόντων και της ενδοχώρας έναντι, γενικά, επιθέσεων όπως και, ειδικότερα, κυβερνοεπιθέσεων σε περίοδο ειρήνης, κρίσεως ή πολέμου, επίσης, επαναβεβαιώνεται μια ανάλογη αποστολή με σκοπό την προστασία του πληροφοριακού δικτύου του οργανισμού καθ αυτού και των πληροφοριακών του δεδομένων.⁸² Προσπαιτούμενο επιτυχίας συνθέτουν (και) τα εξής: α) μια συνεχόμενη ανάπτυξη δικτύων πληροφοριών και εγκαίρου προειδοποίησης. Το DoD δεσμεύεται όπως επεκτείνει / βελτιώσει τις οικείες δομές, συνεργασθεί, δε, με την ευρύτερη πληροφοριακή κοινότητα⁸³, β) μια ανάπτυξη αυτοματοποιημένων εργαλείων απόδοσης πληροφοριών σε κυβερνητικούς οργανισμούς, συμμάχους, επιλεγμένους ιδιωτικούς φορείς⁸⁴, γ) η εξαφάνιση, κατά το δυνατόν, κινδύνων εξ αιτίας εσωτερικών ρηγμάτων και διαρροών⁸⁵, δ) η επίτευξη συνεργατικότητας μεταξύ τμημάτων εσωτερικών / εξωτερικών Πληροφοριών και ανάλογων law enforcement με τους λεγόμενους *acquisition program managers* προς διαφύλαξη πληροφοριακών δεδομένων⁸⁶ -η δημιουργία του Joint Acquisition Protection and Exploitation Cell (JAPEC) κινείται σ' αυτήν την κατεύθυνση. Επιπλέον, το DoD οφείλει όπως προβαίνει σε εκτίμηση ρίσκων / επισφαλειών εξ αιτίας της ανταγωνιστικής κυβερνοκατασκοπίας με σκοπό, μεταξύ άλλων, τη βελτίωση των οικείων προγραμμάτων αντικυβερνοκατασκοπίας⁸⁷, ε) η εφαρμογή στρατηγικών μεγιστοποίησης της αποδοτικότητας της στρατιωτικής αντικατασκοπίας προς αναγνώριση και αντιμετώπιση κυβερνοαπειλών. Τα στρατιωτικά τμήματα CI κατέχοντας τα πλέον κατάλληλα εργαλεία ασφαλείας δύνανται να βελτιώσουν τη γνώση που σχετίζεται τόσο με την πράξη του cyberespionage όσο με την αντιμετώπισή του. Ο αντικατασκοπευτικός σχεδιασμός του DoD καλείται να συντονιστεί με τις αρχές επιβολής νόμου όπως και με τον ευρύτερο κύκλο των Υπηρεσιών κυρίως επί ζητημάτων έρευνας και μικτών, human / technical,

⁸² *The DoD Cyber Strategy*, DoD, Απρίλιος 2015, σ. 2, 7-8, 13-14

⁸³ ό. π., σ. 24

⁸⁴ ό. π., σ. 23

⁸⁵ ό. π., σ. 22

⁸⁶ Αναφερόμαστε στη συνεργασία μεταξύ οργανισμών Ασφαλείας / Πληροφόρησης με την επιστημονική / τεχνολογική κοινότητα με σκοπό την επίρρωση / επίτευξη στρατηγικών εθνικής ασφαλείας -για μια άποψη βλέπε DoD Directive 5000.01, *The Defense Acquisition System*, Μάιος 2003 (επανεπιβεβαίωση: Νοέμβριος 2007), επίσης, Brown Bradford, *Introduction to Defense Acquisition Management*, Defense Acquisition University Press, Fort Belvoir / Virginia, Αύγουστος 2010, σ. 1

⁸⁷ *The DoD Cyber Strategy*, DoD, Απρίλιος 2015, σ. 23

επιχειρήσεων προς ματαίωση σοφιστικές κυβερνοαπειλών έναντι των ΗΠΑ, συμμάχων ή συνεργαζομένων με αυτές-ούς μερών.⁸⁸

Οι Victoria Ekstedt, Tom Parkhouse και Dave Clemente αναφερόμενοι στο NATO υποστηρίζουν πως το Άρθρο 5, περί συλλογικής αμύνης, της συμμαχίας δύναται να ενεργοποιηθεί, επίσης, λόγω κυβερνοκινδύνων. Ωστόσο μια τέτοια θέση δεν βρίσκει άκοπα πρακτική απόδοση. Ότι νοείται ως «κυβερνοασφάλεια» ή «εθνική κυβερνοασφάλεια» συντίθεται από ενέργειες που αφορούν στην προστασία συγκεκριμένων πυλώνων (military cyber, cyber diplomacy and internet governance, Intelligence & Counterintelligence, critical information protection / crisis management). Η ικανοποίηση αυτής της φιλοδοξίας προβληματίζει⁸⁹ υπό την έποψη έλλειψης απτών διαχωριστικών γραμμών -αυτό αποδεικνύεται στην πράξη: η αρχική γνωριμία του NATO με τακτικές κυβερνοεπιθέσεων λαμβάνει χώρα το 1999 στη διάρκεια της επιχείρησης Allied Force κατά της Σερβίας. Γιουγκοσλάβοι και άλλων εθνικοτήτων hackers επιτίθενται κατά ιστοτόπων της Συμμαχίας.⁹⁰ Το αποτέλεσμα των επιθέσεων, ασφαλώς όχι ικανό να ταραξεί, ωθεί στην κατηγοριοποίησή τους: δεν πρόκειται για ενέργειες επίπτουσες στο military cyber αλλά στο cyber crime· καμιά εξ αυτών των ενεργειών δεν προκαλεί τη συλλογική δράση / άμυνα όπως αυτή μεταφράζεται ή ενδέχεται να μεταφραστεί εντός του Βορειοατλαντικού Συμφώνου. Το ίδιο συμβαίνει το 2007 στην περίπτωση της Εσθονίας: παρά την ποιοτική αναβάθμιση των επιθέσεων, το NATO επουδενί υιοθετεί μια στρατιωτική δράση ενεργοποιώντας το Άρθρο 5.⁹¹ ⁹² Μόλα ταύτα ο Οργανισμός αναγνωρίζει ένα έλλειμμα στην αντίδραση του 2007 επιζητώντας την επέκταση των δυνατοτήτων του στον χώρο του κυβερνοδιαστήματος.⁹³ Σ' αυτό το σημείο εγείρεται το ερώτημα: *τι σημαίνει, επιχειρησιακά, συλλογική δράση / άμυνα στον κυβερνοχώρο;* Η απάντηση βρίσκεται στις σελίδες 183 / 184 του *National Cyber Security. Framework Manual* όπου, μεταξύ πολλών άλλων, μνημονεύεται η ανάπτυξη ομάδων που θα συνεργαστούν με το NATO ή με μέλη του NATO σε θέματα κυβερνοασφαλείας και πληροφοριών. Ως παράδειγμα δίδεται μια υποτιθέμενη αποστολή του Financial Services Information Sharing and Analysis Center (FS-ISAC) ή κάποιου στρατιωτικού συνδέσμου σε κάποια χώρα προκειμένου ανταλλαγής διαβαθμισμένων ή μη στοιχείων ή βοήθειας επί διαδικασιών που προάγουν την οικονομική ή στρατιωτική πληροφόρηση.⁹⁴ Με τη σειρά τους οι Jason Healey, Leendert van Bochoven και Klara Tothova Jordan συνιστούν τόσο μια βελτίωση στον τρόπο

⁸⁸ *The DoD Cyber Strategy*, DoD, Απρίλιος 2015, σ. 24

⁸⁹ Ekstedt V., Parkhouse T., Clemente D., "Commitments, Mechanisms and Governance" στο *National Cyber Security. Framework Manual*, ό. π., σ. 181-182

⁹⁰ Healey Jason, van Bochoven, Leendert, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, D.C, 2011, σ. 1-2

⁹¹ Ekstedt V., Parkhouse T., Clemente D., "Commitments, Mechanisms and Governance" στο *National Cyber Security. Framework Manual*, ό. π., σ. 182

⁹² Η ενεργοποίηση του Άρθρου 5 περί στρατιωτικής δράσεως προφανώς δεικνύει εσχάτη καταφυγή. Στο *Defending the Networks. The NATO Policy on Cyber Defense* του 2011 τονίζεται πως ...κάθε συλλογική αμυντική νατοϊκή απάντηση συνιστά πολιτική απόφαση εξαρτώμενη από το Βορειοατλαντικό Συμβούλιο [North Atlantic Council -NAC]. Το NATO επουδενί προδικάζει, χαρακτηρίζεται, δε, από ευελιξία κινήσεων περί των δράσεων που θα ενεργοποιηθούν ή όχι

⁹³ Ekstedt V., Parkhouse T., Clemente D., "Commitments, Mechanisms and Governance" στο *National Cyber Security. Framework Manual*, ό. π., σ. 182

⁹⁴ ό. π., σ. 183-184

διανομής της πληροφορίας εντός του Οργανισμού όσο και μια επένδυση στο θεσμό του Security Intelligence ήγουν, (και) της αντιπληροφόρησης.⁹⁵

Στο *Defending the Networks. The NATO Policy on Cyber Defense* αναφέρεται ότι κύριο ρόλο και έγνοια του NATO συνθέτει η προστασία τόσο των εσωτερικών networks όσο αυτών των χωρών-μελών υπό την προϋπόθεση πως τα τελευταία συμβάλουν στη εκτέλεση / επίτευξη των κεντρικών σκοπών του οργανισμού ήτοι, της συλλογικής άμυνας και της διαχείρισης κρίσεων.⁹⁶ Το paper εκτός των άλλων προτείνει: α) έναν σχεδιασμό προστασίας των κρίσιμων cyber assets τόσο του NATO όσο και των κρατών που συμμετέχουν σ' αυτό, β) την ανάπτυξη σχετικών συμπαγών αμυντικών μηχανισμών, γ) τον προσδιορισμό των ελαχίστων προαπαιτούμενων περί κυβερνοάμυνας τόσο σε κεντρικό (NATO) όσο σε τοπικό / κρατικό επίπεδο, δ) έναν μηχανισμό βοήθειας στα κράτη-μέλη με σκοπό την επίτευξη ενός μίνιμουμ επιπέδου κυβερνοασφαλείας αλλά και την απομείωση τρωτοτήτων σχετιζομένων με εθνικές κρίσιμες υποδομές, ε) τη βελτίωση των συστημάτων εγκαίρου προειδοποίησης (early warning) και επίγνωσης τρεχουσών καταστάσεων (situational awareness).⁹⁷

Τέλος, στη νατοϊκή Σύνοδο Κορυφής του Σεπτεμβρίου του 2014 (Ουαλία) τονίζεται ότι το ζήτημα της κυβερνοασφαλείας συνθέτει μέλημα συλλογικής αμύνης ισότιμο με άλλα (πολιτικής ασφαλείας, στρατιωτικής ασφαλείας κ. λ.). Η ανάγκη βελτίωσης του μηχανισμού απόδοσης πληροφόρησης επανέρχεται με σκοπό την προστασία των επικοινωνιακών και πληροφοριακών δικτύων⁹⁸ -ασκήσεις όπως η *Cyber Coalition* (2015, Ταρτού / Εσθονία) λαμβάνουν χώρα και με αυτό το σκοπό⁹⁹ τη στιγμή που ο στρατηγός Stéphane Abrial (NATO Supreme Allied Commander Transformation) το 2011 σε άρθρο του στους *The New York Times* γράφει πως προκειμένου αντιμετωπίσης κυβερνοαπειλών απαιτείται μια διεθνής συνεργασία διανομής πληροφοριών μεταξύ του εμπορικού, ακαδημαϊκού, κυβερνητικού και στρατιωτικού τομέα¹⁰⁰ -και εδώ επαναβεβαιώνεται ό,τι έχει ήδη καταγράψει.

Συμπεράσματα

Εκ των άνω κατατεθειμένων συνάγεται ότι η φιλοσοφία του cyber counterintelligence δεν διαφέρει από τη φιλοσοφία του κλασσικού counterintelligence, το ίδιο ισχύει λίγο ή πολύ μεταξύ στρατιωτικού και πολιτικού CCI. Αυτό που διαφοροποιεί την κλασσική αντικατασκοπία από την αντικατασκοπία που λαμβάνει χώρα στο κυβερνοπεριβάλλον έχει να κάνει ακριβώς με αυτό ήτοι, το περιβάλλον δράσης. Το κυβερνοδιάστημα δεικνύει ένα αχανές τοπίο εντός του οποίου κρύβονται μυστικά, παγίδες και επισφάλειες όπως συνήθως συμβαίνει σε κάθε άγνωστο κόσμο. Η απειρία

⁹⁵ Healey Jason, van Bochoven, Leendert, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, ό. π., σ. 7, Healey Jason, Jordan Tothova Klara, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, D.C, 2014, σ. 5-7

⁹⁶ *Defending the Networks. The NATO Policy on Cyber Defense*, NATO, 2011, διαθέσιμο και στο <https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf> όπου καταφύγαμε την 23^η Νοεμβρίου 2015

⁹⁷ *Defending the Networks. The NATO Policy on Cyber Defense*, NATO, 2011, ό. π.

⁹⁸ North Atlantic Treaty Organization, "Cyber security" στη διαδικτυακή τοποθεσία της Συμμαχίας http://www.nato.int/cps/en/natohq/topics_78170.htm την οποία επισκεφθήκαμε την 25^η Δεκεμβρίου 2015

⁹⁹ North Atlantic Treaty Organization, "Experts put to the test during NATO's largest annual cyber defence exercise" στο http://www.nato.int/cps/en/natolive/news_124868.htm?selectedLocale=en όπου καταφύγαμε την 25^η Δεκεμβρίου 2015

¹⁰⁰ Abrial Stéphane, "NATO Builds its Cyberdefenses", *The New York Times*, 27 Φεβρουαρίου 2011 στο <http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html> όπου ανατρέξαμε την 6^η Ιανουαρίου 2016

του ανθρώπου όσον αφορά στο τι είναι cyberspace επιβαρύνει την προσπάθεια επίτευξης ασφαλείας εντός αυτού. Εξ αιτίας της συγκεκριμένης πραγματικότητας γίνεται λόγος πολύ περισσότερο για συνεργασία μεταξύ φορέων (εθνικών, υπερεθνικών, πολιτικών, στρατιωτικών, δημοσίων, ιδιωτικών κ. λ.) παρά για δράση Υπηρεσιών. Κατά την έννοια τούτη πιθανολογούμε πως δεν υπάρχει ουσιαστική αντικατασκοπευτική πράξη στο κυβερνοδιάστημα καθώς το τελευταίο παραμένει αχαρτογράφητο. Αυτό για το οποίο κάνουμε λόγο σχετίζεται με νεοπαγείς σχεδιασμούς ασφαλείας, όπως ο όρος ‘ασφάλεια κυβερνοχώρου’ δύναται να εκληφθεί, παρά με κάτι συμπαγές όπως απαιτεί η πρακτική της αντικατασκοπίας.

Κεφάλαιο 9

Η κλήση του 21^{ου} αιώνα. CI, Homeland Security, Law Enforcement

Προκλήσεις / προβληματισμοί

Η ολοένα εξελισσόμενη παρουσία του εγκλήματος φαίνεται πως οδηγεί σε μια προσπάθεια επαναχάραξης του επιχειρησιακού σχεδιασμού των υπηρεσιών CI και law enforcement χωρίς αυτό να σημαίνει ότι παραμερίζονται παραδοσιακές ανησυχίες και καθήκοντα. Στα εισαγωγικά μέρη του *Law Enforcement Counterintelligence* του Lawrence Sulc καταγράφονται ορισμένες μορφές εγκληματικών ενεργειών, μεταξύ αυτών, εμπορία όπλων, ναρκωτικών, λευκής σαρκός, παραχάραξη χαρτονομισμάτων, ξέπλυμα χρήματος, το trafficking κ. λ. χωρίς ασφαλώς να παραλείπεται η τρομοκρατία. Οι αναφερόμενες κακόβουλες δραστηριότητες στη συντριπτική τους πλειοψηφία δεν αποτελούν φαινόμενο του 21^{ου} αιώνα, προϋπήρξαν. Πάρα ταύτα δύο νέα στοιχεία τις χαρακτηρίζουν. Το πρώτο σχετίζεται με την εισπήδηση / συγχώνευση της μίας με την άλλη τόσο σε τοπικό όσο σε διεθνές επίπεδο.¹ Το δεύτερο, που εμμέσως επισημαίνεται από τον Sulc, έχει να κάνει με τη μεταμόρφωση των μεγάλων εγκληματικών δικτύων σε *intelligence* ή, έστω, *intelligence-like forces*. Αν ισχύει κάτι τέτοιο κατανοούμε τόσο τους κινδύνους εθνικής ασφαλείας όσο την ανάγκη, πιθανότατα, εμπλοκής των υπηρεσιών Πληροφοριών και δη και αυτών της Αντικατασκοπίας στην καταδίωξη των συγκεκριμένων δικτύων ή, εναλλακτικά, της απόκτησης (αντι)πληροφοριακών δεξιοτήτων από τις υπηρεσίες επιβολής νόμου.²

Οι αστυνομικές αρχές και οι υπηρεσίες ασφαλείας ως homeland security services κατά το παράδειγμα των ΗΠΑ αντιπροσωπεύοντας τη γραμμή αμύνης έναντι εσωτερικών απειλών κάθε είδους κινούνται βάσει μεικτών σχεδιασμών. Ενσωματώνουν τόσο καθήκοντα επιβολής νόμου όσο και αντιμετώπισης καταστάσεων που, π. χ., δύνανται να υπονομεύσουν τη λειτουργία θεσμών, κρίσιμων κρατικών υποδομών, τη δημόσια υγεία ή ασφάλεια και κατ' επέκταση αυτήν την ίδια την έννοια της κοινωνικής ευταξίας και ασφάλειας. Κατά τον τρόπο τούτο το homeland security intelligence σχετίζεται και με την αντιμετώπιση του υψηλής έντασης σοφιστική εγκλήματος του οποίου τα πλοκάμια δύναται να απλωθούν πέραν των ορίων των εγκλημάτων του λεγόμενου «κοινού ποινικού κώδικα».^{3, 4}

¹ Περί σχετικών παραδειγμάτων βλέπε Lemieux Frédéric, “Financing Terrorism: Entrepreneurship, Business Strategies, and Moral Issues” και Mullins Sam, Dolnik Adam, “Relations between Violent Non-State Actors and Ordinary Crime” στο *Protecting the Homeland from International and Domestic Terrorism Threats: Current Multi-Disciplinary Perspectives on Root Causes, the Role of Ideology, and Programs for Counter radicalization and Disengagement*, επιμ. Fenstermacher Laurie, Rieger Tom, et al., 2010, σ. 208-217 και 219-225 αντιστοίχως

² Ο Sulc όχι μόνο αναγνωρίζει μια ανάγκη απόκτησης αντιπληροφοριακής κουλτούρας από την law enforcement κοινότητα αλλά επίσης προτείνει την εμπλοκή της αντικατασκοπίας στην καταπολέμηση ορισμένων μορφών εγκλήματος όπως και την εμπλοκή της αστυνομικής αρχής στην καταπολέμηση ορισμένων μορφών κατασκοπευτικής δράσης -για μια εικόνα βλέπε Sulc L., *Law Enforcement Counterintelligence*, Varro Press, USA, 1996, σ. vii-viii, 29-31. Πληροφοριακά περί διεθνικού οργανωμένου εγκλήματος (transnational organized crime -TOC) και law enforcement βλέπε Coyne John, Bell Peter, *The Role of Strategic Intelligence in Law Enforcement*, Palgrave Macmillan, 2015, σ. 13-22, επίσης, *United Nations Convention against Transnational Organized Crime*, United Nations Office of Drugs and Crime, UN, Geneva, 2000, σ. 25-26

³ Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, project υποστηριζόμενο από το U. S. Department of Justice / Office of Community Oriented Policing Services, USA, 2009, σ. 14-15

Το US National Intelligence Council έρχεται προς επιβεβαίωση των γραφομένων. Μεταξύ άλλων τονίζει ότι ...εγκληματικές οργανώσεις και δίκτυα με έδρα τη Βόρειο Αμερική, τη Δυτική Ευρώπη, την Κίνα, την Κολομβία, την Ιαπωνία, τη Ρωσία, το Ισραήλ, το Μεξικό και τη Νιγηρία θα αυξήσουν την ένταση, θα επεκτείνουν τους ορίζοντες των δραστηριοτήτων τους. Θα δομήσουν χαλαρές συμμαχίες μεταξύ τους, με μικρότερα εγκληματικά networks, με στασιαστικές ομάδες...⁵. Ο Gary Potter υποστηρίζει ότι το οργανωμένο έγκλημα⁶ στην Αμερική κατανοείται μόνο μέσα από μια δικτυακή προσέγγιση⁷ τη στιγμή που οι James Finckenauer και Elin Waring καταγράφουν τρόπους δράσης της ρωσικής μαφίας.⁸ Από τη μεριά της η γερμανική ΒΚΑ, αντίστοιχη του FBI, μιλά για την ανασύσταση των μεγάλων συμμοριών και της ιταλικής μαφίας⁹ -με άλλα λόγια, γράφει ο Phil Williams, μια δομική μεταβολή στο χώρο του διεθνούς εγκλήματος κάνει την εμφάνισή της.¹⁰ Η συγκεκριμένη μετεξέλιξη περνώντας ειδικά μέσα απ' τον κυβερνοχώρο παρέχει στις εγκληματικές εταιρίες: α) δυνατότητα κάλυψης / απόκρυψης της δράσης τους, β) ευχέρεια διαφυγής σε περίπτωση στοχοποίησης από τις law enforcement υπηρεσίες, γ) ευχέρεια αξιοποίησης των διαφόρων εθνικών νομικών πλαισίων και παραθύρων καθώς οι

⁴ Ιστορικά στην Αμερική οι περισσότερες ομοσπονδιακές law enforcement αρχές είχαν δημιουργήσει πληροφοριακούς τομείς προς αντιμετώπιση πολυπλόκαμων εγκληματικών οργανώσεων όπως η La Cosa Nostra υπό την έποψη της προστασίας της αμερικανικής κοινωνίας. Σε επίπεδο τοπικών αρχών κάτι τέτοιο δεν απετέλεσε προτεραιότητα αν και τα πράγματα δεν ήταν εξ αρχής έτσι. Κατά τη δεκαετία του 1920 πολλά πολιτειακά παραρτήματα επιβολής νόμου διατηρώντας τις περιφέρειες Red Squads επιτηρούσαν αναρχικά, εξτρεμιστικά, κομμουνιστικά και πολιτικώς ύποπτα στοιχεία. Με την πάροδο του χρόνου, την αποκάλυψη υπέρβασης εξουσιών και την επίρρωση των αστικών δικαιωμάτων αυτό άλλαξε, το πεδίο της εσωτερικής ασφαλείας εδώθη αποκλειστικά, χωρίς να αποφευχθούν εκ νέου διαμαρτυρίες, σε εθνικούς οργανισμούς με κυριότερο το FBI. Πάρα ταύτα η 11^η Σεπτεμβρίου επανακαθόρισε τους σχεδιασμούς με τα law enforcement τμήματα κάθε επιπέδου (πλέον των δέκα οχτώ χιλιάδων σε αριθμό) να επαναπροσανατολίζονται στην αντιμετώπιση κινδύνων όπως η τρομοκρατία ή η κατασκοπία -για περισσότερα βλέπε Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA, 2013, σ. 274-275

⁵ National Intelligence Council, *Global Trends 2015*, National Intelligence Council, Washington, D.C., Δεκέμβριος 2000, σ. 41, επίσης βλέπε Quiggin Thomas, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, World Scientific Publishing Co. Pte. Ltd, Singapore, 2007, σ. 18-20

⁶ Ο R. T. Naylor επισημαίνει τα κύρια χαρακτηριστικά του οργανωμένου εγκλήματος ήτοι, τη μόνιμη παρουσία του στην κοινωνία εν είδει «επιχείρησης» και την ικανότητά του να παράγει χρήμα σε αντίθεση με το κοινό έγκλημα που χαρακτηρίζεται από την ευκαιρία της στιγμής και την κατανάλωση του λεηλατημένου προϊόντος -για μια εικόνα βλέπε Naylor T. R., "Mafias, Myths and Markets" στο *Transnational Organized Crime*, 3(3), 1997, σ. 3. Κατά την έννοια τούτη το οργανωμένο έγκλημα απασχολεί κυβερνήσεις, κοινωνίες, αγορές. Σε ορισμένες περιπτώσεις εξελίσσεται σε κυρίαρχο δρόντα, διαπλέκεται με την πολιτική, μετατρέπεται σε κράτος εν κράτει, ταυτίζεται με το επιχειρηματικό "corporate" έγκλημα που ανθεί στις ευκατάστατες κοινωνίες -περί τούτων βλέπε van Duyne, Petrus C., "Organized Crime, Corruption and Power", *Crime, Law and Social Change*, 26, 1997, σ. 201-238, Warner M., "Intelligence as Risk Shifting", *Intelligence Theory. Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, London, UK, 2009, σ. 19-20, Gross J., "Trouble in Paradise", *British Journal of Criminology*, 43, 2003, σ. 64-67, Williams P., Godson R., "Anticipating Organized and Transnational Crime", *Crime, Law and Social Change*, 37, 2002, σ. 315-322, Slapper G., Tombs S., *Corporate Crime*, Harlow, London, 1999, σ. 54-84

⁷ Potter Gary, *Criminal Organizations: Vice Racketeering and Politics in an American City*, Waveland Press, Illinois / USA, 1993

⁸ Finckenauer James, Waring Elin, *Russian Mafia in America*, Northeastern University Press, Boston / USA, 1998

⁹ Federal Broadcast Information Service (CIA), "BKA Registers Less Damaged Caused by Gangs", *Frankfurter Rundschau*, 13 Ιουλίου 1998, σ. 3

¹⁰ Williams Phil, "Transnational Criminal Networks" στο *Networks and Netwars: The Future of Terror, Crime, and Militancy*, επιμ. Arquilla John, Ronfeldt David, RAND, Santa Monica, 2001, σ. 64

δραστηριότητες των δικτυακών εγκληματικών οργανώσεων μπορούν εύκολα να μεταναστεύσουν προς άγραν ευνοϊκότερου περιβάλλοντος.¹¹

Ο Williams προβλέποντας τις δυσκολίες που θα αντιμετωπίσουν οι διωκτικές αρχές εντός των νέων συνθηκών τονίζει μια ανάγκη επανασχεδιασμού των στρατηγικών τους. Στόχος η βελτίωση της διαδικασίας παραγωγής πληροφόρησης, η αρτιότερη διασπορά της μεταξύ αρμοδίων υπηρεσιών / αρχών, η παραγωγή παραπληροφόρησης με στόχο τον αποσυντονισμό των εγκληματικών κόμβων -εάν οι εξελίξεις τον δικαιώσουν, τότε, δικαιώνουν το λεγόμενο *intelligence-led policing / intelligence-led law enforcement* μοντέλο.¹²

Ο Robert Wallace τονίζει ότι counterintelligence σημαίνει ενσωμάτωση κάθε είδους στοιχείων προς ανάπτυξη και εκτέλεση στρατηγικής-ών υπέρ της προστασίας των κρατικών μυστικών *...in its broadest form, counterintelligence (CI) encompasses all elements required for developing and executing a strategy to protect a nation's secrets*, γράφει. Για την πλειοψηφία των Αμερικανών, συνεχίζει, μια διάσταση της αντικατασκοπίας υποστασιοποιείται στην πρόταση του κειμένου του U.S. Oath of Citizenship *...θα στηρίζω και θα υπερασπίζομαι το Σύνταγμα και τους νόμους των Ηνωμένων Πολιτειών της Αμερικής έναντι κάθε εχθρού, εξωτερικού και εσωτερικού...* Σύμφωνα με τον ερευνητή η συγκεκριμένη παραδοχή κατανοεί διασταλτικά το CI ως συνδυασμό law enforcement και στρατιωτικής αμυντικής δράσης εκτελούμενης μέσω οργάνων διαθετόντων αναλυτικών, ανακριτικών εργαλείων / εξουσιών που σχετίζονται με την προστασία και ασφάλεια του έθνους.¹³

Αν η άποψη Wallace εμπλέκει τις Υπηρεσίες στην καταδίωξη της τρομοκρατίας και του οργανωμένου εγκλήματος, υπάρχει αντίλογος. Σύμφωνα με την τυπολογία του David L. Carter τρία είδη intelligence καταγράφονται ήτοι, law enforcement intelligence, homeland security “all-hazards” intelligence και national security intelligence. Κατά τον ερευνητή το law enforcement intelligence (intelligence-led policing / intelligence-led law enforcement ή και *criminal intelligence*) αναφέρεται σε ευθύνες αστυνομικής φύσεως ήτοι, επιβολής νόμου. Ο ίδιος υποστηρίζει ότι law enforcement intelligence καλείται το προϊόν εκείνης της αναλυτικής πληροφοριακής διαδικασίας που φωτίζει αθέατες πτυχές / προοπτικές του εγκλήματος, των τάσεων

¹¹ Williams Phil, “Transnational Criminal Networks”, ό. π., σ. 71. Για μια ευρύτερη εικόνα περί δικτυακού εγκλήματος βλέπε “Cyber Crime - A Growing Challenge for Governments” στο *Issues Monitor*, Volume 8, Ιούλιος 2011, διαθέσιμο στην ηλεκτρονική τοποθεσία <https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf> όπου καταφύγαμε την 25^η Οκτωβρίου

¹² Williams Phil, “Transnational Criminal Networks”, ό. π., σ. 91-97. Ένας οργανισμός πρότυπο που μετέχει επιβοηθητικά στον intelligence-led law enforcement σχεδιασμό υπό την αιγίδα του US Department of the Treasury είναι ο FINCEN (Financial Crimes Enforcement Network). Σκοπός του η καταπολέμηση του οικονομικού εγκλήματος, του ξεπλύματος κεφαλαίων, της χρηματοδότησης της τρομοκρατίας. Εντός των καθηκόντων του περιλαμβάνεται (και) η αρχειοθέτηση πληροφοριών που μέσω τραπεζικών αναφορών (Cash Transaction Reports -CTRs, Suspicious Activity Reports -SARs) καταφθάνουν σ’ αυτόν -ο συγκεκριμένος φορέας συγκαταλέγεται στις λεγόμενες *οικονομικές πληροφοριακές μονάδες (Financial Intelligence Unit -FIU)*, δεν πρόκειται για αστυνομική αρχή. Ο ίδιος στις ιστοσελίδες που διατηρεί ορίζει την παρουσία του ως «σύνδεσμο μεταξύ law enforcement και οικονομικών ρυθμιστικών κοινοτήτων» και την αποστολή του ως «αποστολή προστασίας του οικονομικού συστήματος, καταπολέμησης του ξεπλύματος χρήματος, θωράκισης της εθνικής ασφαλείας μέσω συλλογής, ανάλυσης και διασποράς οικονομικής πληροφόρησης» -για περισσότερα βλέπε στους ιστοτόπους http://www.fincen.gov/about_fincen/www/faqs.html#money και <http://www.fincen.gov/> στους οποίους καταφύγαμε την 8^η Σεπτεμβρίου 2015

¹³ Wallace P., “A Time for Counterespionage” στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, USA, 2009, σ. 102

του αλλά και των εθνικών απειλών ασφαλείας.¹⁴ Ο Antony Antoniou κατηγοριοποιεί το law enforcement intelligence σε τρία επίπεδα ήτοι, το τακτικό, το επιχειρησιακό και το στρατηγικό. Το πρώτο σχετίζεται με επικείμενους κινδύνους, το δεύτερο με μελλοντικούς ανάλογους όπως και με έρευνες περί εγκληματικών οργανώσεων και το τρίτο με εκτιμήσεις περί της συνολικής / μελλοντικής πορείας του εγκλήματος.¹⁵ Κατά το Global Intelligence Working Group ως law enforcement intelligence ορίζεται ...η συλλογή και ανάλυση πληροφορίας (information) με σκοπό την παραγωγή πληροφορόρησης (intelligence) προς εξυπηρέτηση της [law enforcement] διαδικασίας λήψεως αποφάσεων σε τακτικό και στρατηγικό επίπεδο.¹⁶ Η International Association of Law Enforcement Intelligence Analysts υποστηρίζει ότι ...[law enforcement] intelligence σημαίνει πληροφορόρηση που παράγεται από την ανάλυση της συλλεγομένης πληροφορίας με σκοπό την ακριβέστερη κατανόηση ενός κακούργηματος, την αποκάλυψη του δράστη, την πρόβλεψη των μελλοντικών ροών του εγκλήματος αλλά και την παρεμπόδιση του τελευταίου μέσω εκπόνησης κατάλληλων σχεδιασμών.¹⁷ Η Commission on Accreditation for Law Enforcement Agencies σημειώνει ότι «ορισμένες σημαντικές δράσεις οφείλουν να στηρίζονται στην πληροφοριακή διαδικασία αξιοποιώντας μια διαρκή ροή πρωτογενών πληροφοριών που πρέπει να κατευθυνθεί σε έναν κεντρικό δέκτη». Περαιτέρω, τονίζεται η απαίτηση ενός συστήματος αποθήκευσης, ανάκτησης αλλά και διασποράς πληροφορόρησης.¹⁸ Το FBI (Directorate of Intelligence) τονίζει ότι ...intelligence στο law enforcement αλλά και στο national security business σημαίνει πληροφορόρηση γύρω από οντότητες που απειλούν τις Ηνωμένες Πολιτείες υπό την έποψη εκτέλεσης τρομοκρατικών ή άλλων κατά της κοινωνίας πράξεων.¹⁹ Τέλος στο *Navigating Your Agency's Path to Intelligence-Led Policing* της Global Justice Information Sharing Initiative αναφέρεται πως ...intelligence-led policing σημαίνει εργαλειοποίηση του πληροφοριακού κύκλου προς υποστήριξη της διαδικασίας λήψεως αποφάσεων με σκοπό την πρόληψη / αποτροπή του εγκλήματος. Βασικό προαπαιτούμενο επιτυχίας δεικνύει η ακριβής χαρτογράφηση των όποιων law enforcement προτεραιοτήτων.²⁰

¹⁴ Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, ό. π., σ. 9-12, επίσης βλέπε Carter David, *Law Enforcement Intelligence Operations*, 1990, σ. 1-7, διαθέσιμο στην ιστοσελίδα <https://www.ncjrs.gov/pdffiles1/Photocopy/134434NCJRS.pdf> εις την οποία καταφύγαμε τη 14η Οκτωβρίου 2016

¹⁵ Antoniou Antony, *Open Source Information. The Future of Intelligence*, European Intelligence Academy, E-Book, Number 1, Μάιος 2013, σ. 35-36

¹⁶ *National Criminal Intelligence Sharing Plan*, Global Intelligence Working Group, Office of Justice Programs, Washington, D.C., 2003, σ. 6

¹⁷ *Successful Law Enforcement Using Analytic Methods*, International Association of Law Enforcement Intelligence Analysts, Florida, 1996, σ. 1

¹⁸ Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, ό. π., σ. 13, επίσης βλέπε Association of Chief Police Officers (ACPO), *Introduction to Intelligence-Led Policing*, Centre for Policing Excellence, UK, 2007, σ. 3, Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, CRC Press, Florida, 2014, σ. 32-33 αλλά και *Standards for Law Enforcement Accreditation*, Commission on Accreditation of Law Enforcement Agencies, Washington, D.C., 2002

¹⁹ Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, ό. π., σ. 14

²⁰ Global Justice Information Sharing Initiative, *Navigating Your Agency's Path to Intelligence-Led Policing*, US Department of Justice, Washington, D.C., 2009, σ. 2



Εικόνα 31: ο πληροφοριακός κύκλος του law enforcement intelligence καταδεικνύει την κοινότητα στη διαδικασία παραγωγής πληροφόρησης όπως αυτή συναντάται σε πλήθος κρατικών οργανισμών. Η εικόνα ελήφθη από τη σελίδα 58 του *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* του David Carter

Ο Carter συνοψίζει λέγοντας ότι law enforcement intelligence σημαίνει: α) συλλογή πληροφοριών γύρω από εγκληματικές όπως και τρομοκρατικές απειλές, επιβोधία στη σύλληψη επίβουλων στοιχείων, συνεισφορά στην προστασία ευαίσθητων στόχων²¹, β) ενημέρωση των αρμοδίων σχετικά με αλλαγές στη φύση των ευρύτερων law enforcement απειλών, των χαρακτηριστικών και της μεθοδολογίας τους. Σ' αυτή την περίπτωση, συνεχίζει ο Carter, αναφερόμαστε σε strategic intelligence με προσανατολισμό, επίσης, στην εξυπηρέτηση των law enforcement agencies.²² Εκ των αναφερθέντων δεν συνάγεται ανάγκη αναπόδραστης εμπλοκής των οργανισμών Πληροφόρησης και Αντιπληροφόρησης στην καταδίωξη της τρομοκρατίας και του σύγχρονου εγκλήματος από τη στιγμή που υπάρχει η law enforcement αρχή, αρκεί αυτή να λειτουργήσει στα πρότυπα των κλασικών Υπηρεσιών. Από τη μεριά του ο V. Bridgeman διαφωνώντας με τον Robert Wallace υποστηρίζει ότι η άποψη που συνδέει στην Αμερική το CI με τις υπηρεσίες επιβολής νόμου αποτελεί παρανόηση της οποίας οι ρίζες βρίσκονται στη μακρά εμπλοκή των συγκεκριμένων agencies με υποθέσεις (αντι)κατασκοπίας -το FBI δεικνύει κύριο παράδειγμα. Ο Bridgeman εξηγεί γιατί το CI δεν πρέπει να συγχέεται με το law enforcement ή, καλύτερα, γιατί δεν πρέπει να εμπλέκονται τα δύο πεδία τονίζοντας, κυρίως, τη στρατηγική διάσταση του πρώτου (ή, αλλιώς, την παρουσία του στο political decision making) ...counterintelligence is thus correctly viewed as a strategic international relations

²¹ Ο Carter μιλά τόσο για tactical όσο και για operational law enforcement intelligence. Σε γενικές γραμμές το πρώτο σχετίζεται με αντιμετώπιση επικείμενων άμεσων κινδύνων, το δεύτερο με αντιμετώπιση μακροπρόθεσμων απειλών και πολυσύνθετων/ πολυεπίπεδων εγκληματικών δικτύων -για περισσότερα βλέπε Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, ό. π., σ. 9, επίσης βλέπε τους περί intelligence-led policing (ILP) ορισμούς στις σελίδες 79 και 80 του ίδιου

²² Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, ό. π., σ. 9

tool rather than a domestic law enforcement mission, γράφει.²³ Ο Greg Treverton συνηγορεί δηλώνοντας ότι οι law enforcement agencies: α) λειτουργούν προς συλλογή στοιχείων αξιοποιήσιμων εντός των δικαστικών αιθουσών, β) λειτουργούν προς εξιχνίαση ήδη διαπραττομένων εγκλημάτων, γ) λειτουργούν σύμφωνα με τις απαιτήσεις του αμερικανικού Συντάγματος και τους κανόνες της «αποδειξιμότητας» και δ) προκειμένου να υπερασπίσουν την εγκυρότητα των δεδομένων που κομίζουν υποχρεούνται αποκάλυψης πηγών και μεθόδων. Σε αντίθεση με αυτές, συνεχίζει ο Treverton, οι κλασικές Υπηρεσίες: α) δεν ασχολούνται με την καταδίωξη του εγκλήματος αλλά με την απομείωση της αβεβαιότητας προκειμένου να ενισχυθεί η διαδικασία λήψεως στρατηγικών αποφάσεων, β) συλλέγουν στοιχεία πριν την εκδήλωση του όποιου συμβάντος με σκοπό την πρόληψή του, γ) συλλέγουν κάθε είδος αξιοποιήσιμων δεδομένων χωρίς απαραίτητα να ακολουθείται ο κανόνας της «αποδειξιμότητας» και δ) προστατεύουν με κάθε μέσο πηγές και μεθόδους.²⁴ Ο William Odom, διευθυντής της NSA κατά την περίοδο Reagan θεωρεί ότι CI και law enforcement επουδενί μπορούν να ομογενοποιηθούν -οι λόγοι σχετίζονται με την ιδιαιτερότητα των σκοπών, τις επιχειρησιακές δυνατότητες κ. λ.²⁵ Ο Roy Godson αποδεχόμενος τον Odom τονίζει την εγγενή αδυναμία άσκησης οιονεί δράσεων CI εκ μέρους του law enforcement αν και δέχεται ότι υπάρχουν εξαιρέσεις στον κανόνα.²⁶ Κατά τους Jensen, McElreath και Graves δεν είναι λίγοι αυτοί που πιστεύουν ότι το FBI οφείλει να παραμείνει αστυνομική αρχή παραχωρώντας τον αντικατασκοπευτικό και αντιτρομοκρατικό σχεδιασμό σε μια νέα Υπηρεσία εσωτερικής ασφαλείας κατά τα πρότυπα της MI5 χωρίς δικαιώματα σύλληψης και καθήκοντα που σχετίζονται με την επιβολή νόμου²⁷ -σύμφωνα με τον R. A. Posner ...[the] Bureau [FBI] is a criminal investigation agency. Its orientation is toward arrest and prosecution....²⁸

Εντούτοις κάτι τέτοιο δεν ισχύει για το *The 9 / 11 Commission Report* κατά το οποίο: α) το FBI είναι εξοικειωμένο με τη διαχείριση ευαίσθητων πληροφοριών ακολουθώντας το νομικό πλαίσιο της χώρας τη στιγμή που μια νέα Υπηρεσία έξω

²³ Bridgeman H. V., “Defense Counterintelligence, Reconceptualized” στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, ό. π., σ. 130-131. Πάρα ταύτα εμμέσως ο μελετητής, επίσης στη σελίδα 131, δεν αποκλείει την ανάθεση κάποιων «αντικατασκοπευτικών καθηκόντων» στο law enforcement υπό την προϋπόθεση της μη άμεσης δίωξης του όποιου υπόπτου υπέρ μιας στρατηγικής παρακολούθησης, παραπληροφόρησης / χειραγώγησής του εάν και εφόσον αυτό κριθεί προσφορότερο. Σαφέστατα σ’ αυτήν την περίπτωση απαιτείται επιπρόσθετη εκπαίδευση και γνώση των διαφορετικότητων των δύο πεδίων, επιπλέον κάποιος μπορεί να υποθέσει τη δημιουργία μιας μεικτής Υπηρεσίας. Στην υποσημείωση 22, σελίδα 146 του αναφερομένου έργου τονίζεται ότι αν και το *Title 50 of the United States Code* ορίζει την αντικατασκοπία ως υποπεδίο της πληροφόρησης και μόνο, αν και η *Executive Order 12333* δεν κάνει καμία αναφορά σε μια σχέση μεταξύ CI και law enforcement, η όποια σύγχυση σχετίζεται με μια προσπάθεια απόδοσης ποινικών ευθυνών κατά «υπόπτων κατασκοπίας». Είναι μάλιστα χαρακτηριστικό πως αν και ο ορισμός του DoD περί CI (υποσημείωση 9, σελίδα 145 του ιδίου) είναι ξεκάθαρος, υπάρχουν φωνές εντός αυτού που το ταυτίζουν και με το law enforcement (σελίδα 127 του ιδίου). Κάτι ανάλογο συμβαίνει εντός του αμερικανικού Πενταγώνου. Ενώ το τελευταίο αποσυνδέει (κατά το DoD) CI και law enforcement, δύο εκ των τριών κύριων πληροφοριακών / αντιπληροφοριακών Υπηρεσιών του, αναφερόμαστε στο Department of the Navy και στο Department of the Air Force, αλλά και η πάλοι ποτέ κεντρική επιχειρησιακή διεύθυνση Counterintelligence Field Activity (CIFA) διαπλέκουν τους τομείς’ κάτι τέτοιο δεν παρατηρείται εντός του Department of the Army (σελίδες 126-127, 131 του ιδίου)

²⁴ Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA, 2013, σ. 275-276

²⁵ Kierman K., “Counterintelligence and Law Enforcement” στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, ό. π., σ. 162-163

²⁶ Godson R., *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, Transaction Publishers, N. Jersey, ΗΠΑ, 2001, σ. xxviii

²⁷ *ibid*

²⁸ Posner A. Richard, “We Need Our Own MI5”, *The Washington Post*, 14 Αυγούστου 2006

από το Department of Justice θα δρούσε, ενδεχομένως, με όχι τόσο ελέγξιμο τρόπο, β) η δημιουργία μιας νέας Υπηρεσίας θα εξέτρεπε την προσοχή των ήδη υπεύθυνων αξιωματούχων για θέματα αντιτρομοκρατίας δυσχεραίνοντας, δε, περαιτέρω τη διασπορά πληροφόρησης από οργανισμό σε οργανισμό, γ) η εκκίνηση ενός νέου πληροφοριακού συστήματος τέτοιων φιλοδοξιών απαιτεί πολυπληθές προσωπικό και, γενικότερα, πληθώρα πόρων, δ) οι έρευνες για την αντιτρομοκρατία συνεπάγονται και law enforcement δράσεις. Το FBI διαθέτοντας ειδικευμένο προσωπικό καθίσταται η πλέον κατάλληλη Υπηρεσία προς εκτέλεση σχετικών δράσεων ειδικά μετά την παρουσία μιας ασαφούς πλέον γραμμής που από την 11^η Σεπτεμβρίου διαχωρίζει υποθετικά intelligence και law enforcement, ε) η αντιτρομοκρατική έρευνα συχνά συμπίπτει ή σχετίζεται με ανάλογες γύρω από το οργανωμένο έγκλημα.²⁹

Για την Kathleen Kierman πριν την 11^η Σεπτεμβρίου μια σύνδεση counterintelligence και law enforcement είναι, επισήμως τουλάχιστον, απύσχα, μόνο κάποιες λίγες περιπτώσεις συνεργασίας μεταξύ των δύο περιοχών καταγράφονται.³⁰ Ωστόσο μετά την ημερομηνία ορόσημο και τον ακόλουθο πόλεμο κατά της διεθνούς τρομοκρατίας φαίνεται πως το law enforcement οφείλει να λειτουργήσει και ως δομή αντικατασκοπευτικής / αντιτρομοκρατικής δράσης. Η ίδια τονίζει πως στο *National Intelligence Sharing Strategy* του 2009 εμφανίζεται μια νέα περί law enforcement αντίληψη, μία αντίληψη που το θέλει να δρα, πέραν του παραδοσιακού *streetcraft*, προληπτικά έναντι νέων εγκληματικών και τρομοκρατικών τάσεων.³¹ Το ίδιο υποστηρίζει εμμέσως η Michelle van Cleave μιλώντας για τη σπουδαιότητα του έργου της προστασίας του εσωτερικού περιβάλλοντος (homeland protection), μια προστασία που επαφίεται και στη δράση των law enforcement οργανισμών.³² Ο Todd Masse τονίζει ότι μια συνένωση law enforcement και domestic intelligence υπό την επίβλεψη της πολιτείας θα αποδειχθεί ευεργετική για δύο λόγους: α) θα προάγει τη συνεργασία και τον συντονισμό επιχειρήσεων μεταξύ των δύο δομών προς όφελος της εθνικής ασφαλείας³³ και β) θα δημιουργήσει ένα σύστημα ελέγχου των οργανισμών βασισμένο σε μια κουλτούρα σεβασμού του νόμου. Ο μεγαλύτερος

²⁹ *The 9 / 11 Commission Report*, 2004, σ. 423-424, διαθέσιμο στην ιστοσελίδα <http://www.9-11commission.gov/report/911Report.pdf> όπου καταφύγαμε την 5^η Αυγούστου 2015. Επίσης βλέπε Clark J. Ransom, *Intelligence and National Security. A Reference Handbook*, Praeger Security International, USA, 2007, σ. 88-89 με τον συγγραφέα να διερωτάται όχι μόνο αν το FBI δύναται να ανταπεξέλθει στα καθήκοντα ενός οργανισμού εσωτερικής πληροφόρησης αλλά και αν πρέπει. Πάντως στο παλαιότερο *A Review of FBI Security Programs* τονίζεται πως η απάντηση στο αν μπορεί να συνυπάρξει η κουλτούρα του intelligence με την κουλτούρα του law enforcement εντός ενός οργανισμού είναι πολύ δύσκολη -περί τούτου βλέπε Commission for Review of FBI Security Programs, *A Review of FBI Security Programs*, U.S. Department of Justice, Washington, D.C., Μάρτιος 2002, διαθέσιμο στην ιστοσελίδα <http://fas.org/irp/agency/doj/fbi/websterreport.html> εις την οποία ανατρέξαμε την 7^η Αυγούστου 2015

³⁰ ...αν και μια πρώτη σχέση χρονολογείται ήδη από την περίοδο του Αμερικανικού Εμφυλίου όταν το οιονεί αστυνομικό σώμα Pinkerton Detective Agency μισθώθηκε από τους Βορείους με σκοπό την κατασκοπία / αντικατασκοπία έναντι των Νοτίων -για μια άποψη βλέπε Roth P. Mitchel, *Crime and Punishment: A History of the Criminal Justice System*, Wadsworth Publishing, Belmont / California, 2004, σ. 128

³¹ Kierman K., "Counterintelligence and Law Enforcement" στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, ό. π., σ. 149-150

³² van Cleave, M., *Counterintelligence and National Strategy*, National Defense University, USA, 2007, σ. 14

³³ Masse Todd, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, Order Code RL31920, Report to Congress, Μάιος 2013, σ. 11, επίσης βλέπε Bazan B. Elizabeth, CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions* στο <https://fas.org/sgp/crs/intel/RL34279.pdf> εις το οποίο προσφύγαμε την 27^η Αυγούστου 2015

δυνητικός κίνδυνος αυτής της συνένωσης, συνεχίζει ο Masse, σχετίζεται με ένα φόβο μη λογοδοσίας. Σ' αυτήν την περίπτωση ο νέος οργανισμός ενδέχεται να εμπλακεί σε εσωτερικά πολιτικά παίγνια χαρακτηρίζοντας τους όποιους διαφωνούντες με τα συμφέροντά του ως στασιαστικές προσωπικότητες.³⁴ Ο Frederick Manget με τη σειρά του γράφει πως η συνάντηση δύο ασύμβατων κόσμων θα γεννήσει μια «γκρίζα» («μικτή») περιοχή εντός της οποίας θα πρέπει να συνεργαστούν δύο διαφορετικές κουλτούρες ή έστω να μην αποδειχθούν εμπόδιο η μία στην άλλη³⁵ καθώς για μελετητές όπως ο A. Carter ή ο P. Zelikow το σύνορο μεταξύ εθνικής ασφαλείας και νόμου / τάξης είναι βαθιά εντυπωμένο εντός του αμερικανικού πολιτικού συστήματος.³⁶

Μια και ο λόγος περιστρέφεται ιδιαίτερα γύρω από την τρομοκρατία σημειώνουμε την αρχή της αντίθεσης μεταξύ αυτής και της έννοιας «νόμος και τάξη». Η αντίθεση προκύπτει από παραβίαση νομοθεσίας, άρα, οι αστυνομικές αρχές επιφορτίζονται με δικαιοδοσίες πάταξης του φαινομένου. Εντούτοις η τρομοκρατία εκπίπτοντας της πρώτης τοπικής ή περιφερειακής εγκληματικής μορφής μεταβάλλεται σε πράξη της οποίας η εκτέλεση απαιτεί προηγμένες ικανότητες, εξειδίκευση, πειθαρχία, χρήμα, γνώση. Σχετίζεται πλέον και με πρακτικές / πολιτικές ακολουθούμενες από κρατικές και μη οντότητες.³⁷ Κατ' αυτόν τον τρόπο, τέτοιες οργανώσεις όχι μόνο προβαίνουν σε συλλογή / ανάλυση πληροφοριών αλλά ακόμα και στην άσκηση αντικατασκοπευτικών πρακτικών, παραπλάνησης κ. λ. -είναι φανερό πως πρόκειται και για πόλεμο πληροφόρησης.³⁸ Το ζήτημα περιπλέκεται αν σκεφτούμε πως η τρομοκρατία διαμειβεται πολλές φορές, όπως τονίσαμε, με το σύγχρονο έγκλημα -αν και ομιλούμε για διακριτές περιοχές η σύνδεσή τους παρομοιάζεται από τον Sulc ως αυτή των φυλακών με τις συμμορίες.³⁹ Ο Thomas Sanderson γράφει ότι η απόσταση μεταξύ τρομοκρατίας και εγκλήματος όλο και μειώνεται. Η πρώτη μετέρχεται πρακτικών του δευτέρου με σκοπό τη χρηματοδότηση των δραστηριοτήτων της. Με τη σειρά του το έγκλημα συνεργάζεται με την πρώτη διαβλέποντας μια νέα αγορά προς πώληση των υπηρεσιών του.⁴⁰ Ακριβώς αυτή η πραγματικότητα σημάνει έναν από τους λόγους, ίσως τον δεύτερο κύριο, που καλεί σε συζήτηση περί νέων CI και law enforcement προκλήσεων⁴¹, στην ουσία περί domestic / homeland security προκλήσεων. Αυτό υποστηρίζει και η Kierman καταγράφοντας αλλαγές στην αμερικανική νομοθεσία. Αναφέρετε σε νομοθετικές πράξεις που προσέδωσαν στο law enforcement επιπρόσθετες αρμοδιότητες στην εσωτερική αρένα, αρμοδιότητες που

³⁴ Masse Todd, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, Order Code RL31920, Report to Congress, Μάιος 2013, σ. 11-12. Από τη μεριά του ο Stewart Baker γράφει ότι πάντα υπάρχει αυτός ο φόβος στο ενδεχόμενο δημιουργίας ενός domestic law enforcement μολυσμένο με την κουλτούρα της μυστικότητας, των πρακτικών της εξαπάτησης και τη σκληρότητα που απαιτείται στον κόσμο των κατασκόπων -για μια εικόνα βλέπε Baker Stewart, "Should Spies Be Cops?" στο *Foreign Policy*, Winter 1994-1995, σ. 36-37

³⁵ Manget Frederick, "Intelligence and Law Enforcement" στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson L., Oxford University Press, Inc., USA, 2010, σ. 208

³⁶ Carter A., Deutch J., Zelikow P., "Catastrophic Terrorism: Tackling the New Danger", *Foreign Affairs*, Νοέμβριος / Δεκέμβριος 1998

³⁷ Το FBI ορίζει την τρομοκρατία ως ...*unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives* -για περισσότερα βλέπε Sulc L., *Law Enforcement Counterintelligence*, ό. π., σ. 90

³⁸ Sulc L., *Law Enforcement Counterintelligence*, ό. π., σ. 89

³⁹ ό. π., σ. 90

⁴⁰ Sanderson Th., "Transnational Terror and Organized Crime: Blurring the Lines", *SAIS Review*, Volume 24, Number 1, 2004, σ. 49-61

⁴¹ Sulc L., *Law Enforcement Counterintelligence*, ό. π., σ. 90

κατά την ίδια σχετίζονται και με το πεδίο της αντικατασκοπίας -όλα αυτά προς επίτευξη μιας ικανής στρατηγικής έναντι του τρομοκρατικού φαινομένου. Η αναγκαιότητα δημιουργίας γεφυρών μεταξύ CI και law enforcement αλλά και η πολυπλοκότητα του εγχειρήματος, συνεχίζει η συγγραφέας, φαίνεται από τον αριθμό των εκτελεστικών εντολών (executive orders -EO) και των προεδρικών οδηγιών (presidential decision directives -PDD) γύρω, κυρίως, από τη διασπορά της πληροφόρησης εντός των αρμοδίων οργανισμών. Επιπροσθέτως, η Directive 6 (HSPD-6) του Σεπτεμβρίου του 2003 δίδει δικαίωμα πρόσβασης των law enforcement agencies σε πληροφοριακά δεδομένα που μέχρι εκείνη τη στιγμή χειρίζονταν αποκλειστικά οι υπηρεσίες Πληροφοριών. Πριν την 11^η Σεπτεμβρίου οι τοπικές, τουλάχιστον, αμερικανικές αστυνομικές αρχές έβλεπαν την ενασχόληση με την καταδίωξη της τρομοκρατίας ως κάτι, μάλλον, ασύμβατο. Το τραγικό γεγονός αλλάζει την αντίληψη και τον σχεδιασμό ασφαλείας των law enforcement agencies όπως και την κρατική στρατηγική -η δημιουργία, μεταξύ άλλων, του Department of Homeland Security το αποδεικνύει.⁴²

Ο Sulc υπερθεματίζει προς μία κατεύθυνση οιονεί σύμπτυξης counterintelligence και law enforcement εγκαλώντας το τελευταίο περί μη ετοιμότητας αντιμετώπισης του διεθνικού και εσωτερικού οργανωμένου εγκλήματος αλλά και των όποιων εξτρεμιστικών συσσωματώσεων. Ο μελετητής ως έχει καταδειχτεί αντιλαμβάνεται αυτές τις ομάδες ως δίκτυα, συνεπώς, η αντιπληροφόρηση και όχι απλά το law enforcement καλείται να τις αντικρούσει.⁴³ Οι όροι *law enforcement intelligence*, *intelligence-led policing* κ. λ. αναφέρονται σε μια νέα law enforcement νοοτροπία που χρησιμοποιώντας την πληροφορία κατά τα πρότυπα, λίγο πολύ, των Υπηρεσιών στοχεύει στην πρόληψη του εγκλήματος και στην καταστολή της τρομοκρατίας.⁴⁴ Κατ' αυτήν την έννοια η *αστυνομική πληροφόρηση* ή η *αστυνόμευση που καθοδηγείται από την πληροφόρηση* διαπλέκεται άμεσα με την έννοια του homeland security intelligence και διασταλτικά με αυτή του (counter)intelligence.⁴⁵

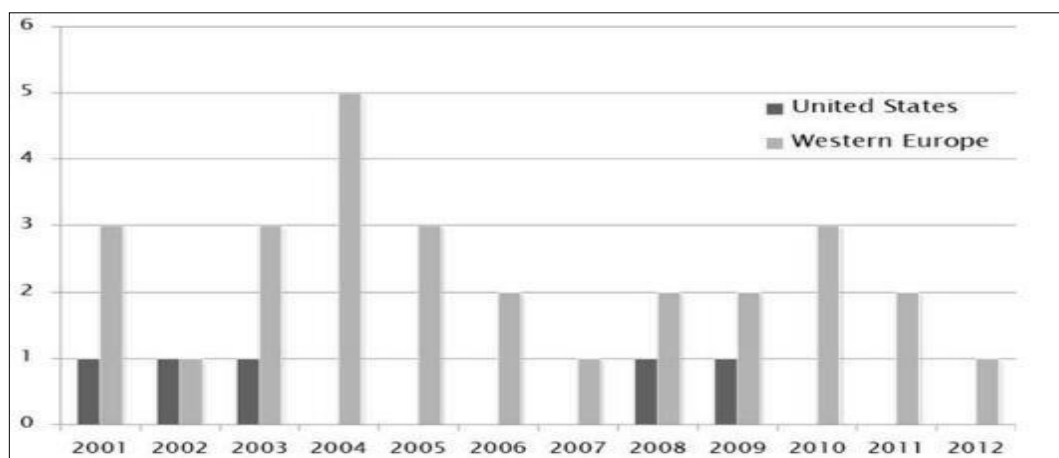
⁴² Kierman K., "Counterintelligence and Law Enforcement" στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, ό. π., σ. 158-161

⁴³ ό. π., σ. 163

⁴⁴ Newman Graeme, Clarke Ronald, *Policing Terrorism: An Executive's Guide*, US Department of Justice / Office of Community Oriented Policing Services, Brief 23

⁴⁵ Chapter 1 "Introduction" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009, σ. 3-5. Στις Ηνωμένες Πολιτείες αξιωματούχοι του law enforcement είχαν επισημάνει τη χρηστικότητα του Βρετανικού Εθνικού Πληροφοριακού Μοντέλου (Britain's National Intelligence Model) επιζητώντας μια intelligence-led policing μεταμόρφωση του εγχώριου συστήματος επιβολής νόμου. Αν και η μεγάλη ώθηση εδόθη μετά το κτύπημα στους Δίδυμους Πύργους, αλήθεια είναι πως μια σειρά σχετικών πληροφοριακών προγραμμάτων με προσανατολισμό στο law enforcement λάμβανε χώρα ήδη από τη δεκαετία του 1970 [The Regional Information Sharing System (RISS) Program, Joint Terrorism Task Forces (JTTFs), High Intensity Drug Trafficking Area (HIDTA) Program], επιπλέον, οι περισσότερες πολιτειακές και μεγάλες τοπικές αστυνομικές διευθύνσεις διέθεταν τμήματα πληροφοριών. Κατά τα τέλη της δεκαετίας του 1990 ένα γκρουπ αξιωματούχων συνδεδεμένο με το International Association of Chiefs of Police (IACP) συνεργάζεται με το International Association of Law Enforcement Intelligence Analysts και το Western States Information Network προκειμένου ανάπτυξης μιας αμερικανικής έκδοσης intelligence-led policing στρατηγικής τη στιγμή που πολλές law enforcement αρχές ήδη προσανατολίζονται, πέραν της πάταξης του κοινού εγκλήματος, στην πρόληψη. Στις αρχές του 2002 το IACP διεξάγει το Criminal Intelligence Sharing Summit παράγοντας το *National Criminal Intelligence Sharing Plan (NCISP)*. Το συγκεκριμένο ντοκουμέντο συνιστά την ανάπτυξη της intelligence-led policing τακτικής εντός κάθε αστυνομικού παραρτήματος ανεξαρτήτου μεγέθους ή ειδικότερων αρμοδιοτήτων -θεωρητικά μια law enforcement υπηρεσία εδύνατο να αξιοποιήσει το πλάνο με στόχο την ανάπτυξη, χρηματοδότηση και διατήρηση πληροφοριακού δυναμικού. Σε τοπικό επίπεδο είναι το New York City Police Department (NYPD) που ενσωματώνει την κουλτούρα της πληροφόρησης περισσότερο από

Τελικά, ρωτάνε οι Jensen, McElreath και Graves, υπάρχει απόδειξη ότι το law enforcement intelligence / intelligence-led policing θα περιορίσει κάποιες από τις διαρκώς μεταλλασσόμενες προκλήσεις; Το γεγονός απουσίας ενός μείζονος κτυπήματος στις Ηνωμένες Πολιτείες από την 11^η Σεπτέμβρη και έπειτα δεν είναι τόσο ενδεικτικό όσο είναι η μελέτη μιας ομάδας ερευνητών κατά την οποία εικοσιοκτώ τρομοκρατικοί σχεδιασμοί την περίοδο 2001-2010 κατεγράφησαν ως απόπειρες και, ευτυχώς, όχι ως συμβάντα. Πιθανότατα στους λόγους αποτυχίας των εξτρεμιστών συγκαταλέγεται μια αλλαγή νοοτροπίας των law enforcement αρχών στα πρότυπα των Υπηρεσιών. Πρόκειται για στροφή που παρατηρείται μετά το 2001 οδηγώντας σε μια «εξυπνότερη» Αστυνομία.⁴⁶



Εικόνα 32: Τρομοκρατικά κτυπήματα της Qaeda σε ΗΠΑ και δυτική Ευρώπη κατά το διάστημα 2001-2012. Η εικόνα αντιγράφηκε από το “The Effectiveness of the Drone Campaign against Al Qaeda Central: A Case Study” του Javier Jordan στο *Journal of Strategic Studies*, Volume 37, Number 1, 2014, σ. 23. Μέχρι και τα μέσα του 2017 η Αμερική φαίνεται να απολαμβάνει πολύ περισσότερη ασφάλεια σε σχέση με την Ευρώπη. Η τελευταία (πλην Ρωσικής Ομοσπονδίας) δέχτηκε 18 πλήγματα από το 2014 μέχρι και τον Ιούλιο του 2016 θρηνώντας 443 ανθρώπινες ζωές. Ως βασικός υπαίτιος φέρεται ο ισλαμικός φονταμενταλισμός -για μια εικόνα βλέπε «Ο τραγικός απολογισμός. Ο χάρτης της φρίκης: 18 τρομοκρατικές επιθέσεις σε 2 χρόνια στην Ευρώπη, 443 νεκροί», *iefimerida*, 27 Ιουλίου 2016 στο <http://www.iefimerida.gr/news/280442/o-hartis-tis-frikis-18-tromokratikes-epitheseis-se-2-hronia-stin-eyropi-443-nekroi> εις το οποίο ανατρέξαμε την 1^η Μαρτίου 2017

κάθε άλλη ανάλογη αρχή «τρέχοντας» το Intelligence Division & Counter-Terrorism Bureau (ID / CTB) -για όλα αυτά βλέπε Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA 2013, σ. 279-282. Σχετικά με το NCISP βλέπε στο *The National Criminal Intelligence Sharing Plan*, U.S. Department of Justice, Ιούνιος 2005, στο http://www.au.af.mil/au/awl/wastage/do/Nat_cram_Intel_share_plan2005.puff όπου καταφύγαμε την 6^η Αυγούστου 2015

⁴⁶ Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, ό. π., σ. 282. Επιπλέον οι τρεις μελετητές στη σελίδα 290 του έργου τους τονίζοντας την ανάπτυξη της υψηλής τεχνολογίας (PCs, Geographic Information Systems -GIS κ. λ.) και των θεωρητικών μοντέλων υπογραμμίζουν μια επανάσταση στο λεγόμενο crime analysis μέσω πρόσληψης εκατομμυρίων πληροφοριακών δεδομένων προκειμένου ορθότερης κατανόησης των εγκληματικών ροών / σχεδιασμών και ταυτοποίησης των όποιων δραστών. Ασφαλώς οι ανερχόμενες policing philosophies (Intelligence-Led Policing, Predictive Policing, Computer Statistics -COMPSTAT) βασιζόμενες στη συλλογή και ανάλυση πληροφορίας έχουν πολύ δρόμο να βαδίσουν. Αν για ευνόητους λόγους δεν λείπουν επικρίσεις, π. χ. από την American Civil Liberties Union, περί μιας οιονεί σύμπτυξης «πληροφοριακών κέντρων», δεν αμφισβητείται, πάντα σε σχέση με την Αμερική, πρώτον, η μη επανάληψη από το 2001 ενός τρομοσók και δεύτερον, η μείωση της εγκληματικότητας στις περισσότερες περιοχές της χώρας από τις αρχές της δεκαετίας του 1990

Τέλος, κάτι που ωθεί περαιτέρω την αλλαγή στον τρόπο κρατικής δράσης αντιμετώπισης κρίσιμων καταστάσεων έχει να κάνει, όπως καταγράφει ο Erbschloe, με απειλές κατά εθνικών αλλά και ιδιωτικών πληροφοριακών υποδομών ούτως ειπείν, με την απειλή του δικτυακού εγκλήματος ή και πολέμου -ο ίδιος αναφέρεται στην περίπτωση *Love Bug* (2000). Ο Erbschloe αποδεχόμενος την μερική προς το παρόν αδυναμία των law enforcement αρχών ως προς την πάταξη του φαινομένου ευελπιστεί σε αναδιάρθρωση των σχετικών οργανισμών καταθέτοντας σειρά προτάσεων που συμπυκνώνονται επιχειρησιακά στον έλεγχο του κυβερνοδιαστήματος και γραφειοκρατικά στη συνεργασία των αρχών επιβολής νόμου με στρατιωτικούς (πληροφοριακούς) φορείς και με φορείς του ιδιωτικού τομέα.⁴⁷

Κάποια παραδείγματα ασφαλείας

Το αγγλοσαξονικό, πλην Ηνωμένων Πολιτειών, παράδειγμα

Η συνεργασία μεταξύ των πληροφοριακών και των law enforcement αρχών δεν αποτελεί έκπληξη, γράφει ο Gregory Treverton, ειδικά σε μια εποχή που οι αντιτρομοκρατικές στρατηγικές βρίσκονται στο ζενίθ τους. Αυτού του είδους η προσέγγιση υποστασιοποιείται στο βρετανικό παράδειγμα ασφαλείας δοθέντος μάλιστα της προϋστορίας των police Special Branches: α) στο μότο «covert intelligence work in relation to national security», β) στην επικουρία της MI5 στην προς εκτέλεση των εκ της Security Service Act (1989) προβλεπομένων, γ) στην επικουρία της MI6 (Home Office Communication Directorate, 2004).⁴⁸ Ο Lindsay Clutterbuck συμφωνεί τονίζοντας τη σχέση των 52 UK Police Forces με την MI5 μέσω των Counter Terrorism Intelligence Units και των Security Service regional offices. Ο ερευνητής καταγράφει τους τρόπους εμπλοκής του law enforcement με το (counter)intelligence καταλήγοντας στο συμπέρασμα μιας συνεργασίας που γίνεται όλο και πιο στενή και με το Executive Liaison Group να δεικνύει το ανώτατο όργανο επιχειρησιακού συντονισμού. Αν και καθ' όλη τη διάρκεια του 20^{ου} αιώνα law enforcement και intelligence απέτέλεσαν διακριτά πεδία, η άνθηση της τρομοκρατίας απαιτεί μια αλλαγή στον τρόπο αντίκρουσης προκλήσεων εθνικής ασφαλείας, κατά συνέπεια, ο Clutterbuck υποθέτει μια μεταμόρφωση της MI5 στα πρότυπα του FBI αν και η εκτελεστική ισχύ (executive power) θα παραμείνει, ως πιστεύει, στα χέρια του UK police.⁴⁹

⁴⁷ Erbschloe M, *Information Warfare. How to Survive Cyber Attacks*, The McGraw-Hill Companies, USA, 2001, σ. 12-13. Ο Erbschloe διαχωρίζει τους ρόλους τονίζοντας την εξωτερικού περιβάλλοντος διάσταση της αποστολής του στρατού σε σχέση με την εσωτερική των αρχών επιβολής νόμου. Πάρα ταύτα ένας πληροφοριακός πόλεμος ως μη πόλεμος γεωγραφικού χώρου απαιτεί προς αντιμετώπισή του τη σύμπληξη όλων των διαθέσιμων τοποθετώντας στο περιθώριο παλαιότερους περιορισμούς -για περισσότερα βλέπε στο ίδιο σ. 27-29

⁴⁸ Η Βρετανία αλλάζοντας την παλαιότερη πολιτική της επί μακρόν παρακολούθησης δεν επιτρέπει πλέον την παραμονή στο δρόμο υπόπτων στοιχείων αν το ρίσκο υπερβαίνει κάποια όρια. Επιχειρησιακά η διαφορά έγκειται στην αμεσότερη εμπλοκή των αστυνομικών ντέντεκτιβς στις εκ της MI5 διεξαγόμενες έρευνες -περί τούτων βλέπε Treverton Gr., *Reorganizing U.S. Domestic Intelligence. Assessing the Options*, RAND, Santa Monica, 2008, σ. 63-64

⁴⁹ Clutterbuck L., "The United Kingdom" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 129-132, 140-141, επίσης βλέπε Masse Todd, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, Order Code RL31920, Report to Congress, Μάιος 2013, σ. 6 και Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, Polity Press, USA, 2012², σ. 56-58

Στον Καναδά η συνεργασία μεταξύ της Canadian Security Intelligence Service (CSIS) και της ομοσπονδιακής Royal Canadian Mounted Police (RCMP) αποτελεί κύρια συνιστώσα εντός του Integrated Threat Assessment Centre (ITAC) και του Integrated National Security Enforcement Teams (INSET) -το National Counter-Terrorism Plan συνθέτει τον κύριο συντονιστικό οδηγό προς επίτευξη βέλτιστης κρατικής αντίδρασης έναντι τρομοκινδύνων. Το 2007 υπήρξαν σκέψεις μεταβίβασης καθηκόντων law enforcement στην CSIS ωστόσο ο φόβος αποκάλυψης της ταυτότητας των ανθρωπίνων πόρων / πηγών της Υπηρεσίας και η μη αποδοχή αλλαγής φύσης της τελευταίας απέτρεψαν μια σχετική υλοποίηση.⁵⁰ Πάρα ταύτα η CSIS επιδιώκοντας μια ουσιαστική σύμπραξη με τις αστυνομικές δυνάμεις διατηρεί τοπικά παραρτήματα με σκοπό την ανταλλαγή πληροφοριών και μέσω αυτής την ακριβέστερη εκτίμηση της όποιας απειλής σε συνδυασμό με μια καλύτερη επιχειρησιακή αντίδραση.⁵¹ Είναι χαρακτηριστικό ότι το 2006 η καναδική αντικατασκοπία σε συνεννόηση με την ομοσπονδιακή αστυνομία απέτρεψε τρομοκρατικό κτύπημα αξιοποιώντας πληροφορίες που μεταφέρθηκαν στην πρώτη μέσω των βρετανικών μυστικών υπηρεσιών. Περαιτέρω έρευνα αποκάλυψε συνομωσία δέκα επτά ατόμων με σκοπό την επίθεση στο καναδικό κοινοβούλιο, την απαγωγή πολιτικών προσώπων, τη δημιουργία χάους στο κέντρο του Τορόντο αλλά και την εκτέλεση του πρωθυπουργού σε περίπτωση άρνησης του τελευταίου να αποσύρει τα καναδικά στρατεύματα από το Αφγανιστάν.⁵²

Το αυστραλιανό National Threat Assessment Centre (NTAC) με έτος ίδρυσης το 2004 επιφορτίζεται με το έργο αποτροπής της τρομοκρατικής δράσης στην επικράτεια της ηπείρου. Η συνεργασία, μεταξύ άλλων, των Australian Security Intelligence Organization (ASIO), Australian Secret Intelligence Service (ASIS) και Australian Federal Police (AFP) θεωρείται απαραίτητη προϋπόθεση προς επίτευξη του σκοπού αυτού. Άλλο σημαντικό όργανο δεικνύει το Joint Counter-Terrorism Intelligence Coordination Unit (JCTICU) με έτος ίδρυσης το 2002 και στόχο την εμβάθυνση της συνεργασίας μεταξύ των μυστικών υπηρεσιών και των αστυνομικών αρχών, ειδικότερα την απόδοση πληροφοριών εκ μέρους των πρώτων στις δεύτερες. Από τη μεριά του το Protective Security Coordination Centre Watch Office (PSCCWO) απασχολώντας προσωπικό προερχόμενο τόσο από το χώρο του intelligence όσο και του law enforcement συγκεντρώνει και αναλύει σε εικοσιτετράωρη βάση πληροφορίες γύρω από ζητήματα ασφαλείας τοπικού, περιφερειακού και εθνικού ενδιαφέροντος. Επιπλέον η μόνιμη εκπροσώπηση της ομοσπονδιακής αστυνομίας στα, φιλοξενούμενα εντός των εγκαταστάσεων της ASIO, NTAC και JCTICU συντείνει στην έγκαιρη ενσωμάτωση αστυνομικών πληροφοριών εντός του ευρύτερου δικτύου προστασίας, καταμέτρησης και εκτίμησης εθνικών απειλών αλλά και στην πληρέστερη αντίληψη εκ μέρους του law enforcement της

⁵⁰ “CSIS does not interpret the end game of counterterrorism in the minutiae of individual arrests and prosecutions; by contrast, the service views its role in far broader, strategic terms, which are essentially aimed at securing Canada’s long-term security interests and safeguarding the welfare of its citizens” -για μια άποψη βλέπε Chalk Peter, “Canada” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 56

⁵¹ Chalk Peter, “Canada”, ό. π., σ. 54-57

⁵² Kirby Aidan, “Domestic Intelligence Agencies After September 11, 2001: How Five Nations Have Grappled with the Evolving Threat” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 147-148

τρομοκρατικής πρόκλησης.⁵³ Πάρα ταύτα ο Aidan Kirby υποστηρίζει ότι το αυστραλιανό domestic intelligence μέχρι και τα τέλη της πρώτης δεκαετίας του 21^{ου} αιώνα στερείτο law enforcement δυνάμεων / πόρων. Την έλλειψη αυτή έρχεται να διορθώσει, με αμφιλεγόμενο για πολλούς τρόπο, η νομοθεσία. Το 2003 περνά το αναθεωρημένο ASIO Bill βάσει του οποίου η αυστραλιανή υπηρεσία Αντικατασκοπίας απολαμβάνει αυξημένες αρμοδιότητες, μεταξύ αυτών σύλληψης / κράτησης υπόπτων για τρομοκρατικούς σχεδιασμούς μέχρι και επτά ημέρες. Έτσι, και παρά την απουσία κτυπημάτων στο εσωτερικό, επαναδιατυπώνεται η σχέση μεταξύ intelligence και law enforcement' ο ερευνητής επιμένει πως μια διακριτή γραμμή ανάμεσα στα δύο πεδία πλέον δεν υφίσταται. Είναι, δε, χαρακτηριστικό ότι τον Νοέμβριο του 2003, ένα χρόνο και κάτι από τη βομβιστική / τρομοκρατική επίθεση στο Μπαλί που αφαίρεσε, μεταξύ άλλων, τη ζωή 88 Αυστραλών, ένα 46μελές γκρουπ της ASIO (απορροφώντας ουσιαστικά και προσωπικό της ομοσπονδιακής και πολιτειακής αστυνομίας) μεταβαίνει στην Ινδονησία προκειμένου να υποστηρίξει τις έρευνες των εκεί τοπικών αρχών. Τέλος, η δεκαεξάμηνη παρακολούθηση, εκ μέρους της ASIO και αστυνομικών Υπηρεσιών, δύο ομάδων συνολικής δύναμης εικοσιτριών ατόμων, οδηγώντας στη σύλληψη των τελευταίων στα τέλη του 2005, αποτρέπει εκδήλωση επιθέσεων έναντι του μοναδικού πυρηνικού αντιδραστήρα της χώρας, του Χρηματιστηρίου Αξιών, κυβερνητικών κτηρίων και σιδηροδρομικών σταθμών -επρόκειτο για τη μεγαλύτερη αντιτρομοκρατική επιχείρηση στην ιστορία της Αυστραλίας.⁵⁴

Το ευρωπαϊκό παράδειγμα

Στην ηπειρωτική Ευρώπη κύριο παράδειγμα domestic intelligence / homeland security θεωρείται το γαλλικό. Η Direction de la Surveillance du Territoire (DST / Directorate of Territorial Surveillance) δεικνύει την πρωταρχική υπηρεσία εσωτερικών πληροφοριών, επίσης, δεν πρέπει να ξεχνάμε τη Direction Centrale des Renseignements Généraux (DCRG / Central Directorate of General Intelligence). Αν η πρώτη γίνεται αντιληπτή ως υπηρεσία Αντικατασκοπίας, η δεύτερη σχετίζεται με ζητήματα τόσο ασφαλείας όσο και law enforcement -η πρώτη προσιδιάζει στην MI5, η δεύτερη στα βρετανικά Special Branches. Και οι δύο οργανισμοί ελέγχονται από την Police Nationale και το Ministère de l'Intérieur.⁵⁵ Είναι γεγονός ότι η DST δύναται σύλληψης ατόμων υπόπτων για τρομοκρατική δράση, ή παρόμοιους σχεδιασμούς, κατά το πρότυπο της υφισταμένης στην Police Nationale, Police Judiciaire. Πάρα ταύτα δεν προβαίνει, συνήθως, στην άσκηση του εν λόγω δικαιώματος. Αν κάτι τέτοιο αποφασιστεί, τότε, η επιχείρηση, στις περισσότερες των περιπτώσεων, οργανώνεται σε συνεργασία με το Sous-Direction Anti-terroriste (SDAT / Anti-Terrorist Sub-Directorate) της Police Judiciaire ή το Section Anti-terroriste Brigade Criminelle της παριζιάνικης αστυνομίας.⁵⁶ Η DST πέραν της

⁵³ Chalk Peter, "Australia" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 27-33

⁵⁴ Kirby Aidan, "Domestic Intelligence Agencies After September 11, 2001: How Five Nations Have Grappled with the Evolving Threat" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 144-147

⁵⁵ Warnes Richard, "France" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 65

⁵⁶ ό. π., σ. 76

σχέσης με την Police Nationale συνδέεται, επίσης, με την Gendarmerie Nationale -πρόκειται για σώμα αστυνόμευσης της γαλλικής υπαίθρου. Όταν μια επιχείρηση εισέρχεται στο τελικό στάδιο και η σύλληψη προσώπων καθίσταται αναγκαία, τότε, είναι η Unite de Coordination de la Lutte Anti-terroriste (UCLAT / Coordination Unit for the Anti-Terrorist Struggle) της Police Nationale που αναλαμβάνει το συντονισμό.⁵⁷ Από τα μέχρι τούδε γραφόμενα γίνεται φανερό ένα άμεσο δούναι και λαβείν μεταξύ των DST / DCRG και της Police Nationale ούτως ειπείν, των υπηρεσιών Αντικατασκοπίας / εσωτερικής Ασφαλείας και του law enforcement. Αυτό ωστόσο στο οποίο στεκόμαστε είναι η παλαιότερη διαφοροποίηση μεταξύ DST και DCRG και οι νεότερες εξελίξεις. Αν και πρόκειται ουσιαστικά για υπηρεσίες εσωτερικών πληροφοριών, η πρώτη εστίαζε στους εντός Γαλλίας κινδύνους προερχομένους από το εξωτερικό, η δεύτερη στους εντός Γαλλίας κινδύνους προερχομένους από εσωτερικούς πυρήνες -οι λόγοι της διπλής αυτής κληρονομιάς ανευρίσκονται στην περίοδο του Β' Π. Π. και στη διάσπαση της γαλλικής κοινωνίας μεταξύ του καθεστώτος Βισύ και των Ελεύθερων Γάλλων του στρατηγού de Gaulle. Παρά τη διαφορετική προέλευση, μια αναπόφευκτη επικάλυψη χαρακτηρίζει τις λειτουργίες τους ειδικά στην εποχή της μεταλλαγής της τρομοκρατικής ταυτότητας: τα μέχρι τώρα γνωστά εσωτερικά ή εξωτερικά εξτρεμιστικά γκρουπ παραχωρούν τη θέση τους σε ένα διεθνές «δίκτυο τρόμου». Η νέα αυτή παράμετρος συσκοτίζει τα όρια μεταξύ ημεδαπών και αλλοδαπών, εσωτερικών και εξωτερικών, τοπικών και διεθνικών απειλών. Κατά συνέπεια DST και DCRG έρχονται ακόμα πιο κοντά. Η έννοια της κλασικής αντικατασκοπίας πλέκεται με αυτή της εσωτερικής ασφαλείας [σε βαθμό πρότασης μιας μεικτής Υπηρεσίας υπό την ονομασία Direction Centrale du Renseignement Intérieur (DCRI / Central Directorate of Interior Intelligence)] και η τελευταία με αυτή του law enforcement.⁵⁸

Κλείνουμε με το παράδειγμα της Γερμανίας. Το 1950 ιδρύεται η Bundesamt für Verfassungsschutz (BfV / Federal Office for the Protection of the Constitution) με πολλαπλούς στη διάρκεια του χρόνου ρόλους. Αρχικό καθήκον δεικνύει η αντικατασκοπευτική δράση έναντι κινδύνων προερχομένων από την ανατολική Γερμανία αλλά και απειλών ασφαλείας προερχομένων από ημεδαπά φιλοναζιστικά και αργότερα φιλομαρξιστικά στοιχεία. Οι ταραγμένες δεκαετίες του 1970 και 1980 με αιματηρές δράσεις αλλοδαπών και εγχώριων ομάδων (Μαύρος Σεπτέμβρης, Rote Armee Fraktion / RAF) αναγκάζουν την BfV να εμπλακεί στον αντιτρομοκρατικό σχεδιασμό. Η πτώση του Τείχους δημιουργεί νέους κινδύνους: παρατηρείται άνοδος του νεοναζισμού τη στιγμή που ευαίσθητα υλικά και τεχνολογία / τεχνογνωσία της πρώην ανατολικής Γερμανίας δεν πρέπει να εξαχθούν προς αγνώστους προορισμούς. Λίγα χρόνια αργότερα είναι η 11^η Σεπτέμβρη που αναταράσσει -η Υπηρεσία ουσιαστικά μετατρέπεται σε υπηρεσία τόσο αντικατασκοπίας όσο και εσωτερικής ασφαλείας αν και ποτέ δεν παραιτείται από το συντονισμό των δεκαέξι ανεξαρτήτων Landes ämter für Verfassungsschutz (LfV / Regional Intelligence Organizations), ένα

⁵⁷ Warnes Richard, "France" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 84

⁵⁸ ό. π., σ. 84, 90-91. Για μια επιπλέον ματιά γύρω από τις σχέσεις μεταξύ DST, DCRG, αστυνομικών αλλά και δικαστικών αρχών βλέπε Kirby Aidan, "Domestic Intelligence Agencies After September 11, 2001: How Five Nations Have Grappled with the Evolving Threat" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 149-152

για κάθε κρατίδιο.⁵⁹ Η BfV δεν έχει δικαίωμα σύλληψης / ανάκρισης υπόπτων, δεν εντέλλεται ερεύνες ή κατάσχεσης στοιχείων. Η έλλειψη, προφανώς, αυτών των εκτελεστικών δυνατοτήτων μετατρέπει την Υπηρεσία αποκλειστικά σε συλλέκτη / αναλυτή πληροφοριών που διασπείρονται στις ομοσπονδιακές Bundesgrenzschutz (BGS / Federal Border Guard) και Bundeskriminalamt (BKA / Federal Criminal Police) όπως και στις Landespolizei ανάλογες αστυνομικές αρχές των κρατιδίων.⁶⁰ Τονίζουμε ότι η BKA συνθέτει σώμα με αρμοδιότητες τόσο law enforcement όσο, κυρίως, εσωτερικής ασφαλείας με αποστολή την πάταξη της τρομοκρατίας και του οργανωμένου εγκλήματος, συνεπώς, η συνεργασία με την BfV θεωρείται δεδομένη.⁶¹ Στα τέλη του 2004 / αρχές του 2005 η γερμανική κυβέρνηση δημιουργεί το Gemeinsamen Terrorismusabwehrzentrum (GTAZ / Joint Counterterrorism Center) με έδρα το Βερολίνο. Σκοπός του οργανισμού καθίσταται η συνεργασία εκπροσώπων από σχεδόν σαράντα Υπηρεσίες [μεταξύ αυτών της BfV, της BKA, της ομοσπονδιακής υπηρεσίας εξωτερικών Πληροφοριών (Bundesnachrichtendienst / BND), της στρατιωτικής υπηρεσίας αντικατασκοπίας και αντιτρομοκρατίας (Militärischer Abschirmdienst / MAD), τοπικών αστυνομικών αρχών κ. λ.] αλλά και ειδικών θεωρητικών από το χώρο του law enforcement και του intelligence.⁶² Παρότι η διαπλοκή των αμιγώς Υπηρεσιών, των ανάλογων εσωτερικής ασφαλείας και του law enforcement καθίσταται σαφής, κάτι άλλο, κατά την άποψή μας αλλά και εμμέσως κατά τον Richard Warnes, πρέπει, επίσης, να ερευνηθεί: κατά πόσο το υπάρχον ευρύ σύστημα εσωτερικών πληροφοριών, ένα σύστημα που κατ' ουσίαν «τρέχει» βάσει του πολιτικού σχεδιασμού των δεκαέξι κρατιδίων, είναι κατάλληλο για την αντιμετώπιση των νέων κινδύνων; Μήπως η «πληροφοριακή αποκέντρωση», απότοκο ξορκίσματος των μεταπολεμικών φοβιών περί επανάκαμψης ενός συγκεντρωτικού κράτους, παρακωλύει τη δημιουργία μιας συνολικής κρατικής στρατηγικής κατά της τρομοκρατίας; Μήπως δυσχεραίνεται η ροή πληροφοριών εντός πάμπολλων Υπηρεσιών; Η συζήτηση, τουλάχιστον μέχρι τα τέλη της δεκαετίας του 2010, ανάβει με εκατέρωθεν επιχειρήματα.⁶³

Επισημάνσεις

Ο A. C. Wasemiller, ήδη από το 1969, γράφει ότι η λεγόμενη 'εσωτερική πληροφόρηση' συνεργάζεται με τις αστυνομικές αρχές λόγω επιχειρησιακών αναγκαιοτήτων. Αυτό δεν σημαίνει ότι αντικατασκοπία και αντιεγκληματική δράση ταυτίζονται. Σχετικά με το ερώτημα του δικαιώματος εκτελεστικής δράσης ή μη από τις Υπηρεσίες, ο ίδιος θεωρεί πως πρόκειται περισσότερο για ένα ακαδημαϊκό ερώτημα παρά για κάτι άλλο. Αν από την άλλη μεριά μια υπηρεσία Πληροφοριών

⁵⁹ Warnes Richard, "Germany" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 93-98

⁶⁰ ό. π., σ. 101

⁶¹ ό. π., σ. 107-108

⁶² ό. π., σ. 108-109

⁶³ ό. π., σ. 114, βλέπε επίσης Daun Anna, "Germany" στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014, σ. 223- 226, Kirby Aidan, "Domestic Intelligence Agencies After September 11, 2001: How Five Nations Have Grappled with the Evolving Threat" στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, ό. π., σ. 152-154

αποκτήσει δικαιώματα law enforcement, τότε, οφείλει να τα διαχειριστεί με φειδώ και συνέπεια.⁶⁴

Ο Adrian James εμμέσως συμφωνεί με τον Wasemiller. Διερωτάται εάν πράγματι η αστυνομική πληροφόρηση αντιπροσωπεύει κάτι νεοφανές ή όχι.⁶⁵ Ο Wesley Skogan τονίζει ότι ο ενθουσιασμός περί intelligence-led policing έχει να κάνει με τους θεωρητικούς και πολύ λιγότερο με τους επιχειρησιακούς του πεδίου.⁶⁶ Ο Robert Reiner βεβαιώνει πως υπάρχουν καλομελετημένα παραδείγματα που αποδεικνύουν ότι το *targeted policing* δύναται να επηρεάσει επί τα βελτίω την πορεία στη μάχη κατά του εγκλήματος.⁶⁷ Πάρα ταύτα, επανέρχεται ο James, η γοητεία του intelligence-led policing παρέμενε και παραμένει περιορισμένη καθώς η αστυνομική ορθοδοξία δείχνει ότι η επίδρασή του είναι πολύ περιορισμένη σε σχέση μ' αυτήν που η ρητορική του ζητήματος υποθέτει.⁶⁸ Τουλάχιστον μέχρι και την τελευταία δεκαετία του 20^{ου} αιώνα, συμπληρώνει ο Brian Flood, το intelligence-led policing δεν γινόταν αποδέκτης ιδιαίτερης προσοχής.⁶⁹

Συμπεράσματα / Προτάσεις Συμπεράσματα

A. Πέριξ των εγκληματικών / τρομοκρατικών γκρουπ με δύο λόγια

- Η ανάδυση διεθνικών εγκληματικών οργανώσεων αποτελεί πραγματικότητα.
- Η ανάδυση διεθνικών τρομοκρατικών οργανώσεων είναι γεγονός.
- Η κουλτούρα της δικτυακής οργάνωσης των εγκληματικών και τρομοκρατικών συσσωματώσεων δεν δύναται να παραβλεφτεί.
- Η χρήση της υψηλής τεχνολογίας από εγκληματικές και τρομοκρατικές ομάδες αποτελεί πλέον σύνηθες φαινόμενο.
- Η διαπλοκή εγκλήματος και τρομοκρατίας θεωρείται δεδομένη.
- Η διαπλοκή εγκλήματος και τρομοκρατίας γεννά καινοφανείς κινδύνους εθνικής ασφαλείας.

B. Πέριξ της πληροφοριακής κοινότητας με δύο λόγια

- Η πληροφοριακή κοινότητα διαθέτοντας πληθώρα μέσων και απόθεμα τεχνογνωσίας δύναται να παίζει επικουρικό ή κεντρικό ρόλο στην αντιμετώπιση των νέων προκλήσεων.
- Η πληροφοριακή κοινότητα διαθέτοντας πλήθος στοιχείων δύναται να σχετίσει περιοχές του εγκλήματος με περιοχές της τρομοκρατίας. Η συγκεκριμένη

⁶⁴ Wasemiller C. A., "The Anatomy of Counterintelligence" στο *Studies in Intelligence*, Volume 13, Number 1, 1969, διαθέσιμο στο https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol13no1/html/v13i1a02p_0001.htm εις το οποίο καταφύγαμε την 5^η Μαΐου 2016

⁶⁵ James Adrian, *Examining Intelligence-Led Policing. Developments in Research, Policy and Practice*, Palgrave Mcmillan, 2013, σ. 2

⁶⁶ Skogan Wesley, "Why Reforms Fail?", *Policing and Society*, 18, 1, March 2008, σ. 23

⁶⁷ Reiner Robert, *The Politics of the Police*, OUP, Oxford, 2000², σ. 217

⁶⁸ James Adrian, *Examining Intelligence-Led Policing. Developments in Research, Policy and Practice*, Palgrave Mcmillan, 2013, σ. 3

⁶⁹ Flood Brian, "Strategic Aspects of the UK National Intelligence Model" στο *Strategic Thinking in Criminal Intelligence*, επιμ. Ratcliffe Jerry, Federation Press, Σύδνεϋ, 2003, σ. 37-51

επικάλυψη δεν είναι πάντα ορατή, έχει να κάνει, δε, με την έκρηξη της τεχνολογίας και το φαινόμενο της παγκοσμιοποίησης.

- Εάν αποφασιστεί μια αποκλειστική ενασχόληση των Υπηρεσιών με τους κινδύνους του 21^{ου} αιώνα θα απαιτηθεί μια αλλαγή στο νομικό πλαίσιο που τις καλύπτει.

Γ. Πέριξ των law enforcement αρχών με δύο λόγια

- Σε πολλές περιπτώσεις οι law enforcement αρχές συνεργάζονται με τους πληροφοριακούς οργανισμούς.
- Αυτόνομα οι law enforcement αρχές δεν διαθέτουν τα μέσα των Υπηρεσιών διά την εξουδετέρωση της νέας γενιάς κινδύνων. Από τη μεριά τους οι αντιτρομοκρατικές μονάδες, είτε ανήκουν στο law enforcement είτε όχι, δομούν μάλλον μια ενδιάμεση, μεταξύ πληροφόρησης και επιβολής νόμου, περιοχή.
- Εάν το law enforcement κληθεί να αντιμετωπίσει αποκλειστικά τις νέες εγκληματικές / τρομοκρατικές συσσωματώσεις, τότε, πρέπει να υιοθετήσει ή να ενισχύσει μια πληροφοριακή κουλτούρα που μέχρι το τέλος του 20^{ου} αιώνα δεν το χαρακτήριζε.

Προτάσεις

Προτάσεις αντιμετώπισης μη συστημικών / ασύμμετρων κινδύνων εθνικής ασφαλείας σε δομικό / γραφειοκρατικό επίπεδο με δυο λόγια

- Αποκλειστική ενασχόληση των Υπηρεσιών και δη και αυτών της Αντικατασκοπίας με σχεδιασμούς εξουδετέρωσης μη συστημικών / ασύμμετρων κινδύνων εθνικής ασφαλείας.
- Αποκλειστική ενασχόληση των law enforcement αρχών με σχεδιασμούς εξουδετέρωσης μη συστημικών / ασύμμετρων κινδύνων εθνικής ασφαλείας υπό την προϋπόθεση ανάπτυξης συναφούς με τις Υπηρεσίες επιχειρησιακής / πληροφοριακής κουλτούρας.
- Συγχώνευση τμήματος ή τμημάτων των Υπηρεσιών με τμήμα ή τμήματα των law enforcement αρχών.
- Δημιουργία νέας διακριτής δομής εν είδει υβριδίου προερχόμενο από τη συνάντηση των πληροφοριακών οργανισμών με τους αντίστοιχους επιβολής νόμου.
- Ενίσχυση της συνεργασίας των Υπηρεσιών με τις law enforcement αρχές.

Σε κάθε περίπτωση οι ανανεωμένες προκλήσεις ασφαλείας επηρεάζουν το σύνολο των οργανισμών που εντέλλονται στην προστασία του εθνικού περιβάλλοντος. Οι κρατικοί δρώντες επιζητούν γνώση των προθέσεων, των δυνατοτήτων, των σχεδιασμών, του modus operandi των, πολλές φορές, αοράτων εχθρών. Πλέον δόκιμη πρόταση σε πρώτη φάση φαντάζει αυτή της περαιτέρω συνεργασίας των υπηρεσιών law enforcement και Πληροφοριών σε εθνικό και διεθνές επίπεδο. Κάτι τέτοιο κάθε άλλο παρά είναι εύκολο για λόγους που σχετίζονται με θέματα γραφειοκρατίας, ανταγωνισμών, κουλτούρας, επιχειρησιακών δυνατοτήτων, λειτουργικών / δομικών διαδικασιών / σχημάτων, πολιτικών προθέσεων, νομικών πλαισίων, συνταγματικών απαιτήσεων, διεθνών στρατηγικών, ιδεολογιών, εθνικών φοβιών κ. λ. Μόλα ταύτα οι σύγχρονες απειλές οδηγούν πιθανώς στη σύμπραξη. Το είδος αυτής μένει να μορφοποιηθεί κατά τις ανάγκες των καιρών.

ΚΕΦΑΛΑΙΟ 10

Τα όρια της πληροφόρησης / αντιπληροφόρησης εντός της προσπάθειας επίρρωσης περιβάλλοντος εθνικής ασφαλείας, επίτευξης κρατικών σχεδιασμών και πλήρωσης ανάλογων συμφερόντων

Οκτώ χρόνια πόλεμος ... ο τεράστιος πληροφοριακός μηχανισμός στέκεται ανίκανος να απαντήσει σε θεμελιώδεις ερωτήσεις περί του περιβάλλοντος εντός του οποίου αμερικανικές και συμμαχικές δυνάμεις επιχειρούν, περί του κόσμου που αυτές οι δυνάμεις επιθυμούν να προσεγγίσουν

Στρατηγός Michael Flynn¹

Τα όρια της πληροφόρησης (I)

Το 2002 ο Donald Rumsfeld προκάλεσε θυμηδία δηλώνοντας πως ...*υπάρχουν πράγματα που γνωρίζουμε ότι γνωρίζουμε, υπάρχουν πράγματα που γνωρίζουμε ότι δεν γνωρίζουμε, αλλά, υπάρχουν και πράγματα που δεν γνωρίζουμε ότι δεν γνωρίζουμε.*² Ουσιαστικά, ο Αμερικανός υπουργός Αμύνης περιέγραφε μια κεντρική και αναπόδραστη πραγματικότητα, την πραγματικότητα μιας αφθονίας αβεβαιοτήτων που καθιστούν το διεθνές πολιτικοστρατιωτικό περιβάλλον αρκούντως ανασφαλές. Εντός αυτού, ακόμα και η πιο οργανωμένη Υπηρεσία δεν μπορεί ποτέ να διεκδικήσει την παντογνωσία.³

Πληροφόρηση, γράφουν οι Gill και Phythian, δεν σημαίνει γνώση του μέλλοντος. Το πληροφοριακό μοντέλο βρίθει προβληματισμών που δύνανται να γίνουν αιτία παραγωγής λανθασμένου προϊόντος. Κάποιες από τις στρεβλώσεις έχουν να κάνουν με εγγενή μειονεκτήματα όπως και με γνωσιακούς περιορισμούς. Άλλες ανακαλύπτονται στην πληροφοριακή διαδικασία καθαυτή. Σχετίζονται με τη δυσκολία αναγνώρισης στόχου, την τάση επικέντρωσης λόγω πρακτικών αναγκαιοτήτων ή ιδεολογιών σε συνήθεις υπόπτους, τις εσωτερικές γραφειοκρατικές κόντρες, την αποτυχία διαμοιρασμού πληροφοριακών δεδομένων κυρίως λόγω της κουλτούρας της μυστικότητας ή, γενικότερα, της «κουλτούρας των Υπηρεσιών».⁴ Επιπλέον, οι όποιοι πληροφοριακοί στόχοι (οργανισμοί, ομάδες ή άτομα) ουδέποτε παραμένουν αδρανείς. Διαθέτοντας δική τους ατζέντα αναπτύσσουν τεχνικές και αντίμετρα προκειμένου να προστατεύσουν τα μυστικά τους εκδηλώνοντας τόσο

¹ Flynn Michael, Pottinger Matt, Batchelor Paul, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan" στο *Voices from the Field* series, Center for a New American Security, Washington, D.C., Ιανουάριος 2010, σ. 7

² Transcript: Defense Department Briefing, February 12, 2002 στο <http://www.usembassy-israel.org.il/publish/peace/archives/2002/february/021301.html> όπου καταφύγαμε την 30^η Ιουλίου 2012, επίσης βλέπε στη σελίδα www.quotationspage.com/quote/30526.html εις την οποία ανατρέξαμε τη 13^η Δεκεμβρίου 2016

³ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, Polity Press, USA, 2012², σ. 143

⁴ Ακριβώς αυτό υποστηρίζει ο Garret Jones της CIA. Πρόκειται περί ζητήματος κουλτούρας, "it's a cultural thing", τονίζει. Αναφέρεται σε μια νοοτροπία που επηρεάζει αποφάσεις / δράσεις που σχετίζονται από το επιχειρησιακό σκέλος της Υπηρεσίας μέχρι τον τρόπο προαγωγών εντός αυτής -για μια εικόνα βλέπε Jones Garret, "It's a Cultural Thing: Thoughts on a Troubled CIA" στο *Secret Intelligence*, επιμ. Aldrich R., Andrew C., Wark W., Routledge, London, 2009, σ. 26-39, εναλλακτικά βλέπε στη δικτυακή τοποθεσία <http://users.clas.ufl.edu/zselden/Course%20Readings/Jones.pdf> ή στον ιστότοπο http://www.unc.edu/depts/diplomat/item/2005/0709/jone/jones_cia2.html, επίσης στη σελίδα του Foreign Policy Research Institute / FPRI <http://www.fpri.org/article/2005/06/its-a-cultural-thing-thoughts-on-a-troubled-cia-part-one/> (κοινή ημερομηνία εισόδου η 5^η Φεβρουαρίου 2017)

αμυντικούς όσο επιθετικούς τακτικισμούς με σκοπό την απόκρουση, αποδιοργάνωση ή παραπλάνηση του αντιπάλου.⁵

Ο Richard Betts ελέγχοντας τους ‘παίκτες’ της πληροφόρησης, γράφει:

Εξετάζοντας τις πλέον γνωστές περιπτώσεις πληροφοριακών αποτυχιών⁶ παρατηρούμε ότι πολύ σπάνια το κρίσιμο λάθος αποδίδεται στους συλλέκτες πρωτογενών στοιχείων, περιστασιακά στους επαγγελματίες της παραγωγής τελικού προϊόντος και πολλάκις στους decisionmakers ήτοι, στους αποδέκτες του τελευταίου. Το πολιτικό περιβάλλον και οι κυβερνητικές αναγκαιότητες περιορίζουν τη δυνατότητα αντίληψης / εκτίμησης των πραγμάτων. Η πληροφοριακή αποτυχία είναι πολιτική και ψυχολογική πολύ περισσότερο από οργανωτική / υπηρεσιακή. Μελετητές τέτοιων εντυπωσιακών γεγονότων συχνά υποθέτουν πως η καταστροφή θα μπορούσε να αποφευχθεί μέσω βελτιστοποίησης των αναλυτικών διαδικασιών. Η συγκεκριμένη ελπίδα είναι ψεύτικη. Η διαδικασία παραγωγής πληροφόρησης μόνο ελάχιστα δύναται να βελτιωθεί μέσω δράσεων που αφορούν στο κομμάτι της ανάλυσης. Αυτή η ελπίδα δεν είναι μόνο φρούδα αλλά και επικίνδυνη εφόσον συνεισφέρει στην άποψη πως ένα, έστω συστηματικό, πρόγραμμα μεταρρυθμίσεων των Υπηρεσιών δύναται να αυξήσει κατακόρυφα την ικανότητα πρόβλεψης απειλών.⁷

Βάσει των ανωτέρω, οι περιορισμοί στην πληροφοριακή διαδικασία υπαγορεύουν την σχεδόν αποδοχή μιας πληροφοριακής αποτυχίας. Εν μέρει πρόκειται για αποτέλεσμα του αδύνατου παραγωγής τέλει ‘πρόβλεψης’, εν μέρει της τάσης των πολιτικών να λανθάνουν φοβούμενοι συνήθως το χειρότερο σενάριο ή, απλώς, της τάσης να αγνοούν την πληροφόρηση όταν αυτή έρχεται σε αντίθεση με τα πιστεύω τους· ο βαθμός έκθεσης σε λάθη συνδέεται με το στρατηγικό περιβάλλον εντός του οποίου καλούνται να δράσουν οι ηγέτες.⁸

Η Amy Zegart έρχεται σε αντίθεση με τον Betts. Ερευνώντας την καταστροφή της 11^{ης} Σεπτεμβρίου υποστηρίζει πως οι λόγοι της αποτυχίας των Υπηρεσιών έχουν να κάνουν με: α) εσωτερικές παθολογίες που δεν επέτρεψαν στους πληροφοριακούς οργανισμούς να υιοθετήσουν νέες τεχνολογίες, ιδέες και τακτικές, β) ένα ακατάλληλο σύστημα προαγωγών των αξιωματούχων των Υπηρεσιών και γ) δομικές αδυναμίες δεκαετιών που εμπόδισαν τη συνεργατική / συνεκτική λειτουργία της αμερικανικής πληροφοριακής κοινότητας.⁹ Κατά την Zegart ο δομικός κερματισμός περιορίζει την

⁵ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 144

⁶ Οι Shulsky και Schmitt ορίζουν την πληροφοριακή αποτυχία ως παρανόηση καταστάσεων που δύναται να οδηγήσουν μια κυβέρνηση σε ακατάλληλη ή αντιπαραγωγική δράση (ή μη δράση) ως προς τα συμφέροντά της -περί τούτου βλέπε Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, Brassey's, Inc., Washington, D. C., ΗΠΑ, 2002³, σ. 63, επίσης ανέτρεξε στο Eiran Ehud, “Preventing the ‘Next Intelligence Failure’? The Three Tensions of Investigating Intelligence Failures”, έγγραφο παρουσιάσθέν στο Ετήσιο Συνέδριο της Ένωσης Διεθνών Μελετών (International Studies Association), Hawaii, 1-5 Μαρτίου 2005, σ. 4 και στο Jensen Mark, “Intelligence Failures: What Are They Really and What Do We Do about Them?” στο *Intelligence and National Security*, Volume 27, Number 2, 2012, σ. 270

⁷ Betts R., “Analysis, War and Decision: Why Intelligence Failures Are Inevitable” στο *World Politics*, 31, 1, 1978, σ. 61-89. Μάλιστα ο Betts στη σελίδα 88 τονίζει πως ...οι πληροφοριακές αποτυχίες είναι τόσο αναπόφευκτες όσο και ‘φυσικές’. Ο Christopher Andrew γράφει πως «οι ιστορικές καταθέσεις αποδεικνύουν ότι πολύ συχνά το ευαίσθητο σημείο στον πληροφοριακό κύκλο ανακαλύπτεται εντός της διαδικασίας της εκτίμησης ή της σχέσεως των Υπηρεσιών με το πολιτικό προσωπικό παρά εντός της συλλεκτικής προσπάθειας. Η απάντηση στο ‘πώς’ και στο ‘γιατί’ μιας αποτυχίας απαιτεί περαιτέρω έρευνα, πρώτα και κύρια, εντός αρχειακού υλικού» -για περισσότερες λεπτομέρειες βλέπε Andrew Christopher, “Intelligence, International Relations and ‘Under-Theorization’” στο *Intelligence and National Security*, Volume 19, Number 2, 2004, σ. 170-184

⁸ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 144

⁹ Zegart Amy, *Spying Blind: The CIA, the FBI and the Origins of 9/11*, Princeton University Press, Princeton, 2007, σ. 4

επικοινωνία, έτσι, το κλειδί της ελαχιστοποίησης των αποτυχιών ανευρίσκεται στην οργανωτική μεταρρύθμιση, στην αλλαγή μοντέλου διοίκησης και στη προθυμία υιοθέτησης ανταγωνιστικών υποθέσεων με σκοπό την πρόκριση της πλέον πιθανής.¹⁰

Ο Frank Snep, κορυφαίος αναλυτής της CIA, αναφέρεται στην τροχοπέδη της λεγόμενης *κυρίαρχης υπόθεσης*. Ο ίδιος θυμάται:

Όταν εκπαιδευόμουν στη CIA προκειμένου να μεταβώ στο Βιετνάμ καθημερινά άκουγα περί της θεωρίας του ντόμινο ... Η υιοθέτηση της συγκεκριμένης θεωρίας απέτέλεσε τρομερό σφάλμα. Εξ αιτίας της διαιωνίσαμε αλλά και δικαιολογήσαμε την παρουσία μας εκεί.¹¹

Η κυρίαρχη υπόθεση (ή *επίμονη πίστη*) απέτέλεσε, όσον αφορά στην περίπτωση της σοβιετικής εισβολής στο Αφγανιστάν, κύριο αναλυτικό εμπόδιο εντός της πληροφοριακής κοινότητας των ΗΠΑ. Ειδικότερα, οι αμερικανικές Υπηρεσίες απέτυχαν να διαγνώσουν την επικείμενη επίθεση του Κόκκινου Στρατού θεωρώντας πως η Σοβιετική Ένωση δεν είχε διάθεση να προχωρήσει σε στρατιωτική κίνηση τέτοιας κλίμακας. Το Μάρτιο του 1979 η CIA συμπέρανε πως:

Οι Σοβιετικοί [θα είναι] ιδιαίτερα διστακτικοί στην προοπτική μετακίνησης ικανού όγκου στρατιωτικών δυνάμεων εντός της επικράτειας του Αφγανιστάν προκειμένου να στηρίξουν μια κυβέρνηση που χάνει τη λαϊκή νομιμοποίηση. Όχι μόνο θα βρεθούν σε τέλμα αλλά θα βλάψουν δυνητικά τις σχέσεις τους με την Ινδία και, σε μικρότερο βαθμό, με το Πακιστάν. Ως πιθανότερη επιλογή προκρίνεται η προσπάθεια επανασύνδεσης με μέλη της αντιπολίτευσης, μέλη με τα οποία στο παρελθόν η Μόσχα έχει συνεργαστεί.¹²

Η εισβολή έπιασε εξαπίνης τους Αμερικανούς. Η πληροφοριακή αποτυχία δεν ήρθε ως αποτέλεσμα έλλειψης στοιχείων αλλά ως αποτέλεσμα πίστης περί «λήψης ορθολογικής απόφασης» εκ μέρους του αντιπάλου. Η CIA δεν έβρισκε εύλογη μια τέτοια επιχείρηση. Προσπάθησε να προσαρμόσει τις ενδείξεις στις εκτιμήσεις παρά να δει την αλήθεια ήτοι, την αντίθεση μεταξύ των πρώτων με τις δεύτερες. Ο Jack Davies σημειώνει: «Όποια και αν είναι η ειδημοσύνη των αναλυτών, το μυαλό τείνει να συντάσσεται με την πληροφόρηση που επιβεβαιώνει παρά προκαλεί μια εγκατεστημένη άποψη / κρίση». Επιπλέον, «παρά τη γνώση της ύπαρξης του μειονεκτήματος της (γνωστικής) αδυναμίας, η όποια προκατάληψη κατά τη διαδικασία εκτίμησης της πληροφορίας δεν απομακρύνεται». ¹³ Η περίπτωση του Αφγανιστάν συμπεριελήφθη το 1983 σε μια έκθεση / έρευνα με σκοπό την ακτινοσκόπηση των πλέον «κτυπητών πληροφοριακών αποτυχιών τα τελευταία είκοσι έτη». Κατά το συγκεκριμένο paper:

¹⁰ Zegart Amy, *Spying Blind: The CIA, the FBI and the Origins of 9/11*, ό. π., σ. 112-115, επίσης βλέπε Dahl J. Erik, "Missing the Wake-up Call: Why Intelligence Failures Rarely Inspire Improved Performance" στο *Intelligence and National Security*, Volume 25, Number 6, 2010, σ. 796-799, Perrow Charles, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*, Princeton University Press, Princeton, 2007, σ. 323

¹¹ BBC Radio 4, *Spies R Us* στο http://www.bbc.co.uk/radio4/history/spies_cia.shtml εις το οποίο καταφύγαμε τη 13^η Δεκεμβρίου 2016

¹² MacEachin D., "Predicting the Soviet invasion of Afghanistan: the intelligence community's record" στον ιστότοπο <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record.html> εις τον οποίο καταφύγαμε την 15^η Δεκεμβρίου 2016

¹³ Davis J., *Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence* στη σελίδα <https://www.cia.gov/library/kent-center-occasional-papers/vol2no2.htm> όπου ανατρέξαμε την 15^η Δεκεμβρίου 2016

Η [αμερικανική] πληροφοριακή κοινότητα εκτίμησε με ακρίβεια τα πλεονεκτήματα και τα μειονεκτήματα της εισβολής. Η κοινότητα βασισμένη στην υπόθεση πως τα δεύτερα είναι πολύ περισσότερα από τα πρώτα έκρινε ότι η Σοβιετική Ένωση θα δρούσε ορθολογικά και σύμφωνα με τα, κατά την εκτίμηση των αμερικανικών Υπηρεσιών, συμφέροντά της. Όσο αληθινό έχει αποδειχτεί το κόστος που πληρώνει η ΕΣΣΔ, τόσο αληθές είναι πως αποτύχαμε να συλλάβουμε τις ανάγκες της σοβιετικής πολιτικής όπως η τελευταία τις συνελάμβανε. Διαθέταμε μια καθαρή εικόνα των δυνατοτήτων τους αλλά κάναμε λάθος ως προς τις προθέσεις τους.¹⁴

Μια άλλη αμερικανική αποτυχία σχετίστηκε με τη (δεύτερη) πυρηνική δοκιμή της Ινδίας, επρόκειτο για σειρά πέντε εκρήξεων σχάσης - σύντηξης που την ενέταξαν στο κλαμπ των χωρών με πλήρη πυρηνική ισχύ. Η Ουάσιγκτον αντιλήφθηκε την εξέλιξη μόνο κατόπιν σχετικής ανακοίνωσης του Δελχί τον Μάιο του 1998¹⁵ η Ινδία απέφυγε επιμελώς οποιαδήποτε γνωστοποίηση των προθέσεων της πριν τα τεστ. Στο *Jeremiah Report* κριτικάρεται η ψευδής εντύπωση των αμερικανικών Υπηρεσιών περί μη διάθεσης των Ινδών να προβούν σε πυρηνικό-ά τεστ¹⁵, ο, δε, Gregory Treverton επικαλείται ένα σύνολο γνωστικών, δομικών και επιχειρησιακών ανεπαρειών / λαθών ήτοι:

- Το mirror-imaging φαινόμενο.
- Την πλημμελή συνεργασία των πληροφοριακών οργανισμών των ΗΠΑ.
- Την απουσία human intelligence εντός Ινδίας.
- Την περί πληροφόρησης εξάρτηση από τεχνητούς δορυφόρους και μόνο.¹⁶

Περαιτέρω, οι George Perkovich και Ronald Kessler σημειώνουν με επικριτική διάθεση:

- Την ενημέρωση Ινδών αξιωματούχων το 1995 από τον Αμερικανό πρόεδρο στη χερσόνησο περί ύπαρξης εικόνων που δείχνουν «προετοιμασίες», άρα, την απόδοση / επίδοση χρόνου προκειμένου κάλυψης / απόκρυψης αυτών ακριβώς των προετοιμασιών και
- την ύπαρξη δορυφορικών απεικονίσεων / αποδείξεων προετοιμασιών σε τελικό στάδιο ακριβώς τη νύκτα πριν την έναρξη των δοκιμών¹⁷ οι αναλυτές της CIA ουδέποτε τις έλαβαν υπόψη.¹⁷

Τόσο στην περίπτωση του Αφγανιστάν όσο και σε αυτή της Ινδίας, η πληροφοριακή αποτυχία έγκειται στην αδυναμία πρόβλεψης συμπεριφοράς του στόχου με αποτέλεσμα τη δημιουργία εκπλήξεων. Ασφαλώς θα ήταν άκοπο για έναν αναλυτή να προβεί σε πρόγνωση καταστάσεων εάν αυτές ακολουθούσαν μία «λογική συνέχεια / συνέπεια» βασισμένη σε μόνιμα patterns. Η απόκλιση από το αναμενόμενο αποτελεί συχνό φαινόμενο, φαινόμενο που οφείλεται στην αλλαγή συμπεριφοράς του άλλου παράγοντα. Μια τέτοια αλλαγή (που θα επηρεάσει ακόλουθες δράσεις) γίνεται

¹⁴ Στο <https://www.cia.gov/library/readingroom/docs/CIA-RDP86B00269R001100100010-7.pdf> με τίτλο “Report on a Study of Intelligence Judgments” (ημερομηνία καταφυγής η 15^η Δεκεμβρίου 2016), επίσης βλέπε *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, επιμ. Westerfield B. H., Yale University Press, New Haven, 1995, σ. 254

¹⁵ Weiner Tim, “CIA Study Details Failures; Scouring of System Is Urged”, 3 Ιουνίου 1998, στη δικτυακή τοποθεσία <http://www.nytimes.com/1998/06/03/world/cia-study-details-failures-scouring-of-system-is-urged.html> εις την οποία ανατρέξαμε τη 16^η Δεκεμβρίου 2016

¹⁶ Treverton Gregory, *Reshaping National intelligence for an Age of Information*, Cambridge University Press, New York, 2003, σ. 1-8

¹⁷ Perkovich George, *India's Nuclear Bomb: The Impact on Global Proliferation*, University of California Press, Berkeley, 1999, σ. 417-418, Kessler Ronald, *The CIA at War*, St. Martin's Press, New York, 2004, σ. 210-212, επικουρικά βλέπε Shelton Christina, “The Roots of Analytic Failures in the Intelligence Community” στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 4, 2011, σ. 645-646

άμεσα αναγνωρίσιμη μόνο μέσω πληροφοριών από πηγές πολύ κοντά στον decisionmaker. Ουσιαστικά ομιλούμε για το «what do they think?» δίλημμα¹⁸, ένα δίλημμα το οποίο θα παρήγαγε, ως γνωστική παίδευση, καρπούς μόνο αν απαλλασσόταν από εγκατεστημένες κυρίαρχες σκέψεις, υποθέσεις ή απόψεις που συνηθέστατα οδηγούν σε λάθος προεικονίσεις.

Πολύ σημαντικό κεφάλαιο στη μελέτη της πληροφοριακής αποτυχίας δεικνύει η σχέση μεταξύ των ανθρώπων των Υπηρεσιών με τους ανθρώπους του πολιτικού συστήματος. Ο Loch Johnson εντός των «επτά αμαρτιών της στρατηγικής πληροφόρησης» εντάσσει το φαινόμενο της παράβλεψης ή και περιφρόνησης των Υπηρεσιών από τους διαμορφωτές πολιτικής.¹⁹ Κάτι τέτοιο συνέβη το 1941 όταν ο Ιωσήφ Στάλιν ηρνείτο επίμονα να δεχτεί πως η Γερμανία ετοίμαζε εισβολή στη χώρα παρά τις σχεδόν σίγουρες πληροφορίες που διέθετε ...κανένα μειονέκτημα στρατηγικής πληροφόρησης δεν μνημονεύεται περισσότερο από αυτό του πολιτικού που αυταπατώντας απορρίπτει στοιχεία μη συμμορφούμενα με το δικό του 'weltanschauung'.²⁰ Το είδος αυτής της πληροφοριακής αποτυχίας καθίσταται εξόχως πολιτικό υπό την έννοια μιας αρνητικής έκβασης που δεν χρεώνεται στην πληροφοριακή κοινότητα πέραν, ίσως, της αδυναμίας της να πείσει περί του επερχόμενου την πολιτική ηγεσία.²¹

Η πολιτικοποίηση της πληροφορίας (politicization)²² ως διαπλοκή μεταξύ Υπηρεσιών - Πολιτείας δύναται να συνδεθεί ή να αποτελέσει ιδιαίτερη εκτύπωση της

¹⁸ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό.π., σ. 149

¹⁹ Johnson Loch, *America's Secret Power: The CIA in a Democratic Society*, Oxford University Press, New York, 1989, σ. 63-64

²⁰ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 149

²¹ ibid

²² Ο Mark Lowenthal κατανοεί τους κινδύνους που εμπεριέχονται εξ αιτίας μη ορθής σχέσης Υπηρεσιών και πολιτικής αρχής. Βέβαια δεν είναι μόνο η κυβέρνηση που ενδέχεται να σύρει προς τις θέσεις της την πληροφοριακή κοινότητα, μπορεί να συμβεί και το αντίθετο. Πάρα ταύτα ο Lowenthal προβαίνει σε τρεις επισημάνσεις. Πρώτον, μια Υπηρεσία ως κάτοχος ευαίσθητων λεπτομερειών είναι φυσικό να διαμορφώνει γνώμη επί του άλφα ή του βήτα ζητήματος. Αν επιδώσει αυτή τη γνώμη στην ηγεσία με ουδέτερο τρόπο, τότε, δεν επιχειρεί κάτι απαράδεκτο. Απαράδεκτο είναι να φορμάρει κατά το δοκούν την πληροφοριακή διαδικασία με σκοπό την παραγωγή μη αντικειμενικού προϊόντος, σ' αυτήν την περίπτωση παγιδεύει την πολιτεία. Δεύτερον, δεν είναι επιλήψιμο για έναν πολιτικό να ζητήσει την άποψη των Υπηρεσιών. Τρίτον, μια κρατική ηγεσία διαθέτει την ευχέρεια να αποδεχτεί ή να απορρίψει ακριβώς αυτήν την άποψη χωρίς τούτο να καταδεικνύει υποχρεωτικά πρόβλημα συνεργασίας ή έλλειψη εμπιστοσύνης. Καθίσταται φανερό πως αν θελήσουν οι πολιτικοί άρχοντες δύνανται να δράσουν αντίθετα με ό,τι η πληροφοριακή ανάλυση ενδεχομένως προτείνει. Από την άλλη μεριά οι Υπηρεσίες δεν μπορούν, τουλάχιστον θεωρητικά, να προβούν σε συστάσεις πολιτικής, ωστόσο, αυτό στην πράξη πολλές φορές δεν ισχύει. Όταν τα ανώτατα κλιμάκια της κυβερνητικής ελίτ συνομιλούν με τα αντίστοιχα των Υπηρεσιών, τότε, η γνώμη ενός πολύπειρου πράκτορα ενδέχεται να εκληφθεί ως / μετατραπεί σε προτροπή -περί αυτών βλέπε Lowenthal M., *Intelligence. From Secrets to Policy*, CQ Press, Washington, 2002, σ. 4, 105-107. Σε αδρές γραμμές, το politicization αφορά σε καταστάσεις κατά τις οποίες οι πληροφοριακοί οργανισμοί: α) εξυπηρετούν πολιτικές βλέψεις και όχι τη διαδικασία λήψεως αποφάσεων, β) χειραγωγούνται μέχρι αλλαγής του τελικού προϊόντος από την κυβέρνηση, γ) ιδρύονται λόγω πολιτικών σκοπιμοτήτων (π. χ. παρακολούθηση εσωτερικών πολιτικών αντιπάλων), δ) στελεχώνονται από άτομα του πολιτικού συστήματος.

Κατά τον Hans Born οι Υπηρεσίες οφείλουν να αποδώσουν την πραγματική εικόνα σύμφωνα, τουλάχιστον, με τα αναλυτικά projects. Προκειμένου «να ειπωθεί η αλήθεια» καλούνται να λειτουργήσουν εντός ενός καθεστώτος *μόνωσης* αλλά επουδενί *απομόνωσης* ...the services should be insulated but not isolated from politics, κατ' αυτόν τον τρόπο αποφεύγεται η χειραγωγή τους, άρα, το τελικό αποτέλεσμα απαλλάσσεται από παρεμβάσεις -για περισσότερα βλέπε Born H., "Parliamentary and External Oversight" στο *Democratic Control of Intelligence Services. Containing Rogue Elephants*, επιμ. Born Hans, Caparini Marina, Ashgate Publishing, 2007, σ. 166. Το ίδιο υποστηρίζει ο James Steinberg τονίζοντας μια ανάγκη *arm's length relationship* υπό την έννοια μιας σχέσεως χωρίς συναλλαγές. Ο Gregory Treverton συνεισφέρει στην περί politicization συζήτηση χωρίς

κυρίαρχης υπόθεσης. Ας εξετάσουμε το εξής παράδειγμα: Έκθεση των αμερικανικών Υπηρεσιών στις αρχές του 1963 αναφέρει πως το Νότιο Βιετνάμ υποφέρει από αριθμό προβλημάτων όπως ανεπάρκεια ηγεσίας σε κάθε επίπεδο διοίκησης, χαμηλό ηθικό στις τάξεις των μαχίμων, σχεδόν ανύπαρκτο σύστημα πληροφοριών, διείσδυση κομμουνιστικών στοιχείων εντός των στρατιωτικών οργανισμών κ. λ. Παρά την αλήθεια του γεγονότος, παράγοντες όπως ο τότε DCI John McCone, η αμερικανική πρεσβεία στη Σαϊγκόν αλλά και πολιτικές προσωπικότητες αξίωναν μια λιγότερο ανησυχητική αποτύπωση. Ο Harold P. Ford γράφει:

Οι εκτιμήσεις των αναλυτών ξεσήκωσαν τις διαμαρτυρίες πολιτικών προσώπων. Τα τελευταία πίεσαν McCone και ONE [Office of National Estimates] ώστε το τελευταίο να ανασκευάσει κατά τρόπο που εξαφανίζει την κριτική στον ARVN [Army of the Republic of Vietnam]. Οι τόνοι πράγματι έπεσαν: στις πρώτες γραμμές του ανανεωμένου National Intelligence Estimate [NIE] τώρα διαβάζουμε ...πιστεύουμε ότι η κομμουνιστική επιρροή

να διαφοροποιείται κάπου δραματικά. Αυτό που κρατάμε από τον μελετητή, και φέροντας κατά νου τα λόγια του Hans Born, είναι το εξής: οι Υπηρεσίες στην προσπάθειά τους να λειτουργήσουν ανεξάρτητα από την πολιτική πρόθεση δεν πρέπει να αποξενωθούν από το περιβάλλον. Αν συμβεί κάτι τέτοιο το πληροφοριακό προϊόν κινδυνεύει να χαρακτηριστεί από ασυνέπεια ως προς τις εθνικές αναγκαιότητες. Πρόκειται για παγίδα εντός της οποίας εγκλωβίζονται οι Υπηρεσίες πολύ πιο συχνά από ό,τι συμβαίνει με την ανάλογη του politicization. Δεν είναι καθόλου σπάνιο να επιδίδονται στην κρατική ηγεσία πληροφορίες που αφορούν σε υποθέσεις που πόρρω απέχουν από τα πραγματικά προβλήματα ή ακόμα ακόμα να μη σχετίζονται με κάτι συγκεκριμένο -για μια ευρύτερη άποψη βλέπε Steinberg J., "The policymaker's Perspective: Transparency and Partnership" και Treverton Gr., "Intelligence Analysis: Between 'Politicization' and Irrelevance" στο *Analyzing Intelligence. Origins, Obstacles, and Innovations*, επιμ. George Roger, Bruce James, Georgetown University Press, Washington, D. C., 2008, σ. 89 και 92-93 αντιστοίχως. Ο Ιωάννης Ραγιές επισημαίνει πως πολλά από τα προβλήματα ενσκήπτουν λόγω της ένταξης πληροφοριακών οργανισμών στη δομή υπουργείων (Αμύνης, Εξωτερικών) -κατά τον τρόπο τούτο οι πιέσεις που ασκούνται προκειμένου να εξυπηρετήσουν προτεραιότητες ή σκοπιμότητες καθίστανται εξουθενωτικές. Η παροχή πληροφοριών επιβεβαίωσης πολιτικών θέσεων μπορεί να συνοδεύεται, ακόμα χειρότερα, με απόκρυψη στοιχείων. Δεν είναι λίγοι εκείνοι που υποστηρίζουν ότι πρέπει να διασφαλιστεί η μη παρουσία των Υπηρεσιών στη διαδικασία διαμόρφωσης πολιτικής, αλλά, κατά πόσο είναι εφικτό αυτό; -για μια άποψη βλέπε Ραγιές Ιωάννης, «Σύγχρονες προκλήσεις για τις Υπηρεσίες Πληροφοριών. Η συνδρομή στην άσκηση πολιτικής» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009, σ. 167-168. Από τη μεριά τους οι Betts και Paul Pillar σημειώνουν ότι: α) η πολιτικοποίηση της πληροφορίας, έστω σε ελάχιστο βαθμό, πάντα θα προκύπτει, β) το άμεσο, *top-down*, politicization δεικνύει την πλέον κατάφωρη παρέμβαση στο έργο των Υπηρεσιών, γ) το έμμεσο, *bottom-up*, politicization αφορώντας σε κανάλια επικοινωνίας μεταξύ Υπηρεσιών και εκτελεστικής εξουσίας ενδέχεται, τουλάχιστον κατά τον Betts, να αποδειχτεί επωφελές υπό την έποψη παραγωγής πληροφοριακού προϊόντος ευρισκόμενου σε άμεση συνάφεια με την πολιτική αναγκαιότητα. Από την άλλη μεριά για κάποιους το φαινόμενο δεν προσφέρεται για ουσιαστική κρίση καθώς η γνώμη των πολιτικών κατά τον έναν ή άλλο τρόπο θα υπερισχύσει, για κάποιους άλλους υφίσταται ως διελκυστίνδα επηρεάζοντας τη λειτουργία των δύο θεσμών -για περισσότερες λεπτομέρειες ανέτρεξε στο Betts R., "Politicization of Intelligence: Costs and Benefits" στο *Paradoxes of Strategic Intelligence*, επιμ. Betts R., Mahnken Thomas, Frank Cass Publishers, London, 2003, σ. 57-77 και στο Pillar Paul, "The Perils of Politicization" στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson L., Oxford University Press, N. York, 2010, κεφ. 29. Ίσως αρετικός εμφανίζεται ο Nathan Woodard. Ο μελετητής υποστηρίζει ότι οι Υπηρεσίες «οφείλουν να πείσουν» τους διαμορφωτές πολιτικής «να ακούσουν» καθώς αυτοί πολλές φορές παρουσιάζονται είτε ανίκανοι, είτε προκατειλημμένοι. Ουσιαστικά ο Woodard μας λέει πως δεν σημάνει κάτι κακό ή ανήθικο η εκ των αναλυτών καθοδήγηση της ηγεσίας υπό την παραδοχή πως οι πρώτοι είναι σε θέση να κατανοήσουν / προλάβουν την εξέλιξη των γεγονότων, πρόκειται για τη λεγόμενη «θετική πολιτικοποίηση / positive politicization» -περί τούτων βλέπε Marrin St., "Revisiting Intelligence and Policy: Problems with Politicization and Receptivity" στο *Intelligence and National Security*, Volume 28, Number 1, 2013, σ. 3-4, ειδικότερα, Woodard N., "Testing the Forbidden Fruit: Unlocking the Potential of Positive Politicization" στο αυτό τεύχος, σ. 91-108

περιορίζεται, πως η κατάσταση βελτιώνεται. Αυτή, συνεχίζει ο Ford, δεν ήταν από τις πλέον περήφανες στιγμές της CIA.²³

Ο Ford επισημάνει πως το μεγαλύτερο πρόβλημα των αναλυτών αναφορικά με την επίδοση του μηνύματος στην ηγεσία των ΗΠΑ σχετίστηκε με το γεγονός της παρουσίας ενός φορτισμένου πολιτικού κλίματος. Η απόφαση περί του «τι θα κάνουμε στο Βιετνάμ;» δεν μπορούσε να μην επηρεαστεί από αυτό.²⁴ Εντός της συγκεκριμένης ατμόσφαιρας η όποια άποψη εκ μέρους των Υπηρεσιών θα έπρεπε να υποστηρίξει τις ήδη ειλημμένες (πολιτικές) αποφάσεις, σε διαφορετική περίπτωση ουδέποτε θα γινόταν αποδεκτή.²⁵

Μια επόμενη περίπτωση είναι η περίπτωση της ιρανικής επανάστασης το 1979. Ο τότε DCI, ναύαρχος Stansfield Turner, υποστήριξε:

Το να βρεθούμε ως πληροφοριακή κοινότητα δίπλα στον Πρόεδρο και να πούμε ...*νομίζουμε ότι το Ιράν βρίσκεται στα πρόθυρα κατάρρευσης...* σηματοδοτεί μέγιστη αλλαγή. Είναι δύσκολο για οποιονδήποτε να κοντράρει τόσο πολύ μια ισχύουσα άποψη, να φτάσει σε ένα συμπέρασμα εντελώς αντιδιαμετρικό ως προς τη σχέση μεταξύ μας [μεταξύ ΗΠΑ-Ιράν].²⁶

Όμως πόσο εύκολο ήταν για την CIA καθαυτή να αποδεχτεί την πραγματικότητα ενός κλονισμένου ιρανικού καθεστώτος έτοιμου να καταρρεύσει τη στιγμή που ακόμα και αναλυτές της ουσιαστικά ήλπιζαν στη διαιώνισή του; Ο Gary Sick, πρώην στέλεχος του National Security Council -NSC με αρμοδιότητα το Ιράν, παρατηρεί πως ...[η]CIA δεν ήτο ένας ουδέτερος θεατής, είχε στοιχηματίσει στο Ιράν. Οι σχέσεις με τον Σάχη και το καθεστώς ήταν σημαντικότερες. Πολύ απλά η Υπηρεσία δεν ήταν έτοιμη να δει την πραγματικότητα...²⁷ Αλήθεια είναι πως το ενδιαφέρον δεν στρεφόταν στην εσωτερική ιρανική σκηνή αλλά στις ισορροπίες που καλούντο να τηρηθούν εντός του ψυχρού πολέμου. Οι τελευταίες απαιτούσαν τη συνεργασία μεταξύ Αμερικής και Ιράν, έτσι ...η CIA θα ήταν η τελευταία που θα παραδεχόταν ότι κάτι τρομερό συνέβαινε...²⁸ Από τη μεριά του ο Robert Jervis καταγράφει την εξής αμφιθυμία: Αν και το διεθνές πολιτικό περιβάλλον επηρέαζε τόσο αναλυτές όσο και ηγεσία, δεν επηρέαζε όλους κατά τον ίδιο τρόπο ...*υπήρχαν αυτοί που πίστευαν ότι το καθεστώς του Σάχη λειτουργούσε υπέρ του λαού, που πίστευαν ότι έπρεπε να στηριχτεί. Αυτοί το θεωρούσαν ισχυρό. Υπήρχαν αυτοί που πίστευαν ότι το ιρανικό καθεστώς*

²³ Ford P. H., "Why CIA Analysts Were So Doubtful About Vietnam", *Studies in Intelligence*, 1997, διαθέσιμο στη δικτυακή σελίδα <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/vietnam.html> εις την οποία ανατρέξαμε τη 15^η Δεκεμβρίου 2016. Επιπλέον, ο McCone αν και επιφορτισμένος με το «telling it like it is» ουδέποτε μπόρεσε να επιδώσει στην πολιτική ηγεσία το σκεπτικισμό της CIA περί της θεωρίας του ντόμινο -περί τούτου βλέπε Ford P. H., "Thoughts Engendered by Robert McNamara's In Retrospect", *Studies in Intelligence*, 1996, διαθέσιμο στην ιστοσελίδα <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/ford.htm> εις την οποία ανατρέξαμε επίσης τη 15^η Δεκεμβρίου 2016

²⁴ Ford P. H., "Thoughts Engendered by Robert McNamara's In Retrospect", ό. π.

²⁵ Woodward Bob, *Plan of Attack*, Simon & Schuster, London, 2004, σ. 249

²⁶ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 152

²⁷ ibid

²⁸ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 152, επίσης, Sick Gary, *All Fall Down: America's Tragic Encounter With Iran*, Penguin, New York, 1986, σ. 106-108, Bill A. James, *The Eagle and the Lion: The Tragedy of American-Iranian Relations*, Yale University Press, 1988, κεφάλαιο 10

λειτουργούσε σε βάρους του λαού, που πίστευαν ότι δεν έπρεπε να στηριχθεί. Αυτοί το θεωρούσαν αδύναμο.²⁹

Ενώ συνέβαιναν αυτά, όπως υπογραμμίζει ο Michael Donovan, ενώ οι σχέσεις των δύο χωρών ήταν κάτι παραπάνω από στενές, η Περσία παρέμενε για τις αμερικανικές Υπηρεσίες ένας «σκληρός στόχος», κατά συνέπεια, η πτώση της βασιλείας ήταν έτσι και αλλιώς δύσκολο να προβλεφθεί. Ο ίδιος γράφει ...μόνο κάποιος με τη βοήθεια του Μαντείου των Δελφών θα μπορούσε εν έτει 1976 και 1977 να προβλέψει την αλλαγή της κατάστασης εξ αιτίας διαδηλώσεων, εξ αιτίας ενός γερασμένου εξόριστου κληρικού...³⁰ Περαιτέρω, συνεχίζει ο Donovan, σειρά θεμελιωδών λαθών έλαβε χώρα. Έρευνα του House of Representatives το 1979 κατέδειξε πως ...στην περίπτωση του Ιράν, η θετική προς το Σάχη αμερικανική στάση παρεμπόδιζε τη συλλογή πληροφόρησης, αδρανοποίησε τη διάθεση ανάλυσης, έκλεισε τα ότα των policymakers στις προειδοποιήσεις των όποιων διαθέσιμων πληροφοριών.³¹

Και σε αυτήν την περίπτωση η πολιτικοποίηση της πληροφόρησης καθίσταται φανερή. Επίσης, η παρουσία της κυρίαρχης υπόθεσης, η τροχοπέδη του wishful thinking, η ελλιπής συλλογή και η ανεπαρκής ανάλυση πληροφοριών -όλα αυτά επουδενί βοήθησαν στην ορθή σύλληψη, στην 'πρόβλεψη' των ερχομένων. Εντούτοις, αυτό που διαφοροποιεί το παράδειγμα του Βιετνάμ από κείνο του Ιράν σχετίζεται με την ένταση του politicization. Στο πρώτο, η πολιτικοποίηση εκδηλώνεται μέσα από τη «σκληρή» της φόρμα, ο Treverton θα την αποκαλούσε *direct pressure politicization* ή, στην καλύτερη περίπτωση, *house line politicization*. Στο δεύτερο, εκδηλώνεται μέσα από την «ήπια» μορφή της (μάλιστα την ηπιότερη), ο Treverton θα την αποκαλούσε *shared mindset politicization* υπό την έποψη πως αυτό που ήθελε να δει η πολιτική ηγεσία ταυτίζονταν με αυτό που ευχόταν η πληροφοριακή κοινότητα.³²

²⁹ Jervis Robert, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*, Cornell University Press, Ithaca, 2010, σ. 107

³⁰ Donovan Michael, "National intelligence and the Iranian revolution" στο *Eternal Vigilance? 50 Years of the CIA*, επιμ. Jeffreys-Jones R., Andrew Christopher, Frank Cass, London, 1997, σ. 159

³¹ ό. π., σ. 160

³² Περί σκληρής και ήπιας πολιτικοποίησης αλλά και για τους πέντε τύπους της βλέπε Treverton Gr., "Intelligence Analysis: Between 'Politicization' and Irrelevance" στο *Analyzing Intelligence. Origins, Obstacles, and Innovations*, ό. π., σ. 93-96. Περί των λόγων για τους οποίους οι πολιτικοί παράγοντες αγνοούν τις Υπηρεσίες βλέπε Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 154, επίσης, Petersen Martin, "The Challenge for the Political Analyst" στο *Studies in Intelligence*, Volume 47, Number 1, 2003, σ. 51-56. Για περαιτέρω πληροφορίες επί του θέματος σε μορφή άρθρων ανέτρεξε: Davis Jack, "Paul Wolfowitz on Intelligence-Policy Relations" στο *Studies in Intelligence*, Volume 39, Number 1, 1995, σ. 35-42, Jervis Robert, "Reports, Politics, and Intelligence Failures: The Case of Iraq" στο *Journal of Strategic Studies*, Volume 29, Number 1, 2006, σ. 3-52, Marrin St., "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis", Lucas Scott, "Recognizing Politicization: The CIA and the Path to the 2003 War in Iraq" στο *Intelligence and National Security*, Volume 26, Number 2-3, 2011, σ. 182-202 και 203-227 αντιστοίχως, Duyvesteyn Isabelle, "Intelligence and Strategic Culture: Some Observations" στο *Intelligence and National Security*, Volume 26, Number 4, 2011, σ. 528-529, Hastedt Glenn, "The Politics of Intelligence and the Politicization of Intelligence: The American Experience", Marrin St., "Rethinking Analytic Politicization", Rovner Joshua, "Is Politicization Ever a Good Thing?" στο *Intelligence and National Security*, Volume 28, Number 1, 2013, σ. 5-31, 32-54 και 55-67 αντιστοίχως, Risen James, "Keeping CIA. Chief Puts Pressure on Relationship", 20 Ιανουαρίου 2001 στη διαδικτυακή τοποθεσία των *New York Times* <http://www.nytimes.com/2001/01/20/us/political-memo-keeping-cia-chief-puts-pressure-on-relationship.html>, Pincus Walter, "Before War, CIA Warned on Negative Outcomes", 3 Ιουνίου 2007 στην ηλεκτρονική σελίδα της *Washington Post* <http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060200905.html>, Gerstein Josh, "Panetta Warns Against Politicization", 18 Μαΐου 2009 στον κόμβο <http://www.politico.com/story/2009/05/panetta-warns-against-politicization-022676> του *Politico*, Norton-Taylor Richard, "Iraq war inquiry: Britain heard US

Εκ των ανωτέρω συνάγουμε τα εξής:

- Ο πληροφοριακός κύκλος λόγω της αρθρωτής του μορφής ενθαρρύνει την αναζήτηση των αιτιών μιας αποτυχίας εντός κάποιου σταδίου του. Εντούτοις, η διάκριση των τελευταίων δεν είναι πάντα τόσο δεδομένη όσο φαίνεται. Οι Peter Gill και Mark Phythian υποστηρίζουν ότι η 11^η Σεπτεμβρίου, η περίφημη υπόθεση περί ιρακινών όπλων μαζικής καταστροφής αλλά και η τρομοκρατική επίθεση στο Λονδίνο την 7^η Ιουλίου 2005 δεικνύουν πληροφοριακές αποτυχίες των οποίων το αίτιο είναι πολύ περισσότερο multi-causal παρά mono-causal. Ειδικότερα και όσον αφορά στην υπόθεση του Ιράκ, οι δύο μελετητές αποφαινόμενοι ότι η πληροφοριακή αποτυχία εντοπίζεται σε πληθώρα, επικαλυπτόμενων κάποιες φορές, επιπέδων -στη συλλογή, στην ανάλυση, στην διασπορά, στη διαχείριση πληροφόρησης.³³
- Η προσπάθεια εντοπισμού των αιτιών μιας αποτυχίας αποκλειστικά εντός της πληροφοριακής διαδικασίας (λειτουργική θεώρηση) δύναται να συσκοτίσει την πραγματικότητα καθώς αποκλείονται οργανωτικοί / δομικοί παράγοντες. Επίσης, παραβλέπεται το πολιτικό περιβάλλον εντός του οποίου λειτουργεί ο κύκλος της πληροφόρησης. Η υπόθεση «φταίει η πληροφοριακή διαδικασία» επικάθεται στην (προ)υπόθεση των «συνετών / ώριμων πολιτικών» που επιθυμούν πάντα αντικειμενική ενημέρωση ασχέτως προτιμήσεων και πιστεύω -η δεύτερη συνθήκη συχνά δεν επιβεβαιώνεται.³⁴
- Η σχέση μεταξύ πληροφόρησης και πολιτικής είναι πολύ πιο σύνθετη από ό,τι ο πληροφοριακός κύκλος αφήνει να εννοηθεί. Η πολιτικοποίηση της πληροφορίας δεν αποτελεί περιστασιακό επεισόδιο στην ιστορία του intelligence.³⁵
- Η αναζήτηση των πληροφοριακών αποτυχιών οφείλει να λάβει χώρα τόσο εντός των διαδικασιών, όσο εντός των δομών των Υπηρεσιών, εντός πολύπλοκων καταστάσεων και καταστάσεων αβεβαιότητας.³⁶
- Οι λειτουργικές, οργανωτικές, δομικές βελτιώσεις δεν μπορούν να εξαλείψουν την πληροφοριακή αποτυχία, δύνανται, ωστόσο, να μειώσουν τις πιθανότητες εκδήλωσής της.³⁷

Τα όρια της πληροφόρησης (II). Ειδικότερες προσεγγίσεις: Richard Betts, Peter Jackson, Jervis & Ford

Ο Richard Betts μιλά για τρεις παράγοντες πληροφοριακής αποτυχίας. Ο πρώτος καλείται *εξωτερικός*, ο δεύτερος *αθώος*, ο τρίτος *εσωτερικός*. Ειδικότερα:

drumbeat for invasion before 9/11”, 24 Νοεμβρίου 2009 στην ηλεκτρονική σελίδα του *The Guardian* <https://www.theguardian.com/uk/2009/nov/24/iraq-war-chilcot-inquiry>, Gates R., “Guarding Against Politicization” στη σελίδα του *Studies in Intelligence* <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/volume-36-number-1/pdf/v36i1a01p.pdf>, Pillar Paul, “Intelligence, Policy, and the War in Iraq” στη διαδικτυακή τοποθεσία του περιοδικού *Foreign Affairs* <https://www.foreignaffairs.com/articles/iraq/2006-03-01/intelligence-policy-and-war-iraq> (ημερομηνία καταφυγής στις άνω σελίδες η 1^η Ιανουαρίου 2017), επίσης βλέπε Bakos Nada, “Politicization of the Intelligence Community is Extremely Dangerous”, 27 Φεβρουαρίου 2017 στην ηλεκτρονική τοποθεσία <http://www.fpri.org/2017/02/politicization-intelligence-community-extremely-dangerous/> του Foreign Policy Research Institute (ημερομηνία καταφυγής η 13^η Απριλίου 2017)

³³ Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, ό. π., σ. 169

³⁴ *ibid*

³⁵ *ibid*

³⁶ *ibid*

³⁷ *ibid*

- Ο πρώτος σχετίζεται με τον αντίπαλο που ως κράτος, ως μη κρατικός δρώντας, ως οργανισμός, ως ομάδα ή ως «μεμονωμένος / μοναχικός λύκος» θα προσπαθήσει να αποκρύψει προθέσεις και δυνατότητες.³⁸
- Ο δεύτερος απειλεί το πληροφοριακό έργο χωρίς να έχει πρόθεση να κάνει κάτι τέτοιο. Συνήθως γίνεται αναφορά σ' αυτόν μετά από αποτυχίες που θα μπορούσαν θεωρητικά να αποτραπούν. Έχει να κάνει με στελέχη που αστόχησαν στο έργο τους, με αμέλεια, με πλημμελή εκτέλεση καθηκόντων, με την εσωστρέφεια των Υπηρεσιών, με εσωτερικούς ανταγωνισμούς, με ανεπαρκή διασπορά, γενικότερα διαχείριση, πληροφορίας, με πολιτικούς ή νομικούς κύκλους που αντιτίθενται σε επιχειρησιακές δράσεις για διαφόρους λόγους κ. λ. Τίποτα από ό,τι εντάσσεται στον δεύτερο παράγοντα δεν επιθυμεί ενσυνειδήτως την τρώση του πληροφοριακού έργου.³⁹
- Ο τρίτος παράγοντας «επιβάλλεται» στον άνθρωπο, φίλιο ή εχθρό, χωρίς αυτός να δύναται αντίδρασης. Έχει να κάνει με αναπάντητα διλήμματα, περιορισμούς της λογικής, άφευκτη αλλαγή προτεραιοτήτων και στόχων που συχνά ακυρώνει (η αλλαγή) εκτιμήσεις ή εξαλείφει μία πηγή κινδύνων δημιουργώντας μια άλλη. Αφορά σε ελαττώματα που παρουσιάζονται σε κάποιο κομμάτι του οργανωτικού σχεδιασμού, ελαττώματα που δεν δύναται να διορθωθούν χωρίς να προκαλέσουν αστάθεια κάπου αλλού. Σχετίζεται με την ανθρώπινη διάνοια που ακόμα και στην καθαρότερη μορφή της συλλαμβάνει, κάποιες ή πολλές φορές, την πληροφόρηση με λάθος τρόπο, «κομμένη» ή μισή, στρεβλωμένη κ. ο. κ. Σχετίζεται με την ύπαρξη πληροφοριακών προκλήσεων που προσκρούουν η μία στην άλλη, βλέπε κεντρική διαχείριση έναντι αποκέντρωσης, μυστικότητα έναντι εξωστρέφειας, προστασία πηγών / μεθόδων έναντι προστασίας ελευθεριών του πολίτη κ. λ. Αυτά και ό,τι άλλο συνθέτει τον τρίτο παράγοντα είναι πολύ λιγότερο κατανοητά / εμφανή τόσο εντός όσο εκτός της πληροφοριακής κοινότητας. Ο εσωτερικός παράγοντας εισβάλλει / διαχέεται εντός της πληροφοριακής διαδικασίας ξανά και ξανά επηρεάζοντας τη δυναμική της, δεικνύοντας αναπόδραστο χαρακτηριστικό της.⁴⁰

Κατά τον Betts οι προβληματισμοί που γεννούν τόσο ο πρώτος όσο και ο δεύτερος παράγοντας δύναται να αντιμετωπιστούν, έστω θεωρητικά, έστω μερικώς. Κάποιες δράσεις σ' αυτήν την κατεύθυνση σχετίζονται με τη βελτίωση των επιπέδων ετοιμότητας, την ποιοτική αναβάθμιση των ανθρωπίνων και τεχνολογικών πόρων, τη διείσδυση εντός των αλλότριων δικτύων, την προσαρμογή / αλλαγή διαφόρων υπηρεσιακών πρωτοκόλλων, την αλλαγή του νομικού πλαισίου προστασίας της λειτουργίας των πληροφοριακών οργανισμών κ. λ.⁴¹ Όσον αφορά στη διαχείριση του τρίτου παράγοντα ο ερευνητής δηλώνει: «η λέξη / έννοια 'δίλημμα' κυριαρχεί, δίλημμα σημαίνει κατάσταση κατά την οποία πρέπει να επιλεγεί μια λύση μεταξύ δύο εξίσου μη ικανοποιητικών»⁴² -ο Betts θεωρεί ότι ο τρίτος παράγοντας / αίτιο πληροφοριακών αποτυχιών σχεδόν δεν αντιμετωπίζεται καθώς αποτελεί παραπροϊόν της δράσης των Υπηρεσιών και της πληροφοριακής ακολουθίας.

³⁸ Betts Richard, *Enemies of Intelligence. Knowledge and Power in American National Security*, Columbia University Press, New York, 2007, σ. 9

³⁹ *ibid*

⁴⁰ Betts Richard, *Enemies of Intelligence. Knowledge and Power in American National Security*, ό. π., σ. 12-14

⁴¹ ό. π., σ. 10

⁴² ό. π., σ. 13-14, επίσης Liaropoulos Andrew, "A Review of: 'The Three Foes of Intelligence'" στο *International Journal of Intelligence and CounterIntelligence*, Volume 21, Issue 2, 2008, σ. 406-407

Ο Peter Jackson γράφει ότι η πληροφοριακή διαδικασία, το τελικό προϊόν αλλά και η χρήση του δύναται να αντιμετωπίσουν προβλήματα που σχετίζονται με:

- Το *χώρο και το χρόνο*: Τόσο ο χώρος όσο και ο χρόνος θέτουν περιορισμούς στους παραγωγούς πολιτικής απόφασης / δράσης. Η ανάγκη συλλογής έγκυρης πληροφόρησης, ανάλυσης και διασποράς συνθέτει πρόβλημα που έχει να κάνει με τον *χρονικό περιορισμό (time bound)* της πληροφορίας ήτοι, το χρονικό διάστημα εντός του οποίου διατηρεί τη χρησιμότητά της. Η περιγραφόμενη από την πληροφοριακή ανάλυση κατάσταση υπόκειται σε αλλαγές. Εάν οι τελευταίες λάβουν χώρα πριν την αξιοποίηση των πληροφοριών, τότε, ακριβώς αυτές οι πληροφορίες καθίστανται παρωχημένες. Τον κίνδυνο διατρέχουν κυρίως οι λεγόμενες βραχυπρόθεσμες (*short-term*) και μεσοπρόθεσμες (*medium-term*) πληροφορίες σε αντίθεση με τις στρατηγικές που παρουσιάζονται ανθεκτικότερες στο χρόνο.⁴³
- Την *οργάνωση / δομή των Υπηρεσιών*: Το εσωτερικό και διεθνές περιβάλλον παράγει μονίμως νέους τύπους απειλών. Το γεγονός περιορίζει την αποτελεσματικότητα μιας ‘στάνταρτ’ πληροφοριακής διαδικασίας. Η σύνθεση των Υπηρεσιών με προσανατολισμό στη συλλογή, ανάλυση και διασπορά πληροφόρησης υπόκειται σε συνεχείς προκλήσεις. Μια παλαιά δομή πιθανόν δεν μπορεί να ανταπεξέλθει σε νεοφανείς κινδύνους. Κατά την έννοια τούτη οι πληροφοριακοί οργανισμοί οφείλουν να χαρακτηρίζονται από ευελιξία. Αυτή η ‘ευελιξία’ δύναται να αποκρυπτογραφεί κατά τον έναν ή άλλο τρόπο. Ίσως ευνοήσει τη μεγέθυνση μιας Υπηρεσίας, ίσως τη διάσπασή της, ωστόσο, κάτι τέτοιο δεν είναι σίγουρο κατά πόσο θα βοηθήσει στην διαλογή και αξιοποίηση των πληροφοριών.⁴⁴
- Την *πολιτικοποίηση της πληροφορίας*.⁴⁵
- Τους *περιορισμούς της ανθρώπινης διάνοησης*: Αν και ο ανθρώπινος εγκέφαλος αποτελεί πανίσχυρο εργαλείο επεξεργασίας πληροφοριών, χαρακτηρίζεται, επίσης, από αδυναμίες. Τα πολύπλοκα κοινωνικά φαινόμενα σπρώχνουν το νου στην ανάπτυξη ιδεών προκειμένου αυτός να διαλεχθεί με το (εξωτερικό) περιβάλλον. Το πρόβλημα έγκειται στο ότι αυτές οι ιδέες αποτελούν συχνά πυκνά υπεραπλουστεύσεις της φυσικής και της πολιτικής πραγματικότητας.⁴⁶

Ο Jackson συμπερασματικά τοποθετείται ως εξής: Η ιδέα μιας πλήρους και αντικειμενικής πληροφοριακής εκτίμησης τείνει στο ιδανικό παρά στο ρεαλιστικό. Η προσπάθεια βελτίωσης / αναδόμησης της πληροφοριακής διαδικασίας δεν μπορεί να οδηγήσει σε ένα σύστημα ικανό αντιμετώπισης των κάθε φορά επερχομένων απειλών. Αυτό δεν σημαίνει ότι οι πληροφοριακοί οργανισμοί θα πάνσουν να

⁴³ Jackson P., “Historical Reflections on the Uses and Limits of Intelligence” στο *Intelligence and Statecraft: The Use and Limits of Intelligence in International Society*, επιμ. Jackson P. Siegel J., Praeger, USA, 2005, σ. 13-14. Επιπλέον δεν πρέπει να ξεχνάμε τον παράγοντα «μυστικότητα» και, όπως γράφει ο Michael Warner, η μυστικότητα κοστίζει (και) σε χρόνο -περί τούτου βλέπε Warner M., “Fragile and Provocative: Notes on Secrecy and Intelligence” στο *Intelligence and National Security*, Volume 27, Number 2, 2012, σ. 239

⁴⁴ Jackson P., “Historical Reflections on the Uses and Limits of Intelligence”, ό. π., σ. 14-15

⁴⁵ ό. π., σ. 15-17

⁴⁶ ό. π., σ. 17. Ο Robert Z. George συντάσσεται εν πολλοίς με τον Jackson κάνοντας λόγο για *cognitive, cultural, organizational* και *political* προκαταλήψεις. Οι πρώτες σχετίζονται με μια έμφυτη / ακούσια εξ ημών στρέβλωση των πραγμάτων λόγω αναπόδραστην «πιστεύω», οι δεύτερες με την εντύπωση πως ο ανταγωνιστής αντιλαμβάνεται την κατάσταση όπως εμείς (*mirror-imaging*), οι τρίτες με μια αφοσίωση στο «δικό μας δίκιο» (οι άλλοι έχουν λάθος) και οι τέταρτες με το φαινόμενο της πολιτικοποίησης -περί τούτων βλέπε George Z. Robert, “Beyond Analytic Tradecraft” στο *International Journal of Intelligence and Counterintelligence*, Volume 23, Issue 2, 2010, σ. 296-306

αποζητούν το καλύτερο. Υπογραμμίζει ωστόσο τις εγγενείς πολυπλοκότητες και ασάφειες που αντιμετωπίζει η κοινότητα των Υπηρεσιών. Το δεύτερο συμπέρασμα, που ακολουθεί το πρώτο, έχει να κάνει με την αναπόφευκτη σύνδεση της εξωτερικής πολιτικής και της πολιτικής ασφαλείας με την αβεβαιότητα. Η πληροφόρηση δύναται να παράξει γνώση περί προθέσεων / δυνατοτήτων, να συνεισφέρει σε μια πετυχημένη στρατηγική. Πάρα ταύτα ο παράγοντας της αμφιβολίας ουδέποτε θα εξαλειφθεί, η ηγεσία οφείλει να το γνωρίζει μη προσδοκώντας μια οιονεί αποκάλυψη του μέλλοντος.⁴⁷

Οι Robert Jervis και Harold Ford συμφωνούν πως οι λόγοι των πληροφοριακών αποτυχιών βρίσκουν τις ρίζες τους:

- Σε *παρανοήσεις*: Ο κόσμος ενδέχεται να είναι διαφορετικός από ό,τι οι αναλυτές ή οι ηγέτες εκλαμβάνουν.
- Σε *προκαταλήψεις*: Η έλλειψη γνώσης σε συνδυασμό με την ύπαρξη προκαταλήψεων δύναται να οδηγήσει τους πληροφοριακούς οργανισμούς σε λανθασμένες εκτιμήσεις.
- Σε *προβλήματα της φύσης του decision making*: Η ‘πρόβλεψη’ περίξ της δράσης του αντιπάλου σε περίοδο πίεσης ή κρίσης (εννοείται πίεσης ή κρίσης του αντιπάλου) δεν είναι μια εύκολη υπόθεση.
- Σε *αλλαγές πλάνων / στόχων*: Μια κρίση είναι ικανή να οδηγήσει σε κάθετες αλλαγές σχεδιασμών. Μια επιθετική τακτική δύναται να μεταπέσει σε αμυντική και αργότερα σε απεγνωσμένη προσπάθεια επιβίωσης. Γίνεται κατανοητό πως προβλεψιμότητα δράσεων εντός επισφαλών περιβαλλόντων μόνο κατά προσέγγιση, και αν, μπορεί να σταθεί.
- Σε *αλλαγές εγκατεστημένων πολιτικών*: Στο πλαίσιο μια μείζονος κρίσεως είναι δυνατόν εγκατεστημένες πολιτικές να αλλάξουν. Μια τέτοια εξέλιξη περιορίζει τη δυνατότητα προεικονίσεων.
- Στην *υπερεκτίμηση δυνατοτήτων*: Κάποιες φορές κράτη, ηγέτες και πληροφοριακά συστήματα υπερεκτιμούν τις δυνατότητές τους τη στιγμή που παραβλέπουν οικείες αδυναμίες και τρωτότητες.
- Στην *αδυναμία προσαρμογής σε νέες πληροφοριακές ροές*: Μια εκτίμηση πρέπει να επανεξετάζεται όταν οι συνθήκες κάτω από τις οποίες δομήθηκε αλλάζουν εν τη παρουσία, μάλιστα, νέων πληροφοριακών ροών.
- Στο *σύνδρομο του mirror-imaging*: Η υπόθεση ότι ο αντίπαλος σκέπτεται με τον ίδιο τρόπο που σκεπτόμαστε προκειμένου να αντιμετωπίσει μια κατάσταση είναι μια πολύ επικίνδυνη υπόθεση.⁴⁸

⁴⁷ Jackson Peter, “On Uncertainty and the Limits of Intelligence” στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson L., Oxford University Press, Inc., New York, 2010, σ. 467-468

⁴⁸ Jervis R., *Perception and Misperception in International Politics*, Princeton University Press, Princeton, New Jersey, 1976, σ. 13-28, 31-57, Ford H., *Estimative Intelligence. The Purposes and Problems of National Intelligence Estimates*, Defense Intelligence College, Maryland, 1989, σ. 18, 23, επίσης, Bar-Joseph, Bar, “The Professional Ethics of Intelligence Analysis” στο *International Journal of Intelligence and Counterintelligence*, Volume 24, Issue 1, 2011, σ. 27-30. Ο Thomas Quiggin έλκοντας από τους δύο πρώτους ερευνητές αλλά και από τους Alex Hybel και Michael Handel σημειώνει ως αίτια αποτυχιών: α) την ταύτιση ημών προθέσεων με προθέσεις του αντιπάλου (π. χ. αφού εμείς προτιθέμεθα να δράσουμε κατ’ αυτόν τον τρόπο, τον ίδιο τρόπο δράσης θα επιλέξει και ο αντίπαλος’ κατ’ ουσία γίνεται αναφορά στο mirror-imaging σύνδρομο), β) τη μη κατανόηση του χαρακτήρα του αντιπάλου όπως και την λανθασμένη εκτίμηση περί της διαθέσεώς του να αναλάβει ρίσκα ή όχι, γ) την λανθασμένη εκτίμηση περί εχθρικών προθέσεων όταν αυτή βασίζεται σε ψευδείς εικόνες περί των δυνατοτήτων του εχθρού, δ) την τάση υποτίμησης / υπερεκτίμησης των δυνατοτήτων

Κατά την ‘παραδοσιακή προσέγγιση / σχολή’ αυτό που οφείλει να απαντηθεί έγκειται στο «ποιος ενέχεται» στην αποτυχία.⁴⁹ Οι Richard Betts και Michael Handel αποδίδουν το φταίξιμο κατά κύριο λόγο στους λήπτες της πληροφόρησης ήτοι, στους policymakers αν και δηλώνουν ότι το σφάλμα, γενικότερα, δεν μπορεί να αποφευχθεί στην πορεία του χρόνου παρά ακόμα και την εξέλιξη της τεχνολογίας.⁵⁰ Ο Betts μεταξύ άλλων κάνει λόγο για παρουσία ενός *παραδόξου κατανόησης* (*paradox of perception*), δηλαδή, για παρουσία ανικανότητας της ηγεσίας να αξιοποιήσει ως πρέπει ακόμα και μια «τέλεια» πληροφορία.⁵¹ Ο Handel από τη μεριά του θεωρεί πως οι policymakers (και δευτερευόντως οι αναλυτές) πέφτουν θύματα μιας *γνωστικής / γνωσιακής* (*cognitive*) αδυναμίας ούτως ειπείν, της αδυναμίας της ανθρώπινης νόησης / ψυχοσύνθεσης να αντιληφθεί την πραγματικότητα στην πλήρη έκτασή της.⁵² Ο Loch Johnson είναι ένας ακόμα διάσημος μελετητής που καταδεικνύει τους διαμορφωτές πολιτικής ως αδύναμο κρίκο. Ο μελετητής τονίζει το κεντρικό πρόβλημα της απροθυμίας των πολιτικών ανδρών να ενστερνιστούν την άποψη των Υπηρεσιών τη στιγμή που αυτές ... *βρίσκονται εκεί έξω μονίμως με σκοπό να τους πείσουν περί των κινδύνων που απειλούν την εθνική ασφάλεια*.⁵³

Αν η εργογραφία επιδίδει κατά κύριο λόγο το βάρος της αποτυχίας στους χρήστες της πληροφόρησης, υπάρχουν ερευνητές που δείχνουν τις Υπηρεσίες. Κορυφαίοι αυτής της τάσης των παραδοσιακών, οι Abram Shulsky και Gary Schmitt. Οι δύο επιρρίπτουν μομφή στην αναλυτική διαδικασία και κατ’ επέκταση στην πληροφοριακή κοινότητα θεωρώντας πως εσωτερικές γραφειοκρατικές παθογένειες επηρεάζουν ποιοτικά το τελικό προϊόν⁵⁴ -σημειώνουμε ότι με τους Shulsky και Schmitt δεν συμφωνούν μόνο διαμορφωτές πολιτικής, που έτσι ή αλλιώς επιδιώκουν μια απόσχιση ευθυνών, αλλά και επιχειρησιακοί όπως ο Patrick J. McGarvey.⁵⁵

του αντιπάλου, ε) το σύνδρομο του ψευδούς συναγερμού (*cry wolf syndrome*) -περί τούτων βλέπε Quiggin Thomas, *Seeing the Invisible. National Security Intelligence in an Uncertain Age*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2007, σ. 58. Ο James Wirtz αποδίδει, μεταξύ άλλων, την πληροφοριακή αποτυχία στην υπερμυστικότητα ή, αλλιώς, στο ‘Ultra Syndrome’, στο *group thinking syndrome* και στον πληροφοριακό θόρυβο -για μια εικόνα βλέπε Wirtz J., “Theory of Surprise” στο *Intelligence Theory. Key questions and debates*, επιμ. Gill P., Marrin St., Phythian M., Routledge, U.K., 2009, σ. 73

⁴⁹ Diaz-Matey, Gustavo, *Methodological Approaches to the Concept of Intelligence Failure*, UNISCI Discussion Papers, 2005, σ. 3

⁵⁰ ό. π., σ. 3-4. Με τους Betts και Handel συμφωνεί ο John Gentry κάνοντας λόγο για μια “[intelligence]state action”, ομιλώντας ουσιαστικά για «πληροφοριακή δράση» που καθοδηγείται συχνά πυκνά από τις (όποιες) κυβερνήσεις καταλήγοντας, τελικά, σε πληροφοριακή αποτυχία -περί τούτου βλέπε Gentry J., “Intelligence Failure Reframed” στο *Political Science Quarterly*, Volume 123, Number 2, 2008, σ. 247-248, επίσης, van Reijn, Joop, “Intelligence and Strategic Culture: Essays on American and British Praxis since the Second World War” στο *Intelligence and National Security*, Volume 26, Number 4, 2011, σ. 441-442

⁵¹ Betts R., Mahnken Th., *Paradoxes of Strategic Intelligence*, Frank Cass, 2001, σ. 63

⁵² ό. π., σ. 166, επίσης βλέπε Handel M., “Intelligence and the problem of strategic surprise” στο *Journal of Strategic Studies*, Number 7, 1984, σ. 45. Ο Walter Laqueur αν και δεν μιλά για γνωσιακή αδυναμία κάνει αναφορά στην έλλειψη γνώσης ή, αλλιώς, στην άγνοια που κατατρέπει Υπηρεσίες και ηγεσία -περί τούτου βλέπε Laqueur W., *A World of Secrets*, Basic Books, New York, 1985, σ. 281

⁵³ Johnson L., “Analysis for a New Age” στο *Intelligence and National Security*, Volume 11, Number 4, 1996, σ. 663

⁵⁴ Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, ό. π., σ. 64-65. Οι δύο ερευνητές πέραν του politicization καταδεικνύουν ως αίτια αποτυχίας: α) τη μη διάθεση πληροφοριών όταν και όπου αυτές χρειάζονται, β) την παγίδα της *κοινής λογικής / conventional wisdom* (βλέπε περίπτωση εισβολής Ιράκ στο Κουβέιτ τον Αύγουστο του 1990 όταν κανείς δεν πίστευε πως το πρώτο θα επιχειρούσε κάτι τέτοιο σχεδόν αμέσως μετά από έναν εξαντλητικό δετή πόλεμο με το Ιράν), γ) το σύνδρομο του mirror-imaging -περί τούτων βλέπε στο ίδιο σ. 65-69

⁵⁵ McGarvey P., “DIA: Intelligence to please” στο *Readings in American Foreign Policy*, επιμ. Halperin M., Kanter A., Little Brown, Boston, Massachusetts, USA, 1973, διαθέσιμο στην διαδικτυακή

Τέλος, η παραδοσιακή πτέρυγα συμπληρώνεται από συγγραφείς που βρίσκουν το αίτιο της αποτυχίας στη δράση του αντιπάλου. Πλέον γνωστός αυτής της τάσης, ο Barton Whaley. Ο Whaley υποστηρίζει ότι το στρατήγημα του αντιπάλου, π. χ. μια εκστρατεία παραπληροφόρησης, είναι ικανό να παρασύρει τις Υπηρεσίες και την ηγεσία σε λάθος κατευθύνσεις.⁵⁶

Η δεύτερη προσέγγιση, αυτή των ‘οπτιμιστών’, διακατέχεται από την αισιοδοξία του τεχνολογικού asset θεωρώντας πως ακριβώς αυτό θα μειώσει το ποσοστό των αποτυχιών. Θιασώτες αυτής της σχολής, όπως ο Joseph Nye και ο William Owens πιστεύουν, π. χ., πως η ‘τεχνολογική ασυμμετρία’ θα προσδώσει στην αμερικανική πληροφοριακή / στρατιωτική κοινότητα μέγιστο προβάδισμα έναντι φίλων και εχθρών.⁵⁷ Αλήθεια είναι πως η συγκεκριμένη σχολή αγκαλιάζει σχετικά λίγους ακαδημαϊκούς εντούτοις είμαστε υποχρεωμένοι να μνημονεύσουμε τους Bruce Berkowitz⁵⁸, Walter Laqueur⁵⁹, Michael Herman⁶⁰ και David Kahn.⁶¹ Ο Robert Steele αποτελώντας επίσης εκπρόσωπο αυτής της άποψης υποστηρίζει ότι οι κίνδυνοι του 21^{ου} αιώνα, βλέπε τρομοκρατία, θα αντιμετωπιστούν πρωτίστως με χρήση ανοικτών πηγών πληροφόρησης. Για τον Steele το πρόβλημα της αποτυχίας έχει να κάνει περισσότερο με ελλιπή συλλογή παρά με ημιτελή ανάλυση, συνεπώς, η τεχνολογία παροχής πληροφοριών θα παίζει ιδιαίτερο ρόλο.⁶²

Κλείνουμε με την τρίτη προσέγγιση, τη λεγόμενη ‘εναλλακτική’. Η συγκεκριμένη υποστηρίζει ότι καμία μελέτη δεν απαντά ικανοποιητικά στο ποιος φταίει για την αποτυχία. Η τελευταία αποτελεί συνισταμένη παραγόντων που δύνανται να διαφεύγουν της προσοχής / αντίληψης του ανθρώπου. Η πληροφοριακή δράση όπως κάθε ανθρώπινη δράση είναι ατελής. Το αντικείμενο ‘πληροφόρηση’ δεν συνθέτει ‘επιστημονικό’ αντικείμενο. Η ίδια πληροφόρηση στο ίδιο περιβάλλον δεν παράγει κάθε φορά την αυτή δράση, αποτέλεσμα κ. λ. Η πληροφοριακή αποτυχία αποτελώντας κομμάτι του intelligence δεικνύει απλά ένα ‘ατυχές συμβάν’. Ο Charles Perrow, πατέρας της ‘normal accident theory’ γράφει ...ατυχείς καταλήξεις εντός πολύπλοκων συστημάτων δεν μπορεί να αποφευχθούν καθώς μια πρόβλεψη περί κάθε είδους πιθανών αποτυχιών δεν μπορεί να υπάρξει.⁶³

τοποθεσία <http://www.unz.org/Pub/WashingtonMonthly-1970jul-00068> εις την οποία ανατρέξαμε την 7^η Ιανουαρίου 2017

⁵⁶ Diaz-Matey, Gustavo, *Methodological Approaches to the Concept of Intelligence Failure*, UNISCI Discussion Papers, 2005, σ. 5. Ο Diaz-Matey επισημαίνει ότι μελετητές όπως ο Abraham Ben-Zvi (βλέπε στο “A conceptual framework for the analysis of surprise attack”, *World Politics*, XXVIII, April 1970) ή ο Ariel Levite (βλέπε στο *Intelligence and Strategic Surprise*, Columbia University Press, New York, 1987) δεν συμερίζονται κάποιες παραδοχές της παραδοσιακής σχολής. Ο πρώτος, π. χ., δεν αποδέχεται την ιδέα της γνωστικής / γνωσιακής αδυναμίας, ο, δε, δεύτερος την ιδέα του φυσικού / αναπότρεπτου μιας αποτυχίας

⁵⁷ Nye Joseph, Owens William, “America’s information edge”, *Foreign Affairs*, Volume 75, Number 2, 1996, σ. 23-24

⁵⁸ Berkowitz Bruce, “Information Age Intelligence”, *Foreign Policy*, Number 103, 1996, σ. 37

⁵⁹ Laqueur W., *A World of Secrets*, ό. π., σ. 308

⁶⁰ Diaz-Matey Gustavo, *Methodological Approaches to the Concept of Intelligence Failure*, ό. π., σ. 6

⁶¹ ibid

⁶² Steele Robert, “The Importance of Open Source Intelligence to the Military”, *International Journal of Intelligence and Counterintelligence*, Volume 8, Issue 4, 1995, σ. 457-470, επίσης βλέπε Steele Robert, “Crafting Intelligence in the Aftermath of Disaster”, *International Journal of Intelligence and Counterintelligence*, Volume 15, Issue 2, 2002, σ. 161-178, Steele Robert, “National Intelligence and Open Source: From School House to White House”, *American Intelligence Journal*, Volume 14, Number 2 / 3, 1993, σ. 29-32

⁶³ Βλέπε κεφάλαιο 1 στο Perrow Charles, *Normal Accident: Living with High-Risk Technology*, Basic Books, New York, 1984

Συμπεράσματα

Ο John Hollister Hedley υποστηρίζει ότι:

- Αιτιάσεις περί πληροφοριακών αποτυχιών πάντα θα υπάρχουν.
- Μεγάλο τμήμα αυτών των αιτιάσεων είναι ισχυρό, η πληροφοριακή αποτυχία είναι πάντα πιθανή.
- Οι πληροφοριακοί οργανισμοί θα υφίστανται αλλά και θα μαθαίνουν από αιτιάσεις και αποτυχίες.
- Αν και η επανάληψη κάποιου έτσι και αλλιώς αναπότρεπτο δεν μπορεί να αποφευχθεί, το ποσοστό της πληροφοριακής επιτυχίας πιθανότατα δύναται να αυξηθεί.⁶⁴

Η φράση «πληροφοριακές αποτυχίες πάντα θα υπάρχουν» ενέχει βεβαιότητα νόμου φυσικής επιστήμης. Δεν υπάρχει οργανισμός που να πέφτει πάντα μέσα στις εκτιμήσεις, μια τέτοια προσδοκία χαρακτηρίζεται ανεδαφική. Οι αναλυτές οφείλουν να αποδεχτούν το ρίσκο που γενούν υλικές / άυλες αδυναμίες και οι χρήστες πληροφόρησης την πραγματικότητα. Η παραγωγή τελικού προϊόντος θα συντελεστεί όσο και αν το πρωτογενές στοιχείο χαρακτηρίζεται από ασάφεια, αντίφαση ή αβεβαιότητα, όσο και αν η επιτυχία της μιας Υπηρεσίας σημαίνει αποτυχία της άλλης, όσο και αν το πληροφοριακό παίγνιο είναι ένα παίγνιο μηδενικού αθροίσματος.



Εικόνα 33: Απεικόνιση του λαβυρίνθου του κόσμου των πληροφοριών, της πολυπλοκότητας εντός της οποίας πρέπει να δράσει και να παράξει ένα τμήμα ανάλυσης. Η εικόνα ελήφθη από το *Introduction to Intelligence Studies* των Jensen, McElreath, Graves, σ. 155

⁶⁴ Hedley J., “Learning from Intelligence Failure” στο *International Journal of Intelligence and CounterIntelligence*, Volume 18, Issue 3, 2005, σ. 435

ΚΕΦΑΛΑΙΟ 11

Το μέλλον της πληροφόρησης, της αντιπληροφόρησης και των Υπηρεσιών ως προς την επίρρωση περιβάλλοντος εθνικής ασφαλείας, επίτευξης κρατικών σχεδιασμών και πλήρωσης ανάλογων συμφερόντων

Το μέλλον της πληροφόρησης. Η θεωρία

Η πληροφορία στην εποχή του 21^{ου} αιώνα παύει να διατηρεί τον παλαιό επικουρικό ρόλο, ίσως, μάλιστα, ανεξαρτητοποιείται όπως αφήνει να εννοηθεί ο καθηγητής Jarrol Manheim στο *Strategic Public Diplomacy and American Foreign Policy*. Χρόνο με το χρόνο εκλαμβάνεται ως όλο και σημαντικότερο συστατικό επί του οποίου κτίζονται γνωστές μορφές ισχύος, εντούτοις, το ερώτημα παραμένει: είναι η πληροφόρηση δομικό υλικό πολιτικής, οικονομικής και στρατιωτικής στρατηγικής ή, ακόμα παραπέρα, κατατείνει στη δημιουργία ενός τέταρτου αυτόνομου πυλώνα; Κατά τους John Arquilla και David Ronfeldt ισχύει μάλλον το δεύτερο ή, ίσως, είναι σοφό να ελέγξουμε και αυτήν την εκδοχή. Το δίδυμο των μελετητών επιχειρηματολογεί στηριγμένο σε δύο παραδοχές ήτοι, της ανάπτυξης της πληροφορι(α)κής επιστήμης και των επικοινωνιακών μέσων / οδών και, δεύτερον, των περιορισμών που η σύγχρονη εποχή θεωρητικά επιβάλλει στη χρήση καθολικής βίας και στον ωμό εξαναγκασμό.¹

Ο George Hull εξετάζοντας τις πληροφοριακές εφαρμογές διαπιστώνει πως: α) η οικονομία και ο παραγωγικός ιστός φαίνεται να αλλάζουν βηματισμό μέσω ενός μοντέλου αξιοποίησης της πληροφορίας αφήνοντας το παλαιότερο της κτήσης / χρήσης φυσικών πόρων πίσω², β) η παγκόσμια αγορά και η ιδιωτική πρωτοβουλία όλο και αναπτύσσονται επί τη βάσει ψηφιακών δεδομένων, τηλεπικοινωνιών και συγκοινωνιών, γ) τα παραδοσιακά ιεραρχικά καθεστώτα και η βεμπεριανή γραφειοκρατία υποχωρούν μπροστά στους νέους πληροφοριακούς διασυνδεδεμένους networked οργανισμούς³, δ) τα προνόμια της κρατικής κυριαρχίας ελέγχονται εκ νέου

¹ Arquilla J., Ronfeldt D., "Information, Power, and Grand Strategy: in Athena's Camp -Section 2" στο *In Athena's Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997, σ. 417-421. Από τη μεριά του ο δρ Σπυρίδων Πλακούδας τονίζει ότι «σε μια εποχή όπου η 'διπλωματία των κανονιοφόρων' και ο πόλεμος υποχωρεί δραματικά, τα κράτη υιοθετούν νέες έμμεσες μεθόδους για να επιβάλουν τη θέλησή τους -περί τούτου βλέπε Πλακούδας Σ., «Νέες Απειλές Ασφαλείας - Υβριδικός Πόλεμος», *Καθημερινή*, 4 / 12 / 2016. Τέλος, ο Joseph Nye παρατηρεί ότι «το διαδίκτυο δημιουργεί μια υπερεθνική επικράτεια υπερκείμενη των κρατών με τον τρόπο που το έκαναν στο παρελθόν οι μεσαιωνικές αγορές» -για μια πληρέστερη εικόνα ανέτρεξε Nye J., *Το Παράδοξο της Αμερικανικής Δύναμης*, μτφρ. Παπαστάμου Ιωάννα, Παπαζήσης / Ινστιτούτο Αμυντικών Αναλύσεων, Αθήνα, 2003, σ. 155

² Μάλιστα μελετητές όπως ο Alvin Toffler εκφράζουν την άποψη ότι η πληροφορία / γνώση δεικνύει σήμερα τον πλέον βασικό οικονομικό πόρο -για μια μελέτη επί της θέσεως βλέπε Toffler Al., *Powershift. Knowledge, Wealth and Violence at the Edge of the 21st Century*, Bantam Books, New York, 1990

³ Η ευχέρεια της διασποράς της πληροφορίας οδηγεί εν μέρει στην κατάρρευση των ιεραρχικών επιπέδων καθώς αυτή (η πληροφορία) δεν αποτελεί πλέον κτήμα ολίγων εκλεκτών που με τη σειρά τους θα την διανείμουν κατά το δοκούν. Έτσι και όσον αφορά, π. χ., στον οικονομικό τομέα, οι εταιρίες που αποφασίζουν να στηριχτούν σε έναν αποκεντρωμένο σχεδιασμό παρουσιάζονται πιο ευέλικτες καθώς το δυναμικό που τις στελεχώνει διαθέτοντας ανά πάσα στιγμή το πληροφοριακό εργαλείο βρίσκεται ένα βήμα μπροστά από το αντίστοιχο των παλαιών δομημένων σε αυστηρά stoveriping ιεραρχικά πρότυπα -για μια άποψη βλέπε Nichiporuk Brian, Builder H. Carl, *Information Technologies and the Future of Land Warfare*, RAND, Santa Monica, 1995, σ. 27-32, επίσης, Νομικός Ιωάννης, «Ο ρόλος των υπηρεσιών Πληροφοριών και Ασφαλείας μετά την 11^η Σεπτεμβρίου» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας,

-οι μεταβολές εκτιμάται πως οφείλονται και στην πληροφοριακή επανάσταση / επέκταση.⁴

Ο τχης David Pistilli γράφοντας για την αξία της πληροφόρησης στο στρατιωτικό τομέα υποστηρίζει πως αυτή συμβάλλει θετικά: α) στην κατανόηση των παρόντων διεθνών προκλήσεων και στη σύλληψη των επόμενων, β) στην κατανόηση του αντιπάλου σε επίπεδο κουλτούρας, γ) στη διοίκηση του στρατεύματος, δ) στην επιμελητεία του στρατεύματος, ε) στην απεικόνιση και ανάλυση του περιβάλλοντος μάχης, στ) στο σχεδιασμό μάχης, ζ) στις επιμέρους αμυντικές / επιθετικές τακτικές. Κατά τον Pistilli η πληροφόρηση γύρω από τον ανταγωνιστή δεικνύει το «Ιερό Δισκοπότηρο» ('Holy Grail' όπως κατά λέξη σημειώνει) κάθε στρατιωτικής ηγεσίας. Αυτή η πληροφόρηση συνεισφέρει, παράλληλα, σε κάτι άλλο: στη δημιουργία ενός σώματος γνώσης και κατ' επέκταση στη δόμηση μιας «τεχνογνωσίας πολέμου» -πρόκειται γι' αυτό που ο ίδιος ονομάζει *οργανωτική αξία της πληροφόρησης* (*organizational value of information*) σε στρατιωτικό επίπεδο.⁵

Ο καθηγητής Νίκος Κυριαζής γράφει πως τα ολοκληρωμένα συστήματα Διοίκησης, Ελέγχου, Επικοινωνιών, Υπολογιστικών Συστημάτων και Πληροφόρησης (Command, Control, Communications, Computers, Intelligence -C4I) έχουν αναγνωριστεί από τους σύγχρονους στρατούς ως πολλαπλασιαστές ισχύος. Κατά τον τρόπο τούτο στους πολέμους του 21^{ου} αιώνα νικητής δεν θα είναι εκείνος που υπερτερεί σε αριθμό ή και ποιότητα μονάδων αλλά εκείνος που υπερέχει σε πληροφόρηση και δυνατότητα αξιοποίησής της σε πραγματικό χρόνο. Συνεπώς, πέραν της φονικής μάχης θα έχουμε και μάχες υπολογιστικών / πληροφοριακών δικτύων. Οι έννοιες 'κεφάλαιο' (τανκς, πλοία, αεροσκάφη κ. λ.) και 'εργασία' (ανθρώπινο δυναμικό) παραχωρούν θέση στην έννοια 'πληροφόρηση'. Μικροί αριθμοί μεικτών, ευέλικτων, καλά εξοπλισμένων δυνάμεων θα δύνανται να κατατροπώσουν πολύ ευρύτερους αριθμητικά εχθρούς που παραμένουν στα δόγματα του 20^{ου} αιώνα ελαχιστοποιώντας τις ένθεν και εκείθεν απώλειες καθώς και τις παράπλευρες ζημιές. Κατά τον Κυριαζή οι συγκεκριμένες προηγμένες δυνάμεις, 'δυνάμεις κυβερνοχώρου / cyberforces' όπως τις ονομάζει, θα προβαίνουν σε πόλεμο ελιγμών, σε συγκέντρωση πυρός από σημείο σε σημείο σε μηδέν χρόνο. Θα χαρακτηρίζονται από διοικητική αποκέντρωση, κάτι που δίδει δικαίωμα στον διοικητή που βρίσκεται εντός πεδίου μάχης να αναλαμβάνει πρωτοβουλίες παρέχοντας ταυτόχρονα στο κεντρικό επιτελείο πληροφόρηση της ανά λεπτό εξέλιξης. Αυτά υπό την προϋπόθεση αξιοποίησης της νέας C4I τεχνολογίας που, ως σε παιχνίδι σκάκι, καθιστά τον ένα παίκτη ικανό λήψης συνολικής εικόνας τη στιγμή που ο άλλος ορά μόνο τμήμα της σκακιέρας. Σ' αυτήν την περίπτωση ο πρώτος,

Αθήνα, 2009, σ. 77. Κατά τον Michael Herman, και μένοντας αυστηρά στον κόσμο των πληροφοριακών οργανισμών, η ραγδαία αύξηση του προσωπικού τους μετά τον Β'. Π. Π. εγκαλείται τόσο για την εμφάνιση χαρακτηριστικών βεμπεριανής γραφειοκρατίας όσο και για την εκδήλωση φαινομένων δημοσιοϋπαλληλικής νοοτροπίας. Αν και η τεχνολογία των υπολογιστών, οι ανοικτές πηγές και τα κοινωνικά δίκτυα φαίνεται να οδηγούν σε αλλαγές, η παλαιά δομή δεν έχει ακόμα κλονιστεί απόλυτα -περί τούτων βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, Ποταμός, Αθήνα, 2015, σ. 10

⁴ Hull George, *The Information Revolution and the Environment of Future Conflict*, μονογραφία κατατεθειμένη στο School of Advanced Military Studies / United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1997, σ. 13-14

⁵ Pistilli D., *Start Making Sense. Managing The Command's Information*, μονογραφία κατατεθειμένη στο School of Advanced Military Studies / United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1995, σ. 8-13

ακόμα και αν διαθέτει λιγότερα πόνια, βρίσκεται σε πλεονεκτικότερη θέση από τον δεύτερο.^{6, 7}

Η χρηστικότητα του όρου *Πληροφοριακή Επανάσταση* ή *Επανάσταση στις Πληροφοριακές Υποθέσεις* (*Revolution in Information / Intelligence Affairs -RIA*)⁸ έχει αναγνωριστεί από τους περισσότερους μελετητές διαφόρων, μάλιστα, κατευθύνσεων. Η λέξη «information-πληροφορία» χαρακτηρίζει το μοντέρνο κόσμο, συμβάλει, επιπλέον, στη δημιουργία των εννοιών *Information Age*⁹ και *Information Society*.¹⁰ Εντούτοις προκύπτει κριτική της οποίας τα κύρια ερείσματα σχετίζονται με: α) το αφηρημένο κατά πολλούς της έννοιας (τι είναι πληροφορία; μήπως περιγραφή, μέτρηση, η κατάληξη μιας διαδικασίας;), β) την πολλαπλότητα της χρήσης της (η ίδια πληροφορία την ίδια στιγμή ενδέχεται να αναγνωστεί / αξιοποιηθεί διαφορετικά από τους όποιους λήπτες), γ) το σχετικό της πολυτιμότητάς της υπό την πίεση του χρόνου (για την πλειοψηφία των δρώντων μια πληροφορία έχει αξία όταν είναι «φρέσκια»), δ) το πολύπλοκο της διαδικασίας μετατροπής της από άγουρο δεδομένο σε γνώση.¹¹ Από την άλλη η λέξη «επανάσταση» συνήθως γίνεται κατανοητή ως ξαφνική δράση φέρουσα κάθετες μετατοπίσεις. Πάρα ταύτα μια πιο προσεκτική ματιά καταδεικνύει πως μια τέτοια διαδικασία δεν είναι πάντα τόσο απροσδόκητη υπό την έννοια μιας

⁶ Ο Κυριαζής αναφέρει το εξής εντυπωσιακό: οι Ιρακινοί στον πόλεμο του 1990-1991 έχοντας απολέσει κάθε δυνατότητα ελέγχου, διοίκησης και πληροφόρησης, ουσιαστικά μη έχοντας εικόνα της πραγματικότητας, απόρρησαν όταν οι διαπραγματεύσεις καθορισμού της γραμμής κατάπαυσης των εχθροπραξιών έληξαν με τους Συμμάχους να την ορίζουν νότια της Βασόρα. Η ιρακινή ηγεσία αγνοούσε ότι ο συμμαχικός συνασπισμός είχε φτάσει έξω από την αναφερόμενη πόλη με το σύνολο των ιρακινών δυνάμεων στο Κουβέιτ περικυκλωμένο -περί τούτου βλέπε Κυριαζής Νίκος, Σπανός Στέλιος, *Το Πρόσωπο του Πολέμου στον 21^ο Αιώνα*, Εστία, Αθήνα, 2000, σ. 123, υποσημείωση 7

⁷ Κυριαζής Νίκος, Σπανός Στέλιος, *Το Πρόσωπο του Πολέμου στον 21^ο Αιώνα*, ό. π., σ. 83-85. Περί βασικών στόχων, λειτουργιών και αρχών C4I βλέπε στο ίδιο, σ. 86-90

⁸ Ο Richard Solomon στο *The Information Revolution and International Conflict Management* του 1997 αποδίδει την πατρότητα του όρου στον Walt Wriston και στο έργο του *The Twilight of Sovereignty* (1977)

⁹ Όρος που εμφανίστηκε το 1980 στο *The Third Wave* των Alvin και Heidi Toffler

¹⁰ Ο Frank Webster προσπαθώντας να λύσει το αίνιγμα της έννοιας «Information Society» ελέγχει πέντε παραμέτρους ως προς τη συμβολή τους στη δημιουργία του όρου: την τεχνολογική (technological), την οικονομική (economic), την εργασιακή / επαγγελματική (occupational), την χωρική (spatial) και την πολιτισμική (cultural). Η πρώτη φαίνεται να απολαμβάνει μέγιστη αποδοχή υπό την παρουσία μιας κοινωνίας που στηρίζει πλείστες δραστηριότητές της στην πληροφοριακή τεχνολογία (information tech -IT). Η δεύτερη αποδίδει ιδιαίτερο ρόλο στον κλάδο της οικονομίας που σχετίζεται με τη βιομηχανία της πληροφορίας. Πρόκειται για ιδέα που ανήκοντας στον Fritz Machlup, συγγραφέα του *The Production and Distribution of Knowledge in the United States* (1962), αποτυπώνει τη συμβολή του συγκεκριμένου τομέα στην παραγωγή / σύνθεση του ΑΕΠ, μάλιστα, ο Machlup υπολόγισε ότι η πληροφοριακή βιομηχανία συνεισέφερε το 29% του δείκτη στις ΗΠΑ κατά το έτος 1958. Η τρίτη αναφέρεται σε εργασιακές / επαγγελματικές μετατοπίσεις και στη δημιουργία θέσεων που αξιοποιώντας τη νέα τεχνολογία πολλαπλασιάζονται τη στιγμή που οι παραδοσιακές χειρωνακτικές εξαφανίζονται. Η τέταρτη έχει να κάνει με τη δυνατότητα των πληροφοριακών δικτύων να εξαφανίζουν αποστάσεις και χρόνους. Η πέμπτη σχετίζεται με τη βιομηχανία του θεάματος, την εμφάνιση των μέσων κοινωνικής δικτύωσης, τις μηχανές αναζήτησης, την ευρύτερη, εν γένει, χρήση της ψηφιακής και επικοινωνιακής πλατφόρμας από το παγκόσμιο κοινό -σαφέστατα υπάρχουν και αντίθετες απόψεις ως προς την ικανότητα των πέντε παραμέτρων να οριοθετήσουν το φαινόμενο. Άλλη σχετική προσπάθεια αφορμάται από την παραδοχή της ποσοτικής / ποιοτικής αύξησης και αναβάθμισης του πληροφοριακού προϊόντος / ρεύματος, ωστόσο, και εδώ υπάρχουν ενστάσεις σχετικά με το βαθμό συνεισφοράς των δύο συνιστωσών -για μια καλύτερη άποψη κατέφυγε στο Webster Fr., "What Information Society?" στο *The Information Society*, Volume 10, Number 1, 1994, σ. 1-24

¹¹ Dunn Myriam, *Information Age Conflict. A Study of the Information Revolution and a Changing Operating Environment*, Center for Security Studies, Ζυρίχη, 2002, σ. 59-61 και Waltz Edward, *Information Warfare. Principles and Operations*, Artech House, Βοστώνη, 1998, σ. 49-50

βαθύτερης προοδευτικής κίνησης που, ωστόσο, δεν παρουσιάζει ξεκάθαρη αρχή ή προβλέψιμο τέλος -σ' αυτήν την περίπτωση ο όρος *εξέλιξη* θα ήταν ορθότερος.¹²

Οι Arquilla και Ronfeldt μελετώντας το φαινόμενο καταλήγουν σε συμπεράσματα σύμφωνα με τα οποία:

- Η πληροφοριακή επανάσταση πρέπει να σχετιστεί όχι τόσο με την τεχνολογία όσο με προκλήσεις που καλούνται να αντιμετωπίσουν οι οργανισμοί που διαχειρίζονται το προϊόν της καθώς δόγματα και στρατηγικές θα διαφοροποιηθούν.¹³
- Η πληροφοριακή επανάσταση ευνοώντας μια «δικτυακή αποκέντρωση» θα οδηγήσει σε κατάρρευση το υπάρχον σύστημα ιεραρχικών δομών. Οι δύο συγγραφείς εισάγουν τον όρο «all-channel networks» θέλοντας να σκιαγραφήσουν πως κατανοούν το ζήτημα. Ομιλούν για τάση αποκαθήλωσης των άκαμπτων κεντρικών γραφειοκρατιών με τις περιφερειακές μονάδες να αναλαμβάνουν πρωτοβουλίες ή να αυτονομούνται. Αυτές ακριβώς θα διεξάγουν τις όποιες, π. χ., στρατιωτικές επιχειρήσεις υπό την προϋπόθεση μιας back-and-forth ικανότητας επικοινωνίας και ανταλλαγής στοιχείων. Κατ' αυτόν τον τρόπο οι μεγάλοι στρατοί οφείλουν να εφεύρουν μια φόρμουλα βάσει της οποίας θα συμφιλιωθεί η συγκεντρωτική διοίκηση με την αποκέντρωση / τοπικότητα -πρόκειται για ζήτημα που δεν αντιμετωπίζουν μικρότεροι δρώντες (βλέπε τρομοκρατικές ή εγκληματικές οργανώσεις, nonstate actors κ. λ.) που, ωστόσο, βρίσκονται πίσω λόγω μη επαρκούς τεχνολογικής υποστήριξης.
- Η πληροφορία θα επηρεάζει όλο και περισσότερο τις εξελίξεις στα πεδία των μαχών. Οι απαντήσεις στο ποιος ξέρει τι, στο πότε και στο πού των συμβάντων, στο γιατί και στο πώς των δράσεων, θα συνθέσουν τη γνώση που θα οδηγήσει κατά τον έναν ή άλλο βαθμό στην κατίσχυση.
- Οι απειλές που η εποχή της πληροφόρησης κομίζει όσον αφορά στον πόλεμο παρουσιάζονται πολύ πιο σύνθετες από ανάλογες άλλων περιόδων. Η προσαρμογή οργανισμών, δογμάτων, στρατηγικών / τακτικών θεωρημάτων κ. λ. στις νέες απαιτήσεις εκλαμβάνεται ως εκ των ων ουκ άνευ.
- Δύο καινοφανείς όροι εμφανίζονται κατηγοριοποιούμενοι εντός του ευρύτερου πεδίου της κοινωνίας και του πολέμου, πρόκειται για τους *netwar* και *cyberwar*.¹⁴

¹² Dunn Myriam, *Information Age Conflict. A Study of the Information Revolution and a Changing Operating Environment*, ό. π., σ. 61-62

¹³ Μαζί τους συμφωνούν τόσο ο Abram Shulsky όσο και ο Gary Schmitt θεωρώντας ότι η τεχνολογία δείχνει μόνο ένα τμήμα της εικόνας. Γι' αυτούς, οι εσωτερικές (behavioral / institutional) αλλαγές στον τρόπο λειτουργίας των οργανισμών πληροφόρησης καθίστανται το ίδιο αν όχι πιο σημαντικές. Άλλες επίκαιρες ερωτήσεις σχετίζονται με: α) την ικανότητα απορρόφησης της πληροφορίας από το πολιτικό προσωπικό, β) τον ανταγωνισμό παραγωγής πληροφόρησης μεταξύ Υπηρεσιών και *nonintelligence* οργανισμών και γ) την κρατική αγωνία περί του καταλληλότερου τρόπου «σύμπτυξης» των παραγομένων προϊόντων τόσο των κλασικών όσο και άλλων πληροφοριακών οργανισμών. Η τελευταία πρόκληση έχει να κάνει και με την παρουσία των ανοικτών πηγών πληροφόρησης: οι δύο ερευνητές ομιλούν για «sources of information outside traditional intelligence channels». Κύριο ζητούμενο αποτελεί η αξιολόγηση / ανάλυση των μη παραδοσιακών πηγών πληροφοριών αλλά και μια απάντηση στο ερώτημα «από ποιους θα επιχειρείται η συγκεκριμένη διαδικασία;». Μια μεικτή σχετική προσέγγιση ως προς το τελευταίο προτείνει: α) τους policymakers, β) τους επιτελικούς βοηθούς αυτών ή γ) τους επαγγελματίες των Υπηρεσιών -για περισσότερα βλέπε Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, Brassey's, Inc., Washington, D. C., ΗΠΑ, 2002³, σ. 7, 141-144

¹⁴ Κατά τους Arquilla και Ronfeldt, το *netwar* αφορά σε «πόλεμο» μεταξύ εθνών, κρατικών και μη κρατικών δρώντων ή / και κοινωνιών. Πρόκειται για πόλεμο που ερείδεται στην πληροφόρηση ή πρόκειται για πόλεμο πληροφόρησης. Σε γενικές γραμμές λέμε ότι μια τέτοια επιχείρηση σε στρατηγικό επίπεδο προσβλέπει στον επηρεασμό της κοινής γνώμης του αντιπάλου. Χρησιμοποιεί την

Και οι δύο αναφέρονται σε μάχη (μάχες) της οποίας η έκβαση θα κριθεί και βάσει του επιπέδου αξιοποίησης των πληροφοριακών δεδομένων.

- Αν και η επανάσταση στις πληροφοριακές υποθέσεις θα παίζει όλο και κεντρικότερο ρόλο, οι παλαιότερες μέθοδοι, π. χ. των επικοινωνιών, δεν πρόκειται να ξεχαστούν ή, πιθανότητα, θα λειτουργήσουν, σε κάποιες περιπτώσεις, επικουρικά ή προς αντικατάσταση, σε περίπτωση κατάρρευσης, των σύγχρονων. Δεύτερον, η επαναληψιμότητα όρων όπως *cyberwar*, *netwar*, *cyberspace*, *infosphere* κ. λ. δεν πρέπει να μας οδηγήσει στο συμπέρασμα ότι οι πόλεμοι θα κρίνονται σε ένα περιβάλλον *virtual reality* εκτός υλικού κόσμου, εκτός της ομίχλης και της άχλης της μάχης.
- Η νέα ορολογία στο σύνολό της, όπως και το νόημα που φέρει, πυροδοτεί συζητήσεις. Κάποιοι την αποδέχονται, κάποιοι όχι. Ορισμένοι ορίζουν το *cyberwar* ή το *netwar* βάσει μιας αντίληψης που δεν βρίσκει σύμφωνους ορισμένους άλλους κ. ο. κ. χωρίς, ωστόσο, να διαφωνούν επί της αρχής.¹⁵

Κατά τον Bruce D. Berkowitz ο *πληροφοριακός πόλεμος* (*Information Operations, Information Warfare -IO / IW*) δεν δεικνύει άλλο από τη «σκοτεινή διάσταση» της εποχής της πληροφόρησης. Τα πληροφοριακά συστήματα / δίκτυα είναι τόσο σημαντικά ως προς την εξυπηρέτηση πολιτικών και στρατιωτικών σκοπών ώστε αποτελούν, πέρα από *asset*, πονοκέφαλο ασφαλείας.¹⁶ Στην πραγματικότητα

προπαγάνδα, την υπονόμηση, την παραπληροφόρηση, τη διείσδυση στους διαύλους ενημέρωσης, στο διαδίκτυο, στα μέσα κοινωνικής δικτύωσης κ. λ. -οι περισσότερες μορφές *netwar* δεν εμπλέκονται άμεσα με στρατιωτική δράση. Από την άλλη μεριά, ό,τι νοείται ως (στρατιωτικό) *cyberwar* σχετίζεται με διεξαγωγή επιχειρήσεων των οποίων την έκβαση επηρεάζει αποφασιστικά η ροή πληροφοριών. Στόχο αποτελεί το αντίπαλο πληροφοριακό δίκτυο για ευνόητους λόγους -η ρήση «turn the balance of information and knowledge» είναι ενδεικτική. Το *cyberwar* εγείρει ζητήματα στρατιωτικής οργάνωσης, στρατιωτικών δογμάτων, στρατηγικών, επιχειρησιακών και τακτικών σχεδιασμών. Εμπλέκεται με περιστατικά περιορισμένης, κλιμακούμενης ή υψηλής έντασης σε κάθε είδους περιβάλλοντα για αμυντικούς ή / και επιθετικούς σκοπούς. Σαν δράση αποτελεί ό,τι νεότερο στην τέχνη του πολέμου του 21^{ου} αιώνα, κάτι ανάλογο με το *blitzkrieg* του περασμένου, η, δε, συμπόρευσή του με την τεχνολογική εξέλιξη καθίσταται αναπόφευκτη -για μια ευρύτερη άποψη κατέφυγε στο Arquilla J., Ronfeldt D., “Cyberwar Is Coming” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997, σ. 27-32

¹⁵ Arquilla J., Ronfeldt D., “A New Epoch and Spectrum of Conflict” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, ό. π., σ. 4-8. Είναι χαρακτηριστικό ότι ο όρος «Cyber Warfare / Cyberwar» μέχρι το 2011 επισήμως δεν είχε εμφανιστεί σε αντίθεση με τους συγγενείς όρους «Information Operations / Information Warfare». Μάλιστα, γύρω στις τριάντα χώρες μέχρι τη συγκεκριμένη χρονολογία ανήγγειλαν προγράμματα κυβερνοπολέμου χρησιμοποιώντας στη φρασεολογία τους τους δύο τελευταίους -για του λόγου το αληθές βλέπε Lewis A. James, Timlin Katrina, *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization*, Center for Strategic and International Studies, Washington, D.C., 2011, σ. 3-4. Από κει και έπειτα τα μεγάλα κράτη αναπτύσσουν ιδιαίτερα δόγματα περί κυβερνοπολέμου που συνήθως δεν διαφέρουν μεταξύ τους ουσιαστικά -περί τούτων βλέπε JP 3-13, *Information Operations*, US DoD, Φεβρουάριος 2006 (περί ΗΠΑ), Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, Ευρωπαϊκό Κοινοβούλιο, Βρυξέλες, 2011 και Heickerö Roland, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency, Στοκχόλμη, 2010 (περί Ρωσίας), Hjortdal Magnus, “China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence” στο *Journal of Strategic Security*, Volume 4, Number 2, Article 2, 2011 (περί Κίνας), *Cyber Security Strategy for Germany*, German Federal Ministry of the Interior, Βερολίνο, 2011 (περί Γερμανίας), *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, UK Cabinet Office, 2011 (περί Βρετανίας). Τέλος, σημειώνουμε τη διαφορετικότητα λήψης του «cyberattack» από θεσμό σε θεσμό

¹⁶ ...η ραγδαία ανάπτυξη των υπολογιστικών δικτύων καθιστά κάθε αυτοματοποιημένο σύστημα δυνητικό στόχο εισβολής. Το γεγονός της αυξανόμενης σύνδεσης της κοινωνίας του ανθρώπου με την

ορισμένοι από τους προβληματισμούς βρίσκονται σε ευθεία σύνδεση με τη φύση της πληροφοριακής τεχνολογίας, έτσι: α) παρατηρείται πως κάθε πενταετία το κόστος συλλογής και διαχείρισης της πληροφορίας μειώνεται κατά 90% σε σχέση με την προηγούμενη, συνεπώς, η όλη προσπάθεια καθίσταται μέρα με τη μέρα πιο προσιτή σε πλήθος δρώντων προθύμων να εμπλακούν ειδικά τη στιγμή που αυτή η πτωτική πορεία προβλέπεται να συνεχιστεί, β) όσο η πληροφορία γίνεται φθηνότερη τόσο απομακρύνεται η δυνατότητα αποκλειστικής κατοχής / χρήσης αλλά και ελέγχου της από μια κεντρική αρχή, γ) κατά το τελευταίο, νέες ροπές βρίσκονται απέναντι σε στρατιωτικές παραδόσεις αιώνων. Η τεχνολογία ευνοεί την κατάκτηση των δράσεων, κατά συνέπεια, πλάνα και εργαλεία που αναφέρονται σε ζητήματα εθνικής ασφαλείας και στρατιωτικών επιχειρήσεων καλούνται να μετασχηματιστούν.¹⁷

Οι Daniel Papp και David Alberts απλώνοντας την τράπουλα διερωτώνται, εν έτει 1997, περί του πώς θα είναι ο κόσμος στο εγγύς μέλλον. Προσπαθώντας να προσεγγίσουν μία απάντηση προβαίνουν σε ορισμένες διαπιστώσεις υποθέτοντας, στον ίδιο χρόνο, κάποιες (δυνητικές) επιπτώσεις στο διεθνές σύστημα και στους παίκτες του, ειδικότερα: α) τα πληροφοριακά δεδομένα / στοιχεία θα αυξάνονται, θα διασπείρονται, θα «κυλούν» όλο και περισσότερο μεταξύ εθνών, οργανισμών, ομάδων, κοινωνιών κ. λ., β) η διαδικασία λήψεως αποφάσεων κατακερματίζεται. Από τη στιγμή που ο δημόσιος και ιδιωτικός βίος κατακλύζεται από πληροφορίες η αποκλειστική δυνατότητα και «δικαίωμα» ανάλυσης εκφεύγει των μέχρι σήμερα ειδικών επιτελείων, γ) μια «πληροφοριακή διαπερατότητα» θα χαρακτηρίσει τα σύνορα των κλασικών οντοτήτων των διεθνών σχέσεων -βλέπε κράτη, οργανισμούς κ. λ., δ) νέοι δρώντες θα κάνουν την εμφάνισή τους στον ψηφιακό και εικονικό κόσμο με την πλειοψηφία αυτών να μην επιβιώνει τη στιγμή που οι παραδοσιακοί παίκτες ίσως τους αγνοήσουν, ίσως όχι, ε) θα παρατηρηθεί μια αναπόφευκτη αποδιοργάνωση των σχέσεων ισχύος μεταξύ των γνωστών διεθνών παραγόντων, στ) τόσο η παγκοσμιοποίηση όσο και η τοπικότητα θα ενισχυθούν παρά την αντίφαση του γεγονότος¹⁸, ζ) η τεχνολογική ψαλίδα και ό,τι σχετίζεται μ' αυτήν θα ανοίξει ως αποτέλεσμα μη ομοιογενούς απορρόφησης των νέων hi tech ανακαλύψεων από το σύνολο των κοινωνιών, η) το όλο σύστημα θα αποκεντρωθεί υπό την έννοια της διασποράς της πληροφορίας και των εξουσιών που η κατοχή της παράγει, μάλιστα, ορισμένοι, ίσως καθ' υπερβολή, ομιλούν για μια επερχόμενη «έλλειψη (διεθνούς) συστήματος».¹⁹

Ο William Nolte, στην αυγή της δεύτερης δεκαετίας του 21^{ου} αιώνα, υποστηρίζει, ερχόμενος εν μέρει σε αντίθεση με τον Berkowitz, πως: α) το κόστος της κτήσης πληροφορόρησης αυξάνεται συν τω χρόνω, β) το εν λόγω κόστος σε εποχές οικονομικής κρίσης πυροδοτεί ερωτήματα τύπου «πόσο περισσότερη ασφάλεια

πληροφοριακή τεχνολογία δίδει δικαίωμα όχι μόνο σε στρατιώτες αλλά σε οποιονδήποτε κατανοούντα να μεταμορφωθεί σε δικτυακό μαχητή... για περισσότερες λεπτομέρειες βλέπε στο “New Form of People’s War” (σ. 1-3) του Wei Jincheng στο *Foreign Broadcast Information Survey -CHI*, Number 159, 1996

¹⁷ Berkowitz D. Bruce, “Warfare in the Information Age” στο *Issues in Science and Technology*, Φθινόπωρο 1995, σ. 59-66

¹⁸ Ο όρος *glocalization* ή *internationalization* αποδίδει σε οικονομική βάση και ως ένα βαθμό το φαινόμενο

¹⁹ Papp D., Alberts D., “The Impacts of the Information Age on International Actors and the International System” στο *The Information Age: An Anthology on Its Impact and Consequences*, επιμ. Alberts D., Papp D., CCRP Publication Series, 1997, σ. 285-296 και “War in the Information Age Military” των ιδίων στο *Information Age Anthology: The Information Age Military*, επιμ. Alberts D., Papp D., CCRP Publication Series, 2001, σ. 1-26. Επίσης βλέπε στο κεφάλαιο “The Information Age” στο *Network Centric Warfare. Developing and Leveraging Information Superiority*, επιμ. Alberts D., Garstka John, Stein Frederick, CCRP Publication Series, 1999², σ. 15-23

κερδίζουμε από χρήση περισσότερης πληροφορίας;», γ) η κεντρικότητα της πληροφόρησης ως προς την προσπάθεια επίρρωσης αισθήματος εθνικής ασφαλείας έχει αυξηθεί, δ) η πληροφοριακή επανάσταση επανακαθορίζει την πολυτιμότητα της κρυφής πληροφόρησης έναντι άλλων μορφών πληροφόρησης²⁰, ε) στο σύγχρονο περιβάλλον ανησυχίες περί ιδιωτικότητας και άλλων αστικών ελευθεριών έρχονται σε αντίθεση με την ανησυχία που επιβάλλουν οι νέες προκλήσεις.²¹

Ο Lars Nicander θεωρεί ότι τέσσερα στοιχεία έχουν επηρεάσει την παγκόσμια πληροφοριακή κοινότητα οδηγώντας σε οργανωτικές καινοτομίες σχεδόν εξ ολοκλήρου ‘εκ των έσω’. Τα συγκεκριμένα τέσσερα στοιχεία αφορούν: α) στην πληροφοριακή / τεχνολογική επανάσταση και στον πολλαπλασιασμό των ανοικτών πηγών πληροφόρησης, β) στην αντιμετώπιση της τρομοκρατίας -πρόκειται για την κορυφαία προτεραιότητα όλων σχεδόν των μυστικών υπηρεσιών ανά την υφήλιο²², γ) στην αντιμετώπιση νέων τρωτοτήτων που γεννά η κοινωνία της πληροφόρησης, δ) στην ανάγκη αναδιαμόρφωσης των πληροφοριακών μηχανισμών ²³ λόγω των αναφερομένων δεδομένων.

Ο Michael Warner, ελάχιστα μετά τους Nolte και Nicander, τονίζει πως: α) η ψηφιακή επανάσταση σηματοδοτεί μια αναπόδραστη αλλαγή στον τρόπο που αποκτάται και χρησιμοποιείται η πληροφορία, β) η ψηφιακή επανάσταση δημιουργεί μια ακόμα πειστικότερη ανάγκη για «ανάλυση και αναλυτές», γ) η ψηφιακή και τεχνολογική επανάσταση ωθεί επιχειρήσεις, οργανισμούς και Υπηρεσίες σε ανασχηματισμό. Ο χρόνος συλλογής, ανάλυσης, διασποράς πληροφόρησης, απόφασης και δράσης έχει συμπιεστεί δραματικά, δ) η επιτυχία στην ψηφιακή εποχή θα στηριχτεί στις συμμαχίες. Αν και ελάχιστα έχουν διαρρεύσει, π. χ., για την περί κυβερνοδιαστήματος διεθνή πληροφοριακή συνεργασία, το όποιο αυστηρά εθνικό πληροφοριακό σύστημα δεν θα παράξει επουδενί το ποσό έργου ενός αντίστοιχου συνεργατικού, ε) η ταχύτητα διασποράς γενικής γνώσης στον 21^ο αιώνα όλο και θα αυξάνεται, στ) παρά τα αναφερόμενα, η ‘πρόοδος’ δεν πρόκειται να ακολουθήσει συμμετρικούς ανά τον κόσμο ρυθμούς, επιπλέον, κάτι που ‘βρίσκεται στον αέρα’ δεν σημαίνει πως έχει παρατηρηθεί ή εκτιμηθεί δεόντως, ζ) η νέα τεχνολογία φαίνεται να εξαυλώνει την ήδη αχνή διαχωριστική γραμμή μεταξύ κρατικών και μη κρατικών

²⁰ Σε σημείο, μάλιστα, να διερωτάται ο Joshua Rovner κατά πόσο οι Υπηρεσίες: α) εξακολουθούν να διατηρούν την παλαιά χρηστικότητά τους, β) οφείλουν να μεταλλαχθούν ακολουθώντας τα κελεύσματα της εποχής -περί τούτων βλέπε Rovner J., “Intelligence in the Twitter Age” στο *International Journal of Intelligence and CounterIntelligence*, Volume 26, Issue 2, 2013, σ. 260-271. Θεωρούμε ότι οι Υπηρεσίες θα διατηρήσουν τη αίγλη τους διότι κανένα μυστικό δεν πρόκειται να αποκαλυφθεί ή διακοινωθεί μέσω ανοικτών πηγών ή social media

²¹ Nolte William, “Valuing Intelligence: Opening a Conversation” στο *Intelligence and National Security*, Volume 26, Number 5, 2011, σ. 618-619. Με αφορμή το σημείο (ε) και τις νέες προκλήσεις, καταγράφουμε την αμφισβήτηση ύπαρξης, πλέον, της διαχωριστικής γραμμής μεταξύ ζητημάτων εξωτερικής και εσωτερικής ασφαλείας. Μάλιστα, ο V. D. Cha εφεύρει τον όρο “intermestic” εκ των λέξεων ‘international’ και ‘domestic’ -περί τούτου βλέπε Cha D. V., “Globalization and the Study of International Security” στο *Journal of Peace Research*, Volume 37, Number 3, 2000, σ. 397, επίσης, Richards Julian, “Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy” στο *Intelligence and National Security*, Volume 27, Number 5, 2012, σ. 772-774

²² Μέσα σε μία νύκτα από την 11^η Σεπτεμβρίου, γράφει η Carole A. Foryst, οι κυβερνήσεις προσάρμοσαν προσωπικό και προϋπολογισμούς στο counterterrorism αφήνοντας σε δεύτερο πλάνο το counterespionage -περί τούτου βλέπε Foryst A. C., “Rethinking National Security Strategy Priorities” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 3, 2010, σ. 400

²³ Nicander Lars, “Understanding Intelligence Community Innovation in the Post 9-11 World” στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 3, 2011, σ. 544-546

δρώντων αποδίδοντας εις χείρας τελευταίων ισχυρά / αόρατα όπλα, η) η «ασφάλεια δεδομένων» ουσιαστικά αποτελεί ευσεβή πόθο.²⁴

Τελικά φαίνεται πως η πληροφοριακή εποχή υπόσχεται έναν νέο κόσμο πλήρη αβεβαιοτήτων, η μόνη βεβαιότητα είναι αυτή, σημειώνουν οι Alberts και Papp. Από την άλλη οι ίδιοι τονίζουν ότι βρισκόμαστε στην ευτυχή θέση να ζούμε την αυγή του φαινομένου -πιθανόν είκοσι χρόνια μετά τη δήλωσή τους δεν έχει αλλάξει κάτι τόσο ριζικά. Αν αυτό ισχύει, τότε, έχουμε ίσως το χρόνο να σκεφθούμε πάνω στις επερχόμενες επιπτώσεις πριν αυτές καταστούν ανεξέλεγκτες, εντούτοις, επισημαίνουν οι δύο συγγραφείς, αυτό το παράθυρο ευκαιρίας θα κλείσει σύντομα.

Το μέλλον της (αντι)πληροφόρησης. Η πράξη

Ο Mark Lowenthal αναφερόμενος στις επιχειρησιακές προκλήσεις που αφορούν στο πεδίο του state intelligence κατά την μετά το 1990 εποχή και κατ' επέκταση κατά την εποχή του 21^{ου} αιώνα ομιλεί για:

- Αντιμετώπιση τρομοκρατίας.
- Αποτροπή διασποράς όπλων μαζικής καταστροφής.
- Μπλοκάρισμα οδών διακίνησης ναρκωτικών ουσιών.
- Εμπλοκή με το οικονομικό πεδίο.
- Αντιμετώπιση περιβαλλοντικών²⁵ / υγειονομικών απειλών.
- Συνεισφορά στην εκπλήρωση επιχειρήσεων peacekeeping.²⁶
- Διεξαγωγή πληροφοριακών επιχειρήσεων -Information Operations / IO.
- Επίτευξη επίγνωσης περιβάλλοντος μάχης -Dominant Battlefield / Battlespace Awareness / DBA.²⁷

Ο George Tenet συμπληρώνει κάνοντας λόγο για:

- Πάταξη οργανωμένου εγκλήματος.
- Παρακολούθηση κρατών-ταραξιτών.
- Αντιμετώπιση απειλών που έχουν να κάνουν με τον πληροφοριακό πόλεμο και, ευρύτερα, με τον κυβερνοχώρο.

²⁴ Warner M., "Reflections on Technology and Intelligence Systems" στο *Intelligence and National Security*, Volume 27, Number 1, 2012, σ. 143-150

²⁵ Η CIA, ήδη από το 2009, εγκαينιάζει το Κέντρο Κλιματικής Αλλαγής και Εθνικής Ασφαλείας με στόχο την πρόβλεψη των επιπτώσεων φαινομένων όπως η άνοδος της στάθμης των θαλασσίων υδάτων, η ερημοποίηση, η μετατόπιση πληθυσμών κ. λ. Ακολουθεί το 2012 το DoD που ιδρύοντας ένα παρόμοιο κέντρο σημειώνει πως οι εντεινόμενες μεταβολές του κλίματος «δεικνύουν απειλή για την αμερικανική εθνική ασφάλεια». Τέλος, σε έκθεσή του το αμερικανικό Center for Naval Analyses (CNA) υποστηρίζει ότι μια κλιματική αλλαγή «θα ενεργήσει καταλυτικά στην αύξηση της αστάθειας και των συγκρούσεων» με τον γεωγραφικό περίγυρο, μάλιστα, της Ελλάδας (Αφρική, Μέση Ανατολή) να παρουσιάζεται πλέον ευαίσθητος -περί τούτων ανέτρεξε "CIA Opens Center on Climate Change and National Security", CIA, 25 Σεπτεμβρίου 2009, 2014 *Climate Change Adaptation Roadmap*, DoD, 2014 και *National Security and the Accelerating Risks of Climate Change*, CNA Military Advisory Board, Alexandria / Virginia, Μάιος 2014, σ. 2

²⁶ Ο Laurie Nathan εξηγεί ότι η διεθνής διαμεσολάβηση διατρέχεται από πληροφοριακές ανάγκες που αφορούν στην κατανόηση εκ των διαμεσολαβητών της κουλτούρας των αντιμαχομένων με ό,τι θετικό δύναται αυτή να συνεισφέρει -για μια εικόνα βλέπε Nathan Laurie, "The Intelligence Requirement of International Mediation" στο *Intelligence and National Security*, Volume 29, Number 2, 2014, σ. 208-226, επίσης, Dorn, A. Walter, "United Nations Peacekeeping Intelligence" στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson Loch, Oxford University Press, Oxford, 2010, σ. 275-295

²⁷ Lowenthal M., *Intelligence. From Secrets to Policy*, CQ Press, Washington, ΗΠΑ, 2002, σ. 190-203

- Αντιμετώπιση «παραδοσιακών ανησυχιών» περίξ εύθραυστων κρατών εντός μεταβαλλόμενων περιοχών, επίσης, περίξ αποτυχημένων κρατών ή κρατών σε μεταβατική περίοδο.²⁸

Από τη μεριά τους οι Carl Jensen, David McElreath και Melissa Graves σημειώνουν πως το DHS έχει υιοθετήσει μια συνολική “all hazards” προσέγγιση προκειμένου αναγνώρισης / αντιμετώπισης ενός πλέγματος καταστάσεων που αφορούν ακόμα και σε φυσικές καταστροφές. Απώτερος σκοπός ο βέλτιστος συντονισμός σε περίπτωση εμπλοκής πλήθους Υπηρεσιών. Οι συγκεκριμένες καταστάσεις σχετίζονται, πέραν των ζητημάτων που θέτουν οι Lowenthal και Tenet, με:

- Ναρκοτρομοκρατία ήτοι, διακίνηση / εμπορεία ουσιών προς χρηματοδότηση εξτρεμιστικών σχεδιασμών.
- Trafficking.
- Κλοπή πνευματικής ιδιοκτησίας.
- Επιβουλή συνοριακής ασφαλείας και μεταναστευτικής πολιτικής.
- Φυσικές θεομηνίες.²⁹

Ο καθηγητής αμυντικής και στρατηγικής ανάλυσης Ιωάννης Ραγιές δίδει έμφαση:

- Στον πολλαπλασιασμό των πολιτικών και στρατιωτικών δρώντων, των πηγών αστάθειας / συγκρούσεων, των μεθόδων χρήσης βίας.
- Στον διεθνικό χαρακτήρα των απειλών.
- Στον κίνδυνο χρήσης της νέας τεχνολογίας από κακόβουλα στοιχεία.
- Στο ολοένα αυξανόμενο ποσοστό ασύμμετρων / μη συμβατικών μορφών σύγκρουσης.
- Στη μετακύλιση της βίας εντός αστικών / ημιαστικών συγκροτημάτων.

Σύμφωνα με τον ίδιο οι νέες περιοχές ενδιαφέροντος / χρήσης πληροφοριών έχουν να κάνουν με:

- Την προστασία καίριων κρατικών υποδομών (critical infrastructure protection -CIP) έναντι κλασικών ή άλλου τύπου επιθέσεων.³⁰
- Τις πολυεθνικές επιχειρήσεις επιβολής ειρήνης, τις στρατιωτικές ή μη στρατιωτικές προσπάθειες διαχείρισης κρίσεων.
- Την επίβλεψη / προστασία συνόρων και λοιπών ευαίσθητων / διάτρητων σημείων εισόδου αγνώστων ατόμων, όπλων μαζικής καταστροφής, ύποπτων ή επικίνδυνων υλικών κ. λ.

Ο μελετητής ασχολούμενος με νέους δρώντες / κινδύνους τονίζει την ύπαρξη:

- Διεθνικών τρομοκρατικών και εγκληματικών ομάδων.
- Κυβερνήσεων που λειτουργούν επικουρικά ως προς τις άνω ομάδες.

²⁸ Tenet G., “The CIA and Security Challenges of the New Century”, *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 2, 2000, σ. 138

²⁹ Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA, 2013, σ. 293-315

³⁰ Κατά την αμερικανική President’s Commission on Critical Infrastructure Protection (PCCIP) του Ιουλίου του 1996 οκτώ είναι οι βασικοί πυλώνες ενός κρατικού μηχανισμού, ειδικότερα: α) τηλεπικοινωνίες, β) τραπεζικό / χρηματοπιστωτικό σύστημα, γ) ηλεκτρικό δίκτυο, δ) δίκτυο αποθήκευσης / διανομής ενεργειακών πόρων (πετρελαιοειδή, φυσικό αέριο κ. λ.), ε) δίκτυο διανομής υδάτινων πόρων, στ) μεταφορές, ζ) υπηρεσίες εκτάκτων καταστάσεων, η) άλλες κυβερνητικές υπηρεσίες -για περισσότερες λεπτομέρειες βλέπε Denning D., *Information Warfare and Security*, ACM Press, USA, 1999, σ. 74-76, επίσης, The Report of the President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructure*, Οκτώβριος 1997 και Presidential Decision Directive / NSC-63, *Critical Infrastructure Protection*, Μάιος 1998, αντιστοίχως στις τοποθεσίες <https://fas.org/sgp/library/pccip.pdf> και <http://fas.org/irp/offdocs/pdd/pdd-63.pdf> όπου προστρέξαμε την 24^η Μαΐου 2015

- Αποτυχημένων, ανυπόληπτων ή οικονομικά κατεστραμμένων κρατών των οποίων η πολιτική απουσία, μάλλον, παρά παρουσία, δύναται να προκαλέσει ενδημικές συγκρούσεις, πληθυσμιακή μεταφορά, εγκληματική / τρομοκρατική δράση ανεξέλεγκτων ομάδων κ. λ.
- Θεσμικά κατοχυρωμένων δυνάμεων ασφαλείας (statutory security forces) επί των οποίων ο κρατικός έλεγχος ασκείται πλημμελώς ή αναποτελεσματικά.
- Μη κυβερνητικών, ιδιωτικών ή παραστρατιωτικών ομάδων / εταιριών επί των οποίων δεν υφίσταται ικανοποιητικός κρατικός έλεγχος.³¹

Τέλος το ODNI, ήδη από το 2008, δημοσιεύει το *Vision 2015* εντός του οποίου καταγράφονται «persistent threats and emerging mission for the IC». Σκοπός η αναζήτηση λύσεων / προτάσεων σχετικών με:

- Αποτυχημένες κρατικές οντότητες.
- Απειλές υγειονομικού τύπου.
- Απειλές μετάδοσης μολύνσεων οικονομικού τύπου.
- Το διάστημα.
- Την κλιματική αλλαγή.
- Κράτη ταραξίες.
- Φυσικούς και ενεργειακούς πόρους.
- Ανερχόμενες δυνάμεις.
- Εξεγέρσεις.
- Το έγκλημα.
- Τα ναρκωτικά.
- Το trafficking.
- Τον κυβερνοχώρο.
- Τα όπλα μαζικής καταστροφής.
- Ασύμμετρες πολιτικές και στρατιωτικές προκλήσεις.

Όσον αφορά σε γνωστά επιχειρησιακά πεδία γίνεται λόγος για σχεδιασμούς περί:

- Την αντιμετώπιση αλλοδαπών Υπηρεσιών.
- Επιχειρήσεων άρνησης και παραπλάνησης (D&D).
- Την αντιμετώπιση του τρομοκρατικού και εξτρεμιστικού φαινομένου.
- Την καταγραφή οικονομικών, στρατιωτικών, πολιτικών και ιδεολογικών τάσεων / δυναμικών περιφερειακών δυνάμεων προς αναγνώριση επικείμενων προκλήσεων.
- Την ευρύτερη αντικατασκοπευτική στρατηγική.³²

Το μέλλον των Υπηρεσιών. Μεταρρύθμιση ή μεταλλαγή;

Σε απάντηση των προκλήσεων / προβληματισμών που απασχολούν τις Υπηρεσίες παγκοσμίως, ο Carole Dumaine προτείνει:

- Μια αυξημένη διεθνή πληροφοριακή συνεργασία.³³

³¹ Ραγιές Ιωάννης, «Σύγχρονες προκλήσεις για τις Υπηρεσίες Πληροφοριών. Η συνδρομή στην άσκηση πολιτικής» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009, σ. 163-164

³² *Vision 2015. A Globally Networked and Integrated Intelligence Enterprise*, ODNI, Washington, D.C., 2008, σ. 4-5 και Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, ό. π., σ. 48

³³ Η συζήτηση περί συνεργασίας Υπηρεσιών με διεθνή προοπτική δεν είναι πρόσφατη. Έχει ξεκινήσει από την αρχή του ψυχρού πολέμου και αλήθεια είναι πως έχει επιδείξει πρακτικό έργο. Σε πολυμερές επίπεδο γνωστή είναι η συνθήκη UKUSA (1948) μεταξύ Αμερικής, Βρετανίας, Καναδά, Αυστραλίας

- Μια περαιτέρω αξιοποίηση των ανοικτών πηγών πληροφόρησης.
- Μια νέα συνεργατική κουλτούρα μεταξύ των αναλυτών των Υπηρεσιών με σκοπό την κατανόηση κινδύνων που σχετίζονται με δράση μη κρατικών δρώντων.³⁴

Ο William Lahneman σημειώνει πως το πρότερο μοντέλο λειτουργίας των πληροφοριακών οργανισμών στηριζόταν στην αποδοχή πραγματικοτήτων όπως: α) του γνώριμου των απειλών, β) της στατικότητας των απειλών και γ) της σχετικής ευκολίας με την οποία μια δυνητικά επίβουλη κατάσταση αποκαλυπτόταν. Εντούτοις, ο 21^{ος} αιώνας καλεί σε μια σύζευξη. Αν και οι παλαιότεροι κίνδυνοι δεν έχουν εκλείψει, η παρουσία νέων ωθεί στη δημιουργία ενός σύνθετου εξελιγμένου παραδείγματος -πρόκειται για το λεγόμενο *adaptive interpretation paradigm*. Αυτό, σύμφωνα με τον Lahneman, δεικνύει κομμάτι της ζητούμενης απάντησης, ωστόσο, προκειμένου να λειτουργήσει απαιτείται:

- Άνοιγμα / συνεργασία Υπηρεσιών τόσο σε κρατικό όσο σε διεθνές επίπεδο.
- Ευρύτερη χρήση ανοικτών πηγών και περιορισμός της ευχέρειας με την οποία διαβαθμίζονται πληροφορίες χωρίς συχνά αυτή (η διαβάθμιση) να είναι απαραίτητη.
- Απομείωση της μυστικότητας πάνω στην οποία στηρίζονται οι Υπηρεσίες όπως και μια ανάπτυξη αμοιβαίας εμπιστοσύνης.

και Ν. Ζηλανδίας, το ετήσιο forum των ευρωπαϊκών Υπηρεσιών υπό την ονομασία The Club of Berne με έτος πρώτης συνάντησης το 1971, το The Kilowatt Group με έτος ιδρύσεως το 1972 και μέλη Υπηρεσίες από τον ευρωπαϊκό και αγγλοσαξονικό χώρο, το Ισραήλ και τη Ν. Αφρική, το The Egmont Group for Financial Intelligence Units κ. λ. Σε διμερές επίπεδο καταγράφεται πλήθος διαμοιβών μεταξύ Υπηρεσιών του ιδίου ιδεολογικού χώρου και πολιτικού προσανατολισμού -βλέπε αυτές της γαλλικής υπηρεσίας εσωτερικής ασφαλείας DST και της CIA, της DST και της γερμανικής ομοσπονδιακής υπηρεσίας Πληροφοριών BND, της αυστραλιανής ASIO και της καναδικής CSIS, των Υπηρεσιών των ανατολικών χωρών ακόμα ακόμα των ισραηλινών πληροφοριακών οργανισμών με τους αντίστοιχους της Ιορδανίας. Αν οι λόγοι συνεργασίας είναι κατανοητοί ξεκινώντας από την ανταλλαγή στοιχείων, τεχνογνωσίας κ. λ. φτάνοντας μέχρι την αντιμετώπιση κοινών απειλών και μια οιοονεί αναπλήρωση μηδενικών ή, έστω, ελλειμματικών διπλωματικών σχέσεων [βλέπε την προσέγγιση γαλλικών και συριακών Υπηρεσιών σε απροσδιόριστο χρόνο προκειμένου αντιμετώπισης του Ισλαμικού Κράτους -περί τούτου ανέτρεξε στο Lequesne Christian, "French foreign and security challenges after the Paris terrorist attack", *Contemporary Security Policy*, Volume 37, Issue 2, 2016, σ. 315] υπάρχουν, επίσης, αντίστοιχοι που την αποτρέπουν. Οι κυριότεροι σχετίζονται με: α) μια διαφορετική αντίληψη απειλών, β) διαφορετικές προτεραιότητες και σχεδιασμούς στην κρατική εξωτερική πολιτική, γ) μια ανόμοια αντιμετώπιση θεμάτων που περιστρέφονται γύρω από τις δημοκρατικές ελευθερίες και τα δικαιώματα του ατόμου, δ) μια φοβία πρόσδεσης της πιο αδύναμης Υπηρεσίας στο άρμα της πιο δυνατής, ε) μια απαίτηση λύσεως νομικών ή συνταγματικών κωλυμάτων, στ) μια φιλοποψία παροχής στοιχείων σε τρίτα μέρη χωρίς προηγούμενη συμφωνία των δύο συνεργαζόμενων, ζ) γενικότερες επιφυλάξεις περί μη τήρησης των συμφωνηθέντων, αλλαγής στάσης στην πορεία λόγω εξωγενών παραγόντων κ. λ.

Είναι γεγονός ότι καμία Υπηρεσία δεν διαθέτει απόλυτη επάρκεια ώστε να μην επιδιώξει στο διάβα του χρόνου κάποιου είδους συναλλαγή με κάποια άλλη. Είναι επίσης γεγονός ότι σε ζητήματα υψηλής ασφαλείας προτιμώνται οι διμερείς παρά οι πολυμερείς διαμοιβές (καθώς οι μόλις αναφερόμενοι προβληματισμοί αντιμετωπίζονται καλύτερα εντός μικρού κύκλου) σε αντίθεση με ζητήματα law enforcement τα οποία επιδέχονται επαφές πολυμερούς χαρακτήρα. Ακριβώς γι' αυτούς τους λόγους, τουλάχιστον κατά τον St éphane Lefebvre, οι συνεργασίες ανοικτού τύπου (NATO, The Club of Berne) διακατέχονται πολύ περισσότερο από έναν πολιτικό παρά από έναν αμιγώς επιχειρησιακό χαρακτήρα -για μια πληρέστερη άποψη βλέπε Lefebvre Stéphane, "The Difficulties and Dilemmas of International Intelligence Cooperation" στο *International Journal of Intelligence and CounterIntelligence*, Volume 16, Issue 4, 2003, σ. 527-537 όπως και Herman Michael, *Intelligence Power in Peace and War*, The Royal Institute of International Affairs, Cambridge University Press, 1996, σ. 200-208

³⁴ Dumaine C., "Intelligence in the New Millennium", CIA Directorate of Intelligence, AFCEA Spring Intelligence Conference, April 18, 2001

- Κτίσιμο κουλτούρας 'πρόβλεψης / πρόληψης' γεγονότων και όχι δράσης μετά την εκδήλωσή τους.³⁵

Ο Fred Schreier υποστηρίζει ότι τα κράτη οφείλουν να πριμοδοτήσουν μια ριζική αναμόρφωση / μεταλλαγή (transformation) των Υπηρεσιών και όχι μια απλή μεταρρύθμιση (reformation). Αν η πρώτη είναι δύσκολο να εκκινήσει, οι απαιτήσεις του μέλλοντος την επιβάλλουν. Η ικανότητα μεταλλαγής με ταχύτητα μάλιστα που υπερβαίνει την ταχύτητα των αλλαγών που παρατηρούνται στο διεθνές περιβάλλον ασφαλείας οφείλει να αποτελέσει χαρακτηριστικό των νέων οργανισμών. Η μεταλλαγή για την οποία κάνουμε λόγο θα στηριχτεί σε ένα πάντρεμα επιλεγμένων τεχνολογικών μέσων, στρατηγικών, πολιτικών και επιχειρησιακών σχεδιασμών αφορώντας σε πληροφοριακά δόγματα, στην οργάνωση / γραφειοκρατία των Υπηρεσιών, στην λειτουργία της ηγεσίας, στην εκπαίδευση. Το αποτέλεσμα αυτής της μεταλλαγής καλείται να αποδώσει στους διαμορφωτές πολιτικής: α) έγκυρη προειδοποίηση, β) τοποθετήσεις επί στρατηγικών αλλά και τακτικών προβληματισμών, γ) πλεονέκτημα στην εκπόνηση αμυντικών / επιθετικών αντιμέτρων που οφείλουν να ενεργοποιούνται σε πρώτο χρόνο έναντι ασύμμετρων επικινδυνοτήτων και αιφνιδιασμών.³⁶

Η Deborah Barger επίσης στηρίζει μια εκ βάθρων ανασύνταξη των πληροφοριακών δομών εφόσον αυτές επιθυμούν να ανταποκριθούν στο κάλεσμα του 21^{ου} αιώνα. Οι Υπηρεσίες οφείλουν να επανεξετάσουν τόσο το ήθος όσο την κουλτούρα τους. Να επανεκτιμήσουν το εξωτερικό περιβάλλον. Να συνδράμουν το προσωπικό στην κατανόηση των κατακλυσμιαίων αλλαγών. Σύμφωνα με την συγγραφέα η απάντηση δεν βρίσκεται στην προσαρμογή αλλά στην μεταμόρφωση. Η πληροφοριακή κοινότητα δεν στερείται καινοτόμων προτάσεων αλλά μεθόδων εξέτασης των τελευταίων. Ένας τρόπος συντίθεται εκ της δημιουργίας μιας «συμμαχίας εγκεφάλων». Αυτή θα καθοδηγείται από μέσα συμπεριλαμβάνοντας, ωστόσο, και άτομα εκτός Υπηρεσιών. Σκοπό δεικνύει η αξιολόγηση του RIA φαινομένου αλλά και η ενθάρρυνση μιας σκέψης που αντιλαμβάνεται το εγχείρημα «πληροφόρηση» και ως ...*σύστημα αλληλένδετων ποιοτήτων* (capabilities) με *κίνητρο το τσεκάρισμα του αντίκτυπου σε μία περιοχή εξ αιτίας αλλαγών σε μια άλλη*. Οι επιτελείς της κοινότητας των πληροφοριών θα αντιμετωπίσουν πολιτικά, οικονομικά και νομικά κωλύματα στην προσπάθεια αναμόρφωσης των γραφειοκρατιών τους. Χωρίς την τριπλή συνεργασία μεταξύ εξωτερικών συντελεστών που θα υποβάλουν ιδέες, επιτηρητών με νομικές γνώσεις που θα τις υποστηρίξουν και εσωτερικών παραγόντων που θα τις εργαλειοποιήσουν, μια αληθινή διαδικασία RIA δεν πρόκειται να υπάρξει. Μια τέτοια συνεργασία, συνεχίζει η Barger, είναι μεν δύσκολο να υλοποιηθεί, όχι όμως ακατόρθωτο.³⁷

³⁵ Ο Lahneman προσπαθώντας να γεφυρώσει το χάσμα ανάμεσα στο παλαιό (traditional) και στο νέο (adaptive) μοντέλο προτείνει, συν τοις άλλοις, τη δημιουργία μιας ενδιάμεσης, μεταξύ secret και open, πληροφοριακής κατηγορίας, αυτής της *trusted* εντός της οποίας θα ενσωματωθούν και απόρρητα δεδομένα. Ο ίδιος υιοθετεί ένα σχέδιο αναδιοργάνωσης του σκληρού πυρήνα των αμερικανικών Υπηρεσιών με στόχο την προσήλωσή τους τόσο στη συγκέντρωση πληροφοριών αποκλειστικά μέσω μυστικών οδών όσο και στην κρυφή δράση (covert action) -για όλα αυτά ανέτρεξε στο Lahneman W., "The Need for a New Intelligence Paradigm" στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 2, 2010, σ. 201-224

³⁶ Schreier Fred, *Transforming Intelligence Services. Making Them Smarter, More Agile, More Effective and More Efficient*, National Defence Academy, Austrian Ministry of Defence and Sports, Geneva Centre for the Democratic Control and Armed Forces, Vienna / Geneva, 2010, σ. 67-68

³⁷ Barger Deborah, "Is It Time to Transform, Not Reform, US Intelligence", *SAIS Review*, Volume 24, Number 1, 2004, σ. 30

Είναι τελικά δυνατόν να αλλάξει μια αυστηρή / άκαμπτη γραφειοκρατία όπως αυτή των μυστικών υπηρεσιών; Υποστηρίζεται, π. χ., πως η αμερικανική πληροφοριακή κοινότητα «θα αναγκαστεί να το κάνει», είτε το θέλει, είτε όχι, λόγω των κλήσεων του διεθνούς περιβάλλοντος.³⁸ Το χρονικό σημείο που απαιτεί τη μεταλλαγή ενός οργανισμού καλείται από τον Steve Grove «strategic inflection point».³⁹ Ακριβώς αυτό το σημείο έχει για τις (αμερικανικές) Υπηρεσίες σημαίνει το 2001. Οκτώ παράγοντες το αποδεικνύουν:

- Η αλλαγή της φύσεως των απειλών ασφαλείας.
- Η αλλαγή της φύσεως του πολέμου και της στρατιωτικής στρατηγικής.
- Η αλλαγή της φύσεως της ειρήνης.
- Η ανάγκη αναπροσαρμογής της φύσεως της εθνικής στρατηγικής ασφαλείας.
- Η αυξανόμενη ποσότητα και η αναβαθμισμένη ποιότητα της παρεχόμενης πληροφόρησης όπως και η ποικιλία των τρόπων διαμοιρασμού της.
- Η αλματώδης τεχνολογική ανάπτυξη που, αλήθεια είναι, δεν μπορεί να υιοθετηθεί άμεσα σε οργανωτικό / επιχειρησιακό επίπεδο ακόμα και από μεγάλους οργανισμούς ή, ίσως, ειδικά από αυτούς.
- Οι ανανεωμένες προσδοκίες των δεκτών της πληροφόρησης ήτοι, των ανωτάτων ηγεσιών.
- Οι υψηλές προσδοκίες της (αμερικανικής) κοινής γνώμης.⁴⁰

Υπηρεσίες στον 21^ο αιώνα: Εξέλιξη ή επανάσταση; Παλαιές ιεραρχίες και νέα δίκτυα

Δύο κατά βάσει γκρουπ ερίζουν για το ρυθμό διά του οποίου πρέπει να προχωρήσουν οι όποιες μεταρρυθμίσεις εντός της (αμερικανικής) πληροφοριακής κοινότητας. Το πρώτο (εξελικτικό -evolutionary) υιοθετώντας μια ρητορική κατά ριζοσπαστικών λύσεων τονίζει ότι μια επανάσταση στο χώρο: α) δεν είναι απαραίτητη διότι δεν παρατηρείται μια ανάλογη σε επίπεδο απειλών, β) δεν δύναται να πραγματοποιηθεί λόγω έλλειψης ανθρωπίνων και χρηματοδοτικών πόρων, γ) δεν δύναται να προ-ελεγχθεί ως προς το αποτέλεσμα της, δ) απαιτεί μόνιμο και απαρέγκλιτο υπηρεσιακό και πολιτικό σχεδιασμό, κάτι που, με τη συχνή αλλαγή προσώπων, δεν μπορεί να επιτευχθεί, ε) δεν δεικνύει ότι καλύτερο υπό την έποψη κατακλυσμιαίων αλλαγών που, ενδεχομένως, αποδειχτούν επιζήμιες, στ) θα συνδεθεί, πιθανόν, με επίδοξες αλλά βραχύβιες προσπάθειες / φιλοδοξίες πολιτικών προσώπων, ζ) δεν συνθέτει κομμάτι των ενδιαφερόντων του μέσου (αμερικανού) πολίτη.

Από την άλλη μεριά, η δεύτερη (επαναστατική -revolutionary) ομάδα ανταπαντώντας υποστηρίζει ότι: α) αν και οι νέες απειλές δεν είναι τόσο νέες (βλέπε τρομοκρατία), η ποιοτική αναβάθμισή τους δεν αντιμετωπίζεται με μη ρηζικέλευθες αλλαγές και λύσεις, β) η έλλειψη πόρων δεν δεικνύει πρόβλημα όσο η έλλειψη, τουλάχιστον, πολιτικής βούλησης / στήριξης, γ) τα όποια «απρόβλεπτα» αποτελέσματα ίσως αποδειχτούν «όχι και τόσο απρόβλεπτα», δ) η αλλαγή προσώπων αφορά κατά κύριο λόγο στα ανώτατα κλιμάκια / αξιώματα, κάτι όχι τόσο δραματικό για την απρόσκοπτη πορεία μιας διαδικασίας, ε) τίποτα δεν αποδεικνύει ότι τα όποια αρνητικά παράγωγα βαθέων αλλαγών δεν υπόκεινται σε διόρθωση, στ) επίδοξες, έστω βραχύβιες, προσπάθειες πολιτικών παραγόντων να κάνουν τη «διαφορά» δεν σημαίνει απαραίτητως αποτυχία, ζ) αν και η κοινή γνώμη δεν ενδιαφέρεται πρωτίστως για μια συζήτηση περί των Υπηρεσιών, η όλη στάση μετά την 11^η Σεπτεμβρίου έχει διαφοροποιηθεί. Περαιτέρω, οι «επαναστατικοί» διατρανώνουν ότι σε περίπτωση που η πληροφοριακή κοινότητα δεν αποδεχτεί ένα εσωτερικού επιπέδου RIA, τότε: α) θα

³⁸ Barger Deborah, "Is It Time to Transform, Not Reform, US Intelligence", ό. π., σ. 28, επίσης, Liaropoulos Andrew, *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm*, Research Paper No 100, RIEAS, Athens, 2006, σ. 6

³⁹ Grove Andrew, *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career*, Doubleday, New York, 1996, σ. 3-6

⁴⁰ Barger Deborah, "Is It Time to Transform, Not Reform, US Intelligence", ό. π.

παρατηρηθεί μια ασυμμετρία μεταξύ τρέχοντος εξωτερικού περιβάλλοντος και υπηρεσιακών δυνατοτήτων εις βάρος των δευτέρων ή β) εξωυπηρεσιακοί συντελεστές / εξωγενή άτομα θα αναλάβουν να οδηγήσουν το άρμα των Υπηρεσιών στο μέλλον με αμφίβολα αποτελέσματα ή γ) θα καταγραφεί μια στασιμότητα σε παρελθοντικές καταστάσεις τη στιγμή που οβιδιακές εξελίξεις θα λαμβάνουν χώρα.⁴¹

Σύμφωνα με τους Arquilla και Ronfeldt η πληροφοριακή επανάσταση κινητοποιεί δυνάμεις που αργά ή γρήγορα θα επαναχαράξουν τη δομή πλήθους οργανισμών. Οι ιεραρχίες παύουν να λειτουργούν στα παλαιά δύσκαμπτα top-down πρότυπα. Μικρότεροι δρώντες ενδέχεται να ενισχυθούν. Οι αρμοδιότητες αλλάζουν. Τα κλειστά συστήματα ανοίγουν. Αν οι εξελίξεις προβληματίζουν τις μεγάλες μονάδες, ευνοούν τη δημιουργία των λεγόμενων *multi-organizational networks* -πρόκειται για άλλη ορολογία των all-channel networks. Οι δυο τους εξετάζουν όλα τα είδη networks επισημαίνοντας την ιδέα που τα συνέχει: τα networks, σε αντίθεση με τους κλασικούς οργανισμούς, συνενώνουν, ή είναι, μικρές ομάδες που δρουν συνεργατικά και διασυνδεδασικά. Η πληροφοριακή επανάσταση φέρει σε επαφή απομακρυσμένους σχηματισμούς καθιστώντας εφικτή την επικοινωνία, τη διαβούλευση, την επίδοση στοιχείων, τη σύμπραξη κ. λ. ⁴² Από τη μεριά τους οι Alberts και Hayes χρησιμοποιούν τον όρο *edge organization* προκειμένου να ονοματοδοτήσουν τα νέα σχήματα διαχωρίζοντάς τα από τα προηγούμενα. Η διάθεση διαμοιρασμού της πληροφορίας και μια αίσθηση ομότιμης *peer-to-peer* σχέσεως μεταξύ των συμμετεχόντων αποτελεί χαρακτηριστικό τους. Κάθε τέτοιος οργανισμός ενισχυμένος με το πληροφοριακό δεδομένο σε πραγματικό χρόνο πριμοδοτείται με ένα οιονεί δικαίωμα ελευθερίας κινήσεων -πρόκειται για δικαίωμα που δεν καταγράφεται εντός μιας παραδοσιακής *line organization* ιεραρχίας. Στην ουσία αναφερόμαστε σε συμπερακτικούς βραχίονες ανοικτού (inclusive) τύπου σε αντίθεση με τις παλαιές κλειστής (exclusive) δομής γραφειοκρατίας.⁴³ Τέλος, οι Berkowitz και Goodman ομιλούν για ένα «decentralized, market-based, fluid model for intelligence» τη στιγμή που ο Thomas Hammond συζητά περί της αποκαθήλωσης της πρακτικής του *compartmentation*, τον περιορισμό της μυστικότητας, τη δημιουργία μιας κεντρικής αλλά όχι κλειστής βάσης δεδομένων («Intellipedia» στη διάλεκτο των επαγγελματιών) στην υπηρεσία της πληροφοριακής κοινότητας.⁴⁴

Κλείνουμε με τον Richard Betts σημειώνοντας πως πρόκειται για έναν από τους λίγους, αν όχι τον μοναδικό εγνωσμένο μελετητή, που δεν φαίνεται να ενδιαφέρεται ιδιαίτερος για ζητήματα μεταρρυθμίσεων των οργανισμών πληροφόρησης. Η στάση αυτή οφείλεται στη βεβαιότητα πως ελάχιστα δύναται να γίνουν σε επίπεδο ανάλυσης προκειμένου οι Υπηρεσίες να ανταποκριθούν καλύτερα σε γεγονότα που, τελικά, δεν θα αποσοβηθούν -ο Betts πιστεύει πως οι πληροφοριακές αποτυχίες είναι αναπόφευκτες. Κατά την έννοια τούτη όχι μόνο δεν ασχολείται με το θέμα «μεταρρύθμιση πληροφοριακών οργανισμών» αλλά το αντιμετωπίζει με καχυποψία. Ο Ανδρέας Λιαρόπουλος συνοψίζει γράφοντας πως ο ερευνητής αντιλαμβάνεται την

⁴¹ Barger D., *Toward a Revolution in Intelligence Affairs*, RAND, Santa Monica, 2005, σ. 33-47

⁴² Για περισσότερες πληροφορίες βλέπε Arquilla J., Ronfeldt D., “Cyberwar Is Coming”, ό. π., σ. 25-27 αλλά και Max Boot, “More Small Wars” στο *Foreign Affairs*, Volume 93, Number 6, 2014, σ. 13 εντός του οποίου ανευρίσκεται ο όρος *interoperability* ακριβώς ως δράση επιχειρησιακής διακλαδικής σύζευξης

⁴³ Alberts S. D., Hayes E. R., *Power to the Edge. Command...Control...in the Information Age*, CCRP Publication Series, 2003, σ. 176-177, επίσης Alston Anthony, et al., *Implementing Edge Organizations: Exploiting Complexity*, Paper Number #107, 10th International Command and Control Research & Technology Symposium, McLean, Virginia, Ιούνιος 2005, διαθέσιμο και στην ιστοσελίδα http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/107.pdf όπου ανατρέξαμε τη 15^η Απριλίου 2015

⁴⁴ Για περισσότερες λεπτομέρειες βλέπε Berkowitz B., Goodman A., *Best Truth: Intelligence in the Information Age*, Yale University Press, ΗΠΑ, 2000, σ. 92 και Hammond T., “Intelligence Organizations and the Organization of Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 4, 2010, σ. 713-717

αναδιάρθρωση περισσότερο ως γεννήτορα νέων προβλημάτων και νέων αναγκών παρά ως κάτι εποικοδομητικό. Η δημιουργία, π. χ., μιας νέας Υπηρεσίας μετακινεί το ενδιαφέρον από μια περιοχή σε μια άλλη με κίνδυνο να παραμεριστούν προηγούμενες προτεραιότητες ή να ατονήσουν παραδεκτές δομές. Πέρα τούτων, η προσθήκη μιας ακόμα γραφειοκρατίας εντός της πληροφοριακής κοινότητας εμπεριέχει την απειλή σύγκρουσης συμφερόντων, ενός άγονου ανταγωνισμού, μιας διαμάχης κατανομής χρηματοδοτικών πόρων κ. λ.⁴⁵

Συμπεράσματα

Η λήξη του ψυχρού πολέμου όχι μόνο δεν μείωσε τους προβληματισμούς των υπηρεσιών Ασφαλείας αλλά τους επαύξησε. Εντός του παλαιού περιβάλλοντος η επιφυλακτικότητα που ο φόβος γεννούσε δεν επέτρεπε σχεδιασμούς που θα παραβίαζαν δεδομένες κόκκινες γραμμές. Οι χώροι ήταν οριοθετημένοι, τα περισσότερα κράτη στοιχίζονταν αμέσως ή εμμέσως εντός αυτών. Αντιθέτως, στη μεταψυχροπολεμική εποχή παρατηρείται μια ασάφεια που έχει να κάνει με το εξής διττό: αν και ο κόσμος δεν είναι χωρισμένος σε ανατολικό και δυτικό στρατόπεδο δεν είναι, την ίδια στιγμή, καθόλου ενοποιημένος. Η περιώνυμος παγκοσμιοποίηση δεν καθιστά φανερό αν οδεύουμε προς ένα μοντέλο ομογενοποίησης ή προς μια έκρηξη διαφορετικότητας. Η ανακούφιση του φόρτου των νέων προκλήσεων απαιτεί μεταξύ άλλων (και) ανάληψη αυξημένων καθηκόντων εκ των Υπηρεσιών στην κατεύθυνση της εύρεσης της πληροφορίας που θα παράξει πληροφόρηση και αυτή με τη σειρά της θα μεταμορφωθεί σε γνώση προς όφελος του ηγέτη, της διαδικασίας λήψεως αποφάσεων και του κρατικού προγραμματισμού.⁴⁶

Ασφαλώς, ο κύκλος των μελετητών της πληροφόρησης και των Υπηρεσιών δεν χαρακτηρίζεται μόνο από φανατικούς οπαδούς αλλά και από πρόσωπα που ζητούν κάποιες διευκρινήσεις χωρίς αυτό να σημαίνει πως δεν κατανοούν το ρόλο τους, αντιθέτως μάλιστα. Έτσι ο Gwilym Hughes αναρωτείται, π. χ., αν μετά την πτώση της Σοβιετικής Ένωσης η ανάγκη ύπαρξης των πληροφοριακών οργανισμών εξακολουθεί να υφίσταται.⁴⁷ Ο John Keegan υποστηρίζει ότι ο ρόλος των πληροφοριών στον πόλεμο είναι υπερτιμημένος.⁴⁸ Οι Gill και Phythian φτάνουν μέχρι υποθέσεων περί

⁴⁵ Liaropoulos Andrew, “A Review of ‘The Three Foes of Intelligence’” στο *International Journal of Intelligence and CounterIntelligence*, Volume 21, Issue 2, 2008, σ. 407, επίσης, Dujmovic Nicholas, “Enemies of Intelligence: Knowledge and Power in American National Security” στο *Studies in Intelligence*, Volume 51, Number 4, 2007, σ. 39-42, Barrett David, “Book Review. Why Intelligence Failure Are (Still) Inevitable” στο *Diplomatic History*, Volume 34, Number 1, 2010, σ. 209. Για ακόμα περισσότερες λεπτομέρειες βλέπε Betts Richard, *Enemies of Intelligence: Knowledge and Power in American National Security*, Columbia University Press, New York, 2007, σ. 124-158

⁴⁶ Ο David Muller χρησιμοποιεί τον όρο *future intelligence* με σκοπό να τονίσει την ανάγκη παραγωγής πληροφοριακού προϊόντος που προσβλέπει στην προεικόνιση μελλοντικών καταστάσεων σε βάθος εικοσαετίας. Κάτι τέτοιο δεν είναι καθόλου εύκολο για ευνόητους λόγους αλλά και λόγους που σχετίζονται κυρίως με την αδιαφορία του πολιτικού προσωπικού -δύσκολα κάποιος κυβερνητικός παράγοντας θα ασχοληθεί με κάτι που ενδέχεται να συμβεί μετά από δύο δεκαετίες όταν ίσως ο ίδιος έχει αποσυρθεί από την πολιτική. Από την άλλη, ο αναλυτής προτρέπει την πολιτεία να προετοιμάζεται πάντα για το μέλλον ακόμα και αν αυτό φαίνεται να αργεί, άλλωστε, ένας στρατηγικός σχεδιασμός δεν περιορίζεται στο παρόν ή στο κοντινό αύριο -για περισσότερα βλέπε Muller D., “Improving Futures Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 3, 2009, σ. 389-390

⁴⁷ Hughes G., “Intelligence in the Cold War” στο *Intelligence and National Security*, Volume 26, Number 6, 2011, σ. 755-758. Υποθέτουμε ότι ο Hughes αναφέρεται στην ανάγκη διατήρησης ή μη της παλιάς δομής

⁴⁸ Keegan J., *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, Hutchinson, London, 2003, σ. 383-384

«θεατρinίστικων ενεργειών» εκ μέρους της αμερικανικής πληροφοριακής κοινότητας προκειμένου να συνεχιστεί μια πετυχημένη παραγωγή μύθων γύρω από τις δυνατότητες και το όνομά της.⁴⁹ Περαιτέρω, πάμπολλες φορές έχει συζητηθεί το ζήτημα του ύψους των προϋπολογισμών των κυριοτέρων πληροφοριακών δομών σε συνδυασμό με το αρνητικό εικαζομένων ή μη αποτυχιών.⁵⁰ Από την άλλη μεριά μια περιήγηση στον γραπτό και ηλεκτρονικό τύπο καταδεικνύει, αμέσως και εμμέσως, το μέγεθος της εμπλοκής των Υπηρεσιών σε ζητήματα εθνικής, πολιτικής, στρατιωτικής, οικονομικής, κοινωνικής κ. λ. ασφαλείας αν και τα σκάνδαλα ποτέ δεν λείπουν.

Κατά τα ανωτέρω υποθέτουμε ότι το ερώτημα μιας μεταρρύθμισης των πληροφοριακών οργανισμών έχει λυθεί με τη συζήτηση να περιστρέφεται γύρω από τον εξελικτικό ή επαναστατικό χαρακτήρα της. Το ερώτημα περί του υπερτιμημένου ή όχι του ρόλου των Υπηρεσιών σε περιπτώσεις συρράξεων ή μη, δεν μπορεί να απαντηθεί κάθετα. Αυτό ουδόλως οφείλει να εκληφθεί ως μομφή καθώς στην κατάληξη / αποτέλεσμα ενός σχετικού συμβάντος εμπλέκεται μια σειρά μετρήσιμων και μη παραγόντων από την ισχύ μέχρι την παρέμβαση της τύχης. Όσον αφορά σε θέματα προϋπολογισμών, υπηρεσιακής προπαγάνδας, δομικής / κρατικής προσαρμογής, ηθικών προαπαιτούμενων κ. λ. συνίσταται μια έρευνα της οποίας το πόρισμα δεν μπορεί να μην περάσει και μέσα από το φίλτρο των εθνικών αναγκαιοτήτων.

Έτσι καθώς: α) οι μορφές πολέμου αλλάζουν (βλέπε Συρία / Ιράκ 2011-), β) οι εξελίξεις απαιτούν κατά περίπτωση λιγότερο φανερές ή ξεκάθαρες δράσεις (βλέπε Ουκρανία 2014-), γ) οι αφορμές πιθανών αναφλέξεων παραμένουν (παλαιστινιακό, τριβές μεταξύ Ισραήλ και Ιράν, τριβές μεταξύ Β. Κορέας και Δύσεως κ. λ.), δ) νέες προτεραιότητες κάνουν την εμφάνισή τους στον ορίζοντα (ενδεχόμενη απόσυρση του αμερικανικού παράγοντα από την Ευρώπη και τη Μ. Ανατολή προς όφελος σχεδιασμών στην περιοχή του Ειρηνικού, ενδεχόμενη κίνηση των μεγάλων δυνάμεων προς τον Αρκτικό Κύκλο), ε) ισχυροποιούνται, τουλάχιστον κατά τα φαινόμενα ή κατά τις αναλύσεις ειδικών, χώρες όπως η Ρωσία, η Κίνα, η Ινδία, στ) ενισχύονται ρεύματα και φαινόμενα των οποίων οι κοινωνικές συνέπειες προβληματίζουν (ισλαμικός φονταμενταλισμός, ανεξέλεγκτη μετατόπιση μαζών, οργανωμένο έγκλημα), ζ) πολλαπλασιάζονται οι αφανείς προκλήσεις (περιβαλλοντική επιβάρυνση, υπερπληθυσμός, υγειονομικές απειλές, κυβερνοκίνδυνοι κ. λ.), τότε, η επιμονή στην ανάγκη όχι μόνο διατήρησης των Υπηρεσιών αλλά συνεχούς λειτουργικής / επιχειρησιακής αναβάθμισής τους καθίσταται εύλογη.⁵¹

⁴⁹ Gill P., Phythian M., *Intelligence in an Insecure World*, Polity Press, London, 2006, σ. 16

⁵⁰ Kupcikas Karolis, "The Importance of Intelligence to International Security", 8 Νοεμβρίου 2013, στη σελίδα <http://www.e-ir.info/2013/11/08/importance-of-intelligence-to-international-security/> όπου ανατρέξαμε την 20^η Απριλίου 2016

⁵¹ Ο Wesley Wark διερωτάται: Πρέπει οι νέες απειλές να επιβαρύνουν τη λειτουργία των Υπηρεσιών; Ο ίδιος απαντά καταφατικά λέγοντας ότι οι τελευταίες ιστορικά καλούνται να καλύψουν τα όποια κενά πληροφόρησης (*information vacuum*) δικαιολογώντας / επιβεβαιώνοντας την παρουσία τους στην κρατική δομή. Από κει και έπειτα οι Υπηρεσίες αποτελούν οιονεί δεξαμενές σκέψης εξοπλισμένες με τεχνολογία αιχμής και εξειδικευμένο προσωπικό -πρόκειται για ατού που δεν συναντάμε εύκολα εντός άλλων οργανισμών. Η μόνη ίσως εγγενής τροχοπέδη στην αποστολή τους είναι η μυστικότητα που δεν επιτρέπει σύνθετες συνεργατικές κινήσεις· ο Wark πιστεύει ότι ακριβώς αυτή η μυστικότητα αργά ή γρήγορα θα θυσιαστεί στο βωμό της επιτυχούς εκπλήρωσης των νέων αποστολών τη στιγμή, μάλιστα, που μελετητές όπως ο John Gearson την εγκαλούν για παρεμπόδιση του «κοινού» έργου κατά της τρομοκρατίας -για περισσότερα βλέπε Wark Wesley, "The Intelligence Revolution and the Future" στο *Studies in Intelligence*, Volume 37, Number 4, 1993, σ. 9-16, Gearson John, "Deterring Conventional Terrorism: From Punishment to Denial and Resilience" στο *Contemporary Security Policy*, Volume 33, Issue 1, 2012, σ. 192

ΠΡΟΣΘΗΚΗ

Πόλεμος και πληροφόρηση στον 21^ο αιώνα. RMA και RIA

11.1.Π Οι θιασώτες του φαινομένου

Ο ιστορικός Martin Van Creveld στο *The Transformation of War. The Most Radical Reinterpretation of Armed Conflict since Clausewitz* (1991) υποστηρίζει ότι το μέλλον του πολέμου θα εξαρτηθεί από την ταχύτητα, την ευελιξία και την προσαρμοστικότητα των μαχομένων. Συνάδελφοί του υποθέτουν πως η ανάπτυξη της τεχνολογίας της πληροφόρησης και των επικοινωνιών πιθανόν οδηγήσει στην εξαφάνιση της κατά πρόσωπο μάχης σε αντίθεση με την όλο και συχνότερα εμφανιζόμενη της απόκρυψης / ενέδρευσης (hide-and-seek battle). Κατά τους Alberts, John Garstka και Frederick Stein η πληροφοριακή επανάσταση επηρεάζει το πολεμικό γίνεσθαι ως εξής: α) ο όρος «battlefield» (πεδίο μάχης) αντικαθίσταται από τον όρο «battlespace» (περιβάλλον μάχης) υπό την έποψη μιας ευρύτερης χωρικής αντίληψης εντός της οποίας βρίσκει θέση όχι μόνο ο φυσικός χώρος των δράσεων αλλά και το άυλο «πληροφοριακό φάσμα» που τροφοδοτεί τις εξελίξεις, β) το μη μάχιμο προσωπικό (π. χ. απλοί πολίτες / κάτοικοι φλεγόμενων περιοχών) διαδραματίζει έναν όλο αυξανόμενο ρόλο στην διεξαγωγή των επιχειρήσεων⁵², γ) το πλεονέκτημα της παρατεταμένης απομόνωσης χάνεται. Ακόμα και ο κοινός τηλεοπτικός δέκτης διαθέτει δύναμη παρουσίασης / έκθεσης γεγονότων, διαδικασιών, κινήσεων κ. λ.⁵³

Ο Πόλεμος του Κόλπου (2003) κατέδειξε ότι ο έχων την ικανότητα απεικόνισης και παρακολούθησης του περιβάλλοντος μάχης κρατά ένα από τα κλειδιά της νίκης. Η συζήτηση γύρω από την επανάσταση στις στρατιωτικές υποθέσεις σχετίζεται με μια αντίστοιχη περί των εξελίξεων στην πληροφόρηση.⁵⁴ Στην πραγματικότητα στόχος είναι η διασφάλιση του πληροφοριακού φάσματος ή, αλλιώς, η αποτροπή του κενού πληροφόρησης.⁵⁵ Μέσω αυτού (του πληροφοριακού φάσματος) επιτυγχάνεται η εκτέλεση πλάνων που μόνο επί τη βάσει μιας συνεχούς ροής δεδομένων εκπονούνται / εκτελούνται. Αυτή η συνακόλουθη πληροφοριακή ανωτερότητα (information

⁵² Άλλωστε κατά τον τχη George Hull *...the boundaries between military and political action are blurring* -για μια άποψη βλέπε Hull George, *The Information Revolution and the Environment of Future Conflict*, μονογραφία κατατεθειμένη στο School of Advanced Military Studies / United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1997, σ. 40

⁵³ Dunn M., *Information Age Conflict. A Study of the Information Revolution and a Changing Operating Environment*, ό. π., σ. 88-89

⁵⁴ Ο Jeffrey Cooper τονίζει ότι η έκρηξη της πληροφόρησης καθιστά αναπόφευκτη τη δημιουργία ενός νέου περιβάλλοντος δράσης εντός του οποίου μπορεί να φιλοξενηθεί ένα υψηλό τέμπο παράλληλων (αλλά αδιαχώριστων -seamless) στρατιωτικών επιχειρησιακών δογμάτων και εγχειρημάτων. Κατά τον ίδιο η πληροφοριακή επανάσταση χαρακτηρίζει και χαρακτηρίζεται από δύο γεγονότα / δυνατότητες: πρώτον, της «γνωσιακής ανάβασης» που μέσω του πρωτογενούς δεδομένου καταλήγει στη γνώση και, δεύτερον, της «ευχέρειας της άμεσης απόφασης σε πραγματικό χρόνο» από επιμέρους μονάδες υπό τη σχεδόν απόλυτη βεβαιότητα μιας ανταλλαγής μηνυμάτων που φτάνουν ως έχουν στον παραλήπτη σε μηδέν χρόνο -για μια ευρύτερη εικόνα βλέπε Cooper J., "Another View of the Revolution in Military Affairs" στο *Conference Proceedings of the Fifth Annual Conference on Strategy*, Strategic Studies Institute, U.S. Army War College, HPIA, 1994

⁵⁵ Ομιλούμε για το λεγόμενο information gap / info-gap. Πρόκειται για τη διαφορά μεταξύ αυτού που, γενικά, κάποιος γνωρίζει και αυτού που ακριβώς χρειάζεται να γνωρίζει, ειδικότερα, προκειμένου να φτάσει στην ορθή απόφαση -περί τούτου βλέπε Ben-Haim, Yakov, "Policy Neutrality and Uncertainty: An Info-Gap Perspective" στο *Intelligence and National Security*, Volume 31, Number 7, 2016, σ. 982-983

superiority)⁵⁶ επιφέρει μια πολύπλευρη επίγνωση επί των καταστάσεων. Πρόκειται για ατού / θεμέλιο πάνω στο οποίο δομείται το σύνολο της «στρατηγικής εφαρμογής στρατιωτικής ισχύος». Οι US Joint Vision 2010 και 2020 ορίζουν μια τέτοια ως σύμπλοκο τεσσάρων στοιχείων, ήτοι:

- Της *κυριαρχίας ελιγμών* (*dominant maneuver*) υπό την ανάγκη επίτευξης διακλαδικής ανάπτυξης μονάδων με τάχιστο ρυθμό στον κατάλληλο χώρο όπως και μεταπήδησης από ένα εύφλεκτο σημείο σε άλλο, πιθανότατα, απομακρυσμένο.⁵⁷
- Του *εντοπισμού και της ακρίβειας εκτέλεσης* (*precision engagement*). Σε πρώτο χρόνο συλλαμβάνουμε, επιτηρούμε, στοχοποιούμε. Σε δεύτερο βάλλουμε, εκτιμούμε, προετοιμάζουμε την επόμενη δράση. Η χρονική αμεσότητα και το καταγιστικό επιχειρησιακό τέμπο συμβάλουν αποφασιστικά στην επιτυχία του εγχειρήματος.⁵⁸
- Της *πλήρους προστασίας των οικείων πόρων* (*full dimensional protection*). Αναφερόμαστε στην ικανότητα διασφάλισης του προσωπικού και των υλικών που διατίθενται προς εκτέλεση μιας αποστολής. Μια πλήρης και ολική προστασία επιτυγχάνεται μέσω ενεργοποίησης πολυεπίπεδων αμυντικών και επιθετικών μέτρων σε αέρα, θάλασσα και ξηρά παγιώνοντας τη δυνατότητα λήψεως πρωτοβουλιών.⁵⁹
- Της *επιμελητείας* (*focused logistics*). Η Joint Vision 2010 υποστηρίζει ότι προς ικανοποίηση των τριών άνω επισημάνσεων αναζητείται μια εκλεκτική μείζη

⁵⁶ Κατά τη *US Joint Vision 2020* η έννοια της πληροφοριακής ανωτερότητας σημασιοδοτεί τον πυρήνα γύρω από τον οποίο περιστρέφεται κάθε νέα στρατιωτική δράση. Κατά την εξέλιξη της παγκόσμιας ιστορίας οι πολιτικοστρατιωτικοί ηγέτες ελάβαιναν κατά περίπτωση την πληροφόρηση ως πολλαπλασιαστική ισχύος και μέσο νίκης. Η πληροφοριακή επανάσταση επιφέρει ποσοτικές και ποιοτικές διαφοροποιήσεις στο πληροφοριακό περιβάλλον που μέχρι το τέλος της τρέχουσας δεκαετίας αναμένεται να επηρεάσουν βαθύτερα το πρόσωπο του πολέμου και της διεξαγωγής των μαχών (για μια περαιτέρω άποψη ανέτρεξε στο *Information Attack: Information Warfare in 2025* του καθηγητού George Stein, διαθέσιμο στην ηλεκτρονική διεύθυνση <http://www.au.af.mil/au/awc/csat/2025/volume3/vol3ch03.pdf> στην οποία προσφύγαμε τη 12^η Οκτωβρίου 2014). Με λίγα λόγια πληροφοριακή ανωτερότητα σημαίνει ικανότητα συλλογής, ανάλυσης και διασποράς πληροφοριών υπό την προϋπόθεση μιας συνεχούς πρόσληψης δεδομένων τη στιγμή που αρνούμαστε στον αντίπαλο αυτήν ακριβώς τη δυνατότητα (JP1-02 *Department of Defense Dictionary of Military and Associated Terms*, 2010, επίσης βλέπε στην ιστοσελίδα <http://acqnotes.com/acqnote/careerfields/information-superiority> όπου καταφύγαμε την 27^η Σεπτεμβρίου 2015). Η έννοια του *πληροφοριακού περιβάλλοντος* (*information environment*) σχετίζεται με το άθροισμα των ανθρωπίνων και τεχνητών πόρων όπως και των οργανισμών που επιχειρούν σε πρώτο χρόνο να φτάσουν στην πληροφοριακή ανωτερότητα και σε δεύτερο να τη διαχειριστούν (JP1-02, 2010). Τονίζουμε ότι η πληροφοριακή ανωτερότητα δεν μπορεί να αποτελέσει ατού αν δεν μεταλλαχθεί σε «ανωτερότητα γνώσης και αποφάσεων» -η πληρέστερη γνώση θα οδηγήσει στην επαρκέστερη απόφαση. Βέβαια το όποιο *decision superiority* επουδενί παράγεται αυτομάτως από τη νίκη στη μάχη των πληροφοριών για να μην αναφερθούμε, συμπληρώνουμε, στο προαπαιτούμενο ενός ικανού επιτελείου παραγωγής αποφάσεων -για μια συνοπτική εικόνα βλέπε *US Joint Vision 2020*, σ. 8-10. Ακριβώς σ' αυτό το σημείο έρχεται η JP 3-13 του 2012 κατά την οποία το πληροφοριακό περιβάλλον δεικνύει άθροισμα τριών αλληλεπιδρουντών διαστάσεων -πρόκειται για τη *φυσική / υλική* (*physical*), την *πληροφοριακή* (*informational*) και τη *γνωστική / νοητική* (*cognitive*). Αν η πρώτη σχετίζεται με συστήματα διοίκησης και ελέγχου (C2), υπηρεσιακούς παράγοντες και γραφειοκρατικές υποδομές, η δεύτερη με την πληροφόρηση ως στοιχείο που πρέπει να συλλεχθεί, να αξιολογηθεί / αξιοποιηθεί και να προστατευθεί, είναι η τρίτη που ...*encompass the minds of those who transmit, receive, and respond to or act on information* -για περισσότερα, JP 3-13 (2012), σ. vii-viii

⁵⁷ *US Joint Vision 2010*, Joint Chiefs of Staff, σ. 20-21 και *US Joint Vision 2020*, Joint Chiefs of Staff, σ. 20-21

⁵⁸ *US Joint Vision 2010*, σ. 21-22 και *US Joint Vision 2020*, σ. 22-23

⁵⁹ *US Joint Vision 2010*, σ. 22-23 και *US Joint Vision 2020*, σ. 26-27

στοιχείων όπως αυτό της πληροφόρησης, της διοικητικής μέριμνας, των τεχνολογιών της επικοινωνίας κ. λ. Η ολοκλήρωση / επιτυχία αυτής της μείξης οδηγεί στην άμεση ανταπόκριση σε περιόδους κρίσεων, στον επανασχεδιασμό πλάνων ακόμα και καθ' οδόν πολέμου, στην επικουρία κινήσεων σε στρατηγικό, επιχειρησιακό και τακτικό επίπεδο. Το ζητούμενο της προσπάθειας έχει να κάνει με διανομή πόρων που οι διασπειρόμενες στρατιωτικές δυνάμεις θα απαιτήσουν προς επίτευξη επιπλέον κινητικότητας, ευελιξίας, προβολής ισχύος. Διά της Joint Vision 2020 αποδίδεται ένας συνεκτικός ορισμός κατά τον οποίο *...focused logistics σημαίνει ικανότητα τροφοδοσίας των δυνάμεων όλων των εμπλεκόμενων κλάδων στον επίμαχο χώρο, στον κατάλληλο χρόνο, καθ' όλη τη διάρκεια των κάθε είδους επιχειρήσεων*.⁶⁰

Εδώ οφείλουμε να σταθούμε σε δυο σημεία. Πρώτον, στην αναφορά, έστω εμμέσως, της ανάπτυξης ενός νέου τρόπου μάχης κατά τον οποίο το πολυκλαδικό στράτευμα συσπειρώνεται και αποσυσπειρώνεται εν είδει βεντάλιας -το γεγονός καθ' αυτό δεν σημαίνει κάτι πρωτοφανές, η (πρακτική) διαφορά έγκειται στην ταχύτητα και αποτελεσματικότητα με την οποία το ένα κτύπημα διαδέχεται το άλλο. Δεύτερον, στη σημασία του λεγόμενου *web-based information system* το οποίο σε συνθήκες real time και en route εφοδιάζει με δεδομένα τα επιτελεία και τις επιχειρησιακές ομάδες προς διασφάλιση ακριβώς αυτής της ταχύτητας / αποτελεσματικότητας, του πληροφοριακού φάσματος και της συνεπαγόμενης πληροφοριακής ανωτερότητας, των συστατικών, δηλαδή, που συντείνουν στην πολεμική επιτυχία.⁶¹

Μια μελετημένη «στρατηγική εφαρμογή στρατιωτικής ισχύος» καθιστά έναν δρώντα ικανό λήψεως πρωτοβουλιών στα πεδία των μαχών. Όπως επισημάναμε στηρίζεται (και) στην πληροφοριακή επικράτηση της οποίας ο ρόλος, ασφαλώς, δεν εξαντλείται εντός του πλαισίου των πολεμικών συρράξεων αλλά αγγίζει το σύνολο των στρατιωτικών κινήσεων (full range military operations -FRMO, military operations other than war -MOOTW) σε περιόδους ειρήνης και μη. Κατ' αυτόν τον τρόπο η, ως προαπαιτούμενο συγκρουσιακής κατίσχυσης, (υπερ)επάρκεια πληροφοριών μεταμορφώνεται σε εργαλείο ευρύτερης πολιτικής κυριαρχίας (υπό την έννοια μιας «full spectrum dominance») ανταποκρινόμενο σε εγχειρήματα που αφορούν (και) σε δράσεις ανθρωπιστικής βοήθειας, peace building, peacekeeping, peace enforcement, στην αντιτρομοκρατία, στην καταδίωξη του οργανωμένου εγκλήματος, στο πόλεμο κατά των παράνομων ουσιών, κατά του λαθρεμπορίου, κατά του trafficking κ. λ.⁶²

⁶⁰ US Joint Vision 2010, σ. 24-25 και US Joint Vision 2020, σ. 24-25

⁶¹ Ο Thomas Mahnken χρησιμοποιεί τον όρο *System of Systems* (εισηγμένο από τον ναύαρχο William Owens στο “The Emerging System of Systems” στο *Military Review*, Volume 75, Number 3, 1995, σ. 15-19) προκειμένου να αναφερθεί σε ένα πληροφοριακό υπερσύστημα που συνδέει όλα τα οικεία μέρη που ενέχονται στη μάχη. Ο Steven Metz ακολουθεί συμφωνώντας τη στιγμή που ο Martin Libicki εισάγει τον όρο *Global Grid* ή, απλά, *Grid* -για περισσότερα στοιχεία βλέπε Mahnken T., “War in the Information Age” στο *Joint Force Quarterly*, τεύχος 10, 1995, σ. 39-43, Metz S., “Lessons from the Military Experience: The US Military and the IR: The Pitfalls of Uneven Adaptation” στο *The Information Revolution and National Security*, επιμ. Copeland Thomas, Strategic Studies Institute, ΗΠΑ, 2000, σ. 56-61, Libicki M., *Illuminating Tomorrow's War*, Institute for National Strategic Studies, National Defense University, ΗΠΑ, 1999, σ. viii και Richter Andrew, “Lessons From the Revolution: What Recent US Military Operations Reveal About the Revolution in Military Affairs and Future Combat” στο *Journal of Military and Strategic Studies*, Volume 7, Issue 3, 2004

⁶² US Joint Vision 2010, σ. 25-27. Πρακτικά, κατά τον στρατηγό Peter J. Schoomaker *...full spectrum dominance* σημαίνει ικανότητα αντίληψης, κατανόησης, απόφασης και δράσης προλαμβάνοντας σε κάθε περίπτωση την όποια ανταγωνιστική ενέργεια -για περισσότερα βλέπε Schoomaker P., *The Way Ahead: Our Army at War ... Relevant and Ready. Moving from the Current Force to the Future Force ...Now!*, Army Strategic Communications, USA, November 2003, σ. 5-6



Εικόνα 34: Full Spectrum Dominance γράφημα όπως απεικονίζεται στον ιστότοπο <http://www.acqnotes.com/acqnote/careerfields/global-information-grid-gig> όπου καταφύγαμε την 27^η Σεπτέμβρη 2015

Τέλος, κατά τους Arquilla και Ronfeldt στην εποχή του πολέμου για την πληροφόρηση αλλά και στον πόλεμο της πληροφοριακής εποχής (*information-age conflict -IAC*) πρέπει να επανεξεταστούν τέσσερις τομείς, ειδικότερα:

- Της *εννοιολογικής θεμελίωσης (conceptual foundation)* της πληροφορίας. Η έννοια «πληροφορία» απαιτεί βαθύτερη ανάγνωση ως προς την αποκωδικοποίησή της. Δεν πρόκειται απλά για κάτι που παράγεται μέσω μιας διαδικασίας (*information processing*) μετουσιώνοντας την πρώτη ύλη σε πληροφόρηση. Πρόκειται για συστατικό (*structural information*) που συνέχει την ίδια τη δομή των οργανισμών που ασχολούνται μ' αυτήν ήτοι, τον απώτερο προορισμό τους υπό το καθήκον της ανάβασης από το δεδομένο στη γνώση και, καταληκτικά, στη σοφία.
- Των *οργανισμών* καθαντών. Η παρουσία των *networks* οδηγεί σε μια υβριδική μορφή λειτουργίας, σε μια «μείξη» παραδοσιακών ηγεσιών / ιεραρχιών και αποκεντρωμένων μονάδων όσον αφορά, κυρίως, σε επιχειρησιακά ζητήματα.
- Του *δόγματος μάχης*. Ένα σύγχρονο δόγμα οφείλει να 'προβλέπει' περί μιας γκάμας καταστάσεων χαμηλής ή υψηλής έντασης / δράσης απευθυνόμενο στο σύνολο των οργανισμών, Υπηρεσιών, μονάδων κ. λ. Φαίνεται ότι μια συμπεριφορά τύπου *swarming* εξαργυρώνει τα πλεονεκτήματα που η πληροφοριακή τεχνολογία προσφέρει υπό την έννοια μιας άμεσης σύμπληξης απομακρυσμένων μεταξύ τους δυνάμεων στο επίμαχο σημείο.
- Της *συνολικής στρατηγικής*, δηλαδή, της στρατηγικής τόσο σε περιόδους ειρήνης όσο και συγκρούσεων. Πρόκειται για εγχείρημα του οποίου η πολλαπλότητα, πολυπλοκότητα και επιτυχία βασίζεται στη διασπορά πληροφόρησης στους κατάλληλους πολιτικούς και στρατιωτικούς δέκτες. Αυτή δεν επιτρέπεται να αγνοήσει τους θεμελιώδεις κανόνες ασφαλείας μετατρεπόμενη σε λεία επίδοξων θηρευτών που, ενδεχομένως, ελλοχεύουν. Η προσοχή με την οποία πρέπει να αντιμετωπιστεί / εκτελεστεί ο όλος σχεδιασμός εισάγοντας την έννοια *guarded openness* υποδηλώνει τον χαρακτήρα του.⁶³

⁶³ Arquilla J., Ronfeldt D., "Looking Ahead: Preparing for Information-Age Conflict" στο *In Athena's Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997, σ. 439-493. Συνδυαστικά, περί δόγματος μάχης και πληροφόρησης, βλέπε Wirtz James, Rosenwasser John, "From Combined Arms to Combined Intelligence: Philosophy, Doctrine and Operations" στο *Intelligence and National Security*, Volume 25, Number 6, 2010, σ. 725-743

11.2.Π Οι σκεπτικιστές

Ο Steven Metz τονίζει ότι η πολεμική νίκη δεν μπορεί να βασιστεί αποκλειστικά στην πληροφόρηση και στις εφαρμογές της· πολύ απλά η υφιστάμενη τεχνολογία δεν υποστηρίζει κάτι τέτοιο. Επιπλέον, ακόμα και αν μια σχετική εκπορευόμενη εκ των Υπηρεσιών επίθεση καταστρέψει βασικές υποδομές του αντιπάλου (τραπεζικό σύστημα, επικοινωνίες, τηλεπικοινωνίες, παροχή ενέργειας κ. λ.) τίποτα δεν αποκλείει τη μη κάμψη της θέλησης και του ηθικού του, πάρα ταύτα, η διενέργεια ενός τέτοιου εγχειρήματος φαντάζει λιγότερο επικίνδυνη από μια κλασική προσβολή. Είναι φανερό ότι ο Metz συνδέει τον πληροφοριακό πόλεμο με τον *πόλεμο υποδομών* (*infrastructure warfare*), άλλωστε, εντός αυτών (των υποδομών) εντάσσει και τη στρατιωτική διάρθρωση. Ένας τέτοιος σχεδιασμός αποκλειστικά προσηλωμένος στην καταστροφή της τελευταίας αποσκοπεί σε δύο σημεία, ήτοι: α) στο μπλοκάρισμα κατά το δυνατό της κινητοποίησης / ανάπτυξης των εχθρικών δυνάμεων ή / και β) στον πειθαναγκασμό μέσω κτυπημάτων και μάλιστα επί του κέντρου βάρους του αντιπάλου -στην ουσία επανερχόμαστε στον πόλεμο υποδομών μέσω, ωστόσο, βίας (βλέπε, π. χ., περίπτωση Σερβίας εν έτει 1999).⁶⁴

Ο στρατηγός Robert Scales υπογράφει τα εξής: α) η πληροφοριακή επανάσταση, αν πράγματι υφίσταται, ισχύει για όλους τους δρώντες, β) οι αυξανόμενες πληροφοριακές ροές δεν είναι βέβαιο ότι δεικνύουν πλεονέκτημα για τα στρατιωτικά επιτελεία, το στρατιωτικό προσωπικό και τις Υπηρεσίες καθώς η διαχείρισή τους αποτελεί, συχνά, πρόβλημα, γ) η πληροφόρηση και η πέριξ αυτής τεχνολογία δεν βοηθά απαραιτήτως τη διαδικασία λήψεως αποφάσεων, αντιθέτως, ίσως την κάνει «βαρύτερη». Ο ίδιος υπογραμμίζει ότι η τεχνολογία αφ' εαυτής ποτέ δεν θα λύσει το πρόβλημα της σύγχυσης, της αμφιβολίας, του φόβου, της τριβής και της ομίχλης της μάχης, η, δε, πληροφόρηση δεν ισούται απαραίτητα με γνώση / σοφία γύρω από τον αντίπαλο, άλλωστε, κατά τον Κλαούζεβιτς «War ...is not the action of a living force upon a lifeless mass...but always the collision of two living [thinking] forces».⁶⁵

Οι Papp και Alberts αν και δέχονται την άποψη μιας πιο 'σοφής', λόγω πληροφόρησης, διαδικασίας λήψεως αποφάσεων δεν διστάζουν να γράψουν ότι το συγκεκριμένο asset ενδέχεται να δημιουργήσει μια κατάσταση πλασματικής βεβαιότητας που με τη σειρά της ίσως οδηγήσει σε μια γρήγορη (βιαστική) απόφαση, κάτι όχι συνετό. Άλλο που συζητείται είναι το κατά πόσο ένας (αυξημένος) όγκος πληροφοριών δικαιολογεί απολύτως την ύπαρξη / υποστήριξη ενός αυτοματοποιημένου συστήματος λήψεως αποφάσεων. Αν υπάρχουν περιπτώσεις επιδεκτικές για κάτι τέτοιο, ποιες είναι αυτές; Πότε ο ανθρώπινος παράγοντας δεν αντικαθίσταται; Η ερώτηση δεν απαντάται εύκολα.⁶⁶ Ένα τρίτο σημείο σχετίζεται με τη γνώση της ύπαρξης επίσης δικτύου πληροφοριών στην υπηρεσία του ανταγωνιστή,

⁶⁴ Metz St., *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*, Strategic Studies Institute, USA, 2000, σ. 59-61

⁶⁵ von Clausewitz, Carl, *On War*, Princeton University Press, USA, 1975, σ. 77. Οι Paul van Riper και E. G. Hoffman τονίζουν ότι ...[ο πόλεμος] δομεί ένα υψηλής έντασης διαδραστικό σύστημα χαρακτηριστικό του οποίου είναι η τριβή, η έλλειψη προγνωσιμότητας, η αταξία, η μεταβλητότητα και όχι η πεμπτοσύνη μιας μηχανικής ακριβείας δράσεων -για μια καλύτερη εικόνα βλέπε van Riper, P., Hoffman E., "Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare" στο *National Security Studies Quarterly*, Volume 4, Number 3, 1998, σ. 5

⁶⁶ Σε επιχειρησιακό στρατιωτικό επίπεδο το αντιαεροπορικό σύστημα Patriot δεικνύει ένα τέτοιο εάν και εφόσον αποφασιστεί η ενεργοποίηση της αυτοματοποιημένης εμπλοκής. Σε μια τέτοια περίπτωση το όπλο κλειδώνει / βάλλει κατά του εναερίου στόχου, υπό την προϋπόθεση ότι ο τελευταίος δεν αναγνωρίζεται ως φίλιος, χωρίς παρέμβαση ανθρώπινου παράγοντα. Πάρα ταύτα βολές κατά οικείων στόχων δεν έχουν αποφευχθεί για τον άλφα ή βήτα λόγο

άρα, οφείλουμε να τον «προλάβουμε», το όλο παίγνιο δύναται να οδηγήσει σε δίνη, σε ένα spiral μη ορθών αποφάσεων.⁶⁷

Ο Ανδρέας Λιαρόπουλος τονίζει ότι πόλεμος στην εποχή της πληροφόρησης δεν σημαίνει παρά χαοτική κατάσταση κατά την οποία: α) νέες μορφές και τρόποι σύγκρουσης εμφανίζονται, β) οι ευκαιρίες κατίσχυσης μέσω των Information Technology εφαρμογών ακολουθούνται από ανάλογες τρωτότητες, γ) η ανάγκη αλλαγής των πολιτικών και στρατιωτικών δογμάτων καθίσταται αναντίρρητη, δ) ερωτήματα περί των καταλληλότερων σχημάτων της «νέας» δράσης επιζητούν απαντήσεις στα επιτελεία πολιτικών, ακαδημαϊκών και επιχειρησιακών κύκλων.

Εντούτοις, ο ίδιος διερωτάται, εάν η όλη συζήτηση συσκοτίζει τη φύση και έννοια του πολεμικού φαινομένου. Διερωτάται μήπως οι προσδοκίες περί χειρουργικών κτυπημάτων, αναίμακτων επιχειρήσεων, μη παράπλευρων απωλειών κ. λ. καθίστανται υπερβολικές αποκρύπτοντας τα αληθινά ρίσκα και κόστη της χρήσης των όπλων. Περαιτέρω, αν ο πόλεμος έχει αλλάξει σε σχέση με πρότερες δεκαετίες, κατά πόσο έχει επηρεαστεί η βαθιά του ουσία / οντολογία, η λογική της αταξίας και η έμφυτη μη γραμμική (non-linear) φύση του;⁶⁸

Revolution in Military Affairs (RMA) / Revolution in Information-Intelligence Affairs (RIA).
Τρεις προσεγγίσεις

Στην πράξη τρία γκρουπ μελετητών ερίζουν γύρω από τη σημαντικότητα των Revolution in Military Affairs και Revolution in Information-Intelligence Affairs φαινομένων. Το πρώτο υποστηρίζει ότι η ανάπτυξη της πληροφοριακής τεχνολογίας συνδεόμενη άμεσα με τις πολεμικές δράσεις οδηγεί σε μια άφευκτη μεταμόρφωση της έννοιας «πόλεμος». Τα πλεονεκτήματα του C4ISR συστήματος και αυτά των standoff όπλων δομούν ένα νέο παράδειγμα στο πεδίο των ενόπλων συρράξεων. Υπόβαθρο της αλλαγής, ασφαλώς, η πληροφόρηση της οποίας η παρουσία δεικνύει πολλαπλασιαστική ισχύος στα χέρια των decisionmakers επιδρώντας στην πολιτικοστρατιωτική στρατηγική, στη δομή των στρατευμάτων, στην τακτική απεικόνιση και στον χαρακτήρα των μαχών και του πολέμου. Η κατίσχυση στο network centric warfare -NCW φέροντας εντός ενιαίου κάδρου απομακρυσμένες διοικήσεις και μονάδες, συνεισφέροντας στην κατάκτηση της συνολικής εικόνας, άρα της γνώσης του χώρου της σύγκρουσης, διαλύει την ομίχλη του πολέμου εφοδιάζοντας τους μαχητές με την περιώνυμη 'επίγνωση περιβάλλοντος μάχης'.

Η δεύτερη ομάδα διατηρώντας μια πιο μετρημένη στάση ακολουθεί έναν κατά κάποιο τρόπο «μέσο δρόμο». Η πολυπλοκότητα του πολέμου, η ανθρώπινη ψυχοσύνθεση και θέληση, η τριβή και αβεβαιότητα της μάχης εξακολουθούν να συντηρούν την αδιαφάνεια της εικόνας. Οπωσδήποτε η πληροφόρηση και η περίξ αυτής τεχνολογίες αποτελούν assets των οποίων, ωστόσο, η παραδεκτή σημαντικότητα δεν αποθεώνεται.

Κατά την τρίτη διάσταση / άποψη δεν πρέπει να επικεντρωθούμε τόσο στη μελέτη της επανάστασης στο χώρο του πολέμου όσο στη σπουδή γύρω από τη στάση του ανθρώπου έναντι του πολεμικού γεγονότος και τη διάθεση αναγνώσεώς του. Σύμφωνα μ' αυτήν την προσέγγιση ο στρατιώτης στη δυτική αντίληψη παύει να εντοπίζεται εντός των αναλωσίμων υλικών. Η τεχνολογία, εφελτήριο ενός εκηβόλου αγώνα, συνδράμει στον περιορισμό των απωλειών και των παράπλευρων καταστροφών. Οι καλούμενοι risk-transfer πόλεμοι στη

⁶⁷ Scales R., *Future Warfare Anthology*, US Army War College, Pennsylvania, 2000, σ. 59, 71 και Papp Daniel, Alberts David, "The Future of Defence Policy: Information Age Trends" στο *Information Age Anthology: The Information Age Military*, επιμ. Alberts D., Papp D., CCRP Publication Series, 2001, σ. 855-857

⁶⁸ Liaropoulos Andrew, "The transformation of warfare in the information age" στο *Themata. Policy and Defence*, τεύχος 28, Απρίλιος 2009

Γιουγκοσλαβία, Αφγανιστάν, Ιράκ απομειώνοντας το όποιο (αξιοσημείωτο) πολιτικό κόστος φαίνεται πως αποτελούν κομμάτι της λύσης αυτής της βασανιστικής ανησυχίας.⁶⁹

Από τη μεριά τους οι Michael O' Hanlon, Colin Gray και Lawrence Freedman, συγκαταλεγόμενοι στους πλέον ένθερμους πολέμιους της RMA ιδέας, βεβαιώνουν ότι η ύπαρξη των πυραυλικών συστημάτων, των δορυφόρων, οι ανεπάρκειες της πληροφοριακής τεχνολογίας, η διασπορά των χημικών και βιολογικών όπλων κ. λ. αποτελούν στοιχείο ανάσχεσης της RMA λογικής. Τέλος, υποστηρίζουν ότι ακόμα και αν μια επανάσταση στη στρατιωτική και πληροφοριακή τεχνολογία λάβει χώρα πάντα υπάρχει το αντίβαρο μιας ασύμμετρης απάντησης της οποίας ο χαρακτήρας ουσιαστικά διαφεύγει των δυτικών προτύπων και προσλαμβάνουσών.⁷⁰

Εν κατακλείδι ο Αντρέας Λιαρόπουλος υπογραμμίζει ότι:

- Το έντονο *informatization* των ενόπλων δυνάμεων δεν οδηγεί αυτομάτως στη νίκη με το πρόβλημα να εντοπίζεται κυρίως σε περιπτώσεις μη συμβατικών συγκρούσεων χαμηλής έντασης.
- Παρά την όποια πληροφοριακή / τεχνολογική ανάπτυξη ο ανθρώπινος παράγοντας παραμένει καίριος.
- Οι εμπειρίες από τον πόλεμο στη Γιουγκοσλαβία και στο Ιράκ καταδεικνύουν ότι η στρατιωτική / στρατηγική λογική δεν έχει διαφοροποιηθεί δραματικά παρά τις όποιες αλλαγές κομίζει η νέα εποχή. Το κλαυζεβιτσιανό μοντέλο του πολέμου της καταστροφής και της αιματοχυσίας δεν αντικαταστάθηκε ή, έστω, δεν αντικαταστάθηκε ικανοποιητικά από ένα ανάλογο *information age / era* πρότυπο που θα επιφέρει την αποδιοργάνωση / παράλυση του εχθρού, θα συνεισφέρει στη μη φονικότητα των συγκρούσεων.⁷¹
- Παράγοντες όπως οι καιρικές συνθήκες, η γεωγραφία, η χρήση οπλισμού φτηνών τεχνικών προδιαγραφών κατά ασύμβατο τρόπο, οι πολιτικές, νομικές και διεθνούς δικαίου προεκτάσεις αποδεικνύουν ότι η τρέχουσα μεταλλαγή του προσώπου του πολέμου αν και επιτυχής σε πολλές εκφάνσεις, υπόκειται σε περιορισμούς. Οφείλει να γίνει κατανοητό πως μια πληροφοριακή / τεχνολογική επανάσταση δεν αρκεί προκειμένου να υπερκεραστούν πολιτικοστρατιωτικά, κοινωνικά, ανθρωπογεωγραφικά και λοιπά κωλύματα.^{72, 73}

⁶⁹ Liaropoulos Andrew, "The transformation of warfare in the information age", ό. π.

⁷⁰ Για περισσότερες λεπτομέρειες και παραδείγματα βλέπε Richter Andrew, "Lessons From the Revolution: What Recent US Military Operations Reveal About the Revolution in Military Affairs and Future Combat", ό. π.

⁷¹ Ο Michael O' Hanlon χρησιμοποιεί τον όρο *anti-Clausewitzian* προκειμένου να χαρακτηρίσει τόσο το υποτιθέμενο νέο μοντέλο πολέμου όσο και τους θιασώτες του -για μια καλύτερη εικόνα βλέπε Richter Andrew, "Lessons From the Revolution: What Recent US Military Operations Reveal About the Revolution in Military Affairs and Future Combat", ό. π.

⁷² Ο Λιαρόπουλος διατηρώντας μια νηφάλια στάση έναντι υποστηρικτών ή αρνητών των RMA, RIA, IO και IW φαινομένων ξεκαθαρίζει ότι αλλαγές πράγματι έχουν συμβεί στα πεδία της αναγνώρισης, κατόπτευσης ή επιτήρησης, ωστόσο, οι τεχνικές παραπλάνησης και η τροχοπέδη της υπερφόρτωσης πληροφοριών παραμένουν εδώ. Αν από τη μία υπάρχουν τα *hi-tech information based networks* υπάρχουν, επίσης, τα *networks based on human activity*. Η πληροφοριακή ανωτερότητα δεν οδηγεί νομοτελειακά σε ένα αποκαθαρμένο, διάφανο, ψηφιακό περιβάλλον μάχης. Οι συγκρούσεις σε ανοικτούς χώρους έχουν παραχωρήσει θέση σ' αυτές των εντός αστικοποιημένων περιοχών έναντι, συνηθέστατα, μη συμβατών αντιπάλων. Ίσως ομιλούμε για εξέλιξη και όχι για επανάσταση στον πόλεμο. Αν πρόκειται για επανάσταση, τότε, το φαινόμενο επιδρά μόνο στο στρατιωτικό / τεχνολογικό επίπεδο ή αφορά, επίσης, στο κοινωνικοπολιτικό; Πώς αυτά τα δύο συμπλέκονται; Κατά πόσο το κλαυζεβιτσιανό παράδειγμα αποσύρεται προς όφελος ενός μεταμοντέρνου υποδείγματος; -περί τούτων βλέπε Liaropoulos Andrew, "The transformation of warfare in the information age", ο. π. Επιπλέον, ο van Creveld σημειώνει πως από τη στιγμή που η λογική / ανάπτυξη της τεχνολογίας ακολουθεί γραμμική πορεία, από τη στιγμή που η πολεμική διαδικασία συγχρωτίζεται με την

Ανατρέχοντας στον Lahneman μνημονεύουμε την προσπάθειά του περί απόδειξης ή μη του RIA φαινομένου μέσα από μια αντίστροφη πορεία. Ο μελετητής δεν εξετάζει πώς αυτό επηρεάζει τις Υπηρεσίες (σε επίπεδο εσωτερικών δομών) και την εθνική ασφάλεια (ναι, εξελίσσεται ένα νέο φαινόμενο και αυτές είναι οι επιπτώσεις του) αλλά ερευνά αν οι εξελίξεις στην πληροφοριακή κοινότητα το δικαιολογούν ή, ίσως, το οδηγούν. Ο Lahneman εφευρίσκει έναν νέο όρο προκειμένου να αναφερθεί στο έργο των Υπηρεσιών, πρόκειται για τον όρο *intelligence enterprise*. Στον ίδιο χρόνο διερωτάται περί του εάν οι δράσεις εντός του *intelligence enterprise*: α) επηρεάζουν την επεξεργασία και χρήση της πληροφορίας / πληροφόρησης, β) αλλάζουν τη δομή των πληροφοριακών οργανισμών, γ) οδηγούν στην άνοδο νέων ελίτ εντός της πληροφοριακής κοινότητας, δ) επιδρούν σε ζητήματα εθνικής ασφαλείας.

Στο πρώτο ερώτημα, και αφού αντιπαραβληθούν είδη απειλών, προτεραιότητες κ. λ. κατά την ψυχροπολεμική και μεταψυχροπολεμική εποχή, η απάντηση έχει ως εξής: *πράγματι η πληροφοριακή κοινότητα οφείλει να τροποποιήσει τις διαδικασίες*

παραδοξότητα, επουδενί μπορούν οι δύο τομείς (τεχνολογία και πόλεμος) να αποτελέσουν υποχρεωτικά ο ένας alter ego του άλλου -η τεχνολογία πρέπει να αντιμετωπιστεί / προσληφθεί ως βοήθημα, όχι ως επαναστατικό εργαλείο. Ο της R. D. Williams συμφωνεί με τον Creveld, τέλος, ο Lawrence Freedman υποστηρίζει ότι πρώτον, το μέλλον του πολέμου πιθανότατα καθορίζεται από μια στροφή στη στρατιωτική / στρατηγική σκέψη και όχι από μια ανάλογη στο στρατιωτικό / τεχνολογικό πεδίο και δεύτερον, το ανθρώπινο στοιχείο πάντα θα είναι παρόν επινοώντας στρατηγήματα, διεξάγοντας πολέμους -για όλα αυτά βλέπε van Creveld, M., *Technology and War. From 2000 B.C. to the Present*, The Free Press, USA, 1991, σ. 319, Williams R. D., “Is the West’s Reliance on Technology the Panacea for Future Conflict or its Achilles heel?” στο *Defence Studies*, Volume 1, Number 2, 2001, σ. 38-56, Freedman Lawrence, *The Revolution in Strategic Affairs* και *The Transformation of Strategic Affairs* στο Adelphi Paper, Volume 38, Issue 318, 1998 και Adelphi Paper, Volume 45, Issue 379, 2006 αντιστοίχως

⁷³ Οι παρατηρήσεις του Ανδρέα Λιαρόπουλου και άλλων ειδικών (Hoehn, Metz, Scales, Papp, Alberts, Phillips) δεν μπορούν να προσπεραστούν ακόμα και από ακραιφνείς υποστηρικτές των νέων θεωρήσεων. Μια ανασκόπηση των πρόσφατα ενημερωμένων περιοδικών τεχνολογίας και στρατηγικής καταδεικνύει τα πλεονεκτήματα αλλά και τις δυσκολίες / παγίδες του ζητήματος παρά το ότι έχουν περάσει δεκαπέντε και πλέον έτη από τις πρώτες τοποθετήσεις των ερευνητών, βέβαια, κάθε τεχνολογικό επίτευγμα είναι καλοδεχούμενο. Για κάποιες δισταύουσες απόψεις ή και μύθους γύρω από το NCW αλλά και σχετικές εφαρμογές βλέπε στα κεφάλαια “NCW Myths” και “Network Centric Warfare” στο *Network Centric Warfare. Developing and Leveraging Information Superiority*, επιμ. Alberts D., Garstka John, Stein Frederick, CCRP Publication Series, 1999², σ. 5-13 και 87-114 αντιστοίχως. Χαρακτηριστικό της αμφιθυμίας που επικρατεί στο χώρο δεικνύει από τη μια η καταγραφή / αποδοχή των βασικών δογμάτων του NCW ήτοι, α) διασπορά πληροφορίας, β) επίγνωση καταστάσεως, γ) επιχειρησιακός συγχρονισμός, δ) αποτελεσματικότητα δράσης (*Power to the Edge: Command... Control... in the Information Age*, CCRP Publication Series, 2003, σ. 107-109 των Alberts και Richard Hayes) και από την άλλη μια επιφυλακτικότητα περί των σχετικών προσδοκιών. Πάρα ταύτα οφείλει να σημειωθεί το εξής: από τον Α΄ Π. Π. μέχρι αυτόν του Βιετνάμ οι Αμερικανοί είχαν, στις μάχες που έλαβαν μέρος, κατά μέσο όρο έναν νεκρό ή τραυματία στρατιώτη στους δεκαπέντε. Με το πέρας της εισβολής στο Ιράκ (2003) η αναλογία εκτινάχθηκε στο 1 / 480. Αυτό σημαίνει ότι μια μέρα πολέμου στη Μέση Ανατολή το 2003 κόστιζε τις ζωές πέντε στρατιωτών τη στιγμή που ο αριθμός των ημερήσιων απωλειών ανέβαινε στους δεκαοκτώ στο Βιετνάμ και στους διακοσίους έντεκα στον Β΄ Π. Π. Αν και οι συγκρίσεις πρέπει να λάβουν υπόψη πλήθος παραγόντων με κυριότερη, ίσως, τη δυναμικότητα των αντιπάλων, οι αριθμοί, σε απόλυτα μεγέθη, δικαιολογούν την, σχετική με τη μείωση απωλειών, έκφραση του Carl Conetta *...a new calculus of war*. Από τη μεριά τους οι Ιρακινοί θρηνούσαν καθημερινά περί τους τετρακόσιους οπλίτες, ο Martin Shaw στηριζόμενος σ’ αυτή την αισθητή διαφορά απωλειών και, εν τοις πράγμασι, ρίσκου, ομιλεί για έναν *risk-transfer militarism* -για περισσότερες λεπτομέρειες βλέπε Cordesman H. Anthony, *The Instant Lessons of the Iraq War*, Executive Summary, Fourth Working Draft, April 2003, σ. 17-18, Conetta Carl, *The New Warfare and the New American Calculus of War*, Project on Defense Alternatives, Brief Memo Number 26, September 2002 και Shaw Martin, *Risk Transfer Militarism and Legitimacy of War after Iraq*, 2004 στο <http://www.antiwar.com/orig/shaw.php?articleid=3054> όπου καταφύγαμε την 1^η Οκτωβρίου 2014

επεξεργασίας και χρήσης πληροφοριών προκειμένου να ανταποκριθεί στα καινοφανή [τεχνολογικά, κοινωνικά] ερεθίσματα. Το δεύτερο ερώτημα έχει να κάνει με οικονομικά προαπαιτούμενα προς αντιμετώπιση απειλών, προαπαιτούμενα ασφαλείας, επιχειρησιακές πρακτικές κ. λ. Ο Lahneman υποστηρίζει ότι μια αλλαγή στη δομή των Υπηρεσιών καθίσταται απαραίτητη προκειμένου οι τελευταίες να πορευτούν επιτυχώς στην μεταψυχροπολεμική φάση. Κατά το τρίτο εξετάζεται η κυρίαρχη μέχρι και το 1990 κουλτούρα σε σχέση με τη μετά το 1990 ανάλογη. Η διαφοροποίηση οδηγώντας σε αλλαγές δομής Υπηρεσιών οδηγεί ταυτόχρονα στην ανάδειξη νέων εσωτερικών ελίτ ή, αλλιώς, ελίτ «νέων ικανοτήτων». Το τέταρτο ερώτημα σχετίζεται σχεδόν αποκλειστικά με το πρόβλημα της τρομοκρατίας. Αν οι παλαιές ψυχροπολεμικές απειλές μπορούσαν να αποτραπούν διά των κλασικών μεθόδων (ύπαρξη ισχυρών στρατευμάτων, ανάλογων οπλικών συστημάτων και δογμάτων, πυρηνικών όπλων κ. λ.), κάτι τέτοιο δεν ισχύει για τις σημερινές ασύμμετρες· ένα από τα κύρια πλεονεκτήματα αντιμετώπισης ενός σχεδόν αόρατου κινδύνου δεικνύει η έγκυρη και ακριβής πληροφορία. Άρα ...*οι αλλαγές στο intelligence enterprise επηρεάζουν την πληροφοριακή διαδικασία, τη δομή των Υπηρεσιών, τις εσωτερικές ελίτ και τις αγωνίες γύρω από ζητήματα εθνικής ασφαλείας. Κατ' αυτήν την έννοια υφίσταται πράγματι μια επανάσταση στις πληροφορικές υποθέσεις, μια αλλαγή παραδείγματος, συνεπώς, μια ανάγκη παραδοχής επαναδόμησης των Υπηρεσιών του 21^{ου} αιώνα που ίσως οδηγεί στην RIA εποχή.*⁷⁴

⁷⁴ Lahneman W., "Is a Revolution in Intelligence Affairs Occurring?" στο *International Journal of Intelligence and CounterIntelligence*, Volume 20, Issue 1, 2007, σ. 6-14. Μάλιστα ο ίδιος στις σελίδες 222-224 του "The Need for a New Intelligence Paradigm" προτείνει οκτώ τρόπους αναδιοργάνωσης της αμερικανικής πληροφοριακής κοινότητας διατεινόμενος ότι αυτοί στηρίζουν ...*a radical departure -a "Revolution in Intelligence Affairs" or a radical "transformation"- from current practices in the intelligence enterprise*

ΚΕΦΑΛΑΙΟ 12

Πληροφόρηση και Ελλάδα

Μια κυβέρνηση χωρίς πληροφορίες ή μέσα αναζήτησής τους δεν είναι τίποτα άλλο από μια φάρσα ή τραγωδία, ή ίσως και τα δύο. Η γνώση θα κυβερνά πάντα την άγνοια και οι άνθρωποι που κυβερνούν πρέπει να εξοπλίζονται με την ισχύ της γνώσης

J. Madison (4 / 8 / 1822)¹

Περί κουλτούρας πληροφοριών. Τι σημαίνει ‘κουλτούρα πληροφοριών’;

Κάπου σ’ αυτό το σημείο κλείνουμε προσπαθώντας να μετουσιώσουμε την κεντρική, περί της αξίας της πληροφόρησης και των Υπηρεσιών, ιδέα του πονήματός μας σε πρακτική αναφορά ήτοι, καταθέτουμε τη δική μας πρόταση πολιτικής εθνικής ασφαλείας με σημείο αναφοράς ασφαλώς την πατρίδα μας. Αλλά ας πάρουμε τα πράγματα από την αρχή...

Ο Gareth Morgan υποστηρίζει πως κάθε οργανισμός χαρακτηρίζεται από τη δική του ιδιαίτερη *κουλτούρα*, πως αυτό που ονομάζεται «κουλτούρα» δύναται να αποτελέσει μια πανίσχυρη δύναμη παρά το ότι πολλοί αδυνατούν να το κατανοήσουν.² Αν και αόρατη, ενυπάρχει ασυνείδητα δεικνύοντας τον νούμερο ένα παράγοντα που θα οδηγήσει, ή όχι, έναν οργανισμό στην επιτυχία.³ Ο Edgar Schein ορίζει την κουλτούρα ως *...σύνολο βασικών ιδεών που ενστερνίζεται και μοιράζεται μια ομάδα. Οι ιδέες αυτές σχηματίζονται κατά την πορεία επίλυσης θεμάτων εξωτερικής προσαρμογής αλλά και εσωτερικής ολοκλήρωσης της ομάδας. Θεωρούνται πολύτιμες, οφείλουν, δε, να περάσουν στα επόμενα μέλη ως τρόπος αντίληψης, σκέψης, αίσθησης αυτών ακριβώς των θεμάτων.*⁴

Κατά την άποψή μας η επίλυση θεμάτων εξωτερικής προσαρμογής ή / και εσωτερικής ολοκλήρωσης μίας ομάδας ή ενός οργανισμού σχετίζονται (και) με την ίδια την επιβίωση της ομάδας ή του οργανισμού. Εάν ένα έθνος-κράτος ή μια πολιτεία αποτελούν έναν οργανισμό, τότε, έχουν χρέος να μορφώσουν ιδέες προκειμένου να επιβιώσουν, ουσιαστικά να εφεύρουν τρόπους συνέχισης της πορείας τους. Κατά τα ανωτέρω και εφόσον η άποψη μας κρίνεται ορθή, τότε, αυτές οι ιδέες ή, αλλιώς, οι τρόποι επιβίωσης διαμορφώνουν, μεταξύ άλλων, την κουλτούρα τους.

Το αρχικό ερώτημα είναι το εξής: αποδεχόμενοι τη σημαντικότητα της πληροφόρησης επί ζητημάτων εθνικής ασφαλείας, πρέπει να τη συμπεριλάβουμε (την πληροφόρηση) στην όλη κουλτούρα επιβίωσης ενός κρατικού οργανισμού; Η προφανής απάντηση είναι *ναι*. Κατά τον τρόπο τούτο δεικνύουμε ένα από τα κομμάτια αυτής ακριβώς της κουλτούρας. Πρόκειται για την επιμέρους «κουλτούρα της πληροφόρησης». Αν σταθούμε λίγο παραπάνω σ’ αυτή καθαυτή την κουλτούρα της πληροφόρησης, τότε, μπορούμε να την ορίσουμε επιχειρησιακά ως προσαρμοσμένο στην ιστορία και γεωγραφία σύνολο ιδεών, δράσεων και συμπεριφορών που αφορούν την πληροφοριακή κοινότητα.⁵ Ουσιαστικά κάνουμε λόγο για δύο κουλτούρες πληροφόρησης. Η πρώτη και ευρύτερη αφορά στο κράτος,

¹ Στο Λυμπέρης Χρήστος, *Εθνική Στρατηγική και Χειρισμός Κρίσεων*, Ποιότητα, Αθήνα, 2009, σ. 49

² Morgan Gareth, *Images of Organization*, Sage Publications, Inc., Thousand Oaks / California, 1997, σ. 1129

³ Hamrah Satgin, “The Role of Culture in Intelligence Reform”, *Journal of Strategic Security*, Volume 6, Number 3, 2013, σ. 164

⁴ Schein Edgar, *Organizational Culture and Leadership*, Jossey Bass, San Francisco, 2010, σ. 17

⁵ Phythian Mark, “Cultures of national intelligence” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014, σ. 34

η δεύτερη και στενότερη στις Υπηρεσίες. Η πρώτη σχετίζεται με την αποδοχή από το κράτος της αξίας της πληροφόρησης, η δεύτερη με την επιχειρησιακή ετοιμότητα και ικανότητα των Υπηρεσιών.

Το δεύτερο ερώτημα σχετίζεται με την Ελλάδα. Υφίσταται πληροφοριακή παράδοση στον νεώτερο ελληνικό χώρο; Η απάντηση κρίνεται επιτακτική. Εάν δεν υφίσταται, τότε, πρέπει να ξεκινήσει να υφαίνεται. Πριν ωστόσο απαντήσουμε επί τη βάση γεγονότων, ας δούμε επιγραμματικά πως αντιλαμβάνονται την πληροφοριακή κουλτούρα κάποιες σημαντικές στο διεθνές σύστημα χώρες. Πρόκειται για τις ΗΠΑ, τη Βρετανία, τη Σοβιετική Ένωση / Ρωσία και την Κίνα. Η επιλογή δεν έγινε τυχαία. Οι ΗΠΑ αποτελούν την υπερδύναμη με τη Ρωσία και την Κίνα να συνθέτουν τους ικανότερους αντιπάλους. Από τη μεριά της η Βρετανία απετέλεσε την πρώτη σύγχρονη διδάξασα του πεδίου. Από αυτές τις τέσσερεις χώρες οι ΗΠΑ και η Βρετανία συνθέτουν δημοκρατίες δυτικού τύπου. Η Ρωσία βρίσκεται σε μια κατάσταση ατελούς, κατά πολλούς, δημοκρατίας. Η Κίνα εξακολουθεί επισήμως να διαβαίνει το σοσιαλιστικό της δρόμο -η επιλογή χωρών με διαφορετικά πολιτικά συστήματα επίσης δεν είναι τυχαία. Τονίζουμε πως θα μπορούσαμε να συμπεριλάβουμε και άλλα κράτη (ίσως το Ισραήλ που λόγω μεγέθους και πληθυσμού αντιπαράβάλλεται πολλές φορές με την Ελλάδα) αλλά δεν αποτελεί πρόθεσή μας μια συγκριτική μελέτη.

ΗΠΑ: Στην Αμερική οι πρώτες προσπάθειες κτήσης πληροφοριών σχετίστηκαν με τον Πόλεμο της Ανεξαρτησίας (1775-1783), ουσιαστικά επρόκειτο για *ad hoc* επιχειρήσεις στην προσπάθεια αποφυγής ήττας στη σύγκρουση με τη Μεγάλη, τότε, Βρετανία. Κατόπιν της νίκης των αμερικανικών δυνάμεων, τα όποια πληροφοριακά δίκτυα περιέπεσαν σε αδράνεια. Τα αίτια ίσως ανευρίσκονται σε μια αίσθηση ασφάλειας έναντι εξωτερικών επιβουλών λόγω γεωγραφίας⁶ όπως και στην ηθική επίδραση της ιδέας του αμερικανικού εξεπισιοναλισμού.⁷

Οι όποιοι λόγοι αδιαφορίας γύρω από την πληροφόρηση έπαψαν να υφίστανται κατόπιν της επίθεσης στο Περλ Χάρμπορ και οπωσδήποτε μόλις η Αμερική συναισθάνθηκε τη θέση της στο παγκόσμιο χρηματιστήριο εθνικής ισχύος. Κατά τη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου, και ασφαλώς του Ψυχρού, οι πληροφοριακές ανάγκες επανήλθαν δριμύτερες σε σχέση με κάθε άλλη φορά. Όσο ο ρόλος των ΗΠΑ επεκτεινόταν στον κόσμο τόσο έπρεπε να αναπτυχθεί ο πληροφοριακός τους μανδύας. Αυτό εις το οποίο αρχικά εδόθη έμφαση ήταν το πεδίο των εξωτερικών πληροφοριών. Το συγκεκριμένο πεδίο εφοδίαζε με στοιχεία τους διαμορφωτές της εξωτερικής πολιτικής συνεισφέροντας στη διαδικασία λήψης αποφάσεων. Κάτι τέτοιο ίσως ωθήσει ορισμένους να υποθέσουν πως εσωτερικά ζητήματα, κατ' ουσίαν ζητήματα κρατικής ασφάλειας, παραμελήθηκαν. Ωστόσο ο όρος 'κρατική ασφάλεια' ή 'εθνική ασφάλεια' στην αμερικανική πολιτική συνείδηση είναι αρκετά ασαφής όσο και εύπλαστος. Άλλωστε, όπως παρατηρεί ο Joseph Romm, η έννοια της (εθνικής) ασφάλειας επανέρχεται στο προσκήνιο ξανά και ξανά από το

⁶ Ford Harold, "The US Government's Experience with Intelligence Analysis: Pluses and Minuses" στο *Intelligence and National Security*, Volume 10, Number 4, 1995, σ. 34-53

⁷ Titus James, "Review of 'Henry L. Stimson: The First Wise Man' by David F. Schmitz" στο *Aerospace Power Journal*, Volume XVI, Number 2, 2002, σ. 111-112

1947⁸ χωρίς κανείς να επιχειρεί να την (περι)ορίσει⁹ -κατά τον τρόπο τούτο εμπεριέχει κάθε σχετική πτυχή της εξωτερικής και εσωτερικής πολιτικής.¹⁰

Με τη λήξη του ψυχρού πολέμου και την εξάλειψη της σοβιετικής απειλής -που αποτελούσε την κύρια αιτία ύπαρξης της αμερικανικής πληροφοριακής κοινότητας- γεννήθηκε το εξής εύλογο: «Ποιος ο ρόλος πλέον των Υπηρεσιών;». Άλλοι υποστήριζαν πως αυτές οφείλουν να κινηθούν προς άγγραν οικονομικών πληροφοριών και πάταξη ανάλογων απειλών, άλλοι υπέθεσαν πως προτεραιότητα οφείλει να αποτελέσει η καταπολέμηση κοινωνικών παθογενειών (εμπόριο ναρκωτικών, διακίνηση ανθρώπων, τρομοκρατία κ. λ.), άλλοι πρότειναν τον περιορισμό τους επί τη βάσει στενά καθορισμένων απειλών εθνικής ασφαλείας¹¹ (ρωτάμε: «ποιες είναι αυτές οι στενά καθορισμένες απειλές εθνικής ασφαλείας;»).

Σε κάθε περίπτωση η αμερικανική πολιτεία δύναται να απεικονισθεί ως κύκλος με κέντρο και ακτίνες. Το κέντρο δεν είναι άλλο από την ομοσπονδιακή κυβέρνηση. Οι ακτίνες αναπαριστούν τους κυβερνητικούς οργανισμούς / μηχανισμούς (βλέπε, λ. χ., Υπουργεία) που διαχειρίζονται τα όποια είδη ισχύος. Σ' αυτό ακριβώς το σημείο εμφανίζονται οι Υπηρεσίες. Καθήκον τους ο προσπορισμός πληροφοριών ώστε να επιτευχθεί η βέλτιστη παραγωγή πολιτικής. Οι Υπηρεσίες είναι αυτές που θα ενημερώσουν επί διαφόρων ζητημάτων τόσο την κεντρική κυβέρνηση (το κέντρο του κύκλου) όσο, εμμέσως ή αμέσως, τα επιμέρους στοιχεία της (τις ακτίνες του κύκλου). Τον συντονισμό σε ανώτατο επίπεδο όπως και τις βασικές πολιτικές επιλογές αναλαμβάνουν και εκπονούν το Συμβούλιο Εθνικής Ασφαλείας (National Security Council -NSC) και ο Πρόεδρος των ΗΠΑ με τη βοήθεια του Συμβούλου Εθνικής Ασφαλείας (National Security Advisor). Σε επίπεδο Υπηρεσιών κεντρικό ρόλο έχουν ο Director of National Intelligence (DNA) και ασφαλώς η CIA.¹²

Βρετανία: Ερχόμενοι στην βρετανική περίπτωση επίσης διαπιστώνουμε πως η πληροφόρηση παίζει ιδιαίτερο ρόλο στην εξέλιξη της πολιτικής ζωής της χώρας. Οι ρίζες του πληροφοριακού πεδίου ανευρίσκονται στον 16^ο αιώνα στις προσπάθειες των αξιωματούχων Francis Walsingham και William Cecil να στήσουν ένα δίκτυο πληροφοριοδοτών υπέρ της βασίλισσας Ελισάβετ Α' της Αγγλίας. Ο Walsingham, επονομαζόμενος και *spymaster*, ελέγχει έναν αριθμό κατασκόπων εντός και εκτός νησιού αποκαλύπτοντας σειρά συνωμοτικών κινήσεων εις βάρος της Ελισάβετ. Ο ίδιος διατηρεί τη θέση του *Principal Secretary of State*, πρόκειται για θέση που τον εξουσιοδοτεί επί της εξωτερικής πολιτικής της χώρας -η σύνδεση μεταξύ πολιτικής / εξωτερικής πολιτικής και πληροφόρησης είναι κάτι παραπάνω από εμφανής.¹³

Το σύγχρονο βρετανικό πληροφοριακό σύστημα εκκινεί εξ αιτίας της γερμανικής απειλής, αλλά και των προβλημάτων στην Ιρλανδία, το 1909 με την ίδρυση του Secret Service Bureau, ουσιαστικά με τη δημιουργία της υπηρεσίας εσωτερικών Πληροφοριών (MI5) και της αντίστοιχης εξωτερικών (MI6, μετονομαζομένης αργότερα σε MI6). Οι δύο Υπηρεσίες, μέχρι την έναρξη του Δευτέρου Παγκοσμίου Πολέμου και παρά τον πολιτικό τους χαρακτήρα, προσανατολίζονται κυρίως στην στρατιωτική πληροφόρηση, ωστόσο, κάποια στιγμή το βρετανικό υπουργείο

⁸ Έτος κατά το οποίο ενεφανίσθη η *National Security Act* και τα εξ αυτής παραγόμενα ήτοι, το National Security Council και η CIA

⁹ Romm Joseph, *Defining National Security: The Nonmilitary Aspects*, Council of Foreign Relations Press, New York, 1993, σ. 3

¹⁰ Marrin Stephen, "The United States" στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 147-148

¹¹ ό. π., σ. 148

¹² ό. π., σ. 148-149

¹³ Goodman Michael, "The United Kingdom" στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 135-136

Εξωτερικών αποφασίζει πως οφείλει να εισπράττει αλλά και να παρέχει πολιτική και διπλωματική πληροφόρηση. Κάπως έτσι το 1936, με πρόταση του Maurice Hankey, δημιουργείται το Joint Intelligence Committee. Πρόκειται για διυπηρεσιακή επιτροπή που συγκεντρώνει κάθε είδους εθνική, πολιτικής ή στρατιωτικής φύσεως, πληροφόρηση διανέμοντάς τη στους αρμοδίους φορείς. Επί της ουσίας το JIC προΐσταται των επιμέρους βρετανικών Υπηρεσιών δεικνύοντας το κέντρο βάρους του όλου πληροφοριακού δικτύου της χώρας. Συγκροτείται από επικεφαλής αυτών ακριβώς των Υπηρεσιών και από αξιωματούχους του πολιτικού χώρου. Από το 2010 συνεπικουρείται από το Συμβούλιο Εθνικής Ασφαλείας (National Security Council -NSC) προκειμένου να βελτιστοποιηθεί η διαδικασία λήψεως πολιτικών αποφάσεων. Το NSC σκοπό έχει «να συμβάλει στην αντιμετώπιση των κινδύνων που απειλούν τη χώρα συντονίζοντας και εναρμονίζοντας τη δράση των αρμοδίων πολιτικών τμημάτων και οργανισμών όπως και κάθε άλλου κυβερνητικού φορέα ικανού προς συμβολή υπέρ της εθνικής ασφαλείας».¹⁴

Για τον Michael Goodman οι βρετανικοί πληροφοριακοί οργανισμοί δεν συνθέτουν τίποτε άλλο από έναν μικρόκοσμο που λειτουργεί εντός του πολιτικού συστήματος. Υποθέτουμε πως ο ερευνητής δηλώνει το αυτονόητο, πως οι πληροφοριακοί οργανισμοί αποτελούν αντανάκλαση του συστήματος ήτοι, ‘καλή Πολιτεία με κακές Υπηρεσίες δεν συνάδει’. Η βρετανική πληροφοριακή κοινότητα εντέλλεται όπως δραστηριοποιηθεί προς άγραν πληροφοριών εθνικού ενδιαφέροντος, όπως επιβοηθήσει τους policymakers προκειμένου λήψεως ορθών και επωφελών αποφάσεων για τη χώρα. Η όλη διαδικασία δεν δύναται να πετύχει χωρίς τη συνεργασία και συνεννόηση του ‘πράκτορα με τον πολιτικό’, χωρίς να ξέρει ο πρώτος τι ζητά ο δεύτερος.¹⁵ Ακριβώς αυτή η γνώση του ενός για τον άλλο και η διάθεση συνεργασίας / συνεννόησης υπέρ εθνικών στοχεύσεων συνθέτει ό,τι ονομάζεται ‘κρατική κουλτούρα πληροφοριών’.

Σοβιετική Ένωση / Ρωσία: Η κουλτούρα της πληροφόρησης ουδέποτε έλειψε στην πάλαι ποτέ αυτοκρατορία της Σοβιετικής Ένωσης. Η διαβόητη KGB, με έτος ίδρυσης το 1954, απετέλεσε τον οργανισμό που διαδέχτηκε μια άλλη εξίσου, το λιγότερο, περιβόητη Υπηρεσία, την Vse Rossiiskaya Cherezvechaninaya Kommissiya ή VChKa ή, απλούστερα ChK (Τσέκα), ιδρυθείσα εν έτει 1917.¹⁶ Ο Oleg Kalugin, πρώην αξιωματούχος της KGB, αναφέρει πως ο Στάλιν περιέγραφε την ChK, ως «τιμωρητικό όργανο της ισχύος της Σοβιετικής Ένωσης ... κάτι σαν στρατιωτικό δικαστήριο με σκοπό τη διάσωση της επανάστασης από τους αντεπαναστάτες της μπουρζουαζίας και τους πράκτορές της»¹⁷ -γίνεται αμέσως κατανοητό ότι η Τσέκα λειτούργησε ως καθεστωτικός μηχανισμός καταπίεσης και αποσόβησης ‘πολιτικών δράσεων και λιποταξιών’. Μετά το 1922, και πιο συγκεκριμένα μεταξύ 1926 και 1934, εμφανίζεται η Obedinyonnoe Gossudarstvennoe Politicheskoe Upravleniye (OGPU) αποτελώντας τη μυστική αστυνομία του συστήματος. Οι αρμοδιότητες της τελευταίας μεταφέρθηκαν το 1936 στην ανασυσταθείσα δομή του Narodniy Kommissariat Vnutrennykh Del (NKVD) -επρόκειτο ουσιαστικά για το υπουργείο Εσωτερικών της Σοβιετικής Ένωσης.¹⁸

¹⁴ Goodman Michael, “The United Kingdom” στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 137

¹⁵ ό. π., σ. 142-143

¹⁶ Brope Reginald, “Russia” στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 229

¹⁷ Kalugin Oleg, *Spymaster: My 32 Years in Intelligence and Espionage Against the West*, Basic Books, London, 2009, σ. 13

¹⁸ Brope Reginald, “Russia” στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 229

Κάποια στιγμή το NKVD μετονομάζεται σε Ministerstvo Vnutrennikh Del (MVD) φιλοξενώντας στους κόλπους του την υπηρεσία που θα γίνει γνωστή με τα αρχικά KGB. Περί το 1953 ξεκινά μια διαδικασία συγχώνευσης μεταξύ του MVD και του Ministerstvo Gosudarstvennoi Bezopasnosti (MGB) ήτοι, του σοβιετικού υπουργείου Ασφαλείας. Έναν χρόνο αργότερα η KGB αποσυνδέεται από το MVD. Μετατρέπεται και επισήμως σε ‘ασπίδα και σπαθί’ του σοβιετικού Κομμουνιστικού Κόμματος. Σε ‘ασπίδα’ προκειμένου να προστατεύσει την ηγεσία του, σε ‘σπαθί’ προκειμένου να επιβάλει τη θέληση ακριβώς αυτής της ηγεσίας τόσο εντός όσο και εκτός χώρας.¹⁹

Αρχικά η KGB προσπάθησε να αποστασιοποιηθεί από τους πληροφοριακούς προκατόχους της γνωρίζοντας πως η πολιτική τους παρακαταθήκη κάθε άλλο παρά ήτο άμεμπτη. Διαδήλωσε πως δεν ήταν μήτε κληρονόμος μήτε διάδοχός τους, πως δεν επρόκειτο να συνεχίσει τον σκαιό τρόπο χειρισμού διαφόρων ζητημάτων που χαρακτήριζε τους ‘παλαιότερους’.²⁰ Ο Kalugin υποστηρίζει ότι η KGB πριμοδότησε τα ακριβώς επόμενα χρόνια μια νέα γενιά πρακτόρων κεκαθαρμένων από τα εγκλήματα της σταλινικής περιόδου²¹, αποσυνδεδεμένων από τον πρώην επικεφαλής της σοβιετικής μυστικής αστυνομίας, Λαβρέντι Μπέρια. Μόλα ταύτα και παρά τα περί του αντιθέτου θρυλούμενα, γράφει ο Brope, συνέχισε να λειτουργεί στο ίδιο μοτίβο παρακολουθώντας την σοβιετική κοινωνία αλλά και τους πολίτες των χωρών του Συμφώνου της Βαρσοβίας υπό το φόβο αποκλινουσών τάσεων όπως και ενδεχόμενων υπονομευτικών, κατά του καθεστώτος, ενεργειών -περιττό να υπενθυμίσουμε πως συνέβαλε τα μέγιστα στην καταστολή των εξεγέρσεων της Βουδαπέστης (1956) και της Πράγας (1968).²²

Η μέχρι αυτού του σημείου μνεία στις Υπηρεσίες της ΕΣΣΔ καταδεικνύει τη συνέχεια και τη σημασία τους στη νεώτερη ιστορία της Ρωσίας. Ακόμα και σήμερα, τονίζει ο Brope, οι πράκτορες της Ρωσικής Ομοσπονδίας και ιδιαίτερα αυτοί της FSB αναφέρονται πολλές φορές ως ‘Τσέκιστς’ με τον όρο να κομίζει τόσο ένα πολιτικό κεφάλαιο όσο και μια κληρονομιά που βρίσκει τις ρίζες της στις προγενέστερες σοβιετικές υπηρεσίες Πληροφοριών.²³

Εάν και εφόσον η KGB συνέθεσε μια μεικτή Υπηρεσία εσωτερικών και εξωτερικών πληροφοριών αλλά και αντικατασκοπίας, απετέλεσε, θα ρωτήσει κάποιος, μια σοβιετική έκδοση των CIA και FBI ή της MI5 και της MI6 μαζί; Αν και πολλοί θα απαντήσουν ναι, ο Brope δεν συμφωνεί υποστηρίζοντας πως η συγκεκριμένη Υπηρεσία ξεπέρασε κατά πολύ τις αρμοδιότητες μιας ανάλογης δυτικής.²⁴ Ο Michael Waller το θέτει ως εξής: «η CIA και το FBI χαρακτηρίζονται από μια κουλτούρα μυστικότητας, αυτή είναι η φύση του επαγγέλματος -η μυστικότητα προς όφελος της δημοκρατίας και της κοινωνίας. Η KGB διαφέρει. Συνέδεσε τη μυστικότητα με τη συνωμοσία προκειμένου να καταπιέσει τις αξίες της δημοκρατίας. Μόνιμο καθήκον της η αναζήτηση εχθρών εντός του ίδιου του λαού σε πανεθνική κλίμακα. Καταχράστηκε την έννοια της πληροφόρησης και της αντιπληροφόρησης αποκτώντας και συντηρώντας μια απολυταρχική πολιτική δύναμη, βλέποντας τον κάθε διαφωνούντα ως εχθρό». Επιπλέον, συνεχίζει ο Waller, κατεγράφη ένας αριθμός πρακτικών και δομικών διαφορών. Ενώ η CIA και το FBI συνθέτουν διακριτές υπηρεσίες Πληροφοριών, η KGB συνθέτει ένα ολόκληρο

¹⁹ Brope Reginald, “Russia” στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 229

²⁰ Albats Yevgenia, *State Within a State: The Secret Police and Its Hold on Russia's Past, Present and Future*, I. B. Tauris, London, 1995, σ. 8

²¹ Kalugin Oleg, *Spymaster: My 32 Years in Intelligence and Espionage Against the West*, ό. π., σ. 22

²² Brope Reginald, “Russia” στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 229-230

²³ ό. π., σ. 229

²⁴ ό. π., σ. 230

σύστημα εξωτερικών πληροφοριών, αντιπληροφόρησης, στρατιωτικής και αστυνομικής κατασκοπίας και αντικατασκοπίας, συλλογής και ανάλυσης στοιχείων, ειδικών ερευνών, κεκαλυμμένων δράσεων, ιδεολογικής επιβολής, πολιτικών ξεκαθαρισμάτων διαθέτοντας έναν εσωτερικό στρατό και μια τεράστια ομάδα συνοριοφυλάκων. Το απέραντο αυτό οικοδόμημα υποστηρίζεται από ένα αχανές δίκτυο διοικητικών και επιμελητηριακών υπαλλήλων όπως και από ένα πλήθος συμβούλων και πληροφοριοδοτών.²⁵

Συνολικά, γράφει ο John Barron, ο ρόλος της KGB υπερέβαινε το ρόλο μιας μυστικής υπηρεσίας.²⁶ Μαζί του συμφωνεί ο Gordon Bennet κατά τον οποίο η KGB απετέλεσε τον πλέον ισχυρό οργανισμό ασφαλείας που υπήρξε ποτέ με παρουσία σε κάθε σημείο της ΕΣΣΔ, με σχεδόν απεριόριστη χρηματοδότηση, με πάμπολλες δυνατότητες, με προσωπικό που εισέδουε σε κάθε κρατική δομή.²⁷

Η KGB συνέθεσε έναν από τους πυλώνες του σοβιετικού κράτους αποδίδοντας λόγο μόνο στο Politburo. Έτσι και αλλιώς όλοι οι αξιωματούχοι της Υπηρεσίας ήταν μέλη του Κόμματος, άρα, υπόκειντο στην κομματική πειθαρχία. Παρ' ελπίδα εάν κάτι λοξοδρομούσε από τον ορθό δρόμο, τότε, υφίσταντο κυρώσεις. Κάπως έτσι ο Khrushchev δεν δίστασε να περικόψει μισθούς, επιδόματα και διάφορα 'τυχερά' των εν ενεργεία αλλά και συντάξεις των πρώην πρακτόρων στα μέσα της δεκαετίας του 1950.²⁸ Τελικά η KGB συμμορφούμενη με το κράτος, ήτοι το ΚΚΣΕ, υποστήριξε την ιδεολογία του και ειδικά τις θέσεις του στην υπαρξιακή μάχη με τη Δύση.²⁹

Η πτώση του κομμουνιστικού καθεστώτος και η αναγκαστική μετεξέλιξη της KGB γέννησαν την FSB. Η μακρά διαδικασία έλαβε χώρα την περίοδο 1991-2004. Τον Ιανουάριο του 1992 στη Ρωσία δραστηριοποιούνταν πέντε νέες Υπηρεσίες, μεταξύ αυτών η SVR (εξωτερικών πληροφοριών και αποστολών) και η δομή που αργότερα έγινε γνωστή ως FSB (εσωτερικών πληροφοριών και δράσεων). Ο εναγκαλισμός μεταξύ κυβερνήσεων και Υπηρεσιών συνεχίζεται με τον Μπορίς Γιέλτσιν να τις ελέγχει και με τη σειρά τους αυτές να συγκεντρώνουν πολιτική ισχύ και λόγο· ορισμένοι κάνουν νύξη για εξάρτηση, τελικά, του Γιέλτσιν από τους πληροφοριακούς οργανισμούς.³⁰

Τη δεκαετία του 1990 τόσο η SVR όσο και η FSB αντιμετώπισαν πλήθος δυσκολιών με κύριο αίτιο την ελεύθερη πτώση της ρωσικής οικονομίας. Περαιτέρω, οι επιχειρούμενες μεταρρυθμίσεις εντός αυτών οδήγησαν μάλλον σε φτωχά αποτελέσματα. Από την άλλη τα εσωτερικά προβλήματα (οργανωμένο έγκλημα, ταραχές στην Τσετσενία) οξύνονταν. Η όλη κατάσταση για την FSB ομοίαζε με εφιάλτη, άλλωστε, η Υπηρεσία πίστευε πως έργο της ήταν η καταδίωξη ξένων πρακτόρων που δρούσαν εντός Ρωσίας και όχι η πάταξη ομάδων που ενέπιπταν μάλλον στην αρμοδιότητα των υπηρεσιών επιβολής νόμου και τήρησης τάξεως.³¹

Τα πράγματα αλλάζουν χαρακτηριστικά με την άνοδο του Βλαδίμηρου Πούτιν στην εξουσία το 2000. Ο νέος Πρόεδρος αυξάνει κατακόρυφα τον προϋπολογισμό, οι, δε, Υπηρεσίες αποδίδουν απευθείας λόγο σ' αυτόν. Η FSB αναλαμβάνει κεντρικό

²⁵ Waller Michael, *Secret Empire: The KGB in Russia Today*, Westview Press, Oxford, 1994, σ. 3, 9-11

²⁶ Barron John, *KGB Today: The Hidden Hand*, Reader's Digest Press, New York, 1983, σ. 12

²⁷ Bennet Gordon, *The SVR: Russia's Intelligence Service*, UK: Conflict Studies Research Center, Camberley, 2000, σ. 2

²⁸ Kalugin Oleg, *Spymaster: My 32 Years in Intelligence and Espionage Against the West*, ό. π., σ. 19, 22

²⁹ Bennet Gordon, *The SVR: Russia's Intelligence Service*, ό. π., 2000, σ. 3

³⁰ Knight Amy, *Spies Without Cloaks: The KGB's Successors*, Princeton University Press, Princeton / New Jersey, 1996, σ. 37

³¹ Bennet Gordon, *The Federal Security Service of the Russian Federation*, Conflict Studies Research Center, Camberley / UK, 2000, σ. 13-19

ρόλο. Αν και επισήμως καταγράφεται ως υπηρεσία εσωτερικών Πληροφοριών συμπράττει με την SVR επί πληροφοριακών ζητημάτων εκτός Ρωσίας. Σε εσωτερικό επίπεδο συνεργάζεται τόσο με αστυνομικές αρχές όσο και με άλλες αρχές εσωτερικής ασφαλείας· στις επιτυχίες της εγγράφεται η εξουδετέρωση πλήθους τρομοκρατικών οργανώσεων ισλαμικής υφής.³²

Οι υπηρεσίες Ασφαλείας και Πληροφοριών της Ρωσίας καταγράφονται εντός των πλέον ενεργών παγκοσμίως. Μετά την πτώση του σοβιετικού μοντέλου έχουν υποστεί ένα εντυπωσιακό 'λίφτινγκ' με κύριο χαρακτηριστικό την πολιτική και ιδεολογική ουδετερότητα ήτοι, έχουν καταστεί εθνικές / κρατικές αποβάλλοντες το κομματικό ένδυμα, ωστόσο, βρίσκονται πάντα δίπλα στην πολιτεία με σκοπό να στηρίζουν τις επιλογές της. Από την άλλη μεριά πολλοί πρώην επιχειρησιακοί της KGB ή και της FSB, κορυφαίο παράδειγμα ο ίδιος ο Πούτιν, δραστηριοποιούνται τόσο πολιτικά όσο και οικονομικά. Κατά την έννοια τούτη η κουλτούρα ασφαλείας και πληροφοριών δεν πρόκειται να λείψει ούτε από την μετασοβιετική Ρωσία. Άλλωστε παρουσία πρώην και νυν πρακτόρων, πέραν αυτής εντός του Κρεμλίνου και εντός των υπηρεσιών επιβολής νόμου και τάξης, καταγράφεται και εντός του ρωσικού Συμβουλίου Ασφαλείας· το τελευταίο αποτελεί το όργανο που συντονίζει τις κύριες κρατικές πολιτικές υπό την επίβλεψη του Ρώσου Προέδρου.³³

Κίνα: Αν και για τις κινεζικές πληροφοριακές επιχειρήσεις δεν γνωρίζουμε πολλά, αυτές καθόλου δεν αποτελούν σύγχρονο φαινόμενο. Η πρακτική της κατασκοπίας στην Κίνα βρίσκει τις ρίζες της τουλάχιστον στον 5^ο αιώνα π. Χ. όπως πληροφορούμεθα από τον Κινέζο στρατηγιστή Σουν Τζου. Ο τελευταίος αποδίδει μέγιστη αξία στην έγκαιρη και έγκυρη πληροφόρηση προκειμένου επίλυσης πολιτικών προβλημάτων και υποστήριξης στρατιωτικών δράσεων. Όπως είναι φυσικό, η σημερινή Κίνα έχει πολύ περισσότερες και πολυπλοκότερες πληροφοριακές ανάγκες από τις ανάγκες που ανάγονται στην αρχαιότητα. Αυτό ωστόσο που επιβιώνει και με το παραπάνω συνδέοντας το παρελθόν με το παρόν είναι η αναγνώριση της πολιτικής ηγεσίας της αξίας της εκ των προτέρων γνώσεως, άρα, της ορθής πληροφόρησης και του αναπόφευκτου των πληροφοριακών κινήσεων. Ο κρατικός πληροφοριακός μηχανισμός της Κίνας δεικνύει κάτι πέρα από επιβοηθητικό μηχανισμό στην υπηρεσία της διαδικασίας λήψεως πολιτικών αποφάσεων. Πολύ απλά, είναι αναπόσπαστα συνδεδεμένος με αυτήν ακριβώς τη διαδικασία αποτελώντας, επιπλέον, εργαλείο οικονομικής ανάπτυξης αλλά και εσωτερικού ελέγχου.³⁴

Για το Κομμουνιστικό Κόμμα της Κίνας οι ειλημμένες αποφάσεις οφείλουν να σέβονται και να υπηρετούν τα πολιτικά, στρατιωτικά αλλά και οικονομικά πλάνα της χώρας. Προκειμένου εξυπηρετήσης αυτών των σχεδιασμών πολλές φορές απαιτείται ο προσπορισμός πληροφοριών από ανεπτυγμένες βιομηχανικά χώρες.³⁵ Κατά τον τρόπο τούτο, είναι οι κινεζικές Υπηρεσίες που έχουν επωμισθεί το βάρος της κλοπής τεχνολογικών, πολιτικών, στρατιωτικών αλλά και οικονομικών στοιχείων / assets που θα ενισχύσουν τον κινεζικό προγραμματισμό για την αυριανή μέρα.³⁶

³² Brope Reginald, "Russia" στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 232-233

³³ ό. π., σ. 233-234

³⁴ Eftimiades Nicholas, "China" στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 191

³⁵ Ακριβώς λόγω των πολιτικών περιορισμών αλλά και των οικονομικών / εμπορικών πρακτικών που ισχύουν στη μεγάλη χώρα της Άπω Ανατολής, πολλές δυτικές δημοκρατίες, και ειδικά η Αμερική, την αντιμετωπίζουν με δυσπιστία μειώνοντας αν όχι περιστέλλοντας τελείως τη ροή πληροφοριών που σχετίζονται με την υψηλή τεχνολογία

³⁶ Eftimiades Nicholas, "China" στο *Routledge Companion to Intelligence Studies*, ό. π., σ. 192

Κατά την άποψή μας η τεράστια παράδοση των κινεζικών μυστικών υπηρεσιών, η αποφασιστικότητα αλλά και τα ρίσκα που αναλαμβάνουν φαίνονται από δύο, επιπλέον, πράγματα: Πρώτον, ουσιαστικά δεν υπάρχει διαφορά μεταξύ ενός αξιωματούχου πληροφοριών και ενός στρατολογημένου (recruit) πράκτορα. Επιχειρησιακά και οι δύο δύναται να προβούν σε εκμαίευση μυστικών στην αλλοδαπή. Ως αποτέλεσμα, ακόμα και ένας Κινέζος αξιωματούχος πληροφοριών που κατά πάσα πιθανότητα καλύπτεται από ασυλία ³⁷ (βλέπε π. χ. έναν διαπιστευμένο διπλωμάτη που ωστόσο κάθε άλλο παρά διπλωματικά είναι τα πραγματικά του ενδιαφέροντα) ρισκάρει την αποκάλυψή του τη στιγμή που θα μπορούσε να καλυφθεί άκοπα πίσω από τη θέση του χειριστή (handler) του στρατολογημένου προσώπου που συνήθως αποτελεί (το στρατολογημένο πρόσωπο) πολίτη της χώρας-στόχου. Δεύτερον, αξιοσημείωτη είναι η αξιοποίηση Κινέζων πολιτών που διαβιούν στην αλλοδαπή, βλέπε πέρα από διπλωμάτες, επίσης, επιχειρηματίες, εμπορικούς αντιπροσώπους, φοιτητές, απλούς εργαζομένους κ. λ ³⁸ -ως φαίνεται το πληροφοριακό tradecraft δεν αποτελεί καθόλου κάτι πρωτοφανές όχι μόνο για την επίσημη κινεζική πολιτεία αλλά και για την κινεζική κουλτούρα.

Ο Ιωάννης Κωνσταντόπουλος είναι ένας ακόμη ερευνητής που επισημαίνει πως μεταξύ των μέσων που χρησιμοποιεί η χώρα των Δράκων προκειμένου να αυξήσει την στρατιωτική και οικονομική της ισχύ είναι και η κατασκοπία. Και συνεχίζει: «Το γεγονός αυτό δεν προκαλεί καμιά έκπληξη στους μελετητές, εάν αναλογιστεί κανείς τη σημασία που έχει η πληροφόρηση διαχρονικά για τη χώρα αυτή. Εάν εξετάσει κανείς προσεκτικά την περιορισμένη διεθνή βιβλιογραφία σχετικά με τη χρήση της πληροφόρησης / κατασκοπίας από την πολιτικοστρατιωτική ηγεσία της Κίνας, θα καταλήξει στο συμπέρασμα ότι η πληροφόρηση / κατασκοπία αποτελεί ένα διαχρονικό χαρακτηριστικό γνώρισμα της εξωτερικής και αμυντικής πολιτικής της χώρας αυτής. Δύο από τους σημαντικότερους μελετητές της Κίνας, ο Ralf Sawyer και ο Nicholas Eftimiades, συμφωνούν με αυτή τη διαπίστωση. Ο πρώτος θεωρεί ότι κανένα κράτος δεν έχει εξασκήσει ή θεωρητικοποιήσει την τέχνη της πληροφόρησης / κατασκοπίας περισσότερο από την Κίνα. Πράγματι τα στρατηγικά έργα των Κινέζων είναι γεμάτα από αναφορές στην κατασκοπία και στη διεξαγωγή μυστικών δραστηριοτήτων / επιχειρήσεων. Ο δεύτερος υποστηρίζει πως η Κίνα προβαίνει σε κατασκοπευτικές ενέργειες τουλάχιστον από τον 5^ο αιώνα π. Χ. Μάλιστα τονίζει ότι η στρατιωτική ιστορία της είναι γεμάτη από παραδείγματα άσκησης κατασκοπίας με στόχο την επίτευξη των πολιτικών και στρατιωτικών σκοπών της όπως αυτοί γίνονταν αντιληπτοί από τους διαμορφωτές των αποφάσεων».³⁹

Αυτό που μέχρι του σημείου τούτου προσπαθούμε να αποδώσουμε σίγουρα δεν είναι μια εικόνα της πληροφοριακής ιστορίας κάποιων μεγάλων κρατών. Ελπίζουμε ωστόσο πως οι συγκεκριμένες αναφορές βοηθούν τον αναγνώστη να αντιληφθεί τι σημαίνει κρατική κουλτούρα πληροφοριών. Η ανωτέρω ελάχιστη αφήγηση είναι ενδεικτική της στάσης που τηρούν έναντι της πληροφόρησης οι χώρες που σχεδιάζουν και οραματίζονται το μέλλον τους και δεν είναι καθόλου απαραίτητο μια χώρα να είναι μεγάλη σε μέγεθος και πληθυσμό προκειμένου να σχεδιάσει τις επόμενες κινήσεις της, ίσως, μάλιστα, ισχύει εντελώς το αντίθετο.

Κάθε μία από τις τέσσερις χώρες του παραδείγματός μας χαρακτηρίζεται από έντονη διάθεση κτήσης και χρήσης πληροφοριών, αυτό φαίνεται από τον τρόπο που

³⁷ Λέμε 'κατά πάσα πιθανότητα' διότι δεν αποκλείεται να είναι απλά ένας illegal

³⁸ Eftimiades Nicholas, *Chinese Intelligence Operations*, Toppan Company, Tokyo, 1995, σ. 116

³⁹ Κωνσταντόπουλος Ιωάννης, *Οικονομία και κατασκοπία. Θεωρία και πράξη*, Ποιότητα, Αθήνα, 2010, σ. 328

τοποθετούνται και δρουν εντός του κρατικού τους συστήματος οι μυστικές υπηρεσίες όπως και από την ιστορία αυτών ακριβώς των τελευταίων.

Σε καμία περίπτωση δεν υποστηρίζουμε πως οι Υπηρεσίες είναι αλάθητες -τουναντίον, πως αποτελούν τα μόνα εργαλεία στήριξης κρατικών σχεδιασμών. Ούτε υποστηρίζουμε πως χρησιμοποιούνται για αγαθούς σκοπούς άλλωστε είναι γνωστό πως εξυπηρετούν και μη δημοκρατικά συστήματα (χωρίς αυτό να σημαίνει πως μη αγαθούς σκοπούς έχουν μόνο οι απολυταρχίες). Ωστόσο κάτι τέτοιο δεν έχει καμία σημασία. Αν μία χώρα είναι πολιτικά απολυταρχική, τότε, οι Υπηρεσίες της θα εξυπηρετήσουν τις επιδιώξεις ενός απολυταρχικού καθεστώτος. Αν είναι δημοκρατική, τότε, θα εξυπηρετήσουν τους σχεδιασμούς μιας δημοκρατίας -και στις δύο περιπτώσεις πράττουν το θεμιτό, το ορθόν και το λογικό, το αυτονόητο. Αυτό που σε κάθε περίπτωση έχει σημασία είναι η ύπαρξη της περιώνυμης κουλτούρας πληροφοριών προς εξυπηρέτηση της κρατικής ηγεσίας.

Αν εντυπώσουμε κατά τι παραπάνω στις περιπτώσεις των άνω χωρών θα διαπιστώσουμε ότι τόσο η Αμερική όσο και η Βρετανία διαθέτουν ξεχωριστές υπηρεσίες εσωτερικών και εξωτερικών Πληροφοριών. Κάτι τέτοιο δεν συνέβαινε στη Σοβιετική Ένωση καθώς η KGB αποτελούσε ενιαίο μεικτό οργανισμό εσωτερικών και εξωτερικών αποστολών. Ακόμα και σήμερα στη Ρωσία και παρά την ύπαρξη της FSB και της SVR, είναι η FSB που μάλλον κάνει κουμάντο στη ρωσική πληροφοριακή κοινότητα. Κάτι παρόμοιο αλλά πιο emphatic φαίνεται να ισχύει και στο παράδειγμα της Κίνας με το Ministry of State Security να αναλαμβάνει το ρόλο του καθοδηγητή των μυστικών υπηρεσιών της χώρας. Αυτό που σε γενικές γραμμές παρατηρείται είναι το εξής: οι μη δημοκρατίες ευνοούν έναν «πληροφοριακό συγκεντρωτισμό», οι, δε, δημοκρατίες έναν «πληροφοριακό αποκεντρωτισμό» με όλα τα συν και τα πλην που οι δύο τάσεις φέρουν καθώς και τους λόγους που επιβάλουν κάτι τέτοιο. Οι πρώτες ενσωματώνουν τις Υπηρεσίες στη διαδικασία λήψης των πολιτικών αποφάσεων με έναν οιονεί δομικό τρόπο, οι δεύτερες τις αξιοποιούν συμβουλευτικά προκειμένου να λάβουν αποφάσεις. Όπως ωστόσο και να δούμε τα πράγματα, με ή χωρίς πολιτικά κριτήρια, διαπιστώνουμε τον σημαίνοντα ρόλο των Υπηρεσιών και πώς αυτός γίνεται καθολικά αποδεκτός από την-ις κρατική-ές ηγεσία-ίες.

Κουλτούρα πληροφοριών στη σύγχρονη ελληνική πολιτική πραγματικότητα. Η ΚΥΠ μέχρι το τέλος της επταετίας των συνταγματαρχών

Η ιστορία των ελληνικών μυστικών υπηρεσιών ξεκινά το έτος 1924 με την ίδρυση του Κέντρου Πληροφοριών Κερκύρας και με σκοπό την αναχαίτιση των ιταλικών κατασκοπευτικών και προπαγανδιστικών ενεργειών στο χώρο της νοτιοανατολικής Μεσογείου· προγενέστερα ο τομέας της συλλογής πληροφοριών ενέπιπτε των αρμοδιοτήτων του Στρατού Ξηράς. Ακολουθεί το 1925 η σύσταση της Υπηρεσίας Ασφαλείας του Κράτους (ΥΑΚ) υπό την Ελληνική Χωροφυλακή. Η εν λόγω Υπηρεσία μετονομάζεται εν έτει 1926 σε Υπηρεσία Γενικής Ασφαλείας του Κράτους (ΥΓΑΚ) αποδίδοντας αρχικά λόγο στον Πρωθυπουργό· μετ' ολίγον υπάγεται εκ νέου στο υπουργείο Εσωτερικών.⁴⁰ Η ΥΓΑΚ καταργείται μέσα στο 1926 μόλις μετά από επτά μήνες λειτουργίας -αποτέλεσμα τούτου η μη ύπαρξη υπηρεσίας Πληροφοριών στον ελληνικό χώρο μέχρι το 1936. Το συγκεκριμένο έτος δημιουργείται η Υπηρεσία Αμύνης του Κράτους με αρμοδιότητα την αντικατασκοπία και τη συλλογή

⁴⁰ Η ΥΓΑΚ είχε γενικές αρμοδιότητες διαφώτισης, αντικατασκοπίας, πάταξης της κομμουνιστικής προπαγάνδας και κατασκοπίας -περί τούτου βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, Παπαζήσης, Αθήνα, 2014, σ. 69

πληροφοριών υπό το υπουργείο Στρατιωτικών και με σκοπό την επίρρωση της κρατικής ασφαλείας. Εν τω μεταξύ ήδη από το 1929 λειτουργεί η Ειδική και Γενική Ασφάλεια προς καταπολέμηση του κομμουνισμού (από την Ειδική Ασφάλεια) όσο και του κοινού εγκλήματος (από τη Γενική Ασφάλεια).⁴¹

Η Υπηρεσία Αμύνης του Κράτους καταργείται και αυτή εντός ενός έτους. Επί κυβερνήσεως Ιωάννου Μεταξά και με τον Αναγκαστικό Νόμο 320/1936 δημιουργείται η Υπηρεσία Αλλοδαπών ως ειδική Διεύθυνση υπαγομένη στο υφυπουργείο Δημοσίας Ασφαλείας και στον περίφημο Κωνσταντίνο Μανιαδάκη. Η συγκεκριμένη Υπηρεσία υπό την ηγεσία του συνταγματάρχη Πυροβολικού Δημητρίου Ξένου φέρει άριστα αποτελέσματα ως προς τον προσπορισμό ζωτικής εθνικής σημασίας πληροφοριών λίγο πριν το ξέσπασμα του Β' Π. Π. αλλά και της ιταλικής επίθεσης.⁴² Ουσιαστικά η Υπηρεσία Αλλοδαπών ασκεί αντικατασκοπία με την κατασκοπία να αποδίδεται σε διπλωματικές και προξενικές αρχές καθώς και στους Στρατιωτικούς Ακολούθους του εξωτερικού.⁴³

Κατά τη διάρκεια της κατοχής οι όποιες πληροφοριακές επιχειρήσεις περνάνε μέσα από Υπηρεσίες που ιδρύονται στο Κάιρο υπό την επίβλεψη, ωστόσο, των Βρετανών. Τέτοιες Υπηρεσίες είναι η Ελληνική Υπηρεσία Πληροφοριών, η Υπηρεσία Ερευνών και Πληροφοριών (ΥΠΕΠ), η Διεύθυνση Ειδικών Υπηρεσιών Πολέμου (ΔΕΥΠ) και η Υπηρεσία Προστασίας Στρατεύματος -ουσιαστικά πρόκειται για μετονομασίες μίας και αυτής Υπηρεσίας και όχι για κάτι διάφορο.⁴⁴

Μετά την απελευθέρωση η Υπηρεσία Προστασίας Στρατεύματος μεταφέρεται στην πατρίδα ή, κατά τον Παύλο Αποστολίδη, επανιδρύεται το 1946. Εν τω μεταξύ οι μόνες οιονεί Υπηρεσίες που παρέμειναν και λειτούργησαν υποτυπωδώς στη χώρα κατά τη διάρκεια της κατοχής ήταν η Διεύθυνση Αλλοδαπών Αθηνών και η Διεύθυνση Αλλοδαπών Θεσσαλονίκης. Το 1948 εν μέσω εμφυλίου πολέμου ανακοινώνεται η ίδρυση Υπηρεσίας Εθνικής Ασφαλείας ενταγμένης στο υπουργείο Δημοσίας Τάξεως -η ανακοίνωση μένει στα λόγια. Την 1^η Μαρτίου 1949 ο αρχιστράτηγος Παπάγος εκδίδει διαταγή βάσει της οποίας συγκροτείται Διεύθυνση Υπηρεσίας Πληροφοριών (ΔΥΠλ) υπαγομένη στον ίδιο και απορροφώντας την Υπηρεσία Προστασίας Στρατεύματος (ΥΠΣ). Η ΔΥΠλ κυρίως εντέλλεται όπως συλλέγει στρατιωτικές πληροφορίες, πληροφορίες πολιτικής φύσεως περί της κατάστασης στα γειτονικά κράτη, πληροφορίες περί του ΚΚΕ και ευρύτερα περί του εσωτερικού κομμουνιστικού κινδύνου. Επίσης εντέλλεται όπως διεξάγει αντικατασκοπευτικές επιχειρήσεις. Μετά την παραίτηση Παπάγου το Μάιο του 1951 η ΔΥΠλ μετονομάζεται, τον Αύγουστο του ίδιου έτους, σε Κεντρική Υπηρεσία Πληροφοριών και Ερευνών (ΚΥΠΕ), υπάγεται, δε, στο ΓΕΕΘΑ. Η αρμοδιότητα της ΚΥΠΕ καλύπτει την εθνική ασφάλεια στο εξωτερικό (sic) και τις αντεθνικές ενέργειες στο εσωτερικό. Αν και η εντολή της φαίνεται διευρυμένη σε σχέση με αυτήν της ΔΥΠλ τίποτα δεν δείχνει ότι παύει να είναι μια αμιγώς στρατιωτική υπηρεσία Πληροφοριών. Εν τέλει ο Παπάγος μετά την ευρεία νίκη του στις εκλογές του Νοεμβρίου του 1952 προχωρεί μέσω του Νομοθετικού Διατάγματος 2421 του

⁴¹ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 63-76

⁴² «Πώς έφτασε η ΕΥΠ στη σημερινή της μορφή. Η ιστορική διαδρομή της Εθνικής Υπηρεσίας Πληροφοριών» στο <http://policenet.gr/article/η-ιστορική-διαδρομή-της-εθνικής-υπηρεσίας-πληροφοριών> όπου καταφύγαμε την 20^η Ιουνίου 2018

⁴³ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 89

⁴⁴ ό. π., σ. 97-108, επίσης βλέπε «Η ιστορική διαδρομή της Εθνικής Υπηρεσίας Πληροφοριών» στην ιστοσελίδα <http://policenet.gr/article/η-ιστορική-διαδρομή-της-εθνικής-υπηρεσίας-πληροφοριών> όπου καταφύγαμε την 20^η Ιουνίου 2018

Μαΐου του 1953 στην ίδρυση της Κεντρικής Υπηρεσίας Πληροφοριών υπαγομένης στον ίδιο.⁴⁵

Αυτό που κυρίως εδώ ενδιαφέρει σχετίζεται με την πορεία και την ιστορία της ΚΥΠ, μετέπειτα ΕΥΠ, εντός του κρατικού ελληνικού συστήματος. Ποια η σχέση της ΚΥΠ με τη CIA; Ποια η στάση της έναντι του κομμουνιστικού κινήματος; Ποιος ο ρόλος της στην επικράτηση της στρατιωτικής χούντας του 1967; Πόσο και προς ποία κατεύθυνση επηρέασε εν γένει η δράση της ΚΥΠ τη σκέψη του εγχωρίου πολιτικού προσωπικού ως προς την αξία της πληροφόρησης; Απέκτησε εν τέλει το μετεμφυλιακό ελληνικό κράτος και η ΚΥΠ / ΕΥΠ γενική και επιχειρησιακή αντιστοίχως κουλτούρα πληροφοριών;

Οι αρμοδιότητες της νεοσύστατης ΚΥΠ, γράφει ο Παύλος Αποστολίδης (Παύλος Αποστολίδης και Σήφης Φιτσανάκης αποτελούν τα μοναδικά πρόσωπα που έχουν μελετήσει επισταμένως την ιστορία της ΚΥΠ / ΕΥΠ), δεν διαφέρουν στην πράξη από εκείνες της ΚΥΠΕ· εσωτερική ασφάλεια, κατασκοπία / αντικατασκοπία αποτελούν τις κύριες κατευθύνσεις με το βάρος να πέφτει στην αντιμετώπιση του κομμουνισμού. Η αλλαγή σε σχέση με την ΚΥΠΕ συνίστατο στον απογαλακτισμό της Υπηρεσίας από το ΓΕΕΘΑ παρά τη διατήρηση της αρμοδιότητας περί την ασφάλεια του στρατεύματος και τη στελέχυσή της, κατά το μάλλον ή ήττον, από αξιωματικούς του Στρατού Ξηράς ⁴⁶ -κατά την έννοια τούτη η ΚΥΠ παύει, έστω φαινομενικά, να αποτελεί μια καθαρά στρατιωτική υπηρεσία Πληροφοριών.⁴⁷ Η άμεση υπαγωγή της στον πρωθυπουργό Αλέξανδρο Παπάγο δημιουργεί υπόνοιες περί δημιουργίας ενός οργάνου μέσω του οποίου θα ασκείται κατά τρόπο απολυταρχικό η πολιτική εξουσία -είναι γεγονός πως οι δημοκρατικές ευαισθησίες του Παπάγου αμφισβητούνται. Στο πνεύμα τούτο, ο στρατηγός Χριστόδουλος Τσιγάντες επικρίνει την υπαγωγή της ΚΥΠ στον πρωθυπουργό αντί του ΓΕΕΘΑ. Ο ίδιος συνεχίζει κριτικάροντας αρνητικά την περί διαφώτισεως αρμοδιότητα αλλά και το δικαίωμα της Υπηρεσίας στην απευθείας συλλογή στοιχείων πέραν, ασφαλώς, του συντονισμού των άλλων κρατικών Υπηρεσιών. Ο στρατηγός ε. α. Αλ. Μερεντίνης απαντά τονίζοντας το απαραίτητο ύπαρξης ενός συντονιστικού πληροφοριακού οργάνου όπως και το απαραίτητο της υπαγωγής της ΚΥΠ στον κυβερνήτη κατά τα πρότυπα της CIA.⁴⁸

Αλλά πώς δημιουργήθηκε η ΚΥΠ; Ο Σήφης Φιτσανάκης γράφει: «Καθ' όλη τη διάρκεια του εμφυλίου πολέμου η ΚΥΠΕ ασχολήθηκε αποκλειστικά με τη δράση της Προσωρινής Δημοκρατικής Κυβέρνησης και του ΔΣΕ. Τέσσερα χρόνια μετά τη λήξη του, το 1953, ο Καραμεσίνης⁴⁹ εισηγείται στον πρωθυπουργό Αλέξανδρο Παπάγο την ίδρυση της ΚΥΠ, η οποία, όπως αναφέρεται και στην ιστοσελίδα της, ...*οργανώθηκε με τη βοήθεια και βάσει του προτύπου της αμερικανικής CIA*. Στην πραγματικότητα, συνεχίζει ο Φιτσανάκης, η ΚΥΠ όχι μόνο κηδεμονευόταν από τη CIA αλλά αποτελούσε κομμάτι της, σε βαθμό, μάλιστα, που ακόμα και οι προαγωγές ή οι τοποθετήσεις ανωτέρων αξιωματικών έπρεπε να εγκριθούν από Αμερικανούς στρατιωτικούς. Επιπλέον, οι μισθοί του προσωπικού καταβάλλονταν από την Ουάσινγκτον δίχως τη μεσολάβηση της ελληνικής κυβέρνησης που, υποθετικά, επέπτενε την ΚΥΠ.⁵⁰ Είναι γεγονός, υποστηρίζει ο μελετητής, ότι την επίταξη των

⁴⁵ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 109-115

⁴⁶ ό. π., σ. 142-143

⁴⁷ Χωρίς βέβαια να λογίζεται πολιτική. Η ΚΥΠ καθίσταται επισήμως πολιτική υπηρεσία, ως ΕΥΠ, το 1986

⁴⁸ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 143

⁴⁹ Πρόκειται για τον Ελληνοαμερικανό αξιωματούχο της CIA Θωμά Καραμεσίνη

⁵⁰ Γράφοντας το 1968 στους *New York Times* ο Ανδρέας Παπανδρέου, έχοντας την πρότερη εμπειρία του επικεφαλής του υπουργείου Προεδρίας και, συνεπώς, του πολιτικά προϊσταμένου της ΚΥΠ, αποκαλύπτει ότι «η ΚΥΠ χρηματοδοτούνταν απευθείας από την CIA και όχι από την ελληνική

ελληνικών υπηρεσιών ασφαλείας από τους Γερμανούς ακολούθησε η σχεδόν ολοκληρωτική τους υποταγή στους Αμερικανούς. Τις πρώτες δεκαετίες του ψυχρού πολέμου η δράση των ελληνικών μυστικών υπηρεσιών εξαρτάται άμεσα από τους πολιτικούς χειρισμούς των ΗΠΑ σε Βαλκάνια και Μέση Ανατολή.⁵¹

Σε κάθε περίπτωση, μας πληροφορεί με τη σειρά του ο Αποστολίδης, το 1953 οι αμερικανικές μυστικές υπηρεσίες αισθάνονται παντοδύναμες εντός της ελληνικής επικράτειας. Μεταξύ αυτών το κλιμάκιο της CIA κατέχει εξέχουσα θέση καθώς, λόγω του Ψυχρού Πολέμου, απολαμβάνει σχεδόν απεριόριστων κονδυλίων και αρμοδιοτήτων.⁵² Η συγκεκριμένη πραγματικότητα ωθεί τις ελληνικές κυβερνήσεις, το Παλάτι, τις Ένοπλες Δυνάμεις όπως και τα Σώματα Ασφαλείας σε προσπάθεια προσεταιρισμού της the Agency είτε χάριν εθνικών είτε χάριν προσωπικών συμφερόντων και σκοπιμοτήτων. Ήταν λοιπόν αναμενόμενο να δημιουργηθούν πρωτίστως στενές σχέσεις μεταξύ της ελληνικής ΚΥΠ και του εν Ελλάδι ευρισκομένου κλιμακίου της CIA με το τελευταίο να συνδράμει αλλά και να κατευθύνει τις δραστηριότητες της πρώτης.⁵³ Από την πλευρά της η ηγεσία της ΚΥΠ

κυβέρνηση [...] Η ΚΥΠ ήταν παράρτημα του ξένου χρηματοδότη της και ούτε εγώ ο ίδιος ούτε οι συνάδελφοί μου ήταν δυνατό να την ελέγξουμε αποτελεσματικά». Τέσσερα χρόνια αργότερα μιλώντας σε αμερικανική εκπομπή καταθέτει την έκπληξη που δοκίμασε όταν αντιλήφθηκε ότι «η ΚΥΠ ενεργούσε οικονομικά και διοικητικά ως παράρτημα της CIA». Και συνέχισε; «Δεν είχαμε καν τη δυνατότητα να την εμποδίσουμε να παρακολουθεί τα υπουργικά μας τηλέφωνα». Σε άλλο σημείο ο Παπανδρέου καταθέτει πως «δεν υπήρχε καμία μορφή διάκρισης μεταξύ των δύο Υπηρεσιών. Συνδύαζαν τις λειτουργίες τους σε μια αλληλένδετη σχέση υποκατάστασης. Στην πραγματικότητα ενεργούσαν ως μία και μοναδική Υπηρεσία» -περί τούτων βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, Ποταμός, Αθήνα, 2015, σ. 94-95, 102-103, επίσης, Deane Philip, *I Should Have Died*, Athenaeum Publishers, New York, 1977, σ. 92

⁵¹ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 100

⁵² Ο Ανδρέας Παπανδρέου καταθέτει πως εν έτει 1960 και ενώ εργαζόταν ως σύμβουλος της Τραπέζης της Ελλάδος δέχτηκε πρόσκληση από τον Λάφλιν Κάμπελ, σταθμάρχη της CIA στην Αθήνα. Ο τελευταίος απαίτησε τη συνδρομή του όπως πείσει τον πατέρα του Γεώργιο περί μίας κατευθυνομένης από τη CIA τροποποίησης του εκλογικού νόμου με σκοπό τη φαλκίδευση των πολιτικών δικαιωμάτων της αριστεράς. Όταν ο Ανδρέας Παπανδρέου ανταπάντησε ότι ο πατέρας του ουδέποτε θα εδέχετο κάτι τέτοιο, ο Κάμπελ αντέδρασε λέγοντας: «Πείτε στον πατέρα σας ότι η CIA πετυχαίνει εκείνο που θέλει». Το συγκεκριμένο περιστατικό, γράφει ο Φιτσανάκης, αποδεικνύει την έκταση της αμερικανικής κυριαρχίας στην μετεμφυλιακή Ελλάδα. Μια κυριαρχία που παγιώνεται μέσω της μόνιμης παρουσίας αμερικανικών στρατευμάτων στην χώρα και της CIA. Σημαίνει δε τερματισμό οποιασδήποτε ανεξάρτητης πορείας της Αθήνας σε θέματα όχι μόνο εξωτερικής αλλά και εσωτερικής πολιτικής -για μια άποψη βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 95-97

⁵³ Σε ό,τι αφορά την κατασκοπευτική δράση, ΚΥΠ και CIA συνεργάστηκαν στη συλλογή πληροφοριών από γειτονικές χώρες. Οι πληροφορίες προσπορίζονταν κυρίως από φυγάδες του παραπετάσματος ή αποτελούσαν προϊόν υποκλοπής τηλεπικοινωνιών. Επιπλέον, η ΚΥΠ διαθέτει μια ιδιαιτέρως πολύτιμη δυνατότητα, τη συλλογή πληροφοριών περί σοβιετικών κινήσεων στο Αιγαίο αλλά και στη Μαύρη Θάλασσα μέσω στρατολόγησης, σε συνεργασία με το Λιμενικό Σώμα, πληρωμάτων του ελληνικού εμπορικού ναυτικού. Από τη μεριά της η CIA χρηματοδοτεί την κατασκευή υποδομών, παρέχει, δε, τεχνικό εξοπλισμό για τη συλλογή στρατιωτικών πληροφοριών από τις βόρειες γειτονικές χώρες -για μια άποψη βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 166-167. Πάντως, μας πληροφορεί ο Σήφης Φιτσανάκης, οι επιχειρήσεις διείσδυσης των ΚΥΠ και CIA στο παραπέτασμα μάλλον δεν 'έτρεξαν' και τόσο καλά. Εκτός της ύπαρξης του διπλού, υπέρ των Σοβιετικών, πράκτορα Κιμ Φίλμιπ που πρόδιδε αφειδώς τους δυτικούς σχεδιασμούς, κακό σύμβουλο απετέλεσε η αλαζονεία και υπεροψία των ανθρώπων της CIA έναντι των Ελλήνων συναδέλφων τους. Π. χ., άγνωστο είναι πόσα ακριβώς στελέχη της ΚΥΠ συνελήφθησαν και εκτελέστηκαν από τις αλβανικές αρχές. Γνωρίζουμε ωστόσο πως ένα από αυτά τα στελέχη υπήρξε ο Γρηγόριος Σταύρου εκτελεσθείς εν έτει 1953 από το καθεστώς Χότζα -για περισσότερες λεπτομέρειες βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 97-98

προσπάθησε κάποιες φορές να περιορίσει τη διείσδυση της αμερικανικής Υπηρεσίας στην ελληνική δημόσια σφαίρα.⁵⁴ Κάτι τέτοιο ωστόσο δεν ήταν καθόλου εύκολο αρκεί να αναλογιστούμε τη σχέση που ανέπτυξε ο κατά καιρούς Σταθμάρχης της the Company τόσο με τη βασιλική οικογένεια όσο και με το εκάστοτε κομματικό προσωπικό.⁵⁵

Στον εσωτερικό χώρο, η ΚΥΠ, υπό τον πρώτο αρχηγό της συνταγματάρχη Αλέξανδρο Νάτσινα, είχε ως κύρια ενασχόληση τη συλλογή και αρχειοθέτηση στοιχείων για Έλληνες πολίτες που εθεωρούντο αριστεροί. Απώτερο σκοπό απετέλεσε το μπλοκάρισμά τους σε περίπτωση που τους εδίδετο κάποια ευκαιρία να εισέλθουν στον κρατικό μηχανισμό. Ασφαλώς ενδιέφερε τα μέγιστα «η αποκάλυψης πάσης κομμουνιστικής κινήσεως σημειουμένης εντός των Ενόπλων Δυνάμεων» ένα από τα ανερχόμενα στελέχη της ΚΥΠ στον αντικομμουνιστικό αγώνα απετέλεσε ο μετέπειτα πρωταγωνιστής του στρατιωτικού πραξικοπήματος του 1967 Γεώργιος Παπαδόπουλος. Στα τέλη της δεκαετίας του 1950 τα πληροφοριακά δίκτυα του Νάτσινα είχαν εξαπλωθεί στο σύνολο της χώρας, αποτελούντο, δε, από 1500 αξιωματικούς και χιλιάδες πράκτορες.^{56, 57}

Σε κάθε περίπτωση γεγονός είναι πως η πολιτική κομμουνιστική δραστηριότητα απετέλεσε στόχο της ΕΥΠ με την έναρξη της λειτουργίας της. Εν έτει 1953 συζητείται η νομιμοποίηση ή όχι του ΚΚΕ και της ΕΔΑ. Η νομιμοποίηση του πρώτου απορρίπτεται, ωστόσο, δεν προκρίνεται η διάλυση της ΕΔΑ. Αυτό δεν σημαίνει πως η τελευταία θα αφεθεί να λειτουργήσει απρόσκοπτα καθώς, σύμφωνα με τον Αποστολίδη, προτείνεται η καταδίωξη των κορυφαίων στελεχών της από την Αστυνομία, η υποβολή μηνύσεων κατά της εφημερίδας *Αυγή* και η δημιουργία προϋποθέσεων για μελλοντική διάλυση του κόμματος. Εντός του ιδίου έτους, η ΕΥΠ ζητά πληροφορίες από τις αστυνομικές αρχές περί των όποιων σεκταριστικών τάσεων μέσα στο ΚΚΕ με σκοπό την ενθάρρυνση αποσχιστικών κινήσεων και κατά συνέπεια την αποδυνάμωση της συνδεδεμένης μ' αυτό ΕΔΑ.⁵⁸

Στις 17 Νοεμβρίου 1953 συγκαλείται από την ΚΥΠ το Συμβούλιο Πληροφοριών με αντικείμενο την αριστερή προπαγάνδα. Αναφέρονται ονόματα δημοσιογράφων που είχαν μεταβεί στη ΕΣΣΔ ύστερα από κρατική σοβιετική πρόσκληση. Επίσης αναφέρονται ονόματα εκδοτών, συγγραφέων κ. λ. με υποτιθέμενες αριστερές πεποιθήσεις. Προτείνονται διάφορα μέτρα πίεσης, μεταξύ αυτών και ο επισταμένος φορολογικός έλεγχος. Η επιτυχία της συνεργασίας αριστεράς-κεντροαριστεράς στις δημοτικές εκλογές του Νοεμβρίου του 1954 δίδει αφορμή για νέες συσκέψεις. Σ' αυτές μετέχουν τόσο κυβερνητικά στελέχη όσο στελέχη από τις ένοπλες δυνάμεις, τη χωροφυλακή και ασφαλώς την ΚΥΠ. Πλέον ακραίο μέτρο φαντάζει η υποχρεωτική

⁵⁴ Είναι αλήθεια πως η ΚΥΠ κινήθηκε από την αρχή με σκοπό να θέσει όρια στη συνεργασία της με τη CIA, να περιστείλει την ανεξέλεγκτη δράση της τελευταίας. Π. χ. τον Οκτώβριο του 1962 τα κεντρικά της ελληνικής Υπηρεσίας δίδουν εντολή σε περιφερειακή μονάδα της Βορείου Ελλάδος όπως αυτή μην αποδίδει στοιχεία περί επαναπατριζομένων Ελλήνων προσφύγων στο τοπικό κλιμάκιο της CIA. Σκοπός της εντολής ήταν η απομείωση δυνατότητας αυτόνομης δράσης εκ μέρους των Αμερικανών μέσω απευθείας στρατολόγησης επαναπατριζομένων -περί τούτου βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 166

⁵⁵ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 165-166

⁵⁶ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 98-99

⁵⁷ Κάπου εδώ εμφανίζεται ένας από τους λόγους τριβής μεταξύ ΚΥΠ και CIA. Η τελευταία φέρεται να διατηρεί το δικό της δίκτυο πληροφοριοδοτών στον σχετικό ελληνικό μηχανισμό αλλά και στο Παλάτι. Αυτό δεν της αρκεί. Απαιτεί άμεση επαφή με τους πληροφοριοδότες της ΚΥΠ, τους οποίους, μάλιστα, επιθυμεί να χρηματοδοτεί η ίδια -για μια άποψη βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 99

⁵⁸ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 146-147

καθιέρωση υποβολής περιοδικής αναφοράς εκάστου δημοσίου υπαλλήλου περί τη συμβολή του στον αντικομμουνιστικό αγώνα.⁵⁹

Στις εκλογές του Φεβρουαρίου του 1956 η ΕΔΑ εντάσσεται στον κεντροαριστερό σοσιαλδημοκρατικό συνασπισμό της Δημοκρατικής Ένωσης. Η πορεία της Ένωσης ανησυχεί την ΚΥΠ. Η τελευταία κάνει προτάσεις που κινούνται στην κατεύθυνση της διαφώτισης του λαού, της δημιουργίας εθνικιστικών οργανώσεων και του εκτοπισμού των πλέον επικινδύνων στελεχών του ΚΚΕ. Παρά το ότι η Δημοκρατική Ένωση λαμβάνει περισσότερους ψήφους από την ΕΡΕ, είναι η ΕΡΕ που κερδίζει την πλειοψηφία των εδρών. Ο Τύπος καταγγέλλει βία και νοθεία με τον Καραμανλή να επιβεβαιώνει εμμέσως ρίχνοντας το βάρος στην ΚΥΠ και προσωπικά στον Νάτσινα.⁶⁰

Στις εκλογές του Μαΐου του 1958 η ΕΔΑ κατεβαίνει αυτόνομα κερδίζοντας τη δεύτερη θέση με 24,4%. Η ΚΥΠ εξακολουθεί να ανησυχεί επαναδιατυπώνοντας προτάσεις περιορισμού της αριστεράς και επισημαίνοντας το γεγονός της μη αποδοχής των έως τότε προτεινομένων της από τις κυβερνήσεις της δεξιάς. Οι εκθέσεις της Υπηρεσίας παρουσιάζονται κατά τι πιο αισιόδοξες την επόμενη χρονιά καθώς επιτυγχάνεται ο περιορισμός της δυναμικής της ΕΔΑ. Σ' αυτό συντελούν μέτρα κατά των στελεχών του ΚΚΕ (δίκη Μανώλη Γλέζου) αλλά και μια ικανή κυβερνητική προπαγάνδα υπό τον στρατηγό, πλέον, Νάτσινα και, κυρίως, του υπουργείου Προεδρίας.⁶¹

Οι προσπάθειες της ΚΥΠ συνεχίζονται βάσει της ίδρυσης ενός νέου εκτελεστικού οργάνου. Πρόκειται για την Υπηρεσία Ειδικών Μελετών (ΥΕΜ). Σημείωμα της ΥΕΜ/ΚΥΠ, εν έτει 1961, αναφέρεται στην υπ' αυτήν έκδοση μελετών σε χιλιάδες αντίτυπα προκειμένου πάταξης των αριστερών ιδεών («Η ανθελληνική προπαγάνδα των Σλαύων για το Μακεδονικό Ζήτημα», «Η Μακεδονία και η Βουλγαρία», «Η Γιουγκοσλαβία και η Μακεδονία», «Η Ρωσία και η Μακεδονία», «Το ΚΚΕ και Βόρεια Ήπειρος»).⁶² Αλληλογραφία μεταξύ ΓΕΕΘΑ και ΚΥΠ αποκαλύπτει προτάσεις της δεύτερης έπειτα ερωτημάτων του πρώτου. Οι προτάσεις υποβλήθηκαν τον Φεβρουάριο του 1961 περιλαμβάνοντας: α) δραστηριοποίηση ανωτάτων οργάνων διαφώτισης, β) εξυγίανση κρατικού μηχανισμού, γ) οικονομικά μέτρα προς όφελος των ασθενεστέρων, δ) ενίσχυση των σωμάτων ασφαλείας, ε) εξουδετέρωση πολιτικών-οργανωτικών στελεχών του ΚΚΕ, στ) περιορισμό της κυκλοφορίας αριστερόστροφων εντύπων, ζ) συνεργασία με κόμματα της εθνικόφρονης αντιπολιτεύσεως, η) χρησιμοποίηση εφένδρων αξιωματικών, θ) δραστηριοποίηση κυβερνητικών βουλευτών.⁶³

Ο σχεδιασμός της κυβερνητικής διαφώτισης συνεχίστηκε μετά τις εκλογές του Οκτωβρίου του 1961 με την ΚΥΠ να καταρτίζει το απαραίτητο καταστατικό περί ίδρυσης φοιτητικών συλλόγων σε Αθήνα και Θεσσαλονίκη υπό την καθοδήγηση της Γενικής Ασφάλειας Αθηνών και της Αστυνομίας Θεσσαλονίκης αντιστοίχως. Εν έτει 1962 η Υπηρεσία παίζει καθοριστικό ρόλο στη διαμόρφωση της κρατικής πολιτικής περί επαναπατρισμού ή μη των πολιτικών προσφύγων που μετά τον ελληνικό εμφύλιο κατέφυγαν κατά κύριο λόγο σε χώρες του παραπετάσματος. Η ΚΥΠ είναι σταθερά

⁵⁹ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 147-148

⁶⁰ ό. π., σ. 148

⁶¹ ό. π., σ. 149-150

⁶² ό. π., σ. 151-152

⁶³ ό. π., σ. 152-153. Πάντως δεν διευκρινίζεται επαρκώς τι νοείται με τη λέξη 'εξουδετέρωση', επίσης δεν διευκρινίζεται πώς θα αξιοποιούνταν οι έφεδροι αξιωματικοί

αντίθετη σε ομαδικές παλιννοστήσεις. Η θέση της επικρατεί με μόνη εξαίρεση τους στρατιωτικούς αιχμαλώτους.⁶⁴

Η έλευση του Γεωργίου Παπανδρέου στη διακυβέρνηση της χώρας τον Φεβρουάριο του 1964 αναγκάζει την ΚΥΠ να παύσει τις δραστηριότητές της περί αντιμετώπισης της εσωτερικής κομμουνιστικής απειλής -αυτό δεν ισχύει για την έξωθεν αντίστοιχη. Τον Αύγουστο του 1964 ενημερώνει το υπουργείο Εξωτερικών για τις προσπάθειες του ΑΚΕΛ να εισδύσει στον κρατικό μηχανισμό. Τον Ιανουάριο του 1965 κατηγορεί το κυπριακό κόμμα για προσπάθεια διαβολής των Ελλήνων αξιωματικών. Το Μάιο του 1965 γίνεται αναφορά στις δυνατότητες της Νεολαίας Λαμπράκη στη Γερμανία όπως και στην παρουσία φίλα κείμενων στην αριστερά προσώπων που υπηρετούν στο ελληνικό εμπορικό ναυτικό.

Μετά την παραίτηση της κυβέρνησης Παπανδρέου τον Ιούλιο του 1965, η ΚΥΠ επανακάμπτει δριμύτερη παρουσιάζοντας τον κομμουνισμό ως εθνική απειλή. Προτείνει την επαναφορά των εκτάκτων μέτρων ασφαλείας και ιδιαίτερα του Α.Ν. 375/1936 «περί τιμωρίας των εγκλημάτων κατασκοπίας και των εγκληματικών ενεργειών των απειλουσών την εξωτερικήν ασφάλειαν της χώρας», ενώ με έκθεσή της περιγράφει την αριστερή δραστηριότητα στο χώρο της διανοήσης. Το Μάρτιο του 1966 συγκαλείται εις διπλούν Συμβούλιο Υπουργών. Εκ των εισηγητών και η ΚΥΠ. Περιγράφεται η κομμουνιστική δυναμική, αναφέρεται η αύξηση του αριθμού των μελών του αριστερού κινήματος, προτείνεται, δε, η ίδρυση Κέντρου Εθνικής Διαφώτισης. Καθ' όλη τη διάρκεια του 1966 η ΚΥΠ εκδίδει μηνιαία δελτία ενημέρωσης των κρατικών οργανισμών περί κομμουνιστικών δραστηριοτήτων. Το 1967 η προσοχή της ΚΥΠ επικεντρώνεται στην ΕΔΑ, στο ΚΚΕ αλλά και σε κάποιες δεξιές παρακρατικές οργανώσεις. Η Υπηρεσία πιστεύει ότι ο Ανδρέας Παπανδρέου επηρεάζει τα σώματα ασφαλείας. Επιπλέον υποστηρίζει ότι η Αστυνομία Πόλεων έχει περιπέσει σε αδράνεια όσον αφορά στην καταδίωξη των αριστερών. Τέλος, τέσσερεις μέρες πριν το στρατιωτικό πραξικόπημα πραγματοποιείται σύσκεψη μεταξύ της ΚΥΠ και της Γενικής Διεύθυνσης Εθνικής Ασφαλείας (ΓΔΕΑ). Σκοπό αποτελεί ο επανακαθορισμός αρμοδιοτήτων. Η ΓΔΕΑ εντέλλεται περί τη συλλογή πληροφοριών και την υποβολή προτάσεων για τον εσωτερικό κομμουνισμό, ενώ η ΚΥΠ περί την κατασκοπία / αντικατασκοπία και περί εθνικών θεμάτων. Δεν γνωρίζουμε γιατί αποκλείστηκε η ΚΥΠ από την ενασχόληση με την αριστερά της χώρας. Κατά τον Αποστολίδη μάλλον βρισκόταν σε ισχύ μια συμφωνία κυρίων που, ωστόσο, παραβιάζονταν συστηματικά από την ΚΥΠ· αυτή η συμφωνία επαναβεβαιώνεται. Πάντως από τα έγγραφα που βρέθηκαν δεν τεκμαίρεται κάποιος ρόλος της ΚΥΠ στην διόγκωση των πληροφοριών περί κομμουνιστικού κινδύνου.⁶⁵

Εν τω μεταξύ την 21^η Απριλίου 1967 αναλαμβάνει πραξικοπηματικά τη διακυβέρνηση της χώρας ο στρατός. Η ΚΥΠ ήδη από 27^{ης} Φεβρουαρίου έχει προβεί σε εκτίμηση της πολιτικής κατάστασης. Σύμφωνα με αυτήν, αριστερά και κεντροαριστερά έχουν εκτοξεύσει την λαοφιλία τους, η, δε, συνολική εκλογική δύναμη της δεξιάς περιορίζεται σε ένα 40%. Κατά την ΚΥΠ μια επιστροφή της Ένωσης Κέντρου θα ήτο καταστροφική οδηγώντας στην κομμουνιστοποίηση τη χώρα. Πάρα ταύτα ουδέν τεκμήριο υπάρχει που να βεβαιώνει την εισήγηση από πλευράς ΚΥΠ μιας στρατιωτικής επέμβασης. Τουναντίον, ο αρχηγός της Υπηρεσίας στρατηγός Κυριάκος Παπαγεωργόπουλος αποκλείει σε διάφορες συζητήσεις ένα κίνημα των ενόπλων δυνάμεων με το επιχείρημα πως βασιλιάς και στρατηγοί ουδόλως επιθυμούν κάτι τέτοιο. Ήταν όμως ειλικρινής ως προς την εκτίμηση; Το

⁶⁴ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 154-155

⁶⁵ ό. π., σ. 185-190

ερώτημα γεννάται διότι σε μεταγενέστερη επιστολή του σημειώνει πως το Ανώτατο Στρατιωτικό Συμβούλιο έχει λάβει απόφαση στρατιωτικής επέμβασης για την 22^α Απριλίου. Εντούτοις ο Παπαδόπουλος και η ομάδα του προλαβαίνουν την ανωτάτη ηγεσία που σκοπό είχε να αποδώσει εκ νέου την εξουσία στους πολιτικούς, κάτι το οποίο επουδενί επιθυμούν οι κινηματίες της 21^{ης} Απριλίου.⁶⁶

Τα πράγματα περιπλέκονται εάν λάβουμε υπόψη τις μελέτες του Σήφη Φιτσανάκη. Ο Φιτσανάκης υιοθετεί την άποψη πως η CIA γνωρίζει περί των προθέσεων της ομάδας Παπαδόπουλου, ωστόσο, δεν τη θεωρεί ικανή όπως μετουσιώσει την πρόθεση σε πράξη. Ουσιαστικά οι Αμερικανοί έχουν στραμμένη την προσοχή τους αλλού. Υποθέτουν την περίπτωση πραξικοπήματος όχι όμως από τους συνταγματάρχες αλλά από τη λεγόμενη 'μεγάλη χούντα'. Ο όρος χρησιμοποιείται για να περιγραφεί η πρόθεση του Παλατιού αλλά και της δεξιάς να προβούν σε στρατιωτικό πραξικόπημα προκειμένου να ανακοπεί η επάνοδος της Ένωσης Κέντρου στην εξουσία. Κατά τον Φιτσανάκη, που βασίζεται μάλιστα σε απομνημονεύματα του Κυριάκου Παπαγεωργόπουλου, ο βασιλιάς Κωνσταντίνος ήδη από τον Φεβρουάριο του 1965 ξεκινά συζητήσεις με την ανωτάτη στρατιωτική ηγεσία με σκοπό την αποτροπή, έστω και μέσω συνταγματικής εκτροπής, της νίκης της Ένωσης Κέντρου στις επερχόμενες εκλογές και την πιθανή συνεργασία της με την ΕΔΑ.⁶⁷ Στις 12 Απριλίου 1967, ο Κωνσταντίνος δηλώνει στον Αμερικανό πρέσβη στην Αθήνα Φίλιπ Τάλμποτ πως βρίσκεται προ διλήμματος, είτε να παραδώσει την Ελλάδα στους Παπανδρέου, είτε να εγκαθιδρύσει δικτατορία. Λίγες μέρες ενωρίτερα ο πρωθυπουργός Παναγιώτης Κανελλόπουλος έχει διαβεβαιώσει τον Τάλμποτ πως «δεν θα παραδώσουμε το έθνος στους κομμουνιστές ή στον Ανδρέα Παπανδρέου».⁶⁸ Τελικά δικτατορία επεβλήθη, όχι όμως από το Παλάτι, τη δεξιά ή την στρατιωτική ηγεσία αλλά από μια ομάδα συνταγματάρχων, τη λεγόμενη 'μικρή χούντα' που ενώ κινείτο εντός των κόλπων της αντίστοιχης 'μεγάλης' χαρακτηριζόταν όχι μόνο από αντικομμουνισμό αλλά και από έναν υποβόσκων, όπως σημειώνει ο Λεωνίδας Καλλιβρετάκης, αντιμοναρχισμό.⁶⁹ Το συγκεκριμένο χαρακτηριστικό ασφαλώς διαχωρίζει τους κινηματίες από τον κορμό της ΚΥΠ, ο οποίος, ιδιαίτερα επί διοικήσεως Παπαγεωργόπουλου, ήτο φιλοβασιλικός. Αυτό δεν σημαίνει, τονίζει ο Φιτσανάκης, πως η ΚΥΠ δεν συμμεριζόταν τις βλέψεις των πραξικοπηματιών. Ωστόσο οι της μικρής χούντας, που ουσιαστικά πρόλαβαν εκείνους της μεγάλης, δεν απήλαυσαν τη στήριξη της ΚΥΠ τη νύχτα της 21^{ης} Απριλίου παρά το ότι κάποια στελέχη της, και πρώτος απ' όλους ο Γεώργιος Παπαδόπουλος, υπηρέτησαν στις τάξεις της.⁷⁰

Εν κατακλείδι τόσο ο Αποστολίδης όσο και ο Φιτσανάκης καταλήγουν στο ότι η ΚΥΠ δεν έπαιξε κάποιο ρόλο στην επιτυχία του πραξικοπήματος -τα διαθέσιμα στοιχεία τους επιβεβαιώνουν. Το πραξικόπημα υπήρξε αποκλειστικά προϊόν του υπουργείου Αμύνης. Τέλος και όσον αφορά στις 8.500 συλλήψεις, κυρίως στην Αθήνα, τις πρώτες ώρες, αυτές πραγματοποιήθηκαν από την Αστυνομία Πόλεων και

⁶⁶ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 191-193

⁶⁷ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 110, επίσης, Παπαγεωργόπουλος Κυριάκος, *Μνήμες πολέμου και ειρήνης*, τόμος Β', Δήλος, χ. τ., 1995, σ. 389-390

⁶⁸ Καλλιβρετάκης Λεωνίδας, «Η ομάδα Παπαδόπουλου στην τελική ευθεία προς την εξουσία» στο *Η στρατιωτική δικτατορία 1967-1974*, επιμ. Καραμανωλάκης Βαγγέλης, ΔΟΛ, Αθήνα, 2010, σ. 59-84

⁶⁹ *ibid*

⁷⁰ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 111-112

την Ελληνική Χωροφυλακή χωρίς τη συμβολή της ΚΥΠ ⁷¹, βασίζονταν, δε, αποκλειστικά σε καταλόγους υπόπτων που είχαν συνταχθεί από το ΓΕΣ με στόχο «την αποτροπή εσωτερικών κινδύνων και ταραχών».⁷²

Αλλά ποια η στάση της Υπηρεσίας κατά τη διάρκεια της χούντας; Όπως αναφέρεται στην ιστοσελίδα της ΚΥΠ ...*Οι επιπτώσεις στο εσωτερικό πεδίο με την κατάλυση του κοινοβουλευτικού πολιτεύματος, είχαν ανάλογο αντίκτυπο τόσο στην οργάνωση, όσο και στη λειτουργία και αποστολή της τότε ΚΥΠ, η οποία κατέστη, ως ένα βαθμό, όργανο των προσωπικών επιδιώξεων των συνταγματαρχών που διοίκησαν τη χώρα επί 7 σχεδόν χρόνια.* ⁷³ Ουσιαστικά η ΚΥΠ, γράφει ο Φιτσανάκης, μετατράπηκε σε όργανο ασφαλείας υπόλογο στον πρωθυπουργό, ωστόσο, η πολιτική αστυνόμευση ανατέθηκε κυρίως στον στρατό και στην αστυνομία, και όχι στην ΚΥΠ. Η Υπηρεσία συνεισέφερε με διάθεση πρακτόρων, επίσης με συλλογή πληροφοριών περίξ των αντιστασιακών οργανώσεων χωρίς ωστόσο τα καλύτερα αποτελέσματα κυρίως λόγω ανικανότητας ηγετικών στελεχών. Με λίγα λόγια αν και η δράση της κατά την επταετία 1967-1974 αντανάκλα τον δικτατορικό χαρακτήρα του καθεστώτος, δεν φαίνεται παρά μια δευτερεύουσα, και σε πολλές περιπτώσεις ασήμαντη, συνεισφορά της στη διατήρηση των πραξικοπηματιών στην εξουσία. Αυτό διαπιστώνεται ιδιαίτερα σε σύγκριση με τη δράση των ενόπλων δυνάμεων και των αστυνομικών αρχών καθόσον απετέλεσαν το κύριο τμήμα του μηχανισμού πολιτικής καταστολής κατά τη διάρκεια της χούντας.⁷⁴

Κατά τι διαφορετική, όσον αφορά την έκταση μάλλον και όχι τόσο την ποιότητα των ενεργειών, αποτυπώνεται η εκτίμηση του Παύλου Αποστολίδη. Σύμφωνα με τον πρώην διοικητή της ΕΥΠ, η ΚΥΠ καταγράφει, σχεδόν με την επιβολή του πραξικοπήματος, τις αντιδράσεις κατά των κινηματιών, αντιδράσεις που ξεκινούν εντός του καθεστώτος από δυσαρεστημένα μέλη. Η ΚΥΠ όπως και οι απριλιανοί φέρονται ενήμεροι για τις βασιλικές προθέσεις αντιπραξικοπήματος τη στιγμή που η Υπηρεσία ενημερώνει τους αρμοδίους φορείς τόσο για αντιστασιακές κινήσεις και οργανώσεις στο εξωτερικό όσο και για τις κινήσεις του ΚΚΕ. Κατά τα έτη 1968 και 1969 συμμετέχει σε ανακρίσεις αντιφρονούντων. Ιδιαίτερο ρόλο διαδραμάτισε στην ανάκριση του τέως βουλευτή του ΚΚΕ Γιώργη Τσαρουχά στη Θεσσαλονίκη, ωστόσο, εδώ η υπόθεση κατέληξε τραγικά με το θάνατο του εν λόγω βουλευτή προφανώς λόγω βασανιστηρίων. Το 1969 ξεκινά η αποστολή εκ μέρους της ΚΥΠ ενημερωτικών δελτίων περί διεθνούς και εσωτερικού κομμουνισμού· τα δελτία προωθούνται σε ευρύ κύκλο παραληπτών μεταξύ των οποίων και οι ελληνικές πρεσβευτικές αρχές στη δυτική Ευρώπη. Την ίδια χρονιά γίνεται αντιληπτή η λειτουργία κέντρου στρατιωτικής εκπαίδευσης ημεδαπών κομμουνιστών στη Βράτσα της Βουλγαρίας, η εν λόγω δραστηριότητα δεν κρίνεται σοβαρή. Εν τω μεταξύ συνεχίζεται η παρακολούθηση υπόπτων για αντικαθεστωτική δράση. Το 1970 το ενδιαφέρον επικεντρώνεται στη δράση του Πανελληνίου Απελευθερωτικού Κινήματος (ΠΑΚ), του Πανελληνίου Αντιδικτατορικού Μετώπου (ΠΑΜ), δημοσιογράφων και φοιτητών. Το 1971 αποστέλλεται στις αρχές ασφαλείας της χώρας έκθεση της Υπηρεσίας σχετική με τις αντιστασιακές οργανώσεις του εσωτερικού. Η έκθεση καλύπτει τα έτη

⁷¹ Καλλιβετάκης Λεωνίδας, «Η ομάδα Παπαδόπουλου στην τελική ευθεία προς την εξουσία» στο *Η στρατιωτική δικτατορία 1967-1974*, ό. π., επίσης, Κάτρης Γιάννης, *Η γέννηση του νεοφασισμού στην Ελλάδα*, Παπαζήσης, Αθήνα, 1974, σ. 44

⁷² Καλλιβετάκης Λεωνίδας, «Η ομάδα Παπαδόπουλου στην τελική ευθεία προς την εξουσία» στο *Η στρατιωτική δικτατορία 1967-1974*, ό. π.

⁷³ <http://www.nis.gr/portal/page/portal/NIS/History/Diktatoria/> (με ημερομηνία καταφυγής την 29^η Ιουνίου 2018)

⁷⁴ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 119-120

1967-1970, συμπληρώνεται, δε, το έτος 1972 για το διάστημα μέχρι και τον Ιούνιο της συγκεκριμένης χρονιάς, μάλλον δεν προκύπτουν ιδιαίτερα ή, τέλος πάντων, αρκούντως ανησυχητικά ευρήματα. Το 1972 η προσοχή της στρέφεται εκ νέου στις οργανώσεις του εξωτερικού. Το 1973 η δράση της ΚΥΠ περιορίζεται μάλλον σε εκτιμήσεις περίξ των αντιδρώντων και των φοιτητικών κινητοποιήσεων. Ο Αποστολίδης γράφει ότι η Υπηρεσία ανέμενε δυναμική δράση της φοιτητώσας νεολαίας, σε αντίθεση με τον Φιτσανάκη που υποστηρίζει ότι η συλλογή πληροφοριών για τις αντικαθεστωτικές κινήσεις δεν ήταν επαρκής. Η δραστηριότητα των διαφόρων οργανώσεων στο εξωτερικό αναφέρεται σε έκθεση του Ιανουαρίου του 1974 προς το Αρχηγείο Ενόπλων Δυνάμεων. Ακολουθούν παρόμοιες εκθέσεις, για εξωτερικό και εσωτερικό καθ' όλο το έτος, τέλος, η Υπηρεσία προτείνει τη λήψη αντιμέτρων εκτός Ελλάδος.⁷⁵

Σε κάθε περίπτωση εκ των άνω στοιχείων δεν προκύπτει κάποια εντυπωσιακή πρωτοβουλία της ΚΥΠ υπέρ της διασφάλισης του απριλιανού καθεστώτος. Η Υπηρεσία έδρασε στα πλαίσια της προστασίας του πολιτικού περιβάλλοντος εντός του οποίου λειτουργούσε. Ασφαλώς οι πολιτικές συνθήκες κάθε άλλο παρά ομαλές υπήρξαν, ωστόσο, δεν αποτελεί καθήκον μιας υπηρεσίας Πληροφοριών να στρέφεται κατά του πολιτικού συστήματος της χώρας που υπηρετεί ακόμα και αν αυτό είναι αυταρχικό ή δικτατορικό.

Εν κατακλείδι και απαντώντας σε κάποια από τα ερωτήματά μας σημειώνουμε πως κατά την περίοδο 1953-1974: α) η σχέση της ΚΥΠ με την CIA υπήρξε θέλοντας και μη στενή λόγω των πολιτικών συνθηκών της εποχής. Η ΚΥΠ απέτελεσε ίσως όμηρό της. Προσπάθησε κάποιες στιγμές να ανεξαρτητοποιηθεί, ωστόσο, η επιρροή των Αμερικανών στο όλο ελληνικό πολιτικό σύστημα ήταν ιδιαιτέρως βαρύνουσα -θυμίζουμε το, έστω από 1950, απόφθεγμα του Γεωργίου Παπανδρέου «η Ελλάς αναπνέει σήμερα με δύο πνεύμονας, τον μεν αγγλικόν, τον δε αμερικανικόν» με αφορμή το κυπριακό αίτημα ένωσης, β) η στάση της ΚΥΠ έναντι του κομμουνιστικού κινήματος υπήρξε ολοφάνερα εχθρική. Πρόκειται για κάτι καθόλα αναμενόμενο. Δεν πρέπει άλλωστε να λησμονάμε την απαγόρευση λειτουργίας του ΚΚΕ ήδη από το 1947 ως συνωμοτική αντεθνική οργάνωση από την κυβέρνηση του, μάλιστα, φιλελεύθερου Θεμιστοκλή Σοφούλη. Η καταδίωξη των αριστερών ήλθε ως πράξη πολιτική και ουδόλως 'πρακτορική' ή, κατά το λεγόμενο, 'κυπατζίδικη'. Η απόδοση των δεινών των πολιτών με αριστερό φρόνημα στην ΚΥΠ αποτελεί υποκρισία και αποποίηση ευθυνών. Η ΚΥΠ υπήρξε όργανο, έστω με δύναμη ή επιρροή, όχι καθοδηγητής. Τους αριστερούς κατεδίωξε πρωτίστως η Πολιτεία, γ) σχετικά με την εκδήλωση και την επικράτηση της χούντας του 1967 σημειώνουμε ότι, βάσει των δεδομένων που διαθέτουμε, η ΚΥΠ δεν έπαιξε κάποιον ιδιαίτερο ρόλο. Ασφαλώς συμπορεύτηκε με το καθεστώς⁷⁶ όπως έκαναν, και με το παραπάνω, οι ένοπλες δυνάμεις και τα σώματα ασφαλείας, δ) φαίνεται πως μέχρι και το 1974 υπήρξε κουλτούρα πληροφόρησης τόσο σε επίπεδο πολιτικής ηγεσίας όσο και σε υπηρεσιακό επίπεδο. Κράτος και ΚΥΠ φέρονται να συνεργάζονται επί μονίμου βάσεως, όχι πάντα αρμονικά⁷⁷, έστω και υπό τον κομμουνιστικό φόβο. Από τη μεριά

⁷⁵ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 223-234

⁷⁶ ...παίζοντας κεντρικό ρόλο, όπως επισημαίνει ο Αποστολίδης, στον έλεγχο της νομιμοφροσύνης των πολιτών προς την 21^η Απριλίου και στη δίωξη των διαφωνούντων -περί τούτου βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 198, 219-223

⁷⁷ Ο Νάτσινας αναφέρει ότι μεταξύ 1956 και 1963 υπήρξε μια κρίση μεταξύ αυτού και της ΚΥΠ από τη μία μεριά και του Καραμανλή από την άλλη. Ο τελευταίος αγνοούσε συστηματικά την Υπηρεσία, αυτό το επιβεβαίωσε και ο Μιλτιάδης Έβερτ αναφέροντας πως ο πρωθυπουργός συνήθιζε να ρίχνει στον κάλαθο των αχρήστων τα ενημερωτικά δελτία της ΚΥΠ -για μια εικόνα βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 142. Άλλη μια κρίση μεταξύ

της η Υπηρεσία έχει ξεκάθαρο κίνητρο λειτουργίας, είναι προσανατολισμένη σε έναν στόχο ακόμα και αν οι φοβίες που παράγει αυτός πολλές φορές κρίνονται, κατά την άποψή μας, υπερβολικές ή και ανύπαρκτες.

Αν και η μικρή έρευνά μας λοιπόν όσον αφορά τις σχέσεις της ΚΥΠ με τη CIA, τη δράση της πρώτης έναντι των αριστερών δυνάμεων αλλά και τη δράση / στάση της πριν και κατά τη διάρκεια της χούντας δεν καταδεικνύει κάτι αφύσικο ή υπερβολικό, είναι γνωστό πως ακριβώς αυτές οι σχέσεις και δράσεις έχουν στιγματιστεί στο μεταπολιτευτικό πολιτικό σκηνικό όχι πάντα με έντιμη διάθεση. Το κακό ασφαλώς δεν βρίσκεται στην καταδίκη πράξεων αλλά στην καταδίκη θεσμών.⁷⁸ Πρόκειται για σφάλμα. Για ένα σφάλμα του οποίου οι παρενέργειες έχουν οδηγήσει μάλλον σε μια απαξία της κεντρικής Υπηρεσίας, σε μια έλλειψη πληροφοριακής κουλτούρας εκ μέρους του ελληνικού κράτους, ίσως, δε, της Υπηρεσίας καθαυτής. Και για ό,τι τόσο σφοδρά πιθανολογούμε, δεν λείπουν τα στοιχεία.

Κουλτούρα πληροφοριών στη σύγχρονη ελληνική πολιτική πραγματικότητα. Η ΚΥΠ από το τέλος της επταετίας των συνταγματαρχών μέχρι τις μέρες μας

Η πτώση της δικτατορίας σημάνει την έναρξη της δεύτερης απόπειρας αλλαγής νοοτροπίας της ΚΥΠ μετά εκείνης επί εποχής Ένωσης Κέντρου. Ο Καραμανλής αντικαθιστά την ηγεσία της Υπηρεσίας με μια σειρά αντιχουντικών αξιωματικών. Εκείνο όμως που κάνει εντύπωση είναι ότι, σύμφωνα με τον ναύαρχο Χρήστο Λυμπέρη, η μεταπολιτευτική στελέχωση της ηγεσίας του στρατεύματος και των μυστικών υπηρεσιών έγινε με βάση τις αναφορές και τους φακέλους ασφαλείας της χούντας, ιδιαίτερα στο Πολεμικό Ναυτικό. Λέει ο Λυμπέρης: «Εντοπίσαμε ποιους

της ΚΥΠ και της πολιτικής ηγεσίας παρουσιάζεται κατά τη διάρκεια της πρωθυπουργίας Γεωργίου Παπανδρέου την περίοδο 1964-1965. Αποτέλεσμα αυτής η αντικατάσταση του επιτελείου Νάτσινα από κεντρικούς αξιωματικούς. Σημειώνουμε ότι ο Νάτσινας και κάποια άλλα ηγετικά στελέχη της Υπηρεσίας είχαν ήδη παραιτηθεί από τον Δεκέμβρη του 1963 προαισθανόμενα την επικράτηση της Ένωσης Κέντρου στις εκλογές του Φεβρουαρίου του 1964. Κάπου λοιπόν εντός του συγκεκριμένου έτους επιχειρείται μια 'εκδημοκρατικοποίηση' της Υπηρεσίας. Η 'νέα' ΚΥΠ ή, τέλος πάντων, ένα σημαντικό κομμάτι της δεν θα συναινέσει στις μεθοδεύσεις του Παλατιού την επόμενη χρονιά. Ουσιαστικά έρχεται σε αντιπαράθεση τόσο με τα ανάκτορα όσο και με τη CIA που σιγοντάρει τις βασιλικές μεθοδεύσεις που θα οδηγήσουν τον Γεώργιο Παπανδρέου στην έξοδο. Κατόπιν αυτής της εξέλιξης οι φιλοπαπανδρεϊκοί αξιωματούχοι εκδιώκονται. Έτσι, η ΚΥΠ επανακαθορίζει την πορεία της σύμφωνα με τη γραμμή του Παλατιού, της Δεξιάς αλλά και της CIA -για μια άποψη ανέτρεξε στο Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 103-108, επίσης, Κάρης Γιάννης, *Η γέννηση του νεοφασισμού στην Ελλάδα*, Παπαζήσης, Αθήνα, 1974, σ. 224

⁷⁸ Ο Φιτσανάκης αν και υποστηρίζει ότι ο ρόλος της ΕΥΠ και των μυστικών υπηρεσιών στη συνολικότερη εξέλιξη της χώρας ήταν δευτερευών ή και ασήμαντος, δεν παραλείπει να τονίσει την εμπλοκή τους σε μηχανορραφίες παραπολιτικών κέντρων όπως και στη συστηματική πολιτική καταπίεση μιας μεγάλης, όπως λέει, μερίδας πληθυσμού που κορυφώθηκε στα χρόνια της δικτατορίας. Γιατί λοιπόν, ρωτάει, οι μεταπολιτευτικές κυβερνήσεις και ειδικότερα το ΠΑΣΟΚ, πέρα από το να περιορίσουν δραστηρίως την εξωθεσμική λειτουργία των πληροφοριακών οργανισμών, δεν προέβησαν στην κατάργησή τους; Διότι, απαντάει ο ίδιος, πρωτάνευσε η λογική της προστασίας του θεσμικού τους χαρακτήρα. Οι πολιτικές ατασθαλίες της ΚΥΠ δεν εναποτέθησαν στη θεσμική φυσιολογία της, οι πολιτικά υπόλογες πράξεις της διαχωρίστηκαν από τη θεσμική της υπόσταση, άλλωστε, οι υπηρεσίες Πληροφοριών δεν χαράσσουν πολιτική αλλά επιβοηθούν στην πραγμάτωσή της. Οι πρακτικές των μυστικών υπηρεσιών δεν είναι φύσει πολιτικές. Αντιθέτως, χρωματίζονται στον χαρακτήρα του ευρύτερου πολιτικού κλίματος εντός του οποίου αυτές λειτουργούν. Έτσι, εντός συνθηκών πολιτικής ομαλότητας οι πληροφοριακές υπηρεσίες θα λειτουργήσουν 'εντός ορίων'. Ακόμα και αν κάτι τέτοιο διαφανεί πως κινδυνεύει, οι επιβλέποντες θεσμικοί ελεγκτικοί μηχανισμοί έχουν τη δυνατότητα να επιβληθούν -περί τούτων βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 135-137, 190

ναύτες και στελέχη φακέλωνε το προηγούμενο καθεστώς [...] Ε, αυτούς επιλέξαμε, δηλαδή κομμουνιστές, αριστερούς και αντιδικτατορικούς δεξιούς και είχαμε ήσυχο το κεφάλι μας». ⁷⁹ Εάν αυτό ίσχυσε και για τη στελέχωση των Υπηρεσιών, τότε, μπορούμε να υποθέσουμε πως αυτή έγινε με κριτήριο όχι τόσο την ικανότητα των νέων στελεχών αλλά τη συμπόρευσή τους με τη νέα πολιτική πραγματικότητα, αυτό τελικά ίσως δεν είναι ο προσφορότερος τρόπος επιλογής προσωπικού.

Παράλληλα με την εκκαθάριση εμφανίζεται για πρώτη φορά οργανωμένος συνδικαλιστικός φορέας εντός της ΚΥΠ. Η παρακολούθηση του νόμιμου πλέον ΚΚΕ διακόπτεται (όχι όμως από την αστυνομία και τη χωροφυλακή που εξακολουθούν αυτήν την πρακτική μέχρι και τα τέλη του 1977). Ξεκινά η συλλογή πληροφοριών περίξ ακροδεξιών οργανώσεων. Τέλος, χαλαρώνει ο εναγκαλισμός ΚΥΠ και CIA παρά το ότι η αμερικανική Υπηρεσία εξακολουθεί και χρηματοδοτεί την ελληνική αντίστοιχη μέχρι τα τέλη της δεκαετίας του 1970.⁸⁰

Ο Αποστολίδης για την προσαρμογή της ΚΥΠ εντός της πρώτης περιόδου διακυβέρνησης της χώρας από τη ΝΔ (1974-1981) γράφει πως η επιρροή και η αποτελεσματικότητά της μειώθηκαν δραματικά. Η αντίδραση της κοινής γνώμης και του πολιτικού κόσμου στην καταπάτηση των ελευθεριών από την χούντα έφερε αλλαγές σε προσανατολισμούς και πρόσωπα στις κρατικές υπηρεσίες ασφαλείας. Και συνεχίζει: «Η ριζική αλλαγή προσωπικού, η απαξίωση της Υπηρεσίας λόγω της ταύτισής της με την χούντα, ο περιορισμός της πληροφοριακής δραστηριότητας στο εσωτερικό λόγω της νομιμοποίησης του ΚΚΕ τον Σεπτέμβριο του 1974 μειώνουν την αξία του πληροφοριακού υλικού της ΚΥΠ. Κατά την επταετία 1974-1981 προβάλλει έντονα η απειλή της διεθνούς και εσωτερικής τρομοκρατίας σε σχέση με την οποία η ΚΥΠ καλείται να παίζει κεντρικό ρόλο λόγω των διασυνδέσεων με ξένες υπηρεσίες Πληροφοριών αλλά και επειδή δεν έχει συγκροτηθεί ειδική Αντιτρομοκρατική Υπηρεσία στην Ελλάδα. Οι αρμοδιότητες της ΚΥΠ έμειναν οι ίδιες από τον Ιδρυτικό Νόμο του 1953 μέχρι το 1986, δείγμα της διαχρονικής απροθυμίας των ελληνικών κυβερνήσεων να αγγίζουν το θέμα ΚΥΠ».⁸¹

Η περιγραφόμενη εκ του Αποστολίδη απαξία και απροθυμία επηρεάζει, ως είναι φυσικό, επιχειρησιακά την Υπηρεσία. Άλλωστε, όπως τονίζει ο Φιτσανάκης, για την ελληνική κυβέρνηση (αναφέρεται πλέον στην πρώτη κυβέρνηση του ΠΑΣΟΚ) προείχε ο εκδημοκρατισμός⁸², η συνταγματική προσαρμογή και ο εκσυγχρονισμός της πολιτικής κουλτούρας της ΚΥΠ. Ο ίδιος ο Ανδρέας Παπανδρέου επιθυμεί

⁷⁹ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 121, επίσης, Λυμπέρης Χρήστος, *Πορεία σε ταραγμένες θάλασσες*, Ποιότητα, Αθήνα, 1999, σ. 72

⁸⁰ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 121-122. Ο Φιτσανάκης μας πληροφορεί πως οι σχέσεις μεταξύ των δύο Υπηρεσιών τελικά διερράγησαν σχεδόν ολοκληρωτικά επί εποχής πρώτης διακυβέρνησης ΠΑΣΟΚ παρά την προσπάθεια της Ουάσινγκτον να γεφυρώσει το διαφαινόμενο χάσμα. Δεν υπήρξε αποτέλεσμα, μάλιστα το 1984 η διάσταση απόψεων μεγεθύνεται με την απέλαση του υποσταθμάρχη της CIA στην Αθήνα για να κορυφωθεί το 1987 όταν στην ηγεσία της Υπηρεσίας (που έχει μετονομαστεί σε Εθνική Υπηρεσία Πληροφοριών -ΕΥΠ) τοποθετείται ο Κωνσταντίνος Τσίμας, ο πρώτος μη στρατιωτικός που αναλαμβάνει τη διοίκηση της κύριας ελληνικής μυστικής υπηρεσίας. Αν κάποιος ρωτήσει το λόγο της διακοπής των σχέσεων μεταξύ των ΚΥΠ / ΕΥΠ και CIA θα τον βρει μεταξύ άλλων και στην υποτιθέμενη εμπλοκή της δεύτερης στην ανατροπή της δημοκρατίας το 1967 όπως καταγγέλλει η κυβέρνηση Ανδρέα Παπανδρέου -για μια εικόνα βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 127-129

⁸¹ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 235-236

⁸² Του οποίου η διαδικασία εμπειρείχε έντονα στοιχεία κομματικοποίησης όπως παραδέχεται ο Φιτσανάκης. Αυτό ωστόσο δεν δείχνει να τον προβληματίζει, αντιθέτως το θεωρεί κάτι μεταξύ φυσικού και αναπόφευκτου -περί τούτου βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 134

πρωτίστως να εξαλείψει την ιστορική και ιδεολογική πρόσδεση της Υπηρεσίας στη δεξιά, προτού αποπειραθεί να την εκσυγχρονίσει επιχειρησιακά. Η συνταγματική λοιπόν προσαρμογή επείγει με την παρουσία μιας επιχειρησιακής σύγχυσης να θεωρείται, τουλάχιστον από τον Φιτσανάκη, αναμενόμενη και σε μεγάλο βαθμό δικαιολογημένη.⁸³

Από την άλλη μεριά ο Αποστολίδης αφήνει σοβαρότατες αιχμές. Σημειώνει ότι ...όπως γίνονταν μέχρι το 1981, και όπως έχει γίνει παράδοση και επαναλαμβάνεται μέχρι σήμερα, όλοι οι ένστολοι της ΚΥΠ αντικαταστάθηκαν από το ΠΑΣΟΚ μόλις αυτό ανέλαβε την εξουσία. Και συνεχίζει ...η διαφορά τη φορά αυτή συνίστατο στο ότι οι νέοι αξιωματικοί που αποσπάστηκαν στην ΚΥΠ δεν ανήκαν στο στρατιωτικό καταστημένο, αλλά στη μερίδα των αξιωματικών που για λόγους κοινωνικής προέλευσης, ιδεολογικών πεποιθήσεων ή και έλλειψης ικανοτήτων είχαν μέχρι τότε παραμεριστεί στο στράτευμα ή αποστρατευτεί -θεωρούμε πως η μνεία σε 'έλλειψη ικανοτήτων' είναι αρκούντως δηκτική. Πέραν τούτου αναφέρεται λεπτομερειακώς σε σειρά γεγονότων που προκαλούν απογοήτευση όπως η επαναφορά στην Υπηρεσία αποστράτων αξιωματικών σε επιτελικές θέσεις λόγω 'κομματικής συνάφειας'⁸⁴, οι ενδοϋπηρεσιακές κόντρες με έπαθλο την καρέκλα της διοικήσεως, η απουσία προοπτικής εξέλιξης των πολιτικών υπαλλήλων τη στιγμή που πολλές φορές ανταποκρίνονταν καλύτερα από τους βαθμοφόρους προϊσταμένους τους, η έλλειψη πρωτοβουλιών εκ μέρους μερίδας αξιωματικών υπό το φόβο 'κάποιου λάθους που θα βλάψει καριέρες', οι εντάσεις και τριβές με την ΕΛΑΣ, οι εντάσεις και τριβές με δυτικές Υπηρεσίες, η άκοπη δραστηριότητα αλλοδαπών εξτρεμιστικών οργανώσεων κ. λ.⁸⁵

Αν όλα αυτά οδηγούν σε μια επιχειρησιακή αδράνεια και, τελικά, στην μερική ή ολική απώλεια της όποιας πληροφοριακής κουλτούρας⁸⁶, τα πράγματα επί της ουσίας δεν βελτιώθηκαν τις επόμενες δεκαετίες. Προσλήψεις, μετατάξεις και επανακάμψεις κομματικού χαρακτήρα που διχάζουν την Υπηρεσία⁸⁷, συνδικαλιστικές έριδες⁸⁸,

⁸³ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 130, 132. Ο Φιτσανάκης δηλώνει πως ακριβώς αυτή η σύγχυση, και 'όχι κάτι άλλο', ευθύνεται για την αναζωπύρωση της δράσης διαφόρων ακροαριστερών οργανώσεων τύπου 17 Νοέμβρη κατά τη δεκαετία του 1980

⁸⁴ Γράφει ο Αποστολίδης: «Εφόσον το κύριο κριτήριο επιλογής των αξιωματικών ήταν η προσήλωση στο ΠΑΣΟΚ, είναι φυσικό οι περισσότεροι να μην είχαν τα προσόντα ή το ενδιαφέρον να αποδώσουν έργο. Αρκετοί εμφανίστηκαν με την περγαμνή του αντιστασιακού, θεωρώντας ότι η απόσπασή τους στην ΕΥΠ ήταν ανταμοιβή για την αντίσταση στην δικτατορία, ώστε να μην απαιτείται να κοπιάσουν» -για μια ιδέα βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 266

⁸⁵ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 263-276

⁸⁶ Που υπήρξε εντέλει στην προ του 1974 ΚΥΠ. Με αφορμή την περιπέτεια Οτσαλάν ο Αποστολίδης γράφει: «Στο υπουργείο Εξωτερικών είχαμε κακή εικόνα για την Υπηρεσία. Τα στελέχη της ήταν μετρίων δυνατοτήτων, οι αναλύσεις για τις εξελίξεις στο εξωτερικό κατώτερες από τις δικές μας πληροφορίες και εκτιμήσεις. Τις μόνες εκθέσεις που θυμάμαι να διαβάζω με ενδιαφέρον ήσαν επί δικτατορίας εκείνες που αφορούσαν τον εσωτερικό και εξωτερικό κομμουνισμό» -για μια άποψη βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 290

⁸⁷ Κατά τα έτη 1987 και 1988 πραγματοποιούνται από την Υπηρεσία προσλήψεις 400 περίπου υπαλλήλων. Οι προσλήψεις ήταν προεκλογικού χαρακτήρα και υπερβολικές σε αριθμό. Η νέα κυβέρνηση Μητσοτάκη μετατάσσει τους προσληφθέντες. Η επιστροφή του ΠΑΣΟΚ στην εξουσία το 1993 δίδει τη δυνατότητα σε όποιους επιθυμούν να επιστρέψουν στην Υπηρεσία. Η αναταραχή που προκλήθηκε εκ του συμβάντος επηρέασε αρνητικά και για χρόνια την απόδοση της ΕΥΠ -για μια ιδέα βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 278-279. Μέχρι το έτος 2000 οι προσλήψεις πολιτικού προσωπικού γίνονταν χωρίς τυπικές ανοικτές διαδικασίας με αποτέλεσμα να ευνοούνται 'φίλοι και γνωστοί'. Το 2000 και το 2001 πραγματοποιήθηκαν δύο ανοικτοί διαγωνισμοί. Παρά το ότι εισήλθαν στην Υπηρεσία ικανοί υποψήφιοι, δεν έλειψε η ευνοϊκή μεταχείριση ορισμένων καθώς στη λίστα των τελικών επιλογών λόγο

παιχνίδια της ηγεσίας της Υπηρεσίας εις βάρος του προσωπικού⁸⁹ είναι κάποια από τα σημάδια που δείχνουν πως κάτι δεν πάει καλά. Ασφαλώς οι επιτυχίες μιας υπηρεσίας Πληροφοριών σπάνια διακοινώνονται, ωστόσο, έχουμε την εντύπωση πως η ΕΥΠ έτσι και αλλιώς δεν έχει να επιδείξει πολλές, με κάποιες εξαιρέσεις όπως η συνεισφορά στην εξάρθρωση της 17 Νοέμβρη.⁹⁰ Από την άλλη, είναι οι αποτυχίες που θέλοντας και μη χαρακτηρίζουν έναν πληροφοριακό οργανισμό δεικνύοντας το βαθμό της σχετικής κουλτούρας τόσο σε κρατικό όσο και σε υπηρεσιακό επίπεδο. Και τέτοιες, μάλιστα σημαντικές, είχαμε ουκ ολίγες τις δύο προηγούμενες δεκαετίες. Ειδικότερα...

Περίπτωση Στίβεν (Σταύρος) Λάλας: Τον Απρίλιο του 1993 συλλαμβάνεται στη Βιρτζίνια από τις αμερικανικές αρχές ο Ελληνοαμερικανός υπηρετών στην πρεσβεία

είχε η επιτροπή των εισαγωγικών εξετάσεων που διοριζόταν από τον εκάστοτε πολιτικό προϊστάμενο της Υπηρεσίας. Η ΕΥΠ λόγω των ιδιαιτεροτήτων της είχε το προνόμιο να μην υπάγεται στο ΑΣΕΠ με ό,τι θετικό ή αρνητικό αυτό κομίζει. Από την άλλη μεριά αρκετοί χρησιμοποιούσαν την είσοδο στην Υπηρεσία ως εφελτήριο προκειμένου να μεταταχθούν σε άλλες υπηρεσίες του δημοσίου με καλύτερο μισθό. Όποιοι αντιμετώπιζαν την άρνηση του διοικητή της ΕΥΠ ως προς το αίτημα μετάταξή τους περιέπιπταν σε μια κατάσταση αδιαφορίας, αν δεν βρίσκονταν σ' αυτήν αρχής εξ αρχής. Σημειωτέον πως υποχρεωτικές μετατάξεις υπαλλήλων, παρά την ύπαρξη σχετικής νομοθετικής πρόβλεψης για την Υπηρεσία, απορρίπτονταν από τα δικαστήρια. Κατά τον τρόπο τούτο η ΕΥΠ δεν μπορούσε να απαλλαγεί από κάποιον απρόθυμο υπάλληλο (ασφαλώς δεν μπορούσε να ζητήσει την απόλυσή του), δεν εδύνάτο να φέρει στις τάξεις της ως μόνιμο κάποιον προσοντούχο από άλλη δημόσια υπηρεσία. Ερχόμενοι στο ένστολο προσωπικό διαπιστώνουμε πως τα πράγματα δεν ήταν καλύτερα. Η πλειονότητα αποσπóταν στην ΕΥΠ βάσει πολιτικών κριτηρίων. Όταν η κυβέρνηση άλλαζε, άλλαζε ολόκληρο το εν λόγω προσωπικό με ό,τι αυτό συνεπάγεται για την εύρυθμη και αποδοτική λειτουργία του οργανισμού -περί αυτών βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 292-294

⁸⁸ Εξ αιτίας της υπόθεσης Οτσαλάν προκαλείται πόλεμος ανακοινώσεων μεταξύ των συνδικαλιστικών παρατάξεων της Υπηρεσίας, πρόκειται για περιστατικό που έβλαψε βαθιά τόσο την δημόσια εικόνα της όσο και το βαθμό παραγωγής της. Είναι χαρακτηριστικό πως μετά από αυτό εμφανίζεται νόμος που επιβάλλει ενιαία ψηφοδέλτια στις σωματειακές εκλογές (ουσιαστικά δεν εφαρμόστηκε, σημειώνουμε). Η ρύθμιση, γράφει ο Αποστολίδης, βοήθησε αλλά δεν έκλεισε την πληγή του συνδικαλισμού -περί τούτου βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 291

⁸⁹ Διαβάζουμε στον ηλεκτρονικό τύπο πως ενώ το 2009 προσελήφθηκαν στην ΕΥΠ περί τα 90 άτομα (ημερομηνία ορκωμοσίας η 21^η Απριλίου 2009), αυτά τα άτομα, δύο χρόνια και πλέον από την πρόσληψή τους, δεν μονιμοποιήθηκαν παραμένοντας δόκιμοι. Γιατί αυτό; Η απάντηση που δίδεται έχει ως εξής: «Διότι απλούστατα η ηγεσία της ΕΥΠ επεδίωξε και πέτυχε με κάθε τρόπο να τους θέσει υπό ομηρεία ώστε στις πρόσφατες εκλογές που έγιναν στα δύο σωματεία της Υπηρεσίας να ψηφίσουν τους αρεστούς της διοίκησης και μόνο αυτούς», δηλαδή, «ψηφίστε 'αυτούς που πρέπει' αν θέλετε να μονιμοποιηθείτε μια ώρα αρχύτερα» -για μια εικόνα βλέπε «Πως γίνεται κάποιος πράκτορας στην ΕΥΠ;», 22/09/2011, στη σελίδα <https://www.newsbeast.gr/greece/arthro/233219/pos-ginetai-kapoiios-praktoras-stin-eup> εις την οποία ανατρέξαμε τη 13^η Ιουνίου 2018

⁹⁰ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 299. Από την άλλη βέβαια ίσως η ΕΥΠ πάσχει στον επικοινωνιακό τομέα άρα κάποιες από τις επιτυχίες δεν έρχονται με τον κατάλληλο τρόπο στην επιφάνεια. Και τέτοιες ήταν η διάσωση Ελλήνων ομογενών της Αμπχαζίας (Σεπτέμβριος 1993, επιχείρηση *Χρυσόμαλλον Δέρας*) και η εκκένωση της κινεζικής πρεσβείας στα Τίρανα (αλλά και της φυγάδευσης πολιτών άλλων εθνικοτήτων) κατά τη διάρκεια της εξέγερσης λόγω του σκασίματος των 'οικονομικών πυραμίδων' στην Αλβανία τον Μάρτιο του 1997 (επιχείρηση *Κοσμάς Αιτωλός*). Και στις δύο επιχειρήσεις η συμβολή της ΕΥΠ και η συνεπικουρία της στις ελληνικές Ειδικές Δυνάμεις υπήρξε καθοριστική -για μια ελάχιστη εικόνα των επιχειρήσεων βλέπε το άρθρο «Ελληνες σε κίνδυνο: Οι ελληνικές ένοπλες δυνάμεις ήταν πάντα εκεί. Δύο ιστορικές επιχειρήσεις» στην ιστοσελίδα στρατιωτικού ενδιαφέροντος OnAlert στην ηλεκτρονική σελίδα http://www.onalert.gr/stories/Ellhnes_se_kindynooi_Ellhnikes_EDhtan_panta_ekediDyo_istorikes_epix_eirhseis/3473 εις την οποία καταφύγαμε την 1^η Ιουλίου 2018, επίσης, Χαρβαλιάς Γιώργος, «Η ΕΥΠ στη σύγχρονη νεοελληνική πραγματικότητα» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009, σ. 121-122

των ΗΠΑ στην Αθήνα Στίβεν Λάλας. Η κατηγορία είναι βαριά: κλοπή απόρρητων διπλωματικών εγγράφων και απόδοσή τους στην ελληνική κυβέρνηση.

Ο Λάλας προσεγγίστηκε πρώτη φορά από την ΕΥΠ όταν υπηρετούσε στο νατοϊκό στρατηγείο στη Σμύρνη (άνοιξη 1977). Οι πληροφορίες που έδινε ήταν πολύτιμες βοηθώντας την κυβέρνηση στην πρόγνωση της αμερικανικής πολιτικής έναντί της. Την περίοδο 1984-1985 οι Αμερικανοί τον μεταθέτουν στο Βελιγράδι, την περίοδο 1985-1989 υπηρετεί στην Κωνσταντινούπολη. Εθεωρείτο ο μεγαλύτερος Έλληνας σύγχρονος κατάσκοπος και κύριο όπλο της ελληνικής μυστικής διπλωματίας.

Όπως φαίνεται μεταξύ 1985 και 1989, αν όχι ενωρίτερα, ‘σύνδεσμος’ του Λάλα με την ΕΥΠ υπήρξε ένας αντισυνταγματάρχης ο οποίος συναντούσε τον Έλληνα πράκτορα κάπου στην περιοχή της Καβάλας στην οποία άλλωστε έδρευε κλιμάκιο της Υπηρεσίας. Ο Λάλας ταξίδευε συχνά από την Κωνσταντινούπολη στη Χρυσούπολη Καβάλας καθώς στην τελευταία διέμενε η οικογένειά του, έτσι είχε την ευχέρεια να συναντά τον ‘σύνδεσμό’ του χωρίς να κινεί υποψίες.

Τα πράγματα μεταβάλλονται όταν ο Λάλας μετατίθεται από τις διπλωματικές αρχές των ΗΠΑ για λίγο στην Ταϊβάν. Δεν είναι ξεκάθαρο αν αυτή την περίοδο συνεχίζονται οι επαφές του με την ΕΥΠ, σαφώς δεν είναι εύκολο, επιπλέον ο ‘χειριστής’ του κάποια στιγμή τοποθετείται στο Πολεμικό Μουσείο αλλάζοντας προφανώς καθήκοντα.

Τον Δεκέμβριο του 1990 επιστρέφει στην πατρίδα ως στέλεχος της αμερικανικής πρεσβείας εμπλεκόμενος με τη Μονάδα Επικοινωνίας Προγραμμάτων. Αρχίζει να παραδίδει εκ νέου απόρρητα σήματα μεταξύ πρεσβείας και αμερικανικών υπηρεσιών και αρχών -κυρίως του Department of State (Στέιτ Ντιπάρτμεντ)- στην ελληνική κυβέρνηση. Ωστόσο μαζί με την κυβερνητική αλλαγή επέρχεται, σύμφωνα με τον Αποστολίδη, χαλάρωση στον χειρισμό του. Ο παλαιός ‘σύνδεσμος’ δεν υπάρχει πλέον. Έχει αντικατασταθεί από τον ταγματάρχη Α. Σ.

Η μοιραία στιγμή έρχεται το Φεβρουάριο του 1993. Η υφυπουργός Εξωτερικών Βιργινία Τσουδερού ενημερώνει τον Έλληνα πρέσβη στις ΗΠΑ για μια πτυχή του θέματος των Σκοπίων που μόνο οι Αμερικανοί γνωρίζουν, μάλιστα είχαν συντάξει υπεραπόρρητο έγγραφο που είχε σταλεί στην Ουάσινγκτον από την πρεσβεία των ΗΠΑ στην Αθήνα. Πιθανολογείται σφόδρα ότι ο Έλληνας πρέσβης στις ΗΠΑ ή, τέλος πάντων, κάποιος αξιωματούχος της εκεί ελληνικής αποστολής άφησε να εννοηθεί, χωρίς ασφαλώς να το θέλει, σε συνομιλία του με παράγοντα του Στέιτ Ντιπάρτμεντ πως η Ελλάδα διαθέτει πληροφορίες που μόνο μέσα από κατασκοπικές δραστηριότητες θα μπορούσε ‘να βάλει στο χέρι’. Η αντίστροφη μέτρηση έχει αρχίσει. Το FBI στοχοποιεί επτά υπαλλήλους της αμερικανικής πρεσβείας της Βασιλίσσης Σοφίας με δυνατότητα εισόδου στη Μονάδα Επικοινωνίας Προγραμμάτων. Ο χώρος παγιεύεται. Εντοπίζονται κινήσεις του Λάλα. Μετ’ ολίγον εντοπίζονται και οι συναντήσεις του με τον Α. Σ. Ο Λάλας καλείται πίσω στη Βιρτζίνια για μια δήθεν ενημέρωση περί ζητημάτων τρομοκρατίας. Συλλαμβάνεται. Καταδικάζεται σε 14 χρόνια κάθειρξη παραμένοντας στις αμερικανικές φυλακές 12 χρόνια πριν επιστέψει στην Ελλάδα.

Ταυτόχρονα στις ελληνικές μυστικές υπηρεσίες ξεσπά πόλεμος για την αποκάλυψή του και κυρίως για το εάν και πώς ‘καρφώθηκε’ η δράση του στην αμερικανική πλευρά. Πολλοί διατυπώνουν κατηγορίες κατά του Α. Σ. (σύμφωνα με δημοσιογραφικές πηγές ο Α. Σ., που απεβίωσε εν έτει 2001, δεν αποτελούσε μάλλον το καλύτερο πρότυπο πράκτορα). Επιπλέον η συνεργασία μεταξύ ΕΥΠ και CIA, που φάνηκε να επαναθεσμοθετείται μετά την πασοκική περίοδο, παγώνει εκ νέου με ό,τι αυτό καταδεικνύει για τις σχέσεις των δύο χωρών. Ο διοικητής της ΕΥΠ Παναγιώτης Μπαλές αποπέμπεται μετ’ ολίγων μηνών από τη νέα κυβέρνηση ΠΑΣΟΚ.

Πιθανότατα, και παρά τις ενστάσεις αρχικά του ίδιου του Λάλα, δεν υπήρξε θέμα συνειδητής πράξης αποκάλυψης του ρόλου του Ελληνοαμερικανού πράκτορα. Αυτό που υπήρξε ήταν ένας συνδυασμός λαθών. Κυριότερο από όλα η διανομή υλικού σε αποδέκτες χωρίς προηγούμενη επεξεργασία, χωρίς να ακολουθηθούν συγκεκριμένες διαδικασίες και 'φίλτρα'. Άνθρωποι της ΕΥΠ σήμερα υποστηρίζουν πως «οι πληροφορίες του Λάλας διοχετεύονταν άκριτα σε πρόσωπα της κυβέρνησης με τα οποία στελέχη της ΕΥΠ διατηρούσαν προσωπικές σχέσεις. Οι πληροφορίες του Λάλας άρχισαν να μοιράζονται σαν φέιγ βολάν, χωρίς καμία επεξεργασία. Και τότε έγινε το λάθος με την αναφορά της Τσουδερού [στον Έλληνα πρέσβη στην Ουάσινγκτον] που πρόδιδε την εκ των έσω ενημέρωση».^{91, 92}

Περίπτωση Ιμίων: Το επόμενο περιστατικό που καταδεικνύει έλλειψη πληροφοριακής κουλτούρας, και όχι μόνο, αφορά στην κρίση των Ιμίων τον Ιανουάριο του 1996. Η όξυνση καλλιεργείτο ήδη από τα τέλη Δεκεμβρίου του 1995 ωστόσο η ολιγωρία της ελληνικής πολιτικής ηγεσίας που ασχολείτο με κομματικά παίγνια, η αδυναμία έγκαιρης κατανόησης της σοβαρότητας του προβλήματος, η απουσία συγκεκριμένων στόχων και συγκροτημένης στρατηγικής αντιμετώπισης κρίσεων οδήγησε στα γνωστά αποτελέσματα. Πέραν όμως του μη συντονισμού διπλωματικών και στρατιωτικών μέσων, της αποσπασματικότητας των ληφθέντων μέτρων, της αδυναμίας συντονισμού ενεργειών φορέων και προσώπων, της απουσίας συστηματικής ανάλυσης σεναρίων / επιλογών κ. λ.⁹³ εντύπωση κάνει η αντιμετώπιση του διοικητή της ΕΥΠ Λεωνίδα Βασιλικόπουλου και εν γένει της Υπηρεσίας από τον τότε πρωθυπουργό της χώρας.

Πιο συγκεκριμένα, οι ελληνικές μυστικές υπηρεσίες λίγα 24ωρα πριν την κορύφωση της κρίσης έλαβαν επί χείρας το περιεχόμενο μιας συνομιλίας του τότε αρχηγού του τουρκικού ΓΕΝ ναυάρχου Ερκάγια, ο οποίος επαίρετο ότι η ιστορία των γκρίζων ζωνών ήταν «δικό του παιδί». Ο Ερκάγια αποκάλυπτε ουσιαστικά ένα σχέδιο που εξυφαινόταν με σκοπό το 'γκριζάρισμα' περιοχών του ανατολικού Αιγαίου ...είμαι βέβαιος, τόνιζε, πως με τα στοιχεία που έχουμε μπορούμε να διεκδικήσουμε τους Καλογήρους, τους Φούρνους. Οι αναλυτές της ΕΥΠ κατάλαβαν πως είχαν μια πληροφορία που έδειχνε ότι η κλιμακούμενη κρίση στα Ίμια αποτελούσε τμήμα ενός ευρύτερου σχεδιασμού. Η πληροφορία προωθήθηκε στα υπουργεία Αμύνης και Εξωτερικών. Εν τω μεταξύ περί τα δύο 24ωρα πριν την έναρξη του κυρίως επεισοδίου το κλιμάκιο της Υπηρεσίας στον Έβρο εντόπισε, μάλιστα από ανοικτά κανάλια επικοινωνίας, εντολές του τουρκικού ΓΕΝ προς δύο περιπολικά του. Οι εντολές ήταν σαφείς: να πλησιάσουν στις βραχονησίδες Ίμια προκειμένου να ελέγξουν αν και πού υπάρχουν Έλληνες κομάντος, επίσης, αν επί των νησίδων κυματίζει ελληνική σημαία. Η σχετική συνομιλία μεταφράστηκε το βράδυ της 29ης Ιανουαρίου, στάλθηκε, δε, στα κεντρικά της Υπηρεσίας το επόμενο πρωί. Από εκεί, μέσω απόρρητου τηλέτυπου, φτάνει στο κέντρο επιχειρήσεων του ΓΕΝ. Είναι μάλλον σαφές πως οι επιτελείς δεν έδωσαν την πρέπουσα σημασία, ενδεχομένως επειδή βομβαρδίζονταν εκείνη την ώρα με πληροφορίες για τις κινήσεις των τουρκικών

⁹¹ Οι πληροφορίες για την υπόθεση Λάλα ελήφθησαν από το Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 279-281 και από το άρθρο του Βασίλη Λαμπρόπουλου «Ποιος κάρφωσε τον Στίβεν Λάλας» στην ηλεκτρονική τοποθεσία της εφημερίδας «Το Βήμα» <http://www.tovima.gr/relatedarticles/article/?aid=167438> με ημερομηνία εισόδου την 14^η Ιουνίου 2018

⁹² Εδώ γεννάται το ερώτημα: Μήπως το υπουργείο Εξωτερικών αγνοούσε τελικά το ανεπεξέργαστο των πληροφοριών Λάλα; Μήπως θεωρούσε πως αυτές είχαν φιλτραριστεί; Ακόμα και αυτό να συνέβη, τι σημαίνει 'επεξεργασμένη πληροφορία'; Μήπως ότι δύναται σε κάθε περίπτωση να αξιοποιηθεί επισήμως;

⁹³ Για όλα αυτά βλέπε Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, Παπαζήσης, Αθήνα, 2005, σ. 257-275

πλοίων. Το βέβαιο πάντως είναι πως η ΕΥΠ είχε προειδοποιήσει εγκαίρως⁹⁴, μια προειδοποίηση η οποία έφθασε επίσης στο πρωθυπουργικό γραφείο.

Ένα από τα σοβαρά προβλήματα εκείνων των ημερών, που καταγράφεται μάλιστα στον Τύπο της εποχής, απετέλεσε η καχυποψία μεταξύ της κυβέρνησης και ορισμένων θεωρουμένων παπανδρεϊκών, μεταξύ αυτών και ο Βασιλικόπουλος. Ο επικεφαλής της ΕΥΠ επισκέφτηκε τον πρωθυπουργό την 30^η Ιανουαρίου επιχειρώντας να του επιδώσει πληροφορίες και στοιχεία που η Υπηρεσία είχε συλλέξει / αναλύσει, επίσης, να ενημερώσει για την μόλις ολίγων ωρών πριν συνομιλία του με το σταθμάρχη της CIA στην Αθήνα. Ο πρωθυπουργός τον άκουσε βιαστικά (με αδιαφορία; με καχυποψία;) και του είπε: «Δεν σας χρειάζομαι άλλο».

Κάποιες ώρες αργότερα και αφού ο Βασιλικόπουλος συνομιλεί εκ νέου με τον Αμερικανό σταθμάρχη αλλά και με τον υφυπουργό Εθνικής Αμύνης Νικόλαο Κουρή (επίσης χαρακτηρισμένο παπανδρεϊκό όπως άλλωστε παπανδρεϊκός χαρακτηρίζεται και ο ΑΓΕΕΘΑ Χρήστος Λυμπέρης) επιχειρεί να δει για δεύτερη φορά τον πρόεδρο της κυβέρνησης στο γραφείο του στη Βουλή. Ο χειρισμός ειδικά σ' αυτή τη δεύτερη συνάντηση είναι καταφανώς απαξιωτικός. Ο πρωθυπουργός ουσιαστικά αρνείται να τον δεχτεί, τον παραπέμπει δε, μέσω της γραμματείας του, σε άλλο κυβερνητικό στέλεχος. Ο διοικητής της ΕΥΠ δεν πτοείται. Περιμένει στον προθάλαμο έξω από την κυβερνητική αίθουσα συσκέψεων τη στιγμή μάλιστα που τον καλούν από το γραφείο του πληροφορώντας τον πως τον ζητεί επειγόντως ο σταθμάρχης της CIA. Κάποια στιγμή η πόρτα της αίθουσας ανοίγει. Ο Βασιλικόπουλος βρίσκει την ευκαιρία να πλησιάσει τον πρωθυπουργό. Τον ενημερώνει όπως κι όπως για να λάβει την εξής απάντηση: «Το θέμα το χειρίζεται ο υπουργός Εξωτερικών, μην κάνετε τίποτα, μην ασχολείστε άλλο». Είναι φανερό πως η ελληνική πολιτεία έχει αποφασίσει ότι δεν χρειάζεται τη συνδρομή της ΕΥΠ 'αδειάζοντας' τον επικεφαλής της, που αποπέμπεται τελικά τον Απρίλιο του 1996, την Υπηρεσία καθαυτή όπως και τον θεσμό που εκπροσωπεί.⁹⁵

Περίπτωση Οτσαλάν: Μια άλλη ανεκδιήγητη περίπτωση είναι η περίπτωση του επικηρυγμένου από την Ιντερπόλ για συμμετοχή σε παραστρατιωτικές δραστηριότητες και καταζητούμενου από την Άγκυρα Κούρδου ηγέτη του αποσχιστικού Εργατικού Κόμματος του Κουρδιστάν (PKK), Αμπτουλάχ Οτσαλάν. Το συγκεκριμένο επεισόδιο ξεγύμνωσε τόσο την ανεπάρκεια της ελληνικής πολιτικής όσο και την επιχειρησιακή αδυναμία των ελληνικών μυστικών υπηρεσιών. Στα μέσα

⁹⁴ Σ' αυτό το συμπέρασμα καταλήγουν οι περισσότεροι μελετητές της κρίσης των Ιμίων. Εξάιρεση αποτελεί ο καθηγητής Αθανάσιος Πλατιάς. Ο Πλατιάς εκτιμά ότι η συλλογή πληροφοριών δεν ανταποκρίθηκε στη ροή των εξελίξεων -για μια εικόνα βλέπε Πλατιάς Αθανάσιος, «Η Ελληνική Αμυντική Πολιτική και η Κρίση στα Ίμια: Σκέψεις και Προβληματισμοί» στο *Η Κρίση στα Ίμια*, Πρακτικά Ημερίδας ΙΣΤΑΜΕ, Απρίλιος / Ιούλιος 1997, σ. 92, επίσης βλέπε Παούνης Νικόλαος, *Η Ελληνοτουρκική Αντιπαράθεση στα Ίμια* (1996). *Ο Μύθος του Εθνικού Τακτικού Πλεονεκτήματος* υπό την αιγίδα του ΕΛΙΑΜΕΠ, Νοέμβριος 2017, σ. 24-25

⁹⁵ Οι πέριξ του συμβάντος πληροφορίες έχουν ληφθεί τόσο από το Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., όσο και από το «Η κρίση των Ιμίων και ο ρόλος της ΕΥΠ, της CIA και της κυβέρνησης» στη διαδικτυακή τοποθεσία του in.gr <http://www.in.gr/2005/11/13/greece/i-krisi-twn-imiwn-kai-o-rol-os-tis-ey-p-tis-cia-kai-tis-kybernis/>, 13 Νοέμβρη 2005, από το «Τι συνέβη τη νύχτα των Ιμίων» του Αλέξη Παπαχελά στη σελίδα <http://www.tovima.gr/politics/article/?aid=169407> της εφημερίδας *Το Βήμα*, 13 Νοέμβρη 2005, από το «Ίμια 1996: το λεπτομερές χρονικό της κρίσης» της αμυντικής ιστοσελίδας e-Amyrna στο <http://e-amyna.com/ιμια-1996-το-λεπτομερές-χρονικό-της-κρίσης/>, 31 Ιανουαρίου 2018, και από το «Η κρίση των Ιμίων: Τι μας δίδαξε και τι έχουμε πράξει» του αντιστρατήγου ε. α. Λάμπρου Τζούμη στην αμυντική ιστοσελίδα του OnAlert <http://www.onalert.gr/stories/h-krisi-imiwn-ti-mas-dida3e-ti-exoume-pra3ei/62625>, 29 Ιανουαρίου 2018 με κοινή ημερομηνία εισόδου την 8^η Ιουνίου 2018

προς τέλος του 1998 ο Οτσαλάν εγκαταλείπει το κέντρο επιχειρήσεών του στη Δαμασκό της Συρίας όταν η τελευταία, λόγω της φιλοξενίας που του προσέφερε, απειλήθηκε με πόλεμο από την Τουρκία. Μετά από μια απέλπιδα περιπλάνηση ανά την Ευρώπη (που έλαβε τη μορφή διαφόρων σταδίων και φάσεων) καταλήγει στο Μίνσκ της Λευκορωσίας και, τελικά, στην Ελλάδα για δεύτερη φορά, στις 29 Ιανουαρίου 1999. Απορία προκαλεί το γεγονός της ιδιωτικής πρωτοβουλίας / κλήσης του Οτσαλάν στη χώρα από τον απόστρατο πλοίαρχο του Πολεμικού Ναυτικού Αντώνη Ναζάκη. Η ελληνική κυβέρνηση και οι μυστικές υπηρεσίες φέρονται να μη γνωρίζουν περί των πρωτοβουλιών Ναζάκη⁹⁶, ουσιαστικά συλλαμβάνονται εξαπίνης.⁹⁷ Από κει πέρα τρέχουν πίσω από τα γεγονότα. Αποφασίζεται η απόκρυψη του Κούρδου ηγέτη και η μεταφορά του στην ελληνική πρεσβεία στο Ναϊρόμπι. Η επιλογή είναι πολλαπλά άστοχη. Η ΕΥΠ φαίνεται να αγνοεί την ύπαρξη στην πρωτεύουσα της Κένυας εκατό και πλέον στελεχών των αμερικανικών μυστικών υπηρεσιών που διερευνούν την τρομοκρατική επίθεση κατά της πρεσβείας των ΗΠΑ στις 7 Αυγούστου 1998.⁹⁸ Στις 2 Φεβρουαρίου 1999 μόλις ο Οτσαλάν αφικνείται στο Ναϊρόμπι και την εκεί ελληνική πρεσβεία οι Αμερικανοί θέτουν την τελευταία υπό παρακολούθηση ειδοποιώντας την ίδια στιγμή τόσο τις κενυατικές όσο και τις τουρκικές αρχές. Λίγες μέρες αργότερα μια ομάδα στελεχών της τουρκικής ΜΙΤ (πρόκειται για τον τουρκικό Εθνικό Οργανισμό Πληροφοριών) καταφτάνει στην πρωτεύουσα του αφρικανικού κράτους συνοδεύει μελών των τουρκικών ειδικών δυνάμεων. Στις 15 Φεβρουαρίου ο Κούρδος ηγέτης, υπό την προστασία ελληνικής ομάδας⁹⁹, μεταφέρεται κατόπιν (υποτιθέμενης) συμφωνίας μεταξύ Ελλάδας και Κένυας προς τον διεθνή αερολιμένα Τζόμο Κενυάτα του Ναϊρόμπι με (υποτιθέμενο) προορισμό το Άμστερνταμ. Ωστόσο ο Κενυάτης οδηγός του οχήματος εις το οποίο

⁹⁶ Γράφει ο Παύλος Αποστολίδης: «Διαπίστωσα τότε ότι λειτουργούσε μια ανορθόδοξη ομάδα ιδιωτών, υποστηρικτών του ΡΚΚ, που η ελληνική κυβέρνηση πίστευε ότι χειραγωγούσε, αλλά που της δημιούργησε την κρίση, φέρνοντας τον Κούρδο ηγέτη στην Αθήνα» -περί τούτου βλέπε Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 289. Οι Ντόκος και Τσάκωνας επισημαίνουν την αδυναμία της ελληνικής κυβέρνησης να διαχειριστεί διαφόρους επωνύμους «ιδιώτες της εξωτερικής πολιτικής» οι πράξεις ή και παραλήψεις των οποίων έφεραν την επίσημη κυβέρνηση αντιμέτωπη με ένα *fait accompli* -για μια εικόνα βλέπε Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., σ. 276. Από τη μεριά του ο Νίκος Μαράκης υποστηρίζει ότι «τα κυκλώματα των μυστικών υπηρεσιών και οι ακραίοι εθνικιστές βουλευτές ήταν εκείνοι που 'επέβαλαν' και οι υπουργοί που χειρίστηκαν την υπόθεση είναι αυτοί που 'αποδέχτηκαν' την ιδέα της ιδιωτικής φιλοξενίας του Οτσαλάν στην Ελλάδα» -για μια ιδέα βλέπε Μαράκης Νίκος, «Το Πραξικόπημα της ΕΥΠ. Το Άγνωστο Παρασκήνιο της Υπόθεσης Οτσαλάν» στο *Το Βήμα της Κυριακής*, 21 Φεβρουαρίου 1999, σ. Α6

⁹⁷ Καταλογίζονται ευθύνες τόσο στην Υπηρεσία Πολιτικής Αεροπορίας (ΥΠΑ) όσο και στην ΕΥΠ. Κατηγορούνται πως απέτυχαν να κάνουν τη δουλειά που τους είχε ανατεθεί (ρωτάμε: περί ποίας δουλειάς ομιλούμε; μήπως περί της παρεμπόδισης της έλευσης Οτσαλάν; υπήρχαν σαφείς οδηγίες;). Οι αστοχίες τους σχετίζονται, υποστηρίζουν οι κατηγοροί, με το άνοιγμα της αίθουσας VIP στις 29 Ιανουαρίου 1999 όπως και με τον πλημμελή έλεγχο των επιβατών της Aegean (κατ' άλλους των επιβατών ιδιωτικής πτήσεως) που υποτίθεται πως ήταν ο υφυπουργός Αμύνης και Εξοπλισμών και σύμβουλος του Προέδρου της Ρωσικής Ομοσπονδίας και οι συν αυτό -για μια εικόνα βλέπε Μαράκης Νίκος, «Το Πραξικόπημα της ΕΥΠ. Το Άγνωστο Παρασκήνιο της Υπόθεσης Οτσαλάν», ό. π., σ. Α6-7. Ασφαλώς υπάρχουν και αυτοί που καθόλου δεν πιστεύουν ότι η ΕΥΠ ή, τέλος πάντων, ένα τμήμα της πιάστηκε εξαπίνης

⁹⁸ Βλέπε και στο Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., σ. 283

⁹⁹ Που ωστόσο επιβαίνει σε άλλο όχημα από αυτό του Οτσαλάν όπως, τουλάχιστον, καταθέτει ο Σάββας Καλεντερίδης στο 98,4 RADIO στις 16 Φεβρουαρίου 2017 -περί τούτου βλέπε στο <https://www.youtube.com/watch?v=9AggJ3miNrM> εις το οποίο ανατρέξαμε τη 10^η Ιουνίου 2018

επιβαίνει ο Οτσαλάν παρεκκλίνει της πορείας παραδίδοντάς τον στις κενυατικές και τουρκικές μυστικές υπηρεσίες.¹⁰⁰

Το σκάνδαλο Οτσαλάν, γράφει ο Φιτσανάκης, ανέδειξε την έκταση της επιχειρησιακής απειρίας και την άγνοια τόσο των Ελλήνων διπλωματών όσο και των ελληνικών μυστικών υπηρεσιών. Οι τελευταίες, συνεχίζει ο μελετητής, αγνοούσαν βασικά μέτρα ασφαλείας επιτρέποντας στον Κούρδο επαναστάτη τη χρήση του προσωπικού του κινητού τηλεφώνου.¹⁰¹ Παράλληλα, οι ενέργειές τους φανερώνουν αδυναμία συνειδητοποίησης του ευάλωτου των επικοινωνιών της πρεσβείας με την Αθήνα και το αντίστροφο. Αρκεί να σημειωθεί πως οι οδηγίες μεταβιβάζονταν από την ελληνική πρωτεύουσα μέσω απροστάτευτης γραμμής και με τη χρήση μιας πρόχειρα κωδικοποιημένης και μάλλον φαιδρής φρασεολογίας¹⁰² προκειμένου να ειδοποιηθούν οι διπλωμάτες και οι εκεί πράκτορες πως ο Οτσαλάν πρέπει να φυγαδευθεί.¹⁰³ Το πλήγμα στην εικόνα της ΕΥΠ υπήρξε βαρύ με την κυβέρνηση να κάνει λόγο για «οργανισμό που εκτρέπεται εύκολα του σκοπού του» και για «αυθαίρετη αυτονόμηση υπαλλήλων» στη διάρκεια της απόπειρας φυγάδευσής του Οτσαλάν¹⁰⁴ χωρίς ωστόσο να διευκρινίζεται, σημειώνουμε, κάτι περαιτέρω.¹⁰⁵ Σε κάθε περίπτωση ήταν προφανές πως το ελληνικό κράτος -κυβέρνηση και Υπηρεσίες- δεν διέθετε τους πολιτικούς και πληροφοριακούς μηχανισμούς που απαιτούν οι χειρισμοί κρίσεων υψηλής έντασης.

Οι Θάνος Ντόκος και Παναγιώτης Τσάκωνας συμφωνούν με τον Φιτσανάκη. Υποστηρίζουν ότι η Ελλάδα αποδείχτηκε ανέτοιμη τόσο όσον αφορά στις μυστικές υπηρεσίες όσο και στο θεσμικό μηχανισμό χειρισμού εκτάκτων αναγκών. Άμεσο αποτέλεσμα της αποτυχίας υπήρξε η προσπάθεια εκσυγχρονισμού της ΕΥΠ. Επιπρόσθετα, συνεχίζουν οι δύο μελετητές, αναδείχθηκε η έλλειψη εμπειρίας και μηχανισμών πραγματοποίησης «μυστικών επιχειρήσεων» στο πλαίσιο της εθνικής ασφαλείας καθώς και η μη ικανότητα αποτελεσματικού χειρισμού κρίσεων.¹⁰⁶ Ασφαλώς, σημειώνουμε, ο διοικητής της ΕΥΠ Χαράλαμπος Σταυρακάκης έχασε τη θέση του.

Τέλος, αν υιοθετήσουμε τις αποκαλύψεις του άρθρου «Το Πραξικόπημα της ΕΥΠ. Το Άγνωστο Παρασκήνιο της Υπόθεσης Οτσαλάν» του Νίκου Μαράκη, τότε, οι

¹⁰⁰ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 168-169

¹⁰¹ Βλέπε και στο Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., σ. 284

¹⁰² Γράφουν, π. χ., οι Ντόκος και Τσάκωνας: «Η επιλογή της κωδικής ονομασίας ‘Δεσποινίς Κατεχάκη’ για την ΕΥΠ μόνο ειρωνικά μειδιάματα μπορεί να προκαλέσει» -περί τούτου ανέτρεξε στο Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., σ. 283

¹⁰³ Θα λέγαμε εκδιωχθεί

¹⁰⁴ Επαναλαμβάνουμε πως επρόκειτο για προσπάθεια εκδίωξης και μάλιστα απίθανης. Οι Ντόκος και Τσάκωνας γράφουν: «Τέσσερα στελέχη της ΕΥΠ υπό την κωδική ονομασία ‘θίασος’ (sic!) εστάλησαν ως ενίσχυση (για να εκδιώξουν, βιαίως αν χρειαστεί, τον Οτσαλάν από την πρεσβεία) στο Ναϊρόμπι χωρίς χρήματα (!) και όπλα (!)» -για μια άποψη βλέπε Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., σ. 283

¹⁰⁵ Ανατρέχοντας στο άρθρο «Υπόθεση Οτσαλάν: Το θρίλερ της απαγωγής που άρχισε στην Αθήνα και τέλειωσε στο Ίμραλι» του Διονύση Θανάσουλα καταλαβαίνουμε ότι η «εκτροπή και αυτονόμηση» των πρακτόρων της ΕΥΠ σχετίζεται (και) με την άρνησή τους, στην εντολή της Αθήνας, να πετάξουν τον Οτσαλάν έξω από την ελληνική πρεσβεία στο Ναϊρόμπι -για μια εικόνα βλέπε Θανάσουλας Διονύσης, «Υπόθεση Οτσαλάν: Το θρίλερ της απαγωγής που άρχισε στην Αθήνα και τέλειωσε στο Ίμραλι», 13 Οκτωβρίου 2016 στο <https://www.protothema.gr/stories/article/618489/upothesi-otsalan-to-thriller-tis-apagogis-pou-arhise-stin-athina-kai-teleiose-sto-imrali/> με ημερομηνία ανάκτησης τη 19^η Ιουνίου 2018

¹⁰⁶ Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, ό. π., σ. 285

ευθύνες της ΕΥΠ ή, τέλος πάντων, κάποιων στελεχών της καθίστανται απερίγραπτες. Σύμφωνα με τον Μαράκη η ΕΥΠ: α) δεν επιτήρησε τα πιθανά σημεία εισόδου του Οτσαλάν στη χώρα κατά παράβαση των εντολών που είχε, β) δεν απέτρεψε την είσοδο Οτσαλάν όταν αυτός κατέφτασε στη χώρα κατά παράβαση των εντολών που είχε, γ) ουσιαστικά προετοίμασε την άφιξη / υποδοχή του Κούρδου ηγέτη μετά βαΐων και κλάδων την 29^η Ιανουαρίου 1999, δ) απέτυχε στον αρχικό σκοπό της ήτοι, να φυγαδεύσει τον Οτσαλάν στη Νότιο Αφρική, ε) επέλεξε ως τόπο διαφυγής την Κένυα τη στιγμή που στη συγκεκριμένη χώρα οι Αμερικανοί πράκτορες κυριολεκτικά αλώνιζαν, στ) δεν διαφύλαξε τις γραμμές τηλεπικοινωνιών από τη στιγμή που ο Άπο εγκατέλειψε τη χώρα στο ταξίδι προς την Κένυα, ζ) τοποθέτησε συνοδό του Οτσαλάν τον ταγματάρχη Σάββα Καλεντερίδη τη στιγμή που ο τελευταίος ήταν γνωστός στις αμερικανικές Υπηρεσίες ως ειδικός στις κουρδικές υποθέσεις¹⁰⁷. αν αυτά ή κάποια από αυτά ισχύουν, τότε, η ανεπάρκεια πληροφοριακής συνείδησης, το λιγότερο, της ΕΥΠ πράγματι εκτοξεύεται.¹⁰⁸

Περίπτωση υποκλοπών Vodafone: Στις 2 Φεβρουαρίου 2006 αποκαλύπτεται τόσο από την εφημερίδα *Τα Νέα* όσο και από την ελληνική κυβέρνηση το σκάνδαλο των τηλεφωνικών υποκλοπών εις βάρος του τότε πρωθυπουργού Κώστα Καραμανλή, στελεχών της κυβέρνησης και άλλων παραγόντων της δημόσιας ζωής μέσω παραβίασης κάποιων ψηφιακών τηλεφωνικών κέντρων της εταιρίας Vodafone Hellas. Η κυβέρνηση αποκαλύπτει ότι είχε λάβει γνώση της υπόθεσης ήδη από τη 10^η Μαρτίου 2005 όταν η Vodafone την ενημέρωσε για την ύπαρξη κάποιου πολύπλοκου λογισμικού στο εσωτερικό του εταιρικού κυκλώματος διαχείρισης τηλεφωνικών συνδιαλέξεων¹⁰⁹, ωστόσο, η κοινή γνώμη δεν ενημερώθηκε διά ‘λόγους εθνικής ασφαλείας’. Ανακοινώνεται επίσης ότι οι υποκλοπές είχαν ξεκινήσει λίγους μήνες πριν την έναρξη των Ολυμπιακών Αγώνων της Αθήνας το καλοκαίρι του 2004 και συνεχίστηκαν με αδιάλειπτο ρυθμό μέχρι την αποκάλυψή τους. Σύμφωνα με τα στοιχεία που συνέλεξαν οι ελληνικές αρχές η λειτουργία του παράνομου λογισμικού έδινε άμεση και συνεχή πρόσβαση στο περιεχόμενο τόσο προφορικών συνδιαλέξεων όσο και γραπτών μηνυμάτων εκατό και πλέον συνδρομητών. Η λίστα των θυμάτων

¹⁰⁷ Βλέπε στο Μαράκης Νίκος, «Το Πραξικόπημα της ΕΥΠ. Το Άγνωστο Παρασκήνιο της Υπόθεσης Οτσαλάν», ό. π., σ. Α6-7 αλλά και στην ιστοσελίδα <http://www.tovima.gr/politics/article/?aid=108257> την οποία επισκεφθήκαμε τη 10^η Ιουνίου 2018. Το άρθρο με τίτλο «Το πραξικόπημα της ΕΥΠ. Το άγνωστο παρασκήνιο της υπόθεσης Οτσαλάν» του Νίκου Μαράκη συμπληρώνει το «Υπόθεση Οτσαλάν: Το θρίλερ της απαγωγής που άρχισε στην Αθήνα και τέλειωσε στο Ίμραλι» του Διονύση Θανάσουλα ως προς την «εκτροπή και αυτονόμηση» της ΕΥΠ

¹⁰⁸ Σ’ αυτό το σημείο οφείλουμε να παραθέσουμε την άποψη του Σάββα Καλεντερίδη όπως αυτή ακούστηκε τη 16^η Φεβρουαρίου 2017 στο 98,4 RADIO (για μια εικόνα ανέτρεξε στη διαδικτυακή τοποθεσία <https://www.youtube.com/watch?v=9AggJ3miNrM> εις την οποία καταφύγαμε τη 10^η Ιουνίου 2018). Σύμφωνα με την άποψη Καλεντερίδη: α) η πρόσκληση Οτσαλάν στην Ελλάδα απευθύνθηκε στον τελευταίο από Έλληνες πολιτικούς, β) συμβουλή του ιδίου προς την κυβέρνηση ήτο η μη εμπλοκή της με την υπόθεση και η μυστική απομάκρυνση του Οτσαλάν, εάν και εφόσον κατέφτανε στη χώρα, διά της θαλασσίας οδού με κάποιο σκάφος, γ) η επιλογή του Ναϊρόμπι έγινε όχι από την ΕΥΠ αλλά από την κυβέρνηση μάλλον κατόπιν αμερικανικών πιέσεων, δ) το ‘δόσιμο’ Οτσαλάν δεν βαρύνει την ΕΥΠ αλλά την ελληνική κυβέρνηση. Είναι η τελευταία που παρέδωσε τον Οτσαλάν λόγω αμερικανικών πιέσεων. Η ελληνική κυβέρνηση, κατά τον Καλεντερίδη, είτε βρέθηκε σε πλήρη σύγχυση, είτε παρέδωσε τον Άπο εσκεμμένα, ε) οι τουρκικές μυστικές υπηρεσίες παρέλαβαν τον Οτσαλάν άκοπα, ουσιαστικά δεν αναμείχθηκαν. Αν υιοθετήσουμε τα λεγόμενα Καλεντερίδη, παρά το ότι δεν απαντούν στις επιχειρησιακές και τεχνικές δυσλειτουργίες, τότε, η ΕΥΠ σχεδόν αθρώνεται με την ευθύνη να αποδίδεται σχεδόν αποκλειστικά στο ελληνικό πολιτικό σύστημα

¹⁰⁹ Ερωτηματικά προκαλεί το γεγονός της ενημέρωσης της κυβέρνησης τη 10^η Μαρτίου τη στιγμή που σύμφωνα με τη δικογραφία η ανακάλυψη από τη Vodafone έγινε την 4^η του ιδίου μήνα καταφαίνεται μια αδικαιολόγητη διαφορά 6 ημερών μεταξύ ανακάλυψης και κυβερνητικής ενημέρωσης. Από τη μεριά της η Vodafone ισχυρίστηκε ότι ενημέρωσε αυτοστιγμεί την ελληνική πολιτεία

περιελάμβανε, εκτός του πρωθυπουργού και της συζύγου του, τους υπουργούς Εξωτερικών, Δημοσίας Τάξεως, Δημοσίων Έργων, τον δήμαρχο Αθηναίων, διαφόρους αξιωματούχους της ΕΛΑΣ και των υπηρεσιών ασφαλείας, βουλευτές, δημοσιογράφους, έναν υψηλόβαθμο υπηρετήσαντα στην ΕΥΠ κ. λ.

Η έκταση και η αποτελεσματικότητα του συστήματος παρακολούθησης οφειλόταν στην απευθείας εγκατάσταση του παράνομου λογισμικού σε τέσσερεις ψηφιακούς διακόπτες τηλεφωνικών κέντρων της Vodafone. Οι τελευταίοι είχαν κατασκευαστεί από τον κολοσσό της Ericson Telecommunications σε συνεργασία με την ελληνικών συμφερόντων Intracom Telecom. Κατά συνέπεια την ανάληψη της εγκατάστασης του ‘κοριού’ πρέπει να ανέλαβε, ίσως, κάποιος τεχνικός είτε της Vodafone, είτε της Ericson, είτε της Intracom, του οποίου οι σχέσεις με άλλα ‘κέντρα’ πρέπει μάλλον να θεωρηθούν δεδομένες. Σε κάθε περίπτωση οι ‘απομακρυσμένοι χειριστές’ του λογισμικού είχαν τη δυνατότητα να αντιγράφουν και να ανακατευθύνουν τις υπό παρακολούθηση συνδιαλέξεις σε επιλεγμένες γραμμές δεκατεσσάρων ‘ορφανών’ καρτοκινητών. Οι δράστες ουσιαστικά βασίστηκαν στη μέθοδο των υποκλοπών των υπηρεσιών ασφαλείας. Οι υποκλοπές θα μπορούσαν να συνεχιστούν επ’ αόριστον εάν κάποιοι συνδρομητές της Vodafone δεν είχαν καταγγείλει την εξαφάνιση των γραπτών μηνυμάτων που έστελναν. Η συγκεκριμένη παρενέργεια ως φαίνεται προκάλεσε την έρευνα των τεχνικών της εταιρίας με αποτέλεσμα το ξεσκέπασμα της συνωμοσίας. Μεταγενέστερη μελέτη κατέδειξε πως η διευκόλυνση της ανακατεύθυνσης των στοχοποιημένων αριθμών λάβαινε χώρα μέσω κυψελών (κεραιών) που είχαν τοποθετηθεί εντός διαμερισμάτων πέριξ της αμερικανικής πρεσβείας στην Αθήνα και πιο συγκεκριμένα στην περιοχή του Λυκαβηττού, της κλινικής Λευκού Σταυρού, της πλατείας Μαβίλη και του Πύργου Αθηνών. Κατά τον τρόπο τούτο εδραιώθηκε η πεποίθηση πως πίσω από το σκάνδαλο βρισκόταν είτε η CIA είτε η NSA. Την όλη υπόθεση περιέπλεξε η υποτιθέμενη αυτοκτονία διαχειριστή του δικτύου της Vodafone Hellas μία μόλις μέρα πριν την ενημέρωση της κυβέρνησης από την εταιρία.¹¹⁰

Το σκάνδαλο υποκλοπών της Vodafone Hellas, γράφει ο Φιτσανάκης, απετέλεσε το πρώτο παγκοσμίως καταγεγραμμένο περιστατικό παραβίασης ενός ολόκληρου συστήματος κινητής τηλεφωνίας μέσω ενός τόσο σοφιστικέ λογισμικού και με τόση πολυπλοκότητα που «σπανίως έχουμε ξαναδεί». Υπήρξε επιπλέον η σημαντικότερη δημοσιοποιημένη υπόθεση κυβερνοκατασκοπίας με εμπλεκόμενη μια εταιρία παροχής υπηρεσιών κινητής τηλεφωνίας με αποτέλεσμα να αλλάξει όλη η συζήτηση όταν αυτή έρχεται σε θέματα ασφαλείας τηλεπικοινωνιών.¹¹¹ Είχε όμως και άμεσα επακόλουθα στην ελληνική πολιτική ζωή. Συγκεκριμένα για πρώτη φορά η ελληνική πολιτεία αναγκάστηκε να παραδεχτεί δημοσίως μια καίρια και παρατεταμένη διείσδυση στις τηλεπικοινωνίες του ηγετικού πολιτικού της προσωπικού με συνέπειες που πλήττουν την εκτελεστική εξουσία, την εθνική ασφάλεια, τις ένοπλες δυνάμεις και τις υπηρεσίες Πληροφοριών. Αναγνώρισε έτσι την αποτυχία προστασίας

¹¹⁰ Οι πληροφορίες περί της υπόθεσης Vodafone ελήφθησαν από το έργο του Σήφη Φιτσανάκη, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 153-157, από το Nomikos John, Liaropoulos Andreas, “Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernization of the Greek National Intelligence Service” στο *Journal of Policing, Intelligence and Counter Terrorism*, Volume 5, Number 1, 2010, σ. 35 και από το άρθρο του Χρήστου Δεμέτη «Υποκλοπές κατά Καραμανλή: Το Σχέδιο Πυθία, η Vodafone, οι Ρώσοι και η ασημένια δραχμή» της 6^{ης} Οκτωβρίου 2016 στη σελίδα <http://www.news247.gr/politiki/ypoklopes-kata-karamanli-to-schedio-pythia-i-vodafone-oi-rosai-kai-i-asimenia-drachmi.6461776.html> εις την οποία προσφύγαμε την 11^η Ιουνίου 2018

¹¹¹ Fitsanakis Joseph, “State-Sponsored Communications Interception: Facilitating Illegality” στο *Information, Communication and Society*, Volume 6, Number 3, 2003, σ. 403-428

ουσιαστικά του συστήματος λήψεων πολιτικών αποφάσεων κρίσιμης σημασίας. Επιπροσθέτως, το σκάνδαλο των υποκλοπών ανέδειξε την αδυναμία των ελληνικών Υπηρεσιών να εγγυηθούν την επικοινωνιακή ασφάλεια που απαιτείται προκειμένου να λειτουργήσει παραγωγικά ένα σύγχρονο κράτος.¹¹² Οι Ανδρέας Λιαρόπουλος και Ιωάννης Νομικός συμφωνούν με τον Φιτσανάκη γράφοντας: «Το σκάνδαλο των τηλεφωνικών υποκλοπών του 2004/5 φανέρωσε την ανικανότητα της ΕΥΠ να αναγνωρίσει τις νέες απειλές ασφαλείας, την ανικανότητά της να προσαρμοστεί στις νέες απαιτήσεις». ¹¹³ Αίσθηση επίσης προκαλεί η παραδοχή της ΕΛΑΣ στην εφημερίδα *Τα Νέα* μέσω αξιωματικών της: «Ουσιαστικά δεν κάναμε καμία έρευνα για να εντοπίσουμε αυτούς που ενεργοποίησαν το παράνομο λογισμικό, τους τρόπους που γίνονταν οι υποκλοπές, πόσους ανθρώπους πραγματικά παρακολουθούσαν και πόσον καιρό διήρκεσε η υποκλοπή. Μάθαμε όσα η Vodafone ήθελε να μάθουμε». Σημειώνουμε ότι σύμφωνα με δημοσιογραφικές πηγές κενό υπήρξε και στην έρευνα που αφορούσε στην αυτοκτονία (;) του διαχειριστή του δικτύου της Vodafone καθώς δεν κατέστη δυνατή η εκ της αστυνομικής αρχής εξέταση του φορητού υπολογιστή του θανόντος υπό την έποψη πιθανής αναφοράς σε έκνομες ενέργειες ή σε οτιδήποτε άλλο που (θα) μπορούσε να σχετιστεί με την υπόθεση.¹¹⁴

Πέραν όμως της δεδομένης ανεπάρκειας της ΕΥΠ, κάτι που αντανακλά στην επιχειρησιακή πληροφοριακή της κουλτούρα, δεν έχει θιγεί κάτι εξίσου σημαντικό. Δεν έχουμε μάθει *αν και τι* είδους μυστικά εκμαιεύθηκαν από τους υποκλοπείς. Αυτό ασφαλώς σχετίζεται με την ευρύτερη κρατική / πολιτική κουλτούρα πληροφοριών και ασφαλείας και με το σοφό που οφείλει να γνωρίζει κάθε πολιτειακό στέλεχος: «Λόγων άπορρήτων έκφορὰν μὴ ποιοῦ» (Περίανδρος ο Κορίνθιος).¹¹⁵

Συμπεράσματα μέχρι τούδε

Άποψή μας είναι ότι, όπως καταδεικνύουν τα γεγονότα, η μεταπολιτευτική Ελλάς στερείται ευρύτερης κρατικής πληροφοριακής συνείδησης και αγωγής, επίσης, πιθανόν στερείται επιχειρησιακής ανάλογης. Ο Παύλος Αποστολίδης (σε μια προσπάθειά ίσως να ανακαλύψει το *γιατί*) γράφει: *Διαπίστωσή μου από τη θητεία μου είναι ότι ο πολιτικός κόσμος της χώρας λίγο ενδιαφέρεται για πληροφορίες που προκύπτουν από την καλώς εννοούμενη δραστηριότητα της ΕΥΠ που αφορά την εθνική ασφάλεια. Ίσως διότι στην Ελλάδα δεν λειτουργούν συλλογικοί μηχανισμοί λήψης αποφάσεων που θα χρησιμοποιούσαν τις πληροφορίες της ΕΥΠ, ή και οι τελευταίες να μην έχουν σταθερά την ποιότητα που θα έπρεπε. Ακόμη, λόγω της παλιάς κακής φήμης της, πολλοί αμφιβάλουν για την αξιοπιστία των πληροφοριών, ακόμα και όταν είναι σημαντικές.*¹¹⁶ *Τα πιο πάνω έχουν επίπτωση και στο μέσο επίπεδο των ενδιαφερομένων*

¹¹² Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 157

¹¹³ Nomikos John, Liaropoulos Andreas, "Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernization of the Greek National Intelligence Service" στο *Journal of Policing, Intelligence and Counter Terrorism*, ό. π., σ. 35

¹¹⁴ Δεμέτης Χρήστος, «Υποκλοπές κατά Καραμανλή: Το Σχέδιο Πυθία, η Vodafone, οι Ρώσοι και η ασημένια δραχμή», ό. π.

¹¹⁵ Η συγκεκριμένη προτροπή, *Λόγων άπορρήτων έκφορὰν μὴ ποιοῦ*, αποτελεί μότο της ΕΠΙδηλούμενο στο έμβλημά της. Από την άλλη μεριά εάν και εφόσον η ελληνική πολιτεία γνώριζε ήδη από το 2005 τα περί υποκλοπών θα μπορούσε να είναι, ενδεχομένως, αυτή που φέρει το πάνω χέρι εργαλειοποιώντας την τακτική της παραπληροφόρησης: πρόκειται για κάτι επί του οποίου δεν φανταζόμαστε, δυστυχώς, ότι μπορεί να ασκηθεί μια σύγχρονη ελληνική κυβέρνηση

¹¹⁶ Ο Φιτσανάκης συνεπικουρεί γράφοντας: *...η ΚΥΠ λειτουργούσε για δεκαετίες στην υπηρεσία των αμερικανικών ψυχοπολεμικών συμφερόντων, τα οποία δεν συμβάδιζαν απαραίτητα με τα ελληνικά... Ως αποτέλεσμα η Ελλάδα στερήθηκε τη δυνατότητα να χτίσει πραγματικά ελληνικές μυστικές υπηρεσίες που*

να υπηρετήσουν στην ΕΥΠ. Οπότε, φαύλος κύκλος. Μη προσοντούχο προσωπικό, προσλαμβανόμενο με μονιμότητα, διαιωνίζει τη μετριότητα.¹¹⁷ Με τη σειρά του ο Μάνος Ηλιάδης, εκ των εγκυροτέρων Ελλήνων στρατιωτικών αναλυτών και ειδικός σε θέματα πληροφοριών ομιλεί για μια ...*συστημική αδυναμία του ελληνικού πολιτικού συστήματος, οφειλόμενη στην έλλειψη σχετικής παιδείας της πολιτικής ηγεσίας και στην άγνοια του ρόλου και της σημασίας των υπηρεσιών πληροφοριών, με χαρακτηριστικότερο σύγχρονο παράδειγμα τον τρόπο με τον οποίο αντιμετωπίστηκε η κρίση των Ιμίων*.¹¹⁸

Εάν οι διαπιστώσεις Αποστολίδη και Ηλιάδη, και ειδικά η υποψία έλλειψης συλλογικών μηχανισμών λήψεως αποφάσεων του πρώτου, είναι ακριβείς, τότε, εξηγείται, με τραγικό μάλιστα τρόπο αλλά μόνο εν μέρει, η ελληνική στέρηση πληροφοριακής κουλτούρας. Ωστόσο δεν είναι μόνο αυτό-ά. Πρόκειται για αίτια που συνήθως αποφεύγεται να θιγούν, πιο συγκεκριμένα: α) το ελληνικό πολιτικό σύστημα και ειδικότερα το κεντροαριστερό του τμήμα, που ουσιαστικά κυβερνά τη χώρα από το 1981 μέχρι τις μέρες μας, υποφέροντας από διαφόρων μορφών 'άγχη' ενίστανται κάθε υποτιθέμενου συντηρητικού, εθνοκεντρικού, αστυνομικού ή 'ασφαλίτικου' θεσμού, β) εντός ενός μεταπολιτευτικού περιβάλλοντος δημοκρατικής, μέρα με την ημέρα, υπερπαραγωγής, ελευθεριασμού και δικαιωματισμού πολύ δύσκολα βρίσκεται χώρος στέγασης και ανάπτυξης αξιόλογων 'πρακτορικών' ιδεών και θεσμών, γ) εάν τα σχεδόν 500 δισεκατομμύρια ευρώ του ελληνικού χρέους ήρθαν ως αποτέλεσμα κακοδιαχείρισης, πολιτικής συναλλαγής, διαφθοράς κ. λ., τότε, ποια κυβέρνηση θα επιθυμούσε την ύπαρξη ικανών μυστικών υπηρεσιών δίπλα της; Υπενθυμίζουμε ότι τα διεφθαρμένα απολυταρχικά καθεστώτα επιθυμούν εξ ανάγκης και μόνο την παρουσία ισχυρών πληροφοριακών θεσμών κυρίως για λόγους παρακολούθησης της εσωτερικής κοινωνίας -κάτι τέτοιο δεν αφορά την ελληνική περίπτωση.

Θεωρούμε ότι το κύριο πρόβλημα που οφείλει να λυθεί είναι το πρόβλημα της **έλλειψης πληροφοριακής κουλτούρας και συνείδησης**. Αν δεν αποκατασταθεί ένα στοιχειώδες επίπεδο κρατικής και επιχειρησιακής πληροφοριακής αγωγής, τότε, κάθε

να ανταποκρίνονται ολοκληρωτικά στα ελληνικά εθνικά ζητήματα... Θα λέγαμε ότι εκεί ακριβώς έγκειται η σχετική δυσπιστία με την οποία ανώτατα κυβερνητικά κλιμάκια αντιμετωπίζουν τη συμβουλευτική λειτουργία της Υπηρεσίας. Με άλλα λόγια, συνεχίζει ο μελετητής, η ΕΥΠ βρίσκεται απομονωμένη μέσα στον κρατικό μηχανισμό, ουσιαστικά ανήμπορη να επιτελέσει το έργο της, λόγω έλλειψης επαφών μεταξύ αυτής και των στρατηγικών κέντρων της κυβέρνησης. Θεωρείται από τους πολιτικούς κάτι σαν την πάλαι ποτέ βασιλεία στην Ελλάδα: δηλαδή σαν ένας ξενόφερτος θεσμός που δεν έχει ελληνικές ρίζες και ιστορικά εξυπηρέτησε κυρίως ξένα συμφέροντα άσχετα αν κάποια από αυτά τα συμφέροντα συνέπιπταν με τα αντίστοιχα ελληνικά -για μια εικόνα βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 233-234

¹¹⁷ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 310. Άλλωστε «στην Ελλάδα η ΕΥΠ αποτελεί μέρος μιας αναποτελεσματικής Δημόσιας Διοίκησης, με όλες τις παθογένειές της», στο ίδιο, σ. 311. Ο Ιωάννης Νομικός επισημαίνει πως οι ελληνικές μυστικές υπηρεσίες ούσες κομμάτι του κρατικού οικοδομήματος δεν γίνεται να μην υποφέρουν από συγγενείς γραφειοκρατικές αδυναμίες. Αναφερόμενος σε ευρύτερο πλαίσιο τονίζει ότι, σύμφωνα με τον Michael Herman, μετά το 1945 ο αριθμός του ανθρώπινου δυναμικού των ανά τον κόσμο Υπηρεσιών αυξήθηκε με αποτέλεσμα την εμφάνιση μιας δημοσιοϋπαλληλικής νοοτροπίας, μιας 'βεμπεριανής γραφειοκρατίας' -για μια εικόνα βλέπε Νομικός Ιωάννης, «Υπηρεσίες Πληροφοριών και Εθνικής Ασφαλείας. Η περίπτωση της Ελλάδας» στο περιοδικό *Επίκαιρα*, τεύχος 149 (Αύγουστος 2012), σ. 36-37, Νομικός Ιωάννης, «Οι προκλήσεις για την ΕΥΠ στον 21^ο αιώνα» στην εφημερίδα *Παραπολιτικά*, 12 Μαΐου 2018, επίσης, Nomikos John, Liaropoulos Andrew, "Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernization of the Greek National Intelligence Service" στο *Journal of Policing, Intelligence and Counter Terrorism*, ό. π., σ. 30

¹¹⁸ Ντόκος Θάνος, «Οι τρύπες των μυστικών υπηρεσιών», 27 Ιανουαρίου 2008 στην διαδικτυακή τοποθεσία <http://www.tovima.gr/books-ideas/article/?aid=186449> εις την οποία ανατρέξαμε την 3^η Ιουνίου 2018

θεσμική, οργανωτική, γραφειοκρατική και λοιπή προσπάθεια αναμόρφωσης των ελληνικών μυστικών υπηρεσιών θα πέσει στο κενό. Πώς όμως δύναται να επιτευχθεί κάτι τέτοιο; Υποθέτουμε πως: (I) μέσω μιας ακαδημαϊκής ‘διαφήμισης’ της αξίας των πληροφοριών, (II) μέσω μιας συνειδητής προσπάθειας των Υπηρεσιών καθ αυτών αναβάθμισης του έργου τους, (III) μέσω πιέσεων από εξωτερικούς παράγοντες (βλέπε παράδειγμα ίδρυσης ΚΥΠ), (IV) μέσω συνολικής ή ατομικής πολιτικής βούλησης (βλέπε περίπτωση Πούτιν), (V) εξ αιτίας ενός καταστροφικού γεγονότος που θα αναγκάσει το πολιτικό προσωπικό να παραδεχτεί το πληροφοριακό έλλειμμα αποδεχόμενο ταυτόχρονα την αξία της πληροφόρησης, (VI) μέσω οτιδήποτε άλλου.

Από τις άνω έξι υποθέσεις την (VI) απλά δεν δυνάμεθα να την προσεγγίσουμε, την (V) την απευχόμαστε, την (III) την αντιμετωπίζουμε με ιδιαίτερη καχυποψία. Απομένουν οι (I), (II) και (IV) οι οποίες μπορούν και οφείλουν να συνδυαστούν / συνλειτουργήσουν. Οπωσδήποτε είναι η τελευταία (IV) που εφόσον μετουσιωθεί σε πράξη θα παίξει τον απόλυτο και καταλυτικό ρόλο.

Προς ένα νέο ελληνικό πληροφοριακό σύστημα

Αν υποθέσουμε ότι το κατά την άποψή μας κύριο πρόβλημα, αυτό της έλλειψης πληροφοριακής κουλτούρας, λύεται, τότε, ποια η ‘τεχνοκρατική’ πρότασή μας ως προς τη δόμηση ενός ικανού ελληνικού πληροφοριακού συστήματος; Αυτή αναλύεται επί τη βάσει 7 επιπέδων, ειδικότερα:

(I) Δομικό / γραφειοκρατικό επίπεδο: Η θεμελιώδης ερώτηση που οφείλει να απαντηθεί είναι η εξής: «Τι είδους (πολιτική) υπηρεσία Πληροφοριών χρειαζόμαστε;». Δηλαδή, χρειαζόμαστε μια μεικτή ενιαία Υπηρεσία; μία εσωτερικών πληροφοριών και μόνο; μια εξωτερικών πληροφοριών και μόνο; δύο ξεχωριστές Υπηρεσίες εσωτερικών η μία, εξωτερικών η άλλη, πληροφοριών;

Ο Παύλος Αποστολίδης σημειώνει πως τα περισσότερα ευρωπαϊκά κράτη διαθέτουν δύο ξεχωριστές Υπηρεσίες, μία υπηρεσία πληροφοριών Ασφαλείας / Εσωτερικού (ας πούμε γενικά ότι ομιλούμε για υπηρεσίες Αντικατασκοπίας / Αντιπληροφόρησης) και μία υπηρεσία πληροφοριών Εξωτερικού (ας πούμε γενικά ότι ομιλούμε για υπηρεσίες Κατασκοπίας / Πληροφόρησης) με την τελευταία να υπάγεται, ιδίως στα μικρά κράτη, συνήθως στις Ένοπλες Δυνάμεις. Από τη μεριά της η ΕΥΠ δεικνύει Υπηρεσία τετραπλού σκοπού: α) εθνικής ασφαλείας / εσωτερικού (αντικατασκοπίας, αντιτρομοκρατίας), β) συλλογής πολιτικών και οικονομικών πληροφοριών στο εξωτερικό, γ) συλλογής στρατιωτικών πληροφοριών, δ) ανάπτυξης τεχνικών μέσων παρακολούθησης τηλεπικοινωνιών στο εσωτερικό και στο εξωτερικό.

¹¹⁹ Αυτό που παρατηρείται λοιπόν είναι πως η ελληνική Υπηρεσία συνθέτει μια ενιαία μεικτή αυτοτελή υπηρεσία Πληροφοριών. Ο Αποστολίδης υποστηρίζει ότι η συγκέντρωση όλων αυτών των αρμοδιοτήτων παρέχει πλεονέκτημα άμεσης διασταύρωσης στοιχείων εσωτερικού και εξωτερικού ενδιαφέροντος για διάφορα θέματα όπως, π. χ., αυτού της τρομοκρατίας. Από την άλλη προκαλεί διάσπαση προσπαθειών¹²⁰ και κατανομής πόρων που τελικά δεν επιτρέπουν την

¹¹⁹ Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 312

¹²⁰ Γράφει χαρακτηριστικά ο Φιτσανάκης: «Ως απόρροια της έλλειψης ακριβούς χαρακτήρα, η ΕΥΠ έχει εξελιχτεί σε μια υπηρεσία της οποίας οι αρμοδιότητες συμπεριλαμβάνουν λίγο από τα πάντα» -περί τούτου βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 232

ιδιαίτερη απόδοση σε κανέναν τομέα ¹²¹ εκτός αν αποφασιστούν ad hoc δράσεις. Πάντως, κατά τον πρώην διοικητή της Υπηρεσίας σημαντικό στόχο στις μέρες μας οφείλει να αποτελέσει η προστασία των κρατικών επικοινωνιών μετά τις συγκλονιστικές αποκαλύψεις του πράκτορα Edward Snowden.¹²² Ό,τι διατυπώνει ο Αποστολίδης έχει επανατεθεί από τον ίδιο σε παλαιότερες μελέτες του. Στο *Οι υπηρεσίες πληροφοριών στο εθνικό σύστημα ασφαλείας. Η περίπτωση της ΕΥΠ* εν έτει 2007 ρωτάει περί του τύπου της Υπηρεσίας που χρειάζεται η Ελλάδα.¹²³ Αν και δεν διαφωνεί με την ύπαρξη μιας ενιαίας μεικτής Υπηρεσίας, εντύπωσή μας είναι πως κλίνει προς μια με αρμοδιότητες κυρίως εσωτερικού. Η εντύπωση κατατείνει σε βεβαιότητα όταν ο ίδιος τον Ιούνιο του 2008 σε ομιλία του σε ημερίδα της Πανελλήνιας Ομοσπονδίας Συλλόγων της ΕΥΠ τονίζει την υστέρηση των μικρών χωρών, κυρίως λόγω οικονομικού και τεχνολογικού χάντικαπ, στην εκμείωση πληροφοριών εξωτερικού. Ωστόσο αυτή η υστέρηση δεν φαίνεται να απασχολεί ιδιαίτερος καθώς κατά τον Αποστολίδη *...τα μικρά κράτη έχουν περιορισμένο ορίζοντα ενδιαφερόντων στο εξωτερικό που δεν δικαιολογεί τις δαπάνες που απαιτούνται για την ανάπτυξη δυνατοτήτων συλλογής εξωτερικών πληροφοριών* ¹²⁴ · θεωρούμε ότι ο Αποστολίδης δείχνει προς μια υπηρεσία εσωτερικών αρμοδιοτήτων.

Από τη μεριά του ο Σήφης Φιτσανάκης καταγράφει τις προτάσεις που κατά καιρό έχουν γίνει με σκοπό τον διαχωρισμό των αρμοδιοτήτων της ΕΥΠ. Έχει, π. χ., προταθεί η απομάκρυνση από την Υπηρεσία της Αρχής Ασφαλείας Πληροφοριών, του Κλάδου Κρυπτανάλυσης και της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και η μεταφορά τους στο υπουργείο Εθνικής Αμύνης. Επίσης έχει προταθεί η απόσπαση από την ΕΥΠ της συλλογής πληροφοριών περίξ τρομοκρατικών οργανώσεων και η απόδοσή της σε μια νέα υπηρεσία εθνικής ασφαλείας (ένα ελληνικό Department of Homeland Security;) υπό την αιγίδα των υπουργείων Δημοσίας Τάξεως και Εσωτερικών. Κατ' αυτόν τον τρόπο υποστηρίζεται πως η ΕΥΠ θα μπορέσει να επικεντρωθεί στη συλλογή / ανάλυση πληροφοριών που άπτονται της εθνικής διπλωματικής και πολιτικής στρατηγικής.¹²⁵

Οποσδήποτε, συνεχίζει ο Φιτσανάκης, επείγει το ζήτημα διαχωρισμού μεταξύ των κλάδων των εσωτερικών και των εξωτερικών πληροφοριών της Υπηρεσίας. Αυτό διότι οι εσωτερικές επιχειρήσεις συνήθως διαφέρουν από τις εξωτερικές τόσο ως προς την οργάνωση όσο και ως προς τα νομικά παρεπόμενα της δράσης τους. Στην πρώτη περίπτωση το στέλεχος της ΕΥΠ εφόσον δρα επί τη βάση του ημεδαπούς νομοθετικού πλαισίου, δεν παρανομεί. Στην δεύτερη, από τη στιγμή που προβλέπεται κατασκοπευτική δράση στην αλλοδαπή, παρανομεί. Κατά τον τρόπο τούτο γίνεται φανερός ο διαφορετικός επιχειρησιακός σχεδιασμός όπως και η διαφορετική κουλτούρα που διέπει τους κλάδους της αντιπληροφόρησης και της πληροφόρησης. Θα ήταν καλύτερα, συνεχίζει ο μελετητής, οι σχέσεις των δύο κλάδων να

¹²¹ «Η πολυπραγμοσύνη αυτή δημιουργεί σύγχυση ως προς τις προτεραιότητες της Υπηρεσίας, το είδος του προσωπικού και τα μέσα που χρειάζεται» -περί τούτου βλέπε Αποστολίδης Παύλος, *Οι υπηρεσίες πληροφοριών στο εθνικό σύστημα ασφαλείας. Η περίπτωση της ΕΥΠ*, ΕΛΙΑΜΕΠ, Αθήνα, 2007, σ. 19

¹²² Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 312

¹²³ Αποστολίδης Παύλος, *Οι υπηρεσίες πληροφοριών στο εθνικό σύστημα ασφαλείας. Η περίπτωση της ΕΥΠ*, ό. π.

¹²⁴ Αποστολίδης Παύλος, «Υπηρεσίες Πληροφοριών και μικρά κράτη: Η πρόταση της Ελλάδας» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 61

¹²⁵ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 236-237, επίσης, περί ενός ελληνικού Department of Homeland Security βλέπε Nomikos John, “Does Greece Need a Department of Homeland Security?”, RIEAS, 2 Νοεμβρίου 2013 στην ηλεκτρονική σελίδα <http://www.rieas.gr/researchareas/homeland-security/2211-does-greece-need-a-department-of-homeland-security> εις την οποία καταφύγαμε τη 15^η Ιουνίου 2018

περιοριστούν σε επίπεδο στρατηγικών πλάνων και συντονισμού ώστε να αποφεύγεται η ανάμειξη αυτών των δύο διαφορετικών πρακτικών.¹²⁶

Αίσθησή μας είναι πως ο Φιτσανάκης, σε αντίθεση με τον Αποστολίδη, προκρίνει την ύπαρξη δύο υπηρεσιών Πληροφόρησης, εσωτερικών η μία, εξωτερικών η άλλη. Πρόκειται για δύο δομές που (θα) συνεργάζονται σε επίπεδο στρατηγικού σχεδιασμού¹²⁷, ωστόσο, δεν (θα) συστεγάζονται υπό την αιγίδα ενός ενιαίου μεικτού αυτοτελούς οργανισμού.

Σε κάθε περίπτωση όπως έχει διαφανεί, η ύπαρξη υπηρεσίας εσωτερικών Πληροφοριών θεωρείται ως εκ των ων ουκ άνευ με την ύπαρξη υπηρεσίας εξωτερικών Πληροφοριών να ακολουθεί. Σ' αυτό το σημείο θα θέλαμε να μεταφέρουμε τμήμα της συνέντευξης του αναπληρωτή υπουργού Προστασίας του Πολίτη (παλαιό υπουργείο Δημοσίας Τάξεως) Γιάννη Πανούση στην *Καθημερινή* της 8^{ης} Φεβρουαρίου 2015. Σύμφωνα μ' αυτή, η ΕΥΠ πρέπει να διακόψει την ενασχόληση με την εσωτερική ασφάλεια και να στραφεί στις πληροφορίες εξωτερικού και μόνο. Ο λόγος δεν σχετίζεται με κάποιον στρατηγικό σχεδιασμό αλλά με την «αυτονόμηση των ελληνικών μυστικών υπηρεσιών και την ανάγκη για έλεγχο της λειτουργίας τους» ούτως ειπείν, με το φόβο ανεξαρτητοποίησης και κακόβουλης εμπλοκής τους στα πολιτικά πράγματα της χώρας.¹²⁸ Θεωρούμε ότι οι συγκεκριμένες δηλώσεις Πανούση φανερώνουν μάλλον υπερβολή και προχειρότητα από τη στιγμή που ενώ αναφέρονται στην κατάργηση του τμήματος εσωτερικών πληροφοριών της ΕΥΠ, ουδόλως αναφέρονται στον τρόπο αντικατάστασής του εκτός και αν δεν προκύπτει τέτοιο ζήτημα.¹²⁹

Άποψή μας είναι πως ενώ πράγματι η Ελλάς δεν είναι μεγάλη πληθυσμιακά ή γεωγραφικά χώρα (πιθανότατα αυτό δεν ισχύει αν συνυπολογίσουμε την έκταση της ελληνικής ΑΟΖ) δεν δύναται να μην διαθέτει τόσο πολιτικό τμήμα, ή Υπηρεσία, εσωτερικών όσο και εξωτερικών πληροφοριών καθώς το γεωστρατηγικό περιβάλλον εντός του οποίου διαβιεί κάθε άλλο παρά 'κενό' είναι. Αν για το τμήμα / Υπηρεσία εσωτερικών πληροφοριών τα πράγματα είναι δεδομένα, το τμήμα / Υπηρεσία εξωτερικών πληροφοριών, λαμβανομένης υπόψη της οικονομικής στενότητας, οφείλει να στοχεύσει αποκλειστικά σε πέριξ της Ελλάδος χώρες και μόνο υπό αδήριτων αναγκών να επεκταθεί. Υποθέτοντας επιπλέον πως λόγω οικονομικής κρίσεως δυο ξεχωριστές γραφειοκρατίες αποτελούν πολυτέλεια προτείνουμε τη διατήρηση μίας και μόνης ενιαίας μεικτής υπηρεσίας Πληροφοριών πιστεύοντας περαιτέρω σε έναν αρτιότερο πληροφοριακό στρατηγικό σχεδιασμό τη στιγμή που προσωπικά δεν διαβλέπουμε μια αγεφύρωτη φιλοσοφία μεταξύ πληροφοριακών και

¹²⁶ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 237-238

¹²⁷ Σ' αυτό το σημείο ασφαλώς πρέπει να απαντηθεί το εξής: «υπάρχει άραγε εθνικό στρατηγικό όραμα;». Η θετική απάντηση αποτελεί προαπαιτούμενο ύπαρξης ικανών μυστικών υπηρεσιών

¹²⁸ «Τα φανερά έργα και οι σκοτεινές ημέρες της ΕΥΠ», 15 Φεβρουαρίου 2015 στο <https://www.newsbeast.gr/weekend/arthro/788812/ta-fanera-erga-kai-oi-skoteines-imeres-tis-eup> εις το οποίο καταφύγαμε τη 15^η Ιουνίου 2018, επίσης βλέπε στο άρθρο της 9^{ης} Φεβρουαρίου 2015 του στρατιωτικού αναλυτή Γιάννη Νικήτα, «Η νέα Υπηρεσία Πληροφοριών» στη δικτυακή διεύθυνση <http://www.rizopoulospost.com/h-nea-yphresia-plhroforiwn/> εις την οποία καταφύγαμε επίσης τη 15^η Ιουνίου 2018

¹²⁹ Την άποψη ότι η ΕΥΠ δεν οφείλει να λειτουργεί ως υπηρεσία εσωτερικών Πληροφοριών εκφράζουν και οι Ανδρέας Λιαρόπουλος και Ιωάννης Κωνσταντόπουλος διευκρινίζοντας πως η αντιμετώπιση του οργανωμένου εγκλήματος και της εγχώριας τρομοκρατίας δύναται να αποτελέσει αντικείμενο εξειδικευμένου πληροφοριακού τμήματος της ΕΛΑΣ -για μια εικόνα βλέπε Liaropoulos Andrew, Konstantopoulos Ioannis, "Reforming the Greek National Intelligence Service: Untying the Gordian Knot" στο *Journal of Mediterranean and Balkan Intelligence*, Volume 3, Number 1, 2014, σ. 9

αντιπληροφοριακών δράσεων. Σχετικά με την «διασπαστική πολυπραγμοσύνη» που φοβάται ο Παύλος Αποστολίδης τονίζουμε ότι αυτή μπορεί να αντιμετωπιστεί εάν και εφόσον αποδοθούν ξεκάθαρες αρμοδιότητες στις επιμέρους διευθύνσεις. Τέλος, εντός μια ενιαίας Υπηρεσίας οι όποιοι πληροφοριακοί *turf wars* και τριβές θα είναι μάλλον ευκολότερο να λυθούν. Οπωσδήποτε η συγκεκριμένη Υπηρεσία θα πρέπει να συνεργάζεται τόσο με την ΕΛΑΣ, το ΛΣ, τις Ένοπλες Δυνάμεις καθώς και με τα κύρια Υπουργεία.¹³⁰ Αν συμβεί αυτό, τότε, ίσως επιτευχθεί, όπως σημειώνει ο Σήφης Φιτσανάκης, η θεσμοθέτηση ενός κεντρικού συντονιστικού οργάνου εθνικής ασφαλείας, ενός οργάνου που δεν υφίσταται σήμερα ¹³¹ παρά την ύπαρξη του διυπουργικού Συντονιστικού Συμβουλίου Διαχείρισης Πληροφοριών.¹³²

Αλλά, θα ρωτήσει κάποιος, «τι γίνεται με τις στρατιωτικές πληροφορίες;». Η Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ) δημιουργήθηκε το 2003. Υπήχθη στον Α/ΓΕΕΘΑ έχοντας ως έργο τη συλλογή, επεξεργασία και αξιολόγηση στρατιωτικών πληροφοριών όπως και την εκπόνηση σεναρίων ψυχολογικών επιθέσεων. Κατά την στρατιωτική ιστοσελίδα OnAlert η ΔΔΣΠ, με επάνδρωση κάτω του 60%, χωρίς κατάλληλη εκπαίδευση προσωπικού και με έναν υπόγειο πόλεμο να μαίνεται μεταξύ αυτής από τη μια μεριά και των Επιτελείων αλλά και της ΕΥΠ από την άλλη, δεν παρουσίασε αξιόλογο έργο. Γύρω στο 2010 συζητείται για πρώτη φορά η αναβάθμισή της σε αυτοτελή Υπηρεσία υπό τον τίτλο Στρατιωτική Υπηρεσία Πληροφοριών με αποκλειστική ευθύνη τη συλλογή στοιχείων στρατιωτικού ενδιαφέροντος από το εξωτερικό και με τα στελέχη της να μην έχουν καμία σχέση με την ΕΥΠ καθώς όλες οι μέχρι τότε προσπάθειες συνεργασίας είχαν πέσει στο κενό.¹³³ Ωστόσο μέχρι τις μέρες μας η σκέψη μιας αυτοτελούς στρατιωτικής υπηρεσίας Πληροφοριών δεν έχει υλοποιηθεί διά λόγους, όπως μας πληροφορεί η στρατιωτική ιστοσελίδα Militaire, που σχετίζονται με το φόβο των επιτελών δημιουργίας μιας Υπηρεσίας που θα ασκηθεί στο κυνήγι ‘εσωτερικών εχθρών’ αλλά και με την υποχρέωση των στελεχών των Ενόπλων Δυνάμεων να ‘εγγράψουν’ κάποια στιγμή στην καριέρα τους ‘χρόνο διοίκησης’. Έτσι, πολλοί αξιωματικοί, συνεχίζει η ιστοσελίδα, που μπορούν να επανδρώσουν μια τέτοια υπηρεσία (κυρίως λόγω της θητείας τους στην ΕΥΠ) ουσιαστικά δεν είναι διαθέσιμοι επί μακρό και ικανό διάστημα προς επιτυχή κατάληξη του εγχειρήματος -αυτό δεν ισχύει για τους αξιωματικούς του Πολεμικού Ναυτικού καθώς οι συγκεκριμένοι εγγράφουν χρόνο διοίκησης κατά την υπηρεσία τους στην ΕΥΠ. Εδώ οφείλει να σημειωθεί ότι η επάνδρωση μιας στρατιωτικής υπηρεσίας πληροφοριών από αξιωματικούς υπηρετήσαντες στην ΕΥΠ καθόλου δεν θεωρείται από όλους απαραίτητη προϋπόθεση καθώς έχει επίσης προταθεί μια στελέχωσή της, σε πρώτη φάση, από προσωπικό που έχει αποφοιτήσει από σχολεία εκμάθησης βαλκανικών γλωσσών (10 τον αριθμό) που λειτουργούν υπό την αιγίδα του ΓΕΕΘΑ.¹³⁴

¹³⁰ Βλέπε Μπεσίρης Νικόλαος (ταξίαρχος ΕΛΑΣ), «Διακλαδική συνεργασία στο πλαίσιο της πληροφοριακής κάλυψης» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 138-142

¹³¹ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 234-235

¹³² Που με την παρουσία τόσων και τόσων υπουργών (Εσωτερικών, Εξωτερικών, Οικονομίας, Εθνικής Αμύνης, Εμπορικής Ναυτιλίας και άλλων αν αποφασιστεί) μάλλον δεν μπορεί να επιτελέσει το έργο για το οποίο καλείται

¹³³ «Στρατιωτική Υπηρεσία Πληροφοριών: ‘Έρχονται χακί κατάσκοποι’ να καλύψουν το κενό της ΕΥΠ», 22 Αυγούστου 2014 στο <http://www.onalert.gr/stories/stratitiki-ypiresia-plioproforion-erxetai-gia-na-kalyfthei-to-keno> με ημερομηνία προσφυγής τη 18^η Ιουνίου 2018

¹³⁴ Καρβουνόπουλος Πάρις, «Στρατιωτική Υπηρεσία Πληροφοριών, αλλά με τι στελέχη;», 27 Σεπτεμβρίου 2016 στο <https://www.militaire.gr/στρατιωτική-υπηρεσία-πληροφοριών-αλ/> εις το οποίο

Τέλος διαβάζουμε στην στρατιωτικού ενδιαφέροντος ιστοσελίδα e-Amyna: «Γεγονός παραμένει ότι η αυξανόμενη ενασχόληση της υποχρηματοδοτούμενης ΕΥΠ με ζητήματα ασφαλείας, αντικατασκοπείας και αντιτρομοκρατίας έχει δημιουργήσει κενό στην ροή στρατιωτικών πληροφοριών επιβάλλοντας την άμεση ανάληψη συγκεκριμένων ενεργειών». Κατά τη σελίδα οι ενέργειες που πρέπει να λάβουν χώρα είναι οι εξής: α) συγκρότηση Σώματος Στρατιωτικών Πληροφοριών ήτοι, αναβάθμιση της ΔΔΣΠ, β) επέκταση των στρατιωτικών σχολείων πληροφοριών / αντιπληροφοριών και των ανάλογων ξένων γλωσσών με έμφαση στην εκμάθηση της τουρκικής και της αραβικής γλώσσας, γ) τροποποίηση της πάγιας διαταγής του ΓΕΣ περί «χρόνου διοικήσεως αξιωματικών» προκειμένου να αντιμετωπισθεί το άνω αναφερθέν πρόβλημα, δ) κατάρτιση κατάλληλου σχετικού νομοθετικού πλαισίου.¹³⁵

Κατά την άποψή μας το Πεντάγωνο μάλλον πρέπει να προχωρήσει στη δημιουργία αυτοτελούς Υπηρεσίας στρατιωτικών πληροφοριών απελευθερώνοντας την ΕΥΠ από τα σχετικά καθήκοντα. Υποστηρίζουμε ότι η συλλογή και ανάλυση στρατιωτικών πληροφοριών δεικνύει αρμοδιότητα των Ενόπλων Δυνάμεων. Έτσι, η όποια στρατιωτική υπηρεσία πληροφοριών θα πάψει να αποτελεί παραπαίδι του ελληνικού συστήματος πληροφοριών. Τόσο η πολιτική όσο και η στρατιωτική υπηρεσία Πληροφοριών ωφελεί να είναι ισόκυρες, να αντιμετωπίζονται ισότιμα από το πολιτικό προσωπικό. Αν αυτό συμβεί, τότε, δύναται να θεσμοθετηθεί ένα κεντρικό συντονιστικό όργανο εθνικής ασφαλείας ως ήδη αναφέρθηκε παραπάνω. Ενός τέτοιου θεσμού δύναται να προηγηθεί το Συμβούλιο Πληροφοριών (και με ευρύ πιλοτικό χαρακτήρα), ασφαλώς ανεξάρτητο και υπαγόμενο στο πρωθυπουργικό γραφείο καθώς σήμερα υπάγεται / συγκαλείται από την ΕΥΠ ¹³⁶ δηλώνοντας τον κυρίαρχο ρόλο της τελευταίας, πριν καταλήξουμε, ίσως αργότερα, σε ένα Συμβούλιο Εθνικής Ασφαλείας.¹³⁷

(II) Λειτουργικό / επιχειρησιακό επίπεδο: Αυτό που ουσιαστικά ενδιαφέρει σε λειτουργικό επίπεδο σχετίζεται με τη βελτίωση των εργασιών συλλογής, ανάλυσης και διάθεσης πληροφοριών ήτοι, με τη βελτίωση του κύκλου της πληροφόρησης. Αυτή δύναται να επιτευχθεί μέσω: α) σταθερής εκπαίδευσης του προσωπικού, β) δημιουργίας Ακαδημίας Πληροφοριών για τα στελέχη των Υπηρεσιών με πανεπιστημιακή μόρφωση, γ) χρήσης της νέας τεχνολογίας, δ) λελογισμένης συνεργασίας με αλλοδαπές Υπηρεσίες. Ασφαλώς οι ελληνικές μυστικές υπηρεσίες και δη και η ΕΥΠ επιχειρούν την επιμόρφωση του προσωπικού τους μέσω εκπόνησης

καταφύγαμε τη 18^η Ιουνίου 2016, επίσης, Καρβουνόπουλος Πάρις, «Σώμα Στρατιωτικών Πληροφοριών: Η εισήγηση του ΓΕΕΘΑ και γιατί είναι επείγον να ‘περάσει’» στη δικτυακή τοποθεσία <https://www.militaire.gr/υπηρεσία-στρατιωτικών-πληροφοριών/> στην οποία προσφύγαμε τη 18^η Ιουνίου 2018

¹³⁵ «Επιτακτική ανάγκη η συγκρότηση Σώματος Στρατιωτικών Πληροφοριών», 26 Οκτωβρίου 2016 στην ιστοσελίδα e-Amyna στο <http://e-amyna.com/επιτακτική-ανάγκη-η-συγκρότηση-σώματ/> όπου ανατρέξαμε την 23^η Ιουνίου 2018

¹³⁶ Nomikos John, “The Internal Modernization of the Greek Intelligence Service (NIS-EYP)” στο *International Journal of Intelligence and CounterIntelligence*, Volume 17, Issue 3, 2004, σ. 438. Το Συμβούλιο Πληροφοριών της ΕΥΠ ανασυστάθηκε βάσει του Νόμου 3649/2008. Χρειάστηκε να περάσουν έξι ολόκληρα χρόνια προκειμένου να συγκληθεί ημερομηνία πρώτης συνεδρίασης η 11^η Φεβρουαρίου 2014 -για μια ματιά ανέτρεξε στο «Για θέματα ασφαλείας συνεδρίασε το Συμβούλιο Πληροφοριών της ΕΥΠ», *Naftemporiki.gr*, 11 Φεβρουαρίου 2014, στη διαδικτυακή τοποθεσία <http://www.naftemporiki.gr/story/764635/gia-themata-asfaleias-sunedriase-to-sumboulio-pliροφοριων-tis-eyp> εις την οποία ανατρέξαμε την 26^η Μαρτίου 2018

¹³⁷ Περί Συμβουλίου Εθνικής Ασφαλείας βλέπε Μάζης Ιωάννης, *Γεωπολιτική προσέγγιση για ένα νέο Ελληνικό Αμυντικό Δόγμα*, Παπαζήσης, Αθήνα, 2006, σ. 109-147, επίσης, Μάζης Ιωάννης, «Δημιουργία Συμβουλίου Εθνικής Ασφαλείας στην Ελλάδα» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009, σ. 155-162

σεμιναρίων ή αποστολών στο εξωτερικό, επίσης, χρησιμοποιούν νέες τεχνολογίες και συναλλάσσονται με αλλοδαπούς πληροφοριακούς οργανισμούς. Πάρα ταύτα πιθανολογούμε πως δύναται να λάβει χώρα μια εντατικοποίηση των προσπαθειών. Εκεί που παρουσιάζεται ξεκάθαρο έλλειμμα είναι στην εγχώρια συστηματοποίηση της πληροφοριακής γνώσης συλλογής και κυρίως ανάλυσης δεδομένων. Θεωρούμε πως μια Ακαδημία Πληροφοριών θα έρθει προς λύση του ζητήματος εκπαιδεύοντας και διαμορφώνοντας μια νέα γενιά αξιωματούχων της πληροφόρησης. Πρόκειται για πρόταση που έχει κατατεθεί από ειδικούς του χώρου όπως ο Ιωάννης Νομικός, ο Ιωάννης Κωνσταντόπουλος και ο Ανδρέας Λιαρόπουλος, ωστόσο, δεν έχει τελεσφορήσει.¹³⁸

Σχετικά με το επιχειρησιακό επίπεδο, θεωρούμε ότι ο Νόμος 3649 του 2008 αλλά και το Προεδρικό Διάταγμα 1/2017 (ΦΕΚ 2/Α/18-1-2017) είναι κατά βάσει αρκετά ώστε να περιγράψουν / καλύψουν τις αρμοδιότητες μιας ενιαίας μεικτής πολιτικής Υπηρεσίας. Πάρα ταύτα πιστεύουμε πως τίποτα δεν επιβάλλει σε μια τέτοια την ενασχόληση με συλλογή / ανάλυση¹³⁹ στρατιωτικών πληροφοριών εάν και εφόσον υπάρχουν ανάλογα στρατιωτικά σώματα· πράγματι σ' αυτό το σημείο παρουσιάζεται μια αχρείαστη πολυπραγμοσύνη. Επιπλέον διαφωνούμε ως προς τον συντονιστικό πληροφοριακό ρόλο που ο Ν. 3649 αποδίδει, στο πλαίσιο των αποφάσεων του ΚΥΣΕΑ, στην όποια πολιτική Υπηρεσία -στην ΕΥΠ στη προκειμένη περίπτωση. Η ΕΥΠ δύναται ενδεχομένως, και κατόπιν συνεννόησης, να συντονίζει τη δράση των πληροφοριακών τμημάτων των Σωμάτων Ασφαλείας όχι όμως των Ενόπλων Δυνάμεων. Η όποια στρατιωτική Υπηρεσία πρέπει, ως έχουμε ήδη πει, να είναι ισόκυρη με την όποια πολιτική. Συντονιστικό ρόλο μεταξύ των δύο δύναται να παίζει ένα ανεξάρτητο Συμβούλιο Πληροφοριών.

(ΙΙΙ) Επίπεδο ανθρώπινων πόρων: Ξεκινάμε από το κατά τη γνώμη μας αυτονόητο ήτοι, τον φραγμό στο φαινόμενο ανάληψης της διοίκησης μιας Υπηρεσίας -εν προκειμένω της ΕΥΠ- από πρόσωπα που δεν ανήκουν σ' αυτήν. Γράφει ο Φιτσανάκης *...η ΕΥΠ θα πρέπει να διαχωρίσει τη θεσμική της υπόσταση από εκείνη της αστυνομίας, του διπλωματικού σώματος και των ενόπλων δυνάμεων [...] Είναι καιρός η ΕΥΠ να ξεκινήσει να παράγει τα δικά της στελέχη και να βασίζει τη στελέχωση των ανωτάτων κλιμακίων της σε δικούς της υπαλλήλους, που έχουν γαλουχηθεί με το οργανωτικό πνεύμα και την επιχειρησιακή παιδεία της Υπηρεσίας.* Επιπλέον ο μελετητής «καταγγέλλοντας» το μεγάλο αριθμό της επάνδρωσης της ΕΥΠ από προσωπικό των Ενόπλων Δυνάμεων, της Αστυνομίας και του Λιμενικού υποθέτει την εξάρτησή της από τους φορείς αυτούς.¹⁴⁰ Εμείς θα σταθούμε στο γεγονός της ανάληψης της διοίκησής της από διπλωμάτες, δικαστικούς ή ανθρώπους της πολιτικής και του Τύπου. Αν έχουμε αντιληφθεί σωστά η στροφή αυτή έγινε με γνώμονα κυρίως την επίτευξη μιας εξωστρέφειας, λόγω της γνώσης επί διεθνών θεμάτων και πολιτικών που κομίζουν τέτοια πρόσωπα (βλέπε διπλωμάτες ή τον σημερινό διοικητή της ΕΥΠ Ιωάννη Ρουμπάτη, πρώην ευρωβουλευτή του ΠΑΣΟΚ, δημοσιογράφο και διδάκτορα Διεθνών Σχέσεων) ή λόγω μιας προσπάθειας ενίσχυσης, εάν και εφόσον χρειαστεί, των μηχανισμών της λεγομένης 'μυστικής

¹³⁸ Liaropoulos Andrew, Konstantopoulos Ioannis, "Reforming the Greek National Intelligence Service: Untying the Gordian Knot" στο *Journal of Mediterranean and Balkan Intelligence*, ό. π., σ. 11 ¹³⁹ Συνηθίζεται η περί επιχειρησιακού επιπέδου συζήτηση να περιορίζεται στη συλλογή πληροφοριών. Στην παρούσα μελέτη αναφέρεται και στην ανάλυση όχι όμως σε άλλες (επιθετικές) δράσεις

¹⁴⁰ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 235-236

διπλωματίας'.¹⁴¹ Προσωπικά διαφωνούμε. Πρώτον, δηλώνεται μια τάση υποτίμησης του καθαυτού μονίμου προσωπικού της ΕΥΠ. Δεύτερον, η σπουδή και γνώση επί διεθνών θεμάτων, πολιτικών και μυστικών διπλωματικών κινήσεων και διαδρομών δεν αποτελεί πλέον προνόμιο ολίγων ειδικών, άλλωστε, αυτοί δύναται να υπηρετήσουν ως καριερίστες στην Υπηρεσία και όχι ως μετακλητοί / αποσπασμένοι υπάλληλοι. Τρίτον, έχουμε την εντύπωση πως οι όποιοι σχεδιασμοί περί εξωστρέφειας έχουν παρεξηγηθεί -οφείλει να γίνει κατανοητό πως μια μυστική υπηρεσία δεν λειτουργεί στα πρότυπα ανοικτών οργανισμών. Πιστεύουμε πως η ΕΥΠ οφείλει να παράγει διοικητές από μέσα, βέβαια σ' αυτήν την περίπτωση η παύση ενός διοικητού από την κυβέρνηση προφανώς δυσκολεύει σε σχέση με τη σημερινή κατάσταση και αυτό πιθανότατα απασχολεί σε μέγιστο βαθμό τους πολιτικούς προϊσταμένους. Αν ωστόσο λάβει χώρα μια τέτοια ρύθμιση, τότε, η Υπηρεσία θα ενδυναμωθεί ως οργανισμός / θεσμός και σίγουρα μια ικανή πολιτεία καθόλου δεν πρέπει να φοβάται κάτι τέτοιο.

Από κει και πέρα και όσον αφορά στο ανώτερο, μέσο και κατώτερο προσωπικό, ο Ν. 3649 αλλά και το Π.Δ. 1/2017 ορίζουν πώς αυτό κατανέμεται / διεκπεραιώνεται εντός της ΕΥΠ. Ασφαλώς λόγω της φύσεως της Υπηρεσίας κάποιες διατάξεις περί τούτου χαρακτηρίζονται από ελαστικότητα (βλέπε άρθρο 11, 12, 16 και 17 του Ν. 3649). Αν και οι σχετικές προβλέψεις, ειδικά του Π.Δ. 1/2017, αναπτύσσονται λεπτομερώς, μπαίνουμε στον πειρασμό να προτείνουμε τα εξής: α) ενδεχόμενη αύξηση του χρόνου υπηρεσίας των διαφόρων ενδιαφερόντων προϊσταμένων της ΕΥΠ, χρόνου που αυτή τη στιγμή κυμαίνεται μεταξύ των δύο και των τριών ετών εξαιρουμένων του Διοικητού και των δύο Υποδιοικητών του¹⁴², β) η πρακτική των αποσπάσεων, πολλές εκ των οποίων χαριστικές, στην ΕΥΠ υπαλλήλων άλλων πολιτικών ή στρατιωτικών και ημιστρατιωτικών φορέων πρέπει να περιοριστεί στο ελάχιστο καθώς η αλόγιστη εισπήδηση προσωπικού ενός οργανισμού σε άλλον μάλλον παρακωλύει παρά διευκολύνει τις λειτουργίες για διαφόρους λόγους. Μάλιστα, οι συγκεκριμένες αποσπάσεις ορισμένου χρόνου -μέχρι πέντε έτη- συχνά λήγουν όταν ο αποσπασμένος έχει πλέον κατανοήσει το αντικείμενο της εργασίας του και είναι έτοιμος να παράξει έργο. Ασφαλώς, σημειώνουμε, πολλές αποσπάσεις λήγουν πολύ ενωρίτερα φανερώνοντας μάλλον το άσκοπο ή το ευκαιριακό της πραγμάτωσής τους. Πιθανολογούμε ότι κάποιες απολύτως ειδικού χαρακτήρος στοχευμένες αποσπάσεις αορίστου χρόνου με προοπτική τη μεταβολή τους σε μετατάξεις θα εξυπηρετήσουν πολύ καλύτερα το έργο της Υπηρεσίας¹⁴³, γ) αν και προβλέπονται αποσπάσεις προσωπικού άλλων ΝΠΔΔ στην ΕΥΠ, δεν προβλέπονται μετατάξεις. Θεωρούμε πως ένα τέτοιο μέτρο πρώτα απ' όλα θα περιορίζε το φαινόμενο των αποσπάσεων δίνοντας δικαίωμα σε προσοντούχα άτομα να

¹⁴¹ Δεν έχουν γραφεί λίγα για μέχρι και φιλικές σχέσεις μεταξύ επιτελών ισραηλινών μυστικών υπηρεσιών και αντίστοιχων αραβικών στα πλαίσια επίλυσης προβλημάτων μέσω της μυστικής διπλωματίας

¹⁴² Που στην μεταπολιτευτική ελληνική πρακτική, Διοικητές και Υποδιοικητές της ΕΥΠ είθισται να υπηρετούν το ανώτερο για 5 χρόνια. Συνήθης λίγο πολύ είναι η ίδια πρακτική στον ευρωπαϊκό χώρο. Ο περιορισμός της θητείας των Διοικητών σε αυτά τα χρονικά επίπεδα σκοπό έχει την αποφυγή συγκέντρωσης υπερβολικής δύναμης στα χέρια τους. Αν το ζήτημα διευθετείται εύκολα μέσω διορισμών / παύσεων μετακλητών λειτουργών, τι μπορεί να προβλεφθεί σε περίπτωση Διοικητών που προέρχονται από τα σπλάχνα της Υπηρεσίας; Θα παύονται υποχρεωτικά με την παρέλευση κάποιου χρονικού διαστήματος; Αν ναι, και εφόσον δεν βρίσκονται σε συντάξιμη ηλικία, από ποιο πόστο θα συνεχίζουν την καριέρα τους; Μήπως θα μετατάσσονται; Μήπως θα συνταξιοδοτούνται τιμητικά;

¹⁴³ Περί του ζητήματος βλέπε στον καταληκτήριο λόγο του διοικητή της ΕΥΠ Ιωάννη Κοραντή στην ημερίδα της ΠΟΣΕΥΠ της 11^{ης} Ιουνίου 2008 στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 179-180, επίσης στο Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 241-242

υπηρετήσουν στις τάξεις της Υπηρεσίας εφόσον η τελευταία αποδεχτεί το αίτημά τους και με τη σύμφωνη πάντα γνώμη του οργανισμού εκ του οποίου προέρχεται ο αιτών, δ) οφείλει να τεθεί σε εφαρμογή η πρόβλεψη των υποχρεωτικών μετατάξεων αδιάφορων ή αντιπαραγωγικών υπαλλήλων της ΕΥΠ σε άλλες λιγότερο νευραλγικές θέσεις του κρατικού τομέα εάν και εφόσον δεν προβλέπεται η οριστική απόλυσή τους (ουσιαστικά δεν προβλέπεται). Οφείλει να ακολουθηθεί πιστά η υπάρχουσα πρόβλεψη, που μάλλον δεν λαμβάνεται υπόψη, μη μονιμοποίησης προσωπικού πριν την έλευση διαστήματος ικανού -ορίζεται στα δύο χρόνια- προς αξιολόγηση ικανοτήτων, ε) πιθανολογείται η αυστηροποίηση των ποινών σε περίπτωση εκούσιας αποκάλυψης εθνικών απορρήτων τόσο από ενεργό προσωπικό όσο και από συνταξιοδοτούμενο, στ) η συνεχής και υποχρεωτική εκπαίδευση και ο ακάματος έλεγχος του προσωπικού επί τη ικανότητα κατοχής και χρήσης ευαίσθητων δεδομένων πρέπει να θεωρούνται όροι *sine qua non* για την εύρυθμη λειτουργία της Υπηρεσίας, ζ) ένα τεράστιο ζήτημα που οφείλει να τεθεί επί τάπητος είναι το ζήτημα του συνδικαλισμού. Πρόκειται για κατάσταση που έχει στηλιτευθεί από πολιτικούς και φυσικούς προϊσταμένους της ΕΥΠ.¹⁴⁴ Παρά το ότι αυτός, κατά το Σήφη Φιτσανάκη, βοήθησε ως ένα βαθμό στον εκδημοκρατισμό της πολιτικής κουλτούρας της ΕΥΠ¹⁴⁵, προσωπικά δεν θα διαφωνούσαμε ακόμα και με την κατάργηση των συνδικαλιστικών κομματικών οργάνων των υπαλλήλων της Υπηρεσίας και την αντικατάστασή τους από ένα ενιαίο συλλογικό υπαλληλικό όργανο στο πλαίσιο μιας βελτιστοποιημένης διάταξης όπως αυτής, π. χ., του Νόμου 2738 του 1999. Το τελευταίο δύναται να προωθεί προς λύση σε συγκεκριμένη Διεύθυνση ή Υποδιεύθυνση της ΕΥΠ τα όποια προβλήματα των ανδρών και γυναικών του οργανισμού. Η αξίωση επίλυσης αυτών των προβλημάτων θα κρίνεται σε τελικό στάδιο από τη Διοίκηση. Αν κριθούν θετικώς, τότε, θα αντιμετωπίζονται, αναλόγως σοβαρότητας, είτε ενδοϋπηρεσιακώς, είτε μέσω των πολιτικών προϊσταμένων της Υπηρεσίας. Οι όποιοι περιορισμοί στη συνδικαλιστική δράση¹⁴⁶, γνωστοί εκ των προτέρων, θα τονίζονται με σαφέστατο τρόπο στους υποψηφίους προς είσοδο στην ΕΥΠ.¹⁴⁷

¹⁴⁴ Μάλιστα το Σεπτέμβριο του 1999 η τότε κυβέρνηση του ΠΑΣΟΚ θέσπισε μια μάλλον αόριστη διάταξη (άρθρο 27, παράγραφος 2 του Νόμου 2738) βάσει της οποίας η συνδικαλιστική δράση εντός της ΕΥΠ απαγορεύεται «να υπερβαίνει τα όρια που προσδιορίζονται από τις ιδιομορφίες της Υπηρεσίας» -για μια άποψη βλέπε «Εθνική Υπηρεσία Πληροφοριών. Εκδημοκρατισμός τέλους», *Ελευθεροτυπία*, 22 Ιανουαρίου 2006, επίσης στο <https://nomoi.info/%CE%A6%CE%95%CE%9A-%CE%91-180-1999-%CF%83%CE%B5%CE%BB-19.html> εις το οποίο καταφύγαμε την 27^η Ιουνίου 2018. Εν έτει 2010 ο τότε υπουργός Προστασίας του Πολίτη συζητώντας με τον Αμερικανό πρέσβη στην Αθήνα απαξιώνει με απίστευτο τρόπο την ΕΥΠ εμπλέκοντας και τους συνδικαλιστές της. Γράφει επί λέξει ο Φιτσανάκης: «Τέτοια υπήρξε η απαξίωση της ΕΥΠ, που το 2010 ο τότε υπουργός Προστασίας του Πολίτη, Μιχάλης Χρυσοχοϊδης, φέρεται να δήλωσε στον Αμερικανό πρέσβη στην Αθήνα, Ντάνιελ Σπέκχαρτ, ότι 'η ΕΥΠ είναι ένα τίποτα, διότι δεν υπηρετεί την αποστολή της, που είναι η προστασία της Ελλάδας'. Αντίθετα, φέρεται να εκμυστηρεύτηκε ο Χρυσοχοϊδης στον Σπέκχαρτ πως η ΕΥΠ 'είναι επικίνδυνη στην εθνική ασφάλεια [της Ελλάδας] λόγω των πολλαπλών μειονεκτημάτων της, ένα από τα οποία είναι οι συνδικαλισμένοι υπάλληλοί της'» -περί τούτων βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 240-241

¹⁴⁵ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 132-133

¹⁴⁶ Μια συνδικαλιστική δράση που οπωσδήποτε δεν είναι άγνωστη, ως μας πληροφορεί ο πρόεδρος της ΠΟΣΕΥΠ Κ. Α. και εμείς οφείλουμε να σημειώσουμε, σε αντίστοιχες Υπηρεσίες κρατών όπως οι ΗΠΑ, η Βρετανία ή η Γερμανία -περί τούτου βλέπε *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 124

¹⁴⁷ Για μια άποψη στη συζήτηση βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 242-243

Υποστηρίζουμε πως αν κάποιες από τις άνω περί προσωπικού προτάσεις καταλήξουν κάπου, τότε, θα ενισχυθεί τόσο ο παραγωγικός μηχανισμός της Υπηρεσίας όσο και το κύρος της. Ωστόσο η ελληνική πολιτεία, μέχρι στιγμής τουλάχιστον, μάλλον δεν θέλει ή ίσως κοντοστέκεται μπροστά στη σκέψη μιας στιβαρής υπηρεσίας Πληροφοριών.

(IV) Νομικό και ελεγκτικό επίπεδο: Πιστεύουμε ότι οφείλει να επανεξεταστεί το νομικό / θεσμικό πλαίσιο της λειτουργίας των τμημάτων ή υπηρεσιών εσωτερικών Πληροφοριών επί τη βάση της επικαιροποίησης των αρμοδιοτήτων / δικαιωμάτων τους ως προς την αντιμετώπιση νέων αναγκαιοτήτων και κινδύνων. Θα πρέπει να αποδοθούν στις υπηρεσίες εσωτερικών πληροφοριών (ουσιαστικά, κατά πολλούς, ασφαλείας) αρμοδιότητες σύλληψης, κράτησης ή προανακριτικού έργου; Υπενθυμίζουμε ότι η πλειοψηφία των μυστικών υπηρεσιών δεν ενδύεται με τέτοιου είδους προνόμια καθώς προκρίνεται η λογική της εξισορρόπησης ήτοι, η λογική της μη απόδοσης τέτοιου είδους 'εργαλείων' προς αντιστάθμισμα του τεχνολογικού τους προβαδίσματος και του πλεονεκτήματός τους να δρουν εν 'κρυπτώ και παραβύστω'. Ουσιαστικά δεν αποδίδονται σ' αυτές τέτοιου είδους προνόμια υπό το φόβο της, μέσω συσσώρευσης δικαιωμάτων, υπερενίσχυσής τους με ό,τι αυτό δύναται να επιφέρει συνειρμικά ή και κυριολεκτικά. Ασφαλώς το FBI δεικνύει την κορυφαία εξαίρεση, ωστόσο, για αρκετούς μελετητές δεν αποτελεί τόσο υπηρεσία πληροφοριών όσο υπηρεσία επιβολής νόμου και τήρησης τάξεως.

Το δεύτερο που οφείλει να εξεταστεί, αυτό με επιτακτικό τρόπο, είναι το μέσο διά του οποίου θα ελέγχεται η συνταγματική νομιμότητα των δράσεων των ελληνικών μυστικών υπηρεσιών και πιο συγκεκριμένα της ΕΥΠ. Υπενθυμίζουμε ότι βάσει του άρθρου 5, παράγραφος 3 του Νόμου 3649 στην ΕΥΠ υπηρετεί αποσπασμένος εισαγγελικός λειτουργός ο οποίος ελέγχει *...τη νομιμότητα των ειδικών επιχειρησιακών δράσεών της, που αφορούν θέματα Δικαιωμάτων του Ανθρώπου και ασκεί όλες άλλες αρμοδιότητες του ανατίθενται με διατάξεις του παρόντος* (3649/2008) νόμου.¹⁴⁸ Αυτό ασφαλώς δεν αρκεί. Πέραν του εισαγγελικού ελέγχου η βαρύτητα ενός οργανισμού όπως αυτού της ΕΥΠ πρέπει να οδηγεί στην απόδοση λόγου ενώπιον της Βουλής των Ελλήνων.¹⁴⁹ Και πράγματι υπάρχει ένα όργανο του ελληνικού κοινοβουλίου περί τούτου, πρόκειται για την Ειδική Μόνιμη Επιτροπή Θεσμών και Διαφάνειας. Ποιο όμως το έργο της συγκεκριμένης Επιτροπής;

Σύμφωνα με την ιστοσελίδα της Βουλής των Ελλήνων, η Ειδική Μόνιμη Επιτροπή Θεσμών και Διαφάνειας εντέλλεται όπως διεξάγει τον κοινοβουλευτικό έλεγχο «επί των ανεξάρτητων διοικητικών αρχών και επί των μέσων μαζικής ενημέρωσης, καθώς και [να διεξάγει] την επεξεργασία προτάσεων που συμβάλουν στη διαφάνεια της δημόσιας ζωής».¹⁵⁰ Αμέσως αυτό που έρχεται στο μυαλό είναι το εξής: «τι σημαίνει ανεξάρτητη διοικητική αρχή; είναι η ΕΥΠ μια τέτοια;». Από μια μικρή αλλά κατατοπιστική έρευνα που κάναμε διαπιστώσαμε ότι: α) οι Ανεξάρτητες Αρχές αποτελούν κρατικά όργανα, ωστόσο, εκφεύγουν του ιεραρχικού ελέγχου ή της εποπτείας της κεντρικής διοίκησης, υπόκεινται, δε, μόνο σε δικαστικό έλεγχο νομιμότητας [εκτός ασφαλώς του κοινοβουλευτικού]. Κατά τον τρόπο τούτο δεν υπέχουν υποχρέωση υπακοής έναντι των οργάνων της εκτελεστικής λειτουργίας, β) τα μέλη των Ανεξάρτητων Αρχών διαθέτουν προσωπική και λειτουργική εξουσία αντίστοιχη αυτής των δικαστών. Με λίγα λόγια η εκτελεστική εξουσία δεν δύναται να

¹⁴⁸ Βλέπε ΦΕΚ, αριθμός φύλλου 39, 3 Μαρτίου 2008, σ. 546

¹⁴⁹ Όχι πάντως δίχως επιφυλάξεις

¹⁵⁰ Για μια πιο ολοκληρωμένη εικόνα βλέπε στο <https://www.hellenicparliament.gr/Koinovouleftikes-Epitropes/CommitteeDetailView?CommitteeId=2b188390-2f24-4d95-b867-912d485fa8cf> εις το οποίο καταφύγαμε την 29^η Ιουνίου 2018

παρέμβει στον τρόπο με τον οποίο αυτά ασκούν τα καθήκοντά τους, γ) οι Ανεξάρτητες Αρχές διαθέτοντας ευρείες κανονιστικές και κυρωτικές αρμοδιότητες δύνανται να ρυθμίζουν ζωτικούς τομείς της πολιτικής, οικονομικής και κοινωνικής ζωής. Οι αποφάσεις τους, δε, λειτουργούν δεσμευτικά για τα άλλα κρατικά όργανα.¹⁵¹

Εάν ισχύουν τα ανωτέρω, τότε, είναι η ΕΥΠ μια Ανεξάρτητη Αρχή; Ασφαλώς όχι, άλλωστε δεν πρέπει να είναι.¹⁵² Η ΕΥΠ χαίρει αυτοτέλειας λόγω της εγγενούς φύσεώς της, επομένως, ωστόσο, προνομίων Ανεξάρτητης Αρχής καθώς οι δράσεις της δεν είναι νοητό να χαρακτηρίζονται από την ανεξαρτησία των εν λόγω Αρχών ή / και να συγκρούονται με την κυβερνητική βούληση. Κατά τούτη την έννοια είναι η ίδια η Επιτροπή Θεσμών και Διαφάνειας και ο εν γένει τρόπος με τον οποίο περαιώνεται ο κοινοβουλευτικός έλεγχος της Υπηρεσίας που προκαλεί. Κατά συνέπεια θεωρούμε ότι η εν λόγω Επιτροπή δεν πρέπει να βαρύνεται με το έργο ελέγχου της κύριας ελληνικής μυστικής υπηρεσίας.

Αλλά ποια η διεθνής πρακτική ελέγχου των μυστικών υπηρεσιών; Σύμφωνα με αυτήν έχουμε: α) τον εσωτερικό έλεγχο των Υπηρεσιών από την ίδια την διοίκησή τους, β) την επίβλεψη των Υπηρεσιών από την εκτελεστική εξουσία ήτοι, την κυβέρνηση, γ) την κοινοβουλευτική επίβλεψη, δ) τη δικαστική επίβλεψη, ε) την επίβλεψη από τα media και την κοινωνία και στ) την επίβλεψη από διεθνείς κυβερνητικούς αλλά και διεθνείς μη κυβερνητικούς οργανισμούς.¹⁵³ Στη Βρετανία, π. χ., έως και τη δεκαετία του 1980 ίσχυαν δύο αρχές: πρώτον, τα ζητήματα της πληροφόρησης και των Υπηρεσιών δεν συζητούνται δημοσίως, ούτε καν στο Κοινοβούλιο και δεύτερον, το Κοινοβούλιο παραιτείται από τις εξουσίες ελέγχου των μυστικών υπηρεσιών προς χάριν της εκτελεστικής εξουσίας.¹⁵⁴ Αυτή η λογική, για διαφόρους λόγους, λίγο μετά το τέλος του ψυχρού πολέμου παύει να ισχύει. Το βρετανικό Κοινοβούλιο μέσω της νεοπαγούς Intelligence and Security Committee -ISC εκκινεί τη διαδικασία κοινοβουλευτικού ελέγχου των Υπηρεσιών με υποστηρικτές αλλά και επικριτές αυτής της νέας πρακτικής.¹⁵⁵

Από τα μέχρι τούδε γραφόμενα προσωπικά κατανοούμε τα εξής: α) η δικαστική επίβλεψη των Υπηρεσιών είναι απαραίτητη, β) η εσωτερική επίβλεψη επίσης, γ) η εκτελεστική επίβλεψη επίσης, δ) η κοινοβουλευτική επίβλεψη το ίδιο -δεν υπεισερχόμαστε στο ζήτημα της επίβλεψης μέσω των media και του κοινού όπως και

¹⁵¹ Για μια πιο ολοκληρωμένη εικόνα βλέπε στο <https://akrivopoulouchristina.wordpress.com/2010/03/02/ανεξάρτητες-αρχές-χαρακτηριστικά-κα/> εις το οποίο καταφύγαμε την 29^η Ιουνίου 2018

¹⁵² Παρά το ότι λόγω της εποπτείας της από την δικαστική, την εκτελεστική αλλά κυρίως την κοινοβουλευτική εξουσία αποτελεί, κατά τον βουλευτή της ΝΔ και πρόεδρο της Επιτροπής Θεσμών και Διαφάνειας της Βουλής Απόστολο Σταύρου, μια «οιονεί Ανεξάρτητη Διοικητική Αρχή μολονότι παραμένει στον πυρήνα της εκτελεστικής λειτουργίας ως αυτοτελής ή αποκεντρωμένη δημόσια πολιτική υπηρεσία» -για μια εικόνα βλέπε στο Σταύρου Απόστολος, «Ο έλεγχος της ΕΥΠ από τη Βουλή» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 37. Προσωπικά θεωρούμε ότι κάπου στα λόγια του Σταύρου εμπεριέχεται μια αντίφαση

¹⁵³ Konstantopoulos Ioannis, "Democracy and Ethics vs Intelligence and Security: From WikiLeaks to Snowden" στο *Democracy and an Open-Economy World Order*, επιμ. Bitros George, Kyriazis Nicholas, Springer, 2017, σ. 6

¹⁵⁴ Ο Christopher Andrew χαρακτηριστικά υποστηρίζει πως τα μυστήρια της πληροφόρησης πρέπει να αφεθούν ολοκληρωτικά στους ενήλικες, ήτοι στις Υπηρεσίες και στην κυβέρνηση, τα, δε, παιδιά, ήτοι το κοινοβούλιο και η κοινωνία, οφείλουν να μην ανακατεύονται με αυτά. Για μια εικόνα βλέπε Andrew Christopher, *Defend the Realm: The Authorized History of MI5*, Alfred A. Knopf, New York, 2009, σ. 753

¹⁵⁵ Για περισσότερες πληροφορίες βλέπε Κωνσταντόπουλος Ιωάννης, «Κοινοβουλευτική Επίβλεψη Υπηρεσιών Πληροφοριών στις Σύγχρονες Δημοκρατίες και η Ευρωπαϊκή Εμπειρία» στην ιστοσελίδα <http://www.idis.gr/?p=3036> του Ινστιτούτου Διεθνών Σχέσεων (ΙΔΙΣ) εις την οποία προσφύγαμε την 30^η Ιουνίου 2018

της επίβλεψης μέσω διεθνών κυβερνητικών ή μη οργανισμών.¹⁵⁶ Αν για το θέμα της δικαστικής επίβλεψης δεν σημειώνουμε κάτι καθώς αυτή ακολουθεί το συνταγματικό πλαίσιο, για τα υπόλοιπα προτείνουμε: α) η εσωτερική επίβλεψη προφανώς θα ενισχυθεί εάν ο διοικητής, λ. χ., της ΕΥΠ αποτελέσει πρόσωπο εις το οποίο καταθέτει την εμπιστοσύνη της η Βουλή (στα αμερικανικά πρότυπα) και όχι μόνο η κυβέρνηση, β) η κυβερνητική επίβλεψη θα ενισχυθεί εφόσον συνταχθεί προς τούτο κυβερνητική επιτροπή ή, τέλος πάντων, επιτροπή που θα δίδει λόγο στην κυβέρνηση και θα αποτελείται από άτομα που φέρουν θεωρητική και πρακτική περί των Υπηρεσιών γνώση, γ) η κοινοβουλευτική επίβλεψη θα ενισχυθεί εφόσον συνταχθεί προς τούτο και μόνο προς τούτο κοινοβουλευτική επιτροπή ή, τέλος πάντων, εξωτερική επιτροπή (στα πρότυπα της ISC) που θα αποδίδει λόγο στο Κοινοβούλιο και θα αποτελείται από άτομα που διαθέτουν θεωρητική και πρακτική περί των Υπηρεσιών γνώση.¹⁵⁷ Ασφαλώς και πέρα τούτων η γενικότερη κρατική επίβλεψη των Υπηρεσιών θα ισχυροποιηθεί εάν και εφόσον υπάρξει ένας, τονίζουμε κατά το δυνατόν, 'σφικτός προγραμματισμός' της πληροφοριακής / επιχειρησιακής ατζέντας αυτών υπό την έποψη του μη εκτροχιασμού τους όσον αφορά στις δράσεις τους. Από την άλλη μεριά επουδενί προτείνουμε: α) τη διάσπαση / πολυκερματισμό των Υπηρεσιών με σκοπό την απομείωση της δύναμης της κάθε επιμέρους Υπηρεσίας και άρα μια ευκολότερη διαδικασία επίβλεψης¹⁵⁸ (έτσι ή αλλιώς για την ελληνική περίπτωση δεν υποστηρίζαμε τον κερματισμό των Υπηρεσιών) και β) τον οικονομικό ευνουχισμό με σκοπό επίσης την απομείωση της δύναμης των Υπηρεσιών και άρα τον ευκολότερο έλεγχο πάνω τους -πρόκειται για δύο μεθόδους που πράγματι δύνανται να ευκολύνουν το ελεγκτικό έργο της κυβερνητικής ή της κοινοβουλευτικής αρχής με τίμημα, ωστόσο, την τρώση της επιχειρησιακής ικανότητας των πληροφοριακών οργανισμών.

Αν λοιπόν καταλήξαμε λίγο έως πολύ σε έναν αριθμό προτάσεων, ποια η τελική επιλογή; Ως φαίνεται, γράφει ο Ιωάννης Κωνσταντόπουλος, η κοινοβουλευτική

¹⁵⁶ Άλλωστε, δράσεις της ΕΥΠ ελέγχονται από εγχώριους οργανισμούς όπως είναι η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) ή η Αρχή Προστασίας Προσωπικών Δεδομένων

¹⁵⁷ Ο Απόστολος Σταύρου, αν και πρόεδρος της Επιτροπής Θεσμών και Διαφάνειας της Βουλής, ουσιαστικά αφήνει ανοικτό το ενδεχόμενο δημιουργίας καθ' ύλην αρμόδιας κοινοβουλευτικής επιτροπής ή ακόμα και επιτροπής ad hoc προς έλεγχο των πεπραγμένων της ΕΥΠ. Τονίζει πως στο επίπεδο της σύγχρονης αντιπροσωπευτικής δημοκρατίας, η Βουλή έχει δικαίωμα και καθήκον να επιτηρεί την ΕΥΠ. Σε κάθε περίπτωση, συνεχίζει, ο Κανονισμός της Βουλής χρήζει τροποποίησης ώστε να θεσπιστεί πληρέστερο νομοθετικό πλαίσιο εντός του οποίου θα καθορίζονται τα όρια και η έκταση του ελέγχου που θα ασκεί η Βουλή -περί τούτων βλέπε Σταύρου Απόστολος, «Ο έλεγχος της ΕΥΠ από τη Βουλή» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 39-40. Με τη σειρά του ο Σήφης Φιτσανάκης προτείνει μία μεικτή κυβερνητική (πρωθυπουργική, όχι υπουργική) και κοινοβουλευτική εποπτεία. Η τελευταία (η κοινοβουλευτική) θα λαβαίνει χώρα μέσω μιας ειδικής μόνιμης επιτροπής εποπτείας και ελέγχου της Υπηρεσίας στα πρότυπα της Επιτροπής Εθνικής Αμυνας και Εξωτερικών Υποθέσεων. Η επιτροπή αυτή θα είναι απαραίτητα διακομματική με αποστολή τη συστηματική εποπτεία και αξιολόγηση του έργου της ΕΥΠ από τους εκλεγμένους αντιπροσώπους του ελληνικού λαού, καθώς και την τακτική ενημέρωση των μελών της πάνω σε κρίσιμα ζητήματα στρατηγικής, επιχειρήσεων και σχεδιασμού της Υπηρεσίας. Παράλληλα, συνεχίζει ο μελετητής, η ισοδύναμη κατανομή της αρμοδιότητας για την εποπτεία της ΕΥΠ μεταξύ πρωθυπουργού και κοινοβουλίου θα επιτρέψει στην Υπηρεσία να απελευθερωθεί από το πλαίσιο του υπουργείου Δημοσίας Τάξεως (ή όποιου άλλου, συμπληρώνουμε) και να διασυνδεθεί θεσμικά με το ανώτατο σώμα δημοκρατικής διαβούλευσης της ελληνικής πολιτείας -για μια άποψη βλέπε Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 239-240

¹⁵⁸ Η συγκεκριμένη πρακτική ακολουθήθηκε στην περίπτωση της μετά το 1990 Ρουμανίας -για μια άποψη βλέπε Κωνσταντόπουλος Ιωάννης, «Κοινοβουλευτική Επίβλεψη Υπηρεσιών Πληροφοριών στις Σύγχρονες Δημοκρατίες και η Ευρωπαϊκή Εμπειρία», ό. π.

επίβλεψη, χωρίς να αποτελεί πανάκεια, είναι αυτή που πιθανότατα δύναται να φέρει τα καλύτερα αποτελέσματα στο αίνιγμα του ελέγχου της δράσης των Υπηρεσιών.¹⁵⁹ Οπωσδήποτε, σημειώνουμε, ομιλούμε για επίβλεψη από μια καταρτισμένη περί τούτου εσωτερική κοινοβουλευτική επιτροπή (ή εξωτερική επιτροπή που θα δίνει λόγο στη Βουλή) και όχι από μία πολυπράγμονα επιτροπή όπως αυτή των Θεσμών και Διαφάνειας.¹⁶⁰ Από κει και έπειτα δεν πρέπει να ξεχνάμε τους παράγοντες που καθιστούν τη λογοδοσία των Υπηρεσιών πολύ δυσκολότερη υπόθεση από τη λογοδοσία άλλων κρατικών οργανισμών. Αυτοί οι παράγοντες σχετίζονται πρώτον, με την παρουσία της αναπόφευκτης μυστικότητας που χαρακτηρίζει πολλές από τις επιχειρήσεις των πληροφοριακών οργανισμών και δεύτερον, με την ανάγκη προστασίας δεδομένων που αφορούν την εθνική ασφάλεια. Θεωρητικά, γράφει ο Κωνσταντόπουλος, οι υπηρεσίες πληροφοριών δύναται να αποκρύψουν μία δράση τους. Σε τελική ανάλυση, συνεχίζει ο ίδιος, είναι οι πολιτικοί άρχοντες που καλούνται να βρουν τη χρυσή τομή στη σχέση μεταξύ της αποτελεσματικής λειτουργίας των Υπηρεσιών και της συμμόρφωσής τους με τα συνταγματικά απαιτούμενα.¹⁶¹

(V) Οικονομικό επίπεδο: Δυστυχώς η οικονομική στενότητα που μαστίζει τη χώρα τη στιγμή που γράφονται αυτές οι γραμμές δεν αφήνει ιδιαίτερα περιθώρια επιλογών. Ωστόσο ο προϋπολογισμός της Υπηρεσίας οφείλει σε κάθε περίπτωση να ανέλθει καθώς είναι μάλλον απαράδεκτο να κατευθύνεται σε ποσοστό 80 με 90 τοις εκατό στη μισθοδοσία του προσωπικού, άραγε ποια γκάμα επιχειρήσεων δύναται να εκκινήσει και με ποια μέσα, πόρους και πηγές με ό,τι, έτσι ή αλλιώς ελάχιστο, απομένει; Αυτό, τουλάχιστον, καταθέτει ο πρώην διοικητής της Υπηρεσίας Παύλος Αποστολίδης όσον αφορά στους χρόνους της διοίκησής του (1999-2004) ¹⁶² , υπενθυμίζουμε πως επρόκειτο για χρόνους ‘παχέων αγελάδων’ και όχι, σκεφτείτε,

¹⁵⁹ Κωνσταντόπουλος Ιωάννης, «Κοινοβουλευτική Επίβλεψη Υπηρεσιών Πληροφοριών στις Σύγχρονες Δημοκρατίες και η Ευρωπαϊκή Εμπειρία», ό. π. Στο ίδιο ο μελετητής σημειώνει τις προϋποθέσεις που καθιστούν αποτελεσματική την κοινοβουλευτική επίβλεψη των Υπηρεσιών. Αυτές είναι: α) πολιτική βούληση, β) ύπαρξη αναγκαίου εκσυγχρονισμένου νομικού πλαισίου, γ) δημιουργία πολιτικής κουλτούρας που θα υπερασπίζεται τη δράση των υπηρεσιών πληροφόρησης, θα τις ελέγχει μη επιτρέποντας παράλληλα τη χρήση τους προκειμένου εξυπηρέτησης κομματικών συμφερόντων, δ) ανεξαρτησία κοινοβουλευτικών επιτροπών, στήριξή τους από το κοινοβούλιο, εκσυγχρονισμός και εκπαίδευση των μελών τους σε θέματα πληροφόρησης, ε) παροχή στις κοινοβουλευτικές επιτροπές διερευνητικών εξουσιών, οικονομικών πόρων, επαρκούς προσωπικού, πρόσβαση σε διαβαθμισμένα έγγραφα, στ) ικανότητα προστασίας της μυστικότητας και ζ) εκπαίδευση των στελεχών των Υπηρεσιών σχετικά με την αναγκαιότητα και τις διαδικασίες της κοινοβουλευτικής επίβλεψης προκειμένου επίτευξης συνεργασίας ‘ελεγχόμενων και ελεγκτών’. Τέλος, περί τύπων κοινοβουλευτικών ελέγχων χωρών της Ευρώπης επί των Υπηρεσιών τους βλέπε Δερβιτσιώτης Άλκης, «Αναζητώντας τη (δύσκολη) νομιμοποίηση των υπηρεσιών Πληροφοριών - Όψεις της ευρωπαϊκής εμπειρίας» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 109-112, επίσης βλέπε Αποστολίδης Παύλος, *Οι υπηρεσίες πληροφοριών στο εθνικό σύστημα ασφαλείας. Η περίπτωση της ΕΥΠ*, ό. π., σ. 18

¹⁶⁰ Βέβαια στην ελληνική περίπτωση ενσκήπτει ένα πρόβλημα που η ‘πολιτική ορθότητα’ της εποχής τείνει να κουκουλώσει: αυτό της ύπαρξης κυβερνητικών ή μη βουλευτών προερχομένων από τη μειονότητα της Θράκης. Οι συγκεκριμένοι ουκ ολίγες φορές έχουν προκαλέσει με τουρκόφιλες αν μη τι άλλο δηλώσεις. Αν λοιπόν ένας κυβερνητικός ή κοινοβουλευτικός έλεγχος διεξάγεται με περιορισμούς ή καχυποψία, τότε, πόσο μπορεί να είναι ενδελεχής; Σ’ αυτήν την περίπτωση, πέραν του δικαστικού ελέγχου, ο εσωτερικός ενδοϋπηρεσιακός φαντάζει ως μια κάποια απάντηση

¹⁶¹ Κωνσταντόπουλος Ιωάννης, «Κοινοβουλευτική Επίβλεψη Υπηρεσιών Πληροφοριών στις Σύγχρονες Δημοκρατίες και η Ευρωπαϊκή Εμπειρία», ό. π.

¹⁶² Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, ό. π., σ. 311. Μάλιστα στη σελίδα 305 του ίδιου συγγράμματος περιγράφεται πώς η ΕΥΠ έλαβε σημαντική βοήθεια για αγορά αυτοκινούμενων μέσων και τεχνικού εξοπλισμού από την Υπηρεσία Καταπολέμησης Απάτης της Ευρωπαϊκής Επιτροπής· ο προϋπολογισμός της, γράφει ο Αποστολίδης, δεν επέτρεπε την αγορά αυτοκινήτων παρά με το σταγονόμετρο

‘ισχνών’ σαν τους σημερινούς. Από κει και πέρα θα πρέπει να προσεχθεί η μισθοδοσία όλων των αξιωματούχων πληροφοριών και εν γένει όλων εκείνων που διαχειρίζονται διαβαθμισμένο υλικό. Οφείλει να γίνει αντιληπτό πως οι ‘πράκτορες’ όλων των ελληνικών μυστικών υπηρεσιών καλό είναι να κατανοούν τη σημαντικότητα του έργου τους και μέσα από το ύψος των αποδοχών τους ασφαλώς σε συνάρτηση με τους δυσπραγείς οικονομικούς χρόνους που βιώνουμε.

(VI) Επικοινωνιακό / ακαδημαϊκό επίπεδο: Ο Σήφης Φιτσανάκης γράφει πως ...η αντίληψη των ελληνικών μυστικών υπηρεσιών από την ευρύτερη κοινωνία, αλλά και από τα μέσα μαζικής ενημέρωσης, πάσχει σε τρεις κυρίως τομείς. Αυτοί σχετίζονται με: α) την πεποίθηση πως η ΕΥΠ αποτελεί έναν οργανισμό ‘πρακτόρων και σπιούνων’ που εμφορείται από ακραίες ιδεολογίες αστυνόμευσης, β) την εντύπωση πως η ΕΥΠ καλύπτεται / προστατεύεται από ένα πέπλο υπερβολικής μυστικότητας που την καθιστά ύποπτη αν όχι σκοτεινή και γ) την άποψη που ισχυρίζεται πως η ύπαρξη των Υπηρεσιών λίγο έχει να κάνει με τα καθημερινά προβλήματα του πολίτη και πολύ περισσότερο με μια προσπάθεια προστασίας της γραφειοκρατίας τους.¹⁶³ Προκειμένου αυτή η εικόνα να αλλάξει, συνεχίζει ο Φιτσανάκης, οφείλει η ΕΥΠ να επικοινωνήσει το έργο της στην ελληνική κοινωνία. Ο ίδιος, μεταξύ άλλων, προτείνει: α) την ανασύνταξη της ιδεολογικής της ταυτότητας (και) μέσω παραδοχής των παρελθοντικών της λαθών ή, αλλιώς, την αποκήρυξη του φαινομένου τής, κατά τον Αμερικανό κοινωνιολόγο Νόρμαν Μπρίνιμπαουμ, «εισβολής στο εσωτερικό πολιτικό γίγνεσθαι των τεχνικών του ψυχρού πολέμου», β) την προβολή μερικών εκ των επιχειρησιακών επιτυχιών της, γ) την έκδοση της επίσημης ιστορίας της από την ίδια, δ) τη δημιουργία ενός σύγχρονου διαδικτυακού προφίλ, ε) τη σύσταση μιας ομάδας στελεχών που θα δύναται να την εκπροσωπούν επωνύμως, να παρίστανται στα ΜΜΕ, να λαμβάνουν μέρος σε ακαδημαϊκά συνέδρια κ. λ.¹⁶⁴ Οποσδήποτε στην όλη προσπάθεια δεν πρέπει να παραβλεφθεί η συνδρομή των ΜΜΕ που θα ενεργήσουν ως δίαυλος νομιμοποίησης των Υπηρεσιών¹⁶⁵ βοηθώντας στην αποδαιμονοποίηση τους ενώ ταυτόχρονα θα τις ‘ελέγχουν’.¹⁶⁶ Προκειμένου όμως να συμβούν αυτά, καταλήγει ο Φιτσανάκης, η ΕΥΠ καλείται όπως προβεί στην εκτέλεση ενός σχεδιασμού στρατηγικής προσέγγισης όσων ΜΜΕ ενδιαφέρονται για μια υπεύθυνη ενημέρωση της ελληνικής κοινωνίας.¹⁶⁷ Από την άλλη μεριά και όσον αφορά σε επίπεδο εξωτερικής επικοινωνιακής πολιτικής θα πρέπει η ΕΥΠ και η Ελλάδα, κατά τον Φιτσανάκη, να ηγηθούν της προσπάθειας διεθνούς αντιμετώπισης κινδύνων που σχετίζονται και με τη δική μας εθνική ασφάλεια. Η προσπάθεια αυτή οφείλει να λάβει χώρα στα πλαίσια της Ευρωπαϊκής Ένωσης και του ΟΗΕ εξαντλώντας την έννοια της «συλλογικής πληροφοριακής δράσης».¹⁶⁸

Προσωπικά θα συμφωνήσουμε με τα περισσότερα εκ των οποίων προτείνει ο Σήφης Φιτσανάκης σε επίπεδο εσωτερικής επικοινωνιακής πολιτικής αν και το αίτημα της δημόσιας απολογίας της ΕΥΠ και αυτό της αξιοποίησης των ΜΜΕ

¹⁶³ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 223-224

¹⁶⁴ ό. π., σ. 224-225

¹⁶⁵ Για μια περί τούτου ιδέα βλέπε Hillebrand Claudia, “The Role of News Media in Intelligence Oversight” στο *Intelligence and National Security*, Volume 27, Number 5, 2012, σ. 689-706

¹⁶⁶ Για μια περί τούτου ιδέα βλέπε Dover Robert, Goodman Michael, “Introduction” στο *Why Intelligence Needs the Media, Why the Media Needs Intelligence*, επιμ. Dover Robert, Goodman Michael, Columbia University Press, New York, 2009, σ. 1-12

¹⁶⁷ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 226-229

¹⁶⁸ ό. π., σ. 229-231

έρχονται κατά την άποψή μας σε δεύτερη, το λιγότερο, μοίρα. Σε επίπεδο εξωτερικής επικοινωνιακής πολιτικής πιθανόν δεν δύναται να γίνουν ιδιαίτερα πράγματα. Υποπευόμαστε πως η ΕΥΠ δεν διαθέτει το ειδικό βάρος ώστε να ηγηθεί προσπαθειών διεθνούς αντιμετώπισης κινδύνων όπως, π. χ., του κινδύνου της διασυννοριακής τρομοκρατίας. Αυτό που μπορεί να γίνει περιορίζεται μάλλον σε μια προσπάθεια αगाστής, κατά το δυνατόν, συνεργασίας με τις μεγάλες δυτικές ή δυτικόστροφες ξένες Υπηρεσίες.

Ωστόσο, πέραν αυτών, υπάρχει κάτι άλλο που δεν έχει θιγεί, νομίζουμε, στον προσήκοντα βαθμό. Πρόκειται για την ακαδημαϊκή πλευρά του ζητήματος. Όπως έχουμε ήδη πει, ελάχιστα έχουν γραφεί για την έννοια της πληροφόρησης και τη δράση των Υπηρεσιών από Έλληνες ακαδημαϊκούς διδασκάλους. Είναι χαρακτηριστικό ότι μόνο δύο, το πολύ τρεις, πανεπιστημιακοί θεωρούνται ειδικοί στον τομέα περνώντας μάλιστα τη γνώση τους όχι μέσα από κάποια διδασκαλικά προγράμματα στην πληροφόρηση αλλά μέσα από προγράμματα σπουδών στις διεθνείς σχέσεις, στην οικονομία ή στις στρατηγικές σπουδές. Αυτό πρέπει να αλλάξει και θα αλλάξει μόνο μέσα από μια θαρρετή στάση της πανεπιστημιακής κοινότητας. Δεν ομιλούμε οπωσδήποτε για πανεπιστημιακές προσεγγίσεις της ‘σκληρής’ έννοιας της πληροφόρησης ήτοι, της πολιτικοστρατιωτικής και πώς αυτή διεκπεραιώνεται μέσα από τις δράσεις των μυστικών υπηρεσιών. Ομιλούμε για μια αρχική προσέγγιση της έννοιας «πληροφόρηση» όπως αυτή εκλαμβάνεται στην σύγχρονη κοινωνία, στον πολιτισμό, στις επιστήμες, στην οικονομία -κατόπιν τούτου δυνάμεθα να προχωρήσουμε στα εσώτερα και πιο ‘κακόφημα’. Ασφαλώς εντός ενός τέτοιου πλαισίου θα πρέπει να εκδηλωθεί ενδιαφέρον εκπόνησης πτυχιακών, μεταπτυχιακών και διδακτορικών εργασιών έστω και αν δεν υπάρχουν προς το παρόν στον ελληνικό χώρο αρκετοί εξειδικευμένοι καθηγητές. Όσον αφορά στο φοιτητικό κομμάτι είμαστε σίγουροι ότι αυτό θα αγκαλιάσει τα όποια σχετικά μαθήματα ή προγράμματα καθώς το εν λόγω αντικείμενο μόνο βαρετό δεν μπορεί να χαρακτηριστεί.¹⁶⁹

Αυτό που πρέπει να γίνει κατανοητό είναι το εξής: η Ελλάς χρειάζεται την πληροφόρηση όπως χρειάζεται τις ισχυρές Ένοπλες Δυνάμεις καθώς, λόγω γεωπολιτικού / γεωστρατηγικού περιβάλλοντος, δεν αποτελεί μια ευτυχισμένη περίπτωση όπως αυτή της Κόστα Ρίκα που από το 1949 δεν διαθέτει εθνικό στράτευμα. Πώς μια χώρα θα κτίσει ικανό πλέγμα πληροφοριακών ροών που θα ‘τρέχει’ μέσω ικανών στελεχών; Εντός των απαντήσεων σε αυτήν την ερώτηση είναι και η εξής: «(και) μέσα από μια ακαδημαϊκή προσέγγιση που θα φέρει το αντικείμενο πιο κοντά στον νέο Έλληνα πολίτη που διερωτάται ίσως περί τέτοιου είδους θεμάτων θέλοντας να τα πλησιάσει εδώ, στη χώρα του, και όχι κάπου στο εξωτερικό».

(VII) Πολιτικό επίπεδο: Κλείνουμε την σε επτά επίπεδα ανεπτυγμένη πρότασή μας για ένα νέο ελληνικό πληροφοριακό δίκτυο ακριβώς με το τελευταίο επίπεδο: το πολιτικό. Χωρίς καμία καθυστέρηση, χωρίς να δώσουμε έκταση, δεν χρειάζεται κάτι τέτοιο για τα αυτονόητα, υποστηρίζουμε πως: α) επουδενί πρέπει να γίνεται χρήση πληροφοριών προς εξυπηρέτηση μικροκομματικών παιγνίων, β) σε καμία περίπτωση δεν αντιμετωπίζονται οι Υπηρεσίες ως όχημα εξυπηρέτησης πελατειακών σχέσεων, γ) επουδενί πρέπει να εμφανίζονται φαινόμενα που έχουν να κάμουν με το λεγόμενο politicization και δ) επουδενί επιτρέπεται η εμπλοκή των Υπηρεσιών στην πολιτική ζωή του τόπου και στην εν γένει ‘συνταγματική νομιμότητα / ομαλότητα’ της χώρας.

¹⁶⁹ Επίσης βλέπε Liapopoulos Andrew, Konstantopoulos Ioannis, “Reforming the Greek National Intelligence Service: Untying the Gordian Knot” στο *Journal of Mediterranean and Balkan Intelligence*, ό. π., σ. 11

Ωστόσο ένα από τα σημαντικότερα ζητήματα που σχετίζεται με τη λειτουργία της ΕΥΠ, ίσως το σημαντικότερο, είναι εκείνο της πολιτικής υπαγωγής της. Υπό ποίου ή ποίων τις πολιτικές επιταγές πρέπει να βρίσκεται η ΕΥΠ; Στη διάρκεια της ιστορίας της η Υπηρεσία (σαν ΚΥΠ αλλά και σαν ΕΥΠ) έχει υπαχθεί στον Πρόεδρο της Κυβέρνησης, στον Πρωθυπουργό, στον υπουργό Προεδρίας, στον υπουργό Δημοσίας Διοίκησης και Αποκέντρωσης, στον υπουργό Δημοσίας Τάξεως ή Προστασίας του Πολίτη, στο υπουργείο Εσωτερικών κ. λ. Σε κάθε περίπτωση η υπαγωγή της Υπηρεσίας σε υπουργεία εσωτερικών ενδιαφερόντων (Εσωτερικών, Δημοσίας Τάξεως κ. λ.) φαίνεται αταίριαστη. Ο Σήφης Φιτσανάκης, π. χ., εξηγεί τους τρεις λόγους που δεν συνάδουν στη σύνδεση ΕΥΠ και υπουργείου Δημοσίας Τάξεως. Αυτοί είναι: α) οι αρμοδιότητες της ΕΥΠ (αρμοδιότητες εσωτερικών και εξωτερικών πληροφοριών) ξεπερνούν τη δικαιοδοσία του εν λόγω υπουργείου, β) οι αρμοδιότητες της ΕΥΠ που πλέον σχετίζονται και με ασύμμετρες απειλές επιβάλουν τον συντονισμό της Υπηρεσίας με πλήθος φορέων συμμετοχής στο έργο της προάσπισης της εθνικής ασφαλείας και όχι μόνο με έναν και γ) η υπαγωγή της ΕΥΠ στο υπουργείο Δημοσίας Τάξεως παραβλέπει την άσκηση επιχειρήσεων συλλογής πληροφοριών στο εξωτερικό.¹⁷⁰ Τα μειονεκτήματα της εν έτει 2001 απόδοσης της ΕΥΠ στο συγκεκριμένο υπουργείο περιγράφονται άριστα και από τους Ανδρέα Λιαρόπουλο και Ιωάννη Κωνσταντόπουλο. Αυτά σχετίζονται με: α) την αύξηση της επιρροής του law enforcement πάνω στην Υπηρεσία άρα τη μείωση της δυνατότητας λήψεως πρωτοβουλιών εκ μέρους της τελευταίας, β) την επαύξηση ενός ανταγωνισμού ‘κάτω από την ίδια στέγη’ μεταξύ ΕΥΠ και ΕΛΑΣ σχετικά με την αντιμετώπιση του τρομοκρατικού φαινομένου και γ) τον μάλλον περαιτέρω περιορισμό του προϋπολογισμού της κεντρικής ελληνικής μυστικής υπηρεσίας.¹⁷¹

Αυτό που επείγει να γίνει, κατά την άποψη του Φιτσανάκη, άλλων ειδικών με τους οποίους έχουμε συζητήσει (Ανδρέας Λιαρόπουλος, Ιωάννης Κωνσταντόπουλος, Ιωάννης Νομικός) αλλά και τη δική μας, είναι να περάσει η υπαγωγή της Υπηρεσίας στον πρωθυπουργό. Ο τελευταίος ως κεφαλή της κυβέρνησης πρέπει να ενημερώνεται, να ελέγχει πολιτικά και να εγκρίνει προσωπικά τις επιχειρήσεις της τόσο στον εσωτερικό όσο, κυρίως, στον εξωτερικό τομέα¹⁷² -κατά την ίδια λογική πιθανολογούμε πως και η όποια στρατιωτική Υπηρεσία οφείλει να υπάγεται στην πρωθυπουργική τελική αρμοδιότητα.¹⁷³ Η υπαγωγή της ΕΥΠ στο πρωθυπουργικό γραφείο θα ανατρέψει τους περιορισμούς και την ευθυνοφοβία της όποιας ανάλογης υπουργικής μετατρέποντάς την σε ανωτάτου κύρους εθνικό οργανισμό με δυνατότητα

¹⁷⁰ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 238-239. Με αντίστροφη λογική η ΕΥΠ δεν θα μπορούσε επίσης να υπαχθεί στο υπουργείο Εξωτερικών

¹⁷¹ Liaropoulos Andrew, Konstantopoulos Ioannis, “Reforming the Greek National Intelligence Service: Untying the Gordian Knot” στο *Journal of Mediterranean and Balkan Intelligence*, ό. π., σ. 8

¹⁷² Ορισμένοι υποστηρίζουν ότι έτσι η κυβέρνηση χάνει τη δυνατότητα της εύλογης αρνήσεως (plausible deniability) επί του ενός ή του άλλου πεπραγμένου. Σε κάθε περίπτωση μας φαίνεται μάλλον παράλογο ή αφελές να πιστέψουμε πως ένας πρωθυπουργός δεν γνωρίζει τι ποιεί μια κρατική υπηρεσία πληροφοριών εκτός αν είναι ανίκανος, ανεύθυνος κ. λ. -για μια άποψη βλέπε επίσης βλέπε Liaropoulos Andrew, Konstantopoulos Ioannis, “Reforming the Greek National Intelligence Service: Untying the Gordian Knot” στο *Journal of Mediterranean and Balkan Intelligence*, ό. π., σ. 10

¹⁷³ Από τη μεριά τους οι δομές κρατικής ασφαλείας συμπεριλαμβανομένης της Αντιτρομοκρατικής, όλες ανήκουσες στην ΕΛΑΣ, όπως και αυτές του Λιμενικού αλλά και του Πυροσβεστικού Σώματος θα υπάγονται στον αρμόδιο πολιτικό προϊστάμενο (υπουργό Δημοσίας Τάξεως, υπουργό Ναυτιλίας, υπουργό Εσωτερικών κ. λ.). Ο τελευταίος, σε συνεργασία με τον ή τους φυσικούς προϊσταμένους, θα κρίνει αν το όποιο ζήτημα εμπίπτει της κατηγορίας ζητημάτων εθνικής σπουδαιότητας, αν οφείλει ουσιαστικά να τεθεί / αντιμετωπιστεί σε ανώτερο συνεργατικό επίπεδο και υπό την τεχνογνωσία μιας καθαντό υπηρεσίας Πληροφοριών

σύναψης επαφών με μια σειρά υπουργείων βαρύνουσας σημασίας.¹⁷⁴ Αρκεί βέβαια να υπάρξει και από την πλευρά του θεσμικά προϊσταμένου της κυβέρνησης η θέληση της ανάληψης της ευθύνης της καθοδήγησης της ΕΥΠ και ενός άμεσου feedback. Πρόκειται για θέληση που έχει εξαμιστεί υποβιβάζοντας ουσιαστικά την Υπηρεσία σε δευτεροκλασάτο οργανισμό κάτι, ασφαλώς, εθνικά επιζήμιο.¹⁷⁵ Τέλος, ακριβώς επειδή ο επικεφαλής της κυβέρνησης δεν μπορεί να μεταβληθεί σε παντογνώστη, προτείνεται η δημιουργία θέσης πρωθυπουργικού συμβούλου πληροφοριών η θέση θα πληρούται από έμπιστο στον πρωθυπουργό πρώην υψηλόβαθμο στέλεχος των πολιτικών ή στρατιωτικών υπηρεσιών Πληροφόρησης με σκοπό την υγιή κριτική στις όποιες προτάσεις κομίζουν στο πρωθυπουργικό γραφείο οι φυσικοί / επιχειρησιακοί προϊστάμενοι των μυστικών υπηρεσιών.

Συμπεράσματα εν γένει

Η Ελλάς συνεχίζει και θα συνεχίζει για καιρό να αντιμετωπίζει τις μέχρι προ ολίγων ετών γνωστές κλασικές ή 'σύμμετρες' πολιτικές, στρατιωτικές ή οικονομικές προκλήσεις. Εκτός αυτών ασφαλώς οφείλει να σταθεί έναντι, όχι πλέον πολύ νέων, ασύμμετρων απειλών όπως η τρομοκρατία (διεθνής, διασυνοριακή ή εγχώρια), η λαθρομετανάστευση, το οργανωμένο εγχώριο ή διεθνικό έγκλημα, η διαδικτυακή κακόβουλη δράση, το ηλεκτρονικό έγκλημα, ο κυβερνοπόλεμος κ. λ. Όλα αυτά έχουν περιγραφεί από θεωρητικούς και επιχειρησιακούς (Μάζης, Τσάκωνας, Φιτσανάκης, Γρίβας, Ραγιές, Νομικός, Ντόκος, Λιαρόπουλος, Κωνσταντόπουλος, Αποστολίδης, Κοραντής κ. λ.) με τον πληρέστερο τρόπο.

Τι πρέπει λοιπόν να κάνει η χώρα μας σε επίπεδο Υπηρεσιών προκειμένου να μην βρεθεί γυμνή έναντι αυτών των απειλών; Μια απάντηση, γνωρίζοντας το δυσεπίλυτο του ερωτήματος, προσπαθήσαμε να δώσουμε μόλις λίγο παραπάνω. Τα πράγματα περιπλέκονται ασφαλώς υπό την έποψη της μη ουσιώδους γνώσης αυτού που ονομάζουμε 'ασύμμετρο'. Ουσιαστικά, υποπτευόμαστε, κάθε νέο άγνωστο που απειλεί θα κατατάσσεται στην κατηγορία του 'ασύμμετρου' με ό,τι αυτό σημαίνει, μάλλον, δεν σημαίνει κάτι κατατοπιστικό.¹⁷⁶

¹⁷⁴ Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, ό. π., σ. 239

¹⁷⁵ Κατά τον Παύλο Αποστολίδη η μη υπαγωγή της ΕΥΠ στον πρωθυπουργό αλλά σε κάποιο υπουργείο εσωτερικού ενδιαφέροντος αποδεικνύει: α) τη φθίνουσα σημασία της ΕΥΠ στα μάτια των κυβερνώντων ή / και μια προσπάθεια αποπομπής της, μέσω ελέγχου, από την εσωτερική πολιτική πραγματικότητα, β) την κυβερνητική τάση θεώρησης της ΕΥΠ ως υπηρεσία Ασφαλείας δίχως αρμοδιότητες εξωτερικών πληροφοριών και γ) την έλλειψη ενδιαφέροντος υπουργείων που εμπλέκονται με την εξωτερική πολιτική (Αμύνης, Εξωτερικών) να συνδεθούν θεσμικά με την Υπηρεσία. Ο πρώην επικεφαλής της Υπηρεσίας θεωρεί πως η τελευταία ως ενιαίος οργανισμός παρουσιάζει πρόβλημα εφόσον δεν υπάγεται στον πρωθυπουργό -για μια άποψη βλέπε Αποστολίδης Παύλος, *Οι υπηρεσίες πληροφοριών στο εθνικό σύστημα ασφαλείας. Η περίπτωση της ΕΥΠ*, ό. π., σ. 12, 19

¹⁷⁶ Ακριβώς εντός του 'ασύμμετρου' περιλαμβάνονται έννοιες των οποίων τη διαχείριση αν αποδώσουμε στις μυστικές υπηρεσίες, τότε, πράγματι οι τελευταίες κινδυνεύουν να αποπροσανατολιστούν. Κατά το νόημα τούτο η απόδοση στην ΕΥΠ αρμοδιοτήτων και ευθυνών περί την κλιματική αλλαγή ή την πρόληψη επιδημιών φαντάζει σε εμάς προσωπικά υπερβολή. Η ΕΥΠ έτσι ή αλλιώς δεν διαθέτει το οικονομικό βάθος και το ατέλειωτο προσωπικό όπως ασχοληθεί με τέτοιου είδους προβληματισμούς -προς το παρόν μάλλον αρκούν η ΕΜΥ και οι ελληνικοί υγειονομικοί οργανισμοί. Ίσως ίσως ακόμα και η απόδοση της ευθύνης πάταξης του οικονομικού οργανωμένου εγκλήματος στην Υπηρεσία αποτελεί υπέρβαση, άλλωστε, υπάρχει το ΣΔΟΕ και η Διεύθυνση Οικονομικής Αστυνομίας -ασφαλώς υποστηρίζουμε τις όποιες μεταξύ των κρατικών αρχών συνεργατικές κινήσεις. Η ΕΥΠ δεν είναι CIA ή FBI, FSB, MI5 ή MI6, δεν έχει τα μέσα να είναι. Η ΕΥΠ οφείλει να περιοριστεί σε ό,τι σχετίζεται άμεσα με την εθνική ασφάλεια ή συμφέρον, κυρίως να

Το πρώτο που έρχεται στο μυαλό κάθε φορά που ενσκήπτει ένα πρόβλημα είναι η λέξη *μεταρρύθμιση*. Και τέτοιες έχουν επιχειρηθεί ουκ ολίγες φορές στην ιστορία των μυστικών υπηρεσιών με αφορμή κάποια αποτυχία. Όπως σημειώνουν οι Λιαρόπουλος και Κωνσταντόπουλος, η αναδιοργάνωση ενός πληροφοριακού οργανισμού φαίνεται πως αποτελεί δημοφιλή πρακτική των κυβερνώντων προκειμένου να δείξουν ότι ‘δεν κάθονται με σταυρωμένα χέρια’ όταν κάτι πάει στραβά.¹⁷⁷ Είναι όμως μία μεταρρύθμιση ή αναδιοργάνωση εύκολο να καταλήξει σε κάτι αποδοτικότερο από το προηγούμενο για το οποίο επιχειρείται μόνο και μόνο επειδή έτσι ελπίζουμε ή θέλουμε να πιστεύουμε; Η απάντηση είναι *όχι*.

Η αναμόρφωση μιας μυστικής υπηρεσίας, συνεχίζουν οι δύο μελετητές, δεικνύει μια πολύπλοκη επιχείρηση. Οφείλει, π. χ., να λάβει υπόψη προτεραιότητες, στόχους, το ζήτημα του διοικητικού συγκεντρωτισμού έναντι του αποκεντρωτισμού, το ζήτημα της προστασίας των πηγών έναντι του ζητήματος της προάσπισης των ανθρωπίνων δικαιωμάτων, το ζήτημα της ισορροπίας μεταξύ ‘παραγωγών και καταναλωτών’ της πληροφόρησης κ. λ.¹⁷⁸ Οφείλει, επιπλέον, να λάβει υπόψη ζητήματα πολιτικά, οικονομικά, γραφειοκρατικά, νομικά, τεχνολογικά, κοινωνικά, πολιτισμικά κ. α.

Στην ιστορία της ΚΥΠ / ΕΥΠ οι δύο μεγαλύτερες αναμορφωτικές προσπάθειες πιθανότατα ήταν αυτές του 1986 και του 2008 με τους σχετικούς νόμους που τότε ψηφίστηκαν να προσπαθούν να αλλάξουν τη φυσιογνωμία της Υπηρεσίας. Βέβαια έλαβαν χώρα και άλλες μικρότερες προσπάθειες όπως αυτή του 2001 που υπήγαγε την ΕΥΠ στο υπουργείο Δημοσίας Τάξεως ή αυτή του 2002 που της απέδωσε αυξημένες αρμοδιότητες και καθήκοντα εσωτερικής ασφαλείας.

Από ό,τι φαίνεται, και ως άνω συζητήσαμε, τα πράγματα πήγαν λιγότερο καλά από ό,τι θα θέλαμε εξού και οι προτάσεις που κατά καιρούς κατατέθηκαν από τους ειδικούς θεωρητικούς και επιχειρησιακούς του χώρου, και εξακολουθούν να κατατίθενται. Εντός αυτού του πλαισίου τολμήσαμε και εμείς με την ελάχιστη γνώση να παραθέσουμε ένα πλάνο για ένα νέο ελληνικό πληροφοριακό σύστημα. Ωστόσο πεποίθησή μας είναι πως πριν την όποια μεταρρυθμιστική προσπάθεια κάτι άλλο οφείλει να συμβεί, και αυτό το κάτι άλλο σχετίζεται με: α) την κατάθεση ενός εθνικού στρατηγικού σχεδιασμού που θα απαντά στο που και πώς η Ελλάς θέλει να δει τον εαυτό της στο διεθνές περιβάλλον του 21^{ου} αιώνα και ειδικότερα στο διεθνές περιβάλλον της νοτιοανατολικής Μεσογείου και β) την απόκτηση κρατικής και επιχειρησιακής, για να επανέλθουμε στα αρχικά του κεφαλαίου, πληροφοριακής παιδείας εάν και εφόσον πιστεύουμε στη δύναμη της πληροφορίας / πληροφόρησης.

Χωρίς αυτά τα δύο, ειδικότερα χωρίς πληροφοριακή συνείδηση μιας και η περί την πληροφόρηση πραγματεία μας, κάθε μεταρρυθμιστική προσπάθεια όσο καινοτόμος και αν είναι θα αποτύχει. Εν αντιθέσει με αυτό το τελευταίο, αν αποκτηθεί μια ικανή πληροφοριακή κουλτούρα, τότε, οι μυστικές υπηρεσίες μας θα πάνε πολύ καλύτερα ακόμα και με το πλέον μινιμαλιστικό ‘λίφτινγκ’ ή ακόμα και χωρίς αυτό -το πρόβλημα, εν κατακλείδι, δεν συνθέτει πρόβλημα μεταρρυθμίσεων / μεταλλαγών αλλά, κύρια και πρώτα, πρόβλημα νοοτροπίας και αποδοχής του *asset πληροφόρησης*.

ασχοληθεί με προκλήσεις πολιτικού χαρακτήρα και κάποιες συγκεκριμένες ασύμμετρου (τρομοκρατία, λαθρομετανάστευση)

¹⁷⁷ Liaropoulos Andrew, Konstantopoulos Ioannis, “Reforming the Greek National Intelligence Service: Untying the Gordian Knot” στο *Journal of Mediterranean and Balkan Intelligence*, ό. π., σ. 7

¹⁷⁸ ό. π., σ. 6-7

ΕΠΙΛΟΓΟΣ

Ο Σήφης Φιτσανάκης υποστηρίζει πως δεν είναι καθόλου σίγουρο ότι οι Σύμμαχοι θα κέρδιζαν τον Β΄ Π. Π. χωρίς τη βοήθεια των μυστικών υπηρεσιών. Οι τελευταίες ασφαλώς δεν μπορεί να γεννηθούν αυτόματα στη διάρκεια ενός πολέμου, ούτε είναι σωστό να εξαφανιστούν με τη λήξη του. Όποιος πιστεύει σε κάτι τέτοιο είναι σαν να πιστεύει, π. χ., σε έναν στρατό, μάλιστα αξιόμαχο, που εμφανίζεται ως διά μαγείας κατά τη σύγκρουση και κατόπιν αποσύρεται στο άγνωστο. Πρόκειται για παραλογισμό. Όταν ο πόλεμος κτυπήσει την πόρτα ενός έθνους είναι πλέον πολύ αργά για προετοιμασίες. Και προετοιμασία δεν σημαίνει διατήρηση μόνο ικανού στρατεύματος αλλά και ικανών Υπηρεσιών.

Κάτι τέτοιο ωστόσο για τις Ηνωμένες Πολιτείες του μεσοπολέμου φάνταζε περιττό. Το 1919 ο αμερικανικός στρατός και το υπουργείο Εξωτερικών της χώρας δημιουργούν το Γραφείο Κωδικών, γνωστό ως «Μαύρο Δωμάτιο». Στόχος απέτελεσε η ορθή ανταπόκριση των ΗΠΑ στις στρατηγικές απαιτήσεις του μεταπολεμικού διεθνούς περιβάλλοντος μέσω της τέχνης της κλοπής και της αποκρυπτογράφησης διπλωματικών μηνυμάτων ξένων κυβερνήσεων. Παραδόξως, σταδιακά, οι κρατικές επιχορηγήσεις προς το Γραφείο έβαιναν μειούμενες. Ακριβώς δέκα χρόνια μετά, ο Χέρμπερτ Γιάρντλεϋ, διευθυντής του «Δωματίου», επισκέπτεται τον Αμερικανό υπουργό Εξωτερικών Χένρι Στίμσον ευελπιστώντας σε αύξηση του προϋπολογισμού του οργανισμού. Προσπαθεί να τον πείσει κομίζοντας δείγμα της δουλειάς του Γραφείου ήτοι, αποκωδικοποιημένα απόρρητα τηλεγραφήματα μεγίστης σημασίας. Η αντίδραση του υπουργού; Κάθε άλλο παρά αναμενόμενη. Αφού σηκώνεται από την καρέκλα δηλώνει, σχεδόν ουρλιάζοντας, στον Γιάρντλεϋ: «Οι τζέντλεμεν δεν υποκλέπτουν την αλληλογραφία άλλων τζέντλεμεν» -το Γραφείο Κωδικών σφραγίζεται για λόγους 'ηθικής τάξεως'.

Αλλά δέκα χρόνια περνούν πριν ο Στίμσον αναλάβει υπουργός Πολέμου στην κυβέρνηση Ρούσβελτ. Ένας νέος μεγάλος πόλεμος, ο μεγαλύτερος, πλησιάζει. Ο υπουργός έχοντας καταλάβει μάλλον το πρότερο σφάλμα του ζητά την ανασύσταση των μυστικών υπηρεσιών. Είναι όμως αργά. Η διάλυση του «Μαύρου Δωματίου» έχει επιφέρει μέγιστο πλήγμα στην αμερικανική ικανότητα κρυπτανάλυσης. Βρετανοί, Γερμανοί, Ιάπωνες, Σοβιετικοί βρίσκονται πολύ μπροστά σε γνώση· θα περάσουν χρόνια προκειμένου οι μυστικές υπηρεσίες των ΗΠΑ να ανανήψουν. Επιπλέον, υποστηρίζεται πως η έλλειψη κρυπταναλυτικών μεθόδων υπήρξε ένας από τους λόγους που η Αμερική δεν αντελήφθη τις ιαπωνικές προπαρασκευές για την επίθεση στο Περλ Χάρμπορ.¹

Το δίδαγμα της άνω μικρής παράθεσης είναι ξεκάθαρο. Οι κλασικοί πληροφοριακοί οργανισμοί διατηρούν μόνιμο και σταθερό ρόλο στον ιστό ασφαλείας και προώθησης συμφερόντων ενός κράτους. Κατασκοπία και αντικατασκοπία αποτελώντας τις δύο όψεις του αυτού νομίσματος καλούνται να υπηρετήσουν την κυβέρνηση, τους πολίτες, την εθνική κοινωνία.

Ειδικότερα, αντικατασκοπία σημαίνει / σημαίνει:

- Το πλέον σκοτεινό, ασαφές, κερματισμένο πληροφοριακό πεδίο.
- Πόλεμος μεταξύ κατασκόπων.
- Κατασκοπία εις βάρος κατασκόπων, μια, δικός μας ο όρος, 'υπερκατασκοπία'.
- Πρακτορική δράση τόσο εντός όσο εκτός συνόρων.

¹ Fitsanakis J., "National Security Agency: The Historiography of Concealment" στο *The History of Information Security*, επιμ. de Leeuw, K. και Bergstra, J., Elsevier BV, Άμστερνταμ, 2006, σ. 523-564

- Κυκλική διαδικασία με την αρχή και το τέλος να ευρίσκονται / συναντιούνται στις ‘ανάγκες της πολιτικοστρατιωτικής ηγεσίας’.
 - Αξιοποίηση κρυφών πηγών, εκμείωση μυστικών, χρήση αδιαφανών μέσων.
 - Συμβολή / σύνδεση με το positive intelligence.
 - Αμυντική / επιθετική πληροφοριακή δράση.
- Η αντικατασκοπία συμβάλει:
- Στην πολιτική, στρατιωτική, οικονομική, κοινωνική, δικτυακή ασφάλεια όπως και στον αντιτρομοκρατικό σχεδιασμό ενός κράτους.
 - Στην εξυπηρέτηση κρατικών συμφερόντων και στρατηγικών.
 - Στην απομείωση της πολιτικής αβεβαιότητας, αμέσως για ορισμένους (positive intelligence), εμμέσως για άλλους (security procedure).
 - Στην πολιτική και στρατιωτική διαδικασία λήψεως αποφάσεων, αμέσως για ορισμένους (positive intelligence), εμμέσως για άλλους (security procedure).
- Η αντικατασκοπία και, γενικότερα, η πληροφόρηση δεν δύνανται:
- Να γνωρίζουν το μέλλον.
 - Να καταλήγουν σε συμπεράσματα που πάντα δικαιώνονται.
 - Να μην περιπέσουν σε λάθη (επιχειρησιακά, ανάλυσης κ. λ.).
 - Να αποτελέσουν το μοναδικό εργαλείο επίρρωσης αισθήματος εθνικής ασφαλείας και πραγμάτωσης εθνικών σχεδιασμών.

Το αντικατασκοπευτικό, ευρύτερα, πληροφοριακό στοιχείο δύναται να αποτελέσει συντελεστή πολιτικής, στρατιωτικής, οικονομικής, κοινωνικής ασφάλειας και ισχύος. Η συγκεκριμένη παραδοχή σημάνει ως έχουμε ήδη αποδεχτεί το απαραίτητο ύπαρξης μυστικών υπηρεσιών ταγμένων στην εξυπηρέτηση του έθνους. Αυτή ουσιαστικά είναι η πρόταση πολιτικής της ανά χείρας μελέτης, η δημιουργία και διατήρηση ικανών Υπηρεσιών, μια δημιουργία και διατήρηση που εξαρτάται από την πολιτική βούληση. Ωστόσο, δεν πρέπει να ξεχνάμε, προηγείται η δόμηση μιας **κουλτούρας ασφαλείας και πληροφοριών** που φαίνεται να χωλαίνει στη χώρα μας. Σ’ αυτό ακριβώς ελπίζει ο Κωνσταντίνος Γρίβας, καθηγητής στη Σχολή Εθνικής Ασφαλείας (Σ.Ε.Θ.Α.) και στην Στρατιωτική Σχολή Ευελπίδων (Σ.Σ.Ε.), που κλείνει την παρουσίασή του -και μας βοηθά και μας να κλείσουμε τη μελέτη- στην ημερίδα της ΠΟΣΕΥΠ της 11^{ης} Ιούνη 2008 ως εξής:

Σε κάθε περίπτωση, αυτό που θα ήθελα να κρατήσετε από την ομιλία μου είναι ότι θα πρέπει να αφήσουμε πίσω μας το στερεότυπο της ‘σκοτεινής δύναμης’ που έχουμε για μια υπηρεσία πληροφοριών, ή αυτό του ‘κατασκόπου που δουλεύει στο σκοτάδι’ και να την αντιμετωπίσουμε ως ένα ισχυρό εργαλείο στα χέρια της κοινωνίας για την ερμηνεία προβλημάτων κρίσιμης σημασίας και πρόγνωσης των πιο ζοφερών εκφάνσεων του μέλλοντος, όχι βέβαια για να κινδυνολογήσει αλλά για να επιχειρήσει να τις αποφύγει.²

² Γρίβας Κ., «Οι ασύμμετρες απειλές ως γεωπολιτικό φαινόμενο και ο ρόλος των υπηρεσιών Πληροφοριών στην αντιμετώπισή τους» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, ό. π., σ. 95

ΑΡΚΤΙΚΟΛΕΞΟ Ι

ΓΔΕΑ -Γενική Διεύθυνση Εθνικής Ασφαλείας
ΓΕΕΘΑ -Γενικό Επιτελείο Εθνικής Αμύνης
ΓΕΣ -Γενικό Επιτελείο Στρατού
ΔΔΣΠ -Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών
ΔΕΥΠ -Διεύθυνση Ειδικών Υπηρεσιών Πολέμου
ΔΥΠλ -Διεύθυνση Υπηρεσία Πληροφοριών
ΕΥΠ -Εθνική Υπηρεσία Πληροφοριών
ΚΥΠ -Κρατική Υπηρεσία Πληροφοριών
ΚΥΠΕ -Κρατική Υπηρεσία Πληροφοριών και Ερευνών
ΚΥΣΕΑ. -Κυβερνητικό Συμβούλιο Εξωτερικών και Αμύνης
ΟΑΣΕ -Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη
ΟΟΣΑ -Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΥΑΚ -Υπηρεσία Ασφαλείας Κράτους
ΥΓΑΚ -Υπηρεσία Γενικής Ασφαλείας Κράτους
ΥΠΕΠ -Υπηρεσία Ερευνών και Πληροφοριών
ΥΠΣ -Υπηρεσία Προστασίας Στρατεύματος

ΑΡΚΤΙΚΟΛΕΞΟ ΙΙ

AUS: Αυστραλία
CAN: Καναδάς
DE: Γερμανία
EU: Ευρωπαϊκή Ένωση
FRA: Γαλλία
ISR: Ισραήλ
RUS: Ρωσία
UK: Ηνωμένο Βασίλειο
US: Ηνωμένες Πολιτείες
USSR: Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών

ACIC -Army Counterintelligence Center (US)
ACPO -Association of Chief Police Officers
ADA -Air Defense Artillery (US)
AFOSI -Air Force Office of Special Investigations (US)
AFP -Australian Federal Police (AUS)
AF-SAB -Air Force Scientific Advisory Board (US)
AO -Area of Operation
AR -Army Regulation (US)
ARVN -Army of the Republic of Vietnam
ASCC -Army Service component command (US)
ASIO -Australian Security Intelligence Organization (AUS)
ASIS -Australian Secret Intelligence Service (AUS)
AT/FP -Antiterrorism Force Protection (US)
BI -Business Intelligence
BfV -Bundesamt für Verfassungsschutz / Federal Office for the Protection of the Constitution (DE)
BGS -Bundesgrenzschutz / Federal Border Guard (DE)
BKA -Bundeskriminalamt / Federal Criminal Police (DE)
BND -Bundesnachrichtendienst / Federal Intelligence Service (DE)
CA -Civil Affairs

CASIS -Canadian Association for Security and Intelligence Studies (CAN)
 CCI -Cyber-Counterintelligence
 CDC -Cleared Defense Contractor
 CE -Counterespionage
 C-E -Communications / Electronics
 CEPOL -Coll ège Europ éen de Police (EU)
 CERN -Computer Emergency Response Team
 CERT -Computer Emergency Readiness Team (EU)
 CFSO -Counterintelligence Force Protection Source Operations
 CHIS -Covert Human Intelligence Source (US)
 C-HUMINT -Counter Human Intelligence
 CI -Counterintelligence, Counterinformation, Combat Intelligence, Competitor Intelligence
 CI MAGTF -Counterintelligence Marine Air-Ground Task Force (US)
 CIA -Central Intelligence Agency (US)
 CIFA -Counterintelligence Field Activity (US)
 CIKR -Critical Infrastructures and Key Resources
 C-IMINT -Counter Imagery Intelligence
 CIP -Critical Infrastructure Protection
 CNA -Computer Network Attack
 CNAs -Center for Naval Analyses (US)
 CNCI -Comprehensive National Cybersecurity Initiative (US)
 CND -Computer Network Defense
 CNE -Computer Network Exploitation
 CNO -Computer Network Operations
 COA -Course of Action
 COIN -Counterinsurgency
 COMPSTAT -Computer Statistics
 COMSEC -Communications Security
 CONTEST -Counter-Terrorism Strategy
 COSI -Committee on Operational Cooperation on Internal Security (EU)
 C-SIGINT -Counter Signals Intelligence
 CSC -Council Security Committee (EU)
 CSIS -Canadian Security Intelligence Service (CAN), Center for Strategic and International Studies (US)
 CSTARC -Cyber Security Tracking, Analysis, and Response Center (US)
 CTD -Counterterrorism Division (US)
 CTR -Cash Transaction Report
 CYBERCOM -Cyber Command (US)
 C2 -Command and Control
 C2W -Command and Control Warfare
 C4I -Command, Control, Communications, Computers, Intelligence
 C4ISR -Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
 DBA -Dominant Battlefield / Battlespace Awareness
 DCI -Director of Central Intelligence (US)
 DCIP -Defense Critical Infrastructure Program (US)
 DCRG -Direction Centrale des Renseignements G énéraux / Central Directorate of General Intelligence (FRA)

DCRI -Direction Centrale du Renseignement Intérieur / Central Directorate of Interior Intelligence (FRA)
 D&D -Denial & Deception
 DoD -Department of Defense (US)
 DoDD -Department of Defense Directive (US)
 DoDI -Department of Defense Instruction (US)
 DoE -Department of Energy (US)
 DEA -Drug Enforcement Administration (US)
 DECA -Developing Espionage and Counterintelligence Awareness (US)
 DGSE -Direction Générale de la Sécurité Extérieure / General Directorate for External Security (FRA)
 DHS -Department of Homeland Security (US)
 DIA -Defense Intelligence Agency (US)
 DNI -Director of National Intelligence (US)
 DPSD -Direction de la Protection et de la Sécurité de la Défense (FRA)
 DSS -Defense Security Service (US)
 DST -Direction de la Surveillance du Territoire / Directorate of Territorial Surveillance (FRA)
 EC3 -European Cyber Crime Center
 EDA -European Defence Agency (EU)
 EEAS - European External Action Service (EU)
 EEI -Essential Elements of Information
 EEFI -Essential Elements of Friendly Information
 ELINT -Electronic Intelligence
 ENISA -European Network and Information Security Agency (EU)
 EO -Executive Order (US)
 EPW -Enemy Prisoner of War
 FBI -Federal Bureau of Investigations (US)
 FINCEN -Financial Crimes Enforcement Network (US)
 FININT -Financial Intelligence
 FIS -Foreign Intelligence Services
 FISMA -Federal Information Security Management Act (US)
 FISS -Foreign Intelligence and Security Services
 FIU -Financial Intelligence Unit
 FM -Field Manual
 FRMO -Full Range Military Operations
 FSB / ФСБ -Federal Security Service / Federal'naya Sluzhba Bezopasnosti / Федеральная Служба Безопасности / ФСБ (RUS)
 FS-ISAC -Financial Services Information Sharing and Analysis Center
 GAO -Government Accountability Office (US)
 GATT -General Agreement on Tariffs and Trade
 GCHQ -Government Communications Headquarters (UK)
 GIS -Geographic Information System
 GTAZ -Gemeinsamen Terrorismusabwehrzentrum / Joint Counterterrorism Center (DE)
 HA -Humanitarian Assistance
 HIDTA -High Intensity Drug Trafficking Area (US)
 HSPD -Homeland Security Presidential Directive (US)
 HST -Human Intelligence Support Teams
 HUMINT -Human Intelligence

HVAs -Human Intelligence Vulnerability Assessments
 IA -Information Assurance
 IAC -Information-Age Conflict
 IACP -International Association of Chiefs of Police
 IB -Intelligence Branch
 IC -Intelligence Community
 ICD -Intelligence Community Directive (US)
 ICS -Intelligence Community Standard (US)
 ID / CTB -Intelligence Division & Counter-Terrorism Bureau (NYPD)
 IDF -Israel Defense Force (ISR)
 ILP -Intelligence-Led Policing
 IMINT -Imagery Intelligence
 INSET -Integrated National Security Enforcement Teams (CAN)
 IO -Information Operations
 IPB -Intelligence Preparation of the Battlefield
 IR -International Relations
 ISA -Israel Security Agency (ISR), International Studies Association (US)
 ISACs -(Private Sector) Information Sharing and Analysis Centers
 ISC -Intelligence and Security Committee (UK)
 IT -Information Technology
 ITAC -Integrated Threat Assessment Centre (CAN)
 ITO -International Terrorist Organizations
 IW -Information Warfare
 I&W -Indication & Warning
 JCTICU -Joint Counter-Terrorism Intelligence Coordination Unit (AUS)
 JIC -Joint Intelligence Committee (UK)
 JP -Joint Publication (US)
 JTF-CND -Joint Task Force-Computer Network Defense (US)
 JTF-CNO -Joint Task Force-Computer Network Operations (US)
 JTTFs -Joint Terrorism Task Forces (US)
 J-2X -Joint Force Counterintelligence and Human Intelligence Staff Element (US)
 KGB -Committee for State Security / Komitet Gosudarstvenniy Bezopasnosti /
 Комитет Государственной Безопасности / KGB (USSR)
 LAA -Limited Access Authorization
 LeT -Lashkar-e-Taiba / Army of the Good
 LfV -Landes ämter für Verfassungsschutz / Regional Intelligence Organizations (DE)
 LIC -Low Intensity Conflict
 MAD -Milit ärischer Abschirmdienst / Military Counterintelligence Service (DE)
 MAGTF -Marine Air Ground Task Force (US)
 MASINT -Measurement and Signatures Intelligence
 MCTL -Military Critical Technologies List (US)
 MCWP -Marine Corps Warfighting Publication (US)
 MDCI -Multidisciplinary Counterintelligence
 MEF -Marine Expeditionary Force (US)
 MGB -Ministry of State Security / Ministerstvo Gosudasrtvennoi Bezopasnosti /
 Министёрство Росудárственной Везопáсности / MRB (USSR)
 MI -Military Intelligence
 MILDEC -Military Deception
 MOOTW -Military Operations other than War
 MP -Military Police

MVD -Ministry of Internal Affairs / Ministerstvo Vnutrennikh Del /
 Министерство Внутренних Дел / МВД (USSR)
 NAC -North Atlantic Council
 NACIC -National Counterintelligence Center (US)
 NASA -National Aeronautics and Space Administration (US)
 NATO -North Atlantic Treaty Organization
 NCISP -National Criminal Intelligence Sharing Plan
 NCIX -National Counterintelligence Executive (US)
 NCSD -National Cyber Security Division (US)
 NCSRS -National Cyberspace Security Response System (US)
 NCTC -Counterterrorism Center (US)
 NCTL -National Critical Technologies List (US)
 NCW -Network Centric Warfare
 NGA -National Geospatial-Intelligence Agency (US)
 NIE -National Intelligence Estimate (US)
 NIS -Network and Information Security
 NKVD -People's Commissariat for Internal Affairs / Narodniy Kommissariat
 Vnutrennykh Del / Народный Комиссариат Внутренних Дел /
 НКВД (USSR)
 NMSP-WOT -National Military Strategic Plan for the War on Terrorism (US)
 NRO -National Reconnaissance Office (US)
 NSA -National Security Agency (US)
 NSAs -Non-State Actors
 NSA 47 -National Security Act 1947 (US)
 NSC -National Security Council (US / UK)
 NSCID -National Security Council Intelligence Directive (US)
 NSTL -National Security Threat List (US)
 NTAC -National Threat Assessment Centre (AUS)
 NYPD -New York City Police Department
 ODNI -Office of the Director of National Intelligence (US)
 OECD -Organization of Economic Cooperation and Development
 OIA -Office of Intelligence and Analysis (US)
 ONCIX -Office of the National Counterintelligence Executive (US)
 ONE -Office of National Estimates (US)
 ONI -Office of Naval Intelligence (US)
 OOTW -Operations Other Than War
 OPSEC -Operations Security
 OSCE -Organization for Security and Cooperation in Europe
 OSD -Office of Secretary of Defense (US)
 OSINT -Open Source Intelligence
 PCCIP -President's Commission on Critical Infrastructure Protection (US)
 PCO -Peacetime Contingency Operations
 PDD -Presidential Decision Directive (US)
 PPP -Public Private Partnerships
 PSC -Political and Security Committee (EU)
 PSCCWO -Protective Security Coordination Centre Watch Office (AUS)
 PSI -Personnel Security Investigation
 RAF -Rote Armee Fraktion / Red Army Faction ή Red Army Fraction (DE)
 RCMP -Royal Canadian Mounted Police (CAN)
 RIA -Revolution in Information-Intelligence Affairs

RISS -Regional Information Sharing System (US)
 RMA -Revolution in Military Affairs
 RSA -Revolution in Security Affairs
 SALUTE -Size, Activity, Location, Unit, Time, Equipment
 SAP -Special Assess Program
 SAR -Suspicious Activity Report
 SATRAN -Satellite Reconnaissance Advance Notice
 SCADA -Supervisory Control And Data Acquisition
 SCSR -Service Canadien de Sécurité et de Renseignements / Canadian Security Intelligence Service (CAN)
 SDAT -Sous-Direction Anti-terroriste / Anti-Terrorist Sub-Directorate (FRA)
 SECNAVINST -Secretary of the Navy Instruction (US)
 SGDN -Secrétariat Général de la Défense Nationale / National Defense General Secretariat (FRA)
 SIAR -Surveillance Industrielle de l' Armement (FRA)
 SIGINT -Signals Intelligence
 SIS -Secret Intelligence Service / MI6 -Military Intelligence, Section 6 (UK)
 SOF -Special Operations Forces
 SS -Security Service / MI5 -Military Intelligence, Section 5 (UK)
 SSCI -Senate Select Committee on Intelligence (US)
 S&TI -Scientific & Technical Intelligence
 SVR -Russian Foreign Intelligence Service / Sluzhba Vneshney Razvedki / Служба Внешней Разведки / CBP (RUS)
 SWOT -Strengths, Weaknesses, Opportunities, Threats
 TEMPEST -Transient Electromagnetic Pulse Emanation Standard
 TOC -Transnational Organized Crime
 TSC -Terrorist Screening Center (US) TSC[M]
 -Technical Security Countermeasures
 TSCM -Technical Surveillance Countermeasures
 TTP -Tactics, Techniques, Procedures
 UCLAT -Unite de Coordination de la Lutte Anti-terroriste / Coordination Unit for the Anti-Terrorist Struggle (FRA)
 USCYBERCOM -U.S. Cyber Command (US)
 USPACOM -U.S. Pacific Command (US)
 USSPACECOM -U.S. Space Command (US)
 USSOCOM -U.S. Special Operations Command (US)
 USTRANSCOM -U.S. Transportation Command (US)
 VNA -Violent Non-State Actor

ΕΛΛΗΝΙΚΗ Ή ΜΕΤΑΦΡΑΣΜΕΝΗ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ /
ΑΡΘΡΟΓΡΑΦΙΑ

Αποστολίδης Παύλος, *Οι υπηρεσίες πληροφοριών στο εθνικό σύστημα ασφαλείας. Η περίπτωση της ΕΥΠ*, ΕΛΙΑΜΕΠ, Αθήνα, 2007

Αποστολίδης Παύλος, «Υπηρεσίες Πληροφοριών και μικρά κράτη: Η πρόταση της Ελλάδας» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Αποστολίδης Παύλος, *Μυστική δράση. Υπηρεσίες πληροφοριών στην Ελλάδα*, Παπαζήσης, Αθήνα, 2014

Αρχιμανδρίτης Νικόλαος, *Ψυχολογικός Πόλεμος. Κατασκοπεία. Αντικατασκοπεία*, Αθήνα, 1960

Bonanate Luigi, *Διεθνής Τρομοκρατία*, μτφρ. Σιδέρη Ντίνα, Κέδρος, Αθήνα, 2009

van Evera, Stephen, *Εισαγωγή στη Μεθοδολογία της Πολιτικής Επιστήμης*, μτφρ. Συλογίδου Έλλη, Ποιότητα, Αθήνα, 2009⁴

Guisnel Jean, *Πόλεμοι στον Κυβερνοχώρο. Μυστικές Υπηρεσίες και Internet*, μτφρ. Ζακοπούλου Γεωργία, Στάχυ, Αθήνα, 1997

Γρίβας Κωνσταντίνος, «Οι ασύμμετρες απειλές ως γεωπολιτικό φαινόμενο και ο ρόλος των Υπηρεσιών Πληροφοριών στην αντιμετώπισή τους» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Δερβιτσιώτης Άλκης, «Αναζητώντας τη (δύσκολη) νομιμοποίηση των υπηρεσιών Πληροφοριών - Όψεις της ευρωπαϊκής εμπειρίας» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Καλλιβρετάκης Λεωνίδας, «Η ομάδα Παπαδόπουλου στην τελική ευθεία προς την εξουσία» στο *Η στρατιωτική δικτατορία 1967-1974*, επιμ. Καραμανωλάκης Βαγγέλης, ΔΟΛ, Αθήνα, 2010

Κάτρης Γιάννης, *Η γέννηση του νεοφασισμού στην Ελλάδα*, Παπαζήσης, Αθήνα, 1974

Καφφές Γιώργος, *Κοινωνιολογία της Τρομοκρατίας*, Παπαζήσης, Αθήνα, 2010

Κολιόπουλος Κ., *Στρατηγικός Αιφνιδιασμός. Υπηρεσίες Πληροφοριών και Αιφνιδιαστικές Επιθέσεις*, Ελληνικά Γράμματα, Αθήνα, 2000

Κράουντι Τ., *Ιστορία της Κατασκοπίας*, μτφρ. Μηλιαρέσης Γ., Lector, Αθήνα, 2007

Krause D., *Η Τέχνη του Πολέμου για Στελέχη Επιχειρήσεων*, μτφρ. Ναθαναήλ Ν., Κριτική, Αθήνα, 1998

Κυριαζής Νίκος, Σπανός Στέλιος, *Το Πρόσωπο του Πολέμου στον 21^ο Αιώνα*, Εστία, Αθήνα, 2000

Κωνσταντόπουλος Ι., *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, Ποιότητα, Αθήνα, 2010

Κυριαζής Νίκος, Σπανός Στέλιος, *Το Πρόσωπο του Πολέμου στον 21^ο Αιώνα*, Εστία, Αθήνα, 2000

Λυμπέρης Χρήστος, *Πορεία σε ταραγμένες θάλασσες*, Ποιότητα, Αθήνα, 1999

Λυμπέρης Χρήστος, *Εθνική Στρατηγική και Χειρισμός Κρίσεων*, Ποιότητα, Αθήνα, 2009

Μάξης Ιωάννης, *Γεωπολιτική προσέγγιση για ένα νέο Ελληνικό Αμυντικό Δόγμα*, Παπαζήσης, Αθήνα, 2006

Μάξης Ι., «Δημιουργία Συμβουλίου Εθνικής Ασφαλείας στην Ελλάδα» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Μαράκης Νίκος, «Το Πραξικόπημα της ΕΥΠ. Το Άγνωστο Παρασκήνιο της Υπόθεσης Οτσαλάν» στο *Το Βήμα της Κυριακής*, 21 Φεβρουαρίου 1999

Μαριγκέλα Κάρλος, *Το Εγχειρίδιο του Αντάρτη των Πόλεων*, μτφρ. Σύρρου Κατερίνα, Ελεύθερος Τύπος, Αθήνα

Μαυρόπουλος Παναγιώτης, *Εισαγωγή στη Θεωρία του Πολέμου και της Στρατηγικής*, Αθήνα, 2012

Baylis John, «Διεθνής και παγκόσμια ασφάλεια στην μεταψυχροπολεμική εποχή» στο *Η παγκοσμιοποίηση της διεθνούς πολιτικής*, επιμ. Baylis J., Smith St., Owens P. (επιμ. ελληνικής έκδοσης Υφαντής Κ.), Επίκεντρο, Αθήνα, 2007

Μπεσίρης Νικόλαος (ταξίαρχος ΕΛΑΣ), «Διακλαδική συνεργασία στο πλαίσιο της πληροφοριακής κάλυψης» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Nye J., *Το Παράδοξο της Αμερικανικής Δύναμης*, μτφρ. Παπαστάμου Ιωάννα, Παπαζήσης / Ινστιτούτο Αμυντικών Αναλύσεων, Αθήνα, 2003

Νομικός Ιωάννης, «Ο ρόλος των υπηρεσιών Πληροφοριών και Ασφαλείας μετά την 11^η Σεπτεμβρίου» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Νομικός Ιωάννης, «Υπηρεσίες Πληροφοριών και Εθνικής Ασφαλείας. Η περίπτωση της Ελλάδας» στο περιοδικό *Επίκαιρα*, τεύχος 149 (Αύγουστος 2012)

Νομικός Ιωάννης, «Οι προκλήσεις για την ΕΥΠ στον 21^ο αιώνα» στην εφημερίδα *Παραπολιτικά*, 12 Μαΐου 2018

Ντόκος Θάνος, «Ασύμμετρες απειλές και διεθνής ασφάλεια» στο *Διεθνείς Σχέσεις. Σύγχρονη Θεματολογία και Προσεγγίσεις*, επιμ. Τριανταφύλλου Δ., Υφαντής Κ. κ. α., Παπαζήσης, Αθήνα, 2008

Ντόκος Θ., Τσάκωνας Π., *Στρατηγική Εθνικής Ασφαλείας. Οικοδομώντας το Ελληνικό Μοντέλο στον Εικοστό Πρώτο Αιώνα*, Παπαζήσης, Αθήνα, 2005

Παούνης Νικόλαος, *Η Ελληνοτουρκική Αντιπαράθεση στα Ίμια (1996). Ο Μύθος του Εθνικού Τακτικού Πλεονεκτήματος* υπό την αιγίδα του ΕΛΙΑΜΕΠ, Νοέμβριος 2017

Παπαγεωργόπουλος Κυριάκος, *Μνήμες πολέμου και ειρήνης*, τόμος Β', Δήλος, χ. τ. 1995

Πλακούδας Σ., «Νέες Απειλές Ασφαλείας - Υβριδικός Πόλεμος», *Καθημερινή*, 4 / 12 / 2016

Πλατιάς Αθανάσιος, «Η Ελληνική Αμυντική Πολιτική και η Κρίση στα Ίμια: Σκέψεις και Προβληματισμοί» στο *Η Κρίση στα Ίμια*, Πρακτικά Ημερίδας ΙΣΤΑΜΕ, Απρίλιος / Ιούλιος 1997

Ραγιές Ιωάννης, «Σύγχρονες προκλήσεις για τις Υπηρεσίες Πληροφοριών. Η συνδρομή στην άσκηση πολιτικής» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Σταύρου Απόστολος, «Ο έλεγχος της ΕΥΠ από τη Βουλή» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

Steans Jill, Pettiford Lloyd, κ. α., *Εισαγωγή στη Θεωρία των Διεθνών Σχέσεων*, μτφρ. Μορφόπουλος Άγγελος, Τουρίκης, Αθήνα, χ. χ.

Φιτσανάκης Σήφης, *Εθνική ασφάλεια και σύγχρονες υπηρεσίες κατασκοπείας στην Ελλάδα*, Ποταμός, Αθήνα, 2015

Χαρβαλιάς Γιώργος, «Η ΕΥΠ στη σύγχρονη νεοελληνική πραγματικότητα» στο *Κράτος-Ασφάλεια και ο ρόλος των Υπηρεσιών Πληροφοριών. Η περίπτωση της Ελλάδας*, Σάκκουλας, Αθήνα, 2009

«Εθνική Υπηρεσία Πληροφοριών. Εκδημοκρατισμός τέλος», *Ελευθεροτυπία*, 22 Ιανουαρίου 2006

ΑΓΓΛΟΣΑΞΩΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ / ΑΡΘΡΟΓΡΑΦΙΑ

Abdullah bin Khaled al-Saud, “The Tranquillity Campaign: A Beacon of Light in the Dark World Wide Web” στο *Perspectives on Terrorism*, Volume 11, Issue 2, 2017

Albats Yevgenia, *State Within a State: The Secret Police and Its Hold on Russia's Past, Present and Future*, I. B. Tauris, London, 1995

Network Centric Warfare. Developing and Leveraging Information Superiority, επιμ. Alberts D., Garstka John, Stein Frederick, CCRP Publication Series, 1999²

Alberts S. D., *Defensive Information Warfare*, NDU Press Book, Washington, D.C., 1996

Alberts S. D., Hayes E. R., *Power to the Edge. Command...Control...in the Information Age*, CCRP Publication Series, 2003

Alexander Martin, Dulan Huw, “A Century of Intelligence (1909-2009): International Perspectives” στο *Intelligence and National Security*, Volume 28, Number 3, 2013

Allen George, “Professionalization of Intelligence” στο *Ethics of Spying. A Reader for the Intelligence Professional*, Volume 2, επιμ. Goldman Jan, The Scarecrow Press, Inc., UK, 2010

Aly Anne, “Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization” στο *Studies in Conflict and Terrorism*, Volume 40, Issue 1, 2017

Andrew Christopher, “Intelligence, International Relations and ‘Under-Theorization’” στο *Intelligence and National Security*, Volume 19, Number 2, 2004

Andrew Christopher, *Defend the Realm: The Authorized History of MI5*, Alfred A. Knopf, New York, 2009

Andrew C., Mitrokhin V., *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, Basic Books, New York, 2000

Antoniou Antony, *Open Source Information. The Future of Intelligence*, European Intelligence Academy, E-Book, Number 1, Μάιος 2013

Arango R. Carlos, “Counterintelligence vs. Insurgency”, *Studies in Intelligence*, Volume 12, Number 2, 1968

Arango R. Carlos, “Insurgent Counterintelligence”, *Studies in Intelligence*, Volume 12, Number 1, 1968

Argomaniz Javier, Bures Oldrich, Kaunert Christian, “A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment” στο *Intelligence and National Security*, Volume 30, Number 2-3, 2015

Ariely Ad Gil, “Adaptive Responses to Cyberterrorism” στο *Cyberterrorism. Understanding, Assessment, and Response*, επιμ. Chen Tomas, Jarvis Lee, Macdonald Stuart, Springer, New York, 2014

Arquilla J., Ronfeldt D., “Information, Power, and Grand Strategy: in Athena’s Camp -Section 2” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997

Arquilla J., Ronfeldt D., “Cyberwar Is Coming” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997

Arquilla J., Ronfeldt D., “A New Epoch and Spectrum of Conflict” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997

Arquilla J., Ronfeldt D., “Looking Ahead: Preparing for Information-Age Conflict” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997

Baker Stewart, “Should Spies Be Cops?” στο *Foreign Policy*, Winter 1994-1995

Ball Desmond, “Desperately Seeking Bin Laden: The Intelligence Dimension of the War Against Terrorism” στο *Worlds in Collision: Terror and the Future of Global Order*, επιμ. Booth Ken, Dunne Tim, Palgrave, New York, 2002

Bar-Joseph, Bar, “The Professional Ethics of Intelligence Analysis” στο *International Journal of Intelligence and Counterintelligence*, Volume 24, Issue 1, 2011

Bar-Joseph Uri, “Israel’s Military Intelligence Performance in the Second Lebanon War” στο *International Journal of Intelligence and CounterIntelligence*, Volume 20, Issue 4, 2007

Barger Deborah, “Is It Time to Transform, Not Reform, US Intelligence”, *SAIS Review*, Volume 24, Number 1, 2004

Barger D., *Toward a Revolution in Intelligence Affairs*, RAND, Santa Monica, 2005

Barkawi Tarak, Laffey Mark, “The Post-Colonial Moment in Security Studies” στο *Review of International Studies*, Volume 32, Issue 2, 2006

Barrett David, “Book Review. Why Intelligence Failure Are (Still) Inevitable” στο *Diplomatic History*, Volume 34, Number 1, 2010

Barron John, *KGB Today: The Hidden Hand*, Reader’s Digest Press, New York, 1983

Bay Sebastian, *Intelligence Theories. A Literary Overview*, Lund University, Sweden, 2007

Bell B. J., “Toward a Theory of deception” στο *International Journal of Intelligence and CounterIntelligence*, Volume 16, Issue 2, 2003

Ben-Haim, Yakov, “Policy Neutrality and Uncertainty: An Info-Gap Perspective” στο *Intelligence and National Security*, Volume 31, Number 7, 2016

Bennet Gordon, *The SVR: Russia’s Intelligence Service*, UK: Conflict Studies Research Center, Camberley / UK, 2000

- Bennet Gordon, *The Federal Security Service of the Russian Federation*, Conflict Studies Research Center, Camberley / UK, 2000
- Bennett Michael, Waltz Edward, *Counterdeception Principles and Applications for National Security*, Artech House, Inc., Norwood / Massachusetts, 2007
- Benny J. Daniel, *Industrial Espionage. Developing a Counterespionage Program*, CRC Press, 2014
- Berkowitz Bruce, “Warfare in the Information Age” στο *Issues in Science and Technology*, Φθινόπωρο 1995
- Berkowitz Bruce, “Information Age Intelligence”, *Foreign Policy*, Number 103, 1996
- Berkowitz Bruce, “Homeland Security Intelligence: Rationale, Requirements, and Current Status” στο *Analyzing Intelligence. Origins, Obstacles, and Innovations*, επιμ. George Roger, Bruce James, Georgetown University Press, Washington, D.C., 2008
- Berkowitz Bruce, Goodman Allan, *Strategic Intelligence and American National Security*, Princeton University Press, New Jersey / USA, 1989
- Berkowitz B., Goodman A., *Best Truth: Intelligence in the Information Age*, Yale University Press, ΗΠΑ, 2000
- Bertram Stewart, Ellison Keith, “Sub Saharan African Terrorist Groups’ use of the Internet” στο *Journal of Terrorism Research*, Volume 5, Issue 1, 2014
- Betts Richard, “Analysis, War and Decision: Why Intelligence Failures Are Inevitable” στο *World Politics*, Volume 31, Number 1, 1978
- Betts R., Mahnken Th., *Paradoxes of Strategic Intelligence*, Frank Cass, 2001
- Betts R., “Fixing Intelligence” στο *Foreign Affairs*, Volume 81, Number 1, 2002
- Betts R., “Politicization of Intelligence: Costs and Benefits” στο *Paradoxes of Strategic Intelligence*, επιμ. Betts R., Mahnken Thomas, Frank Cass Publishers, London, 2003
- Betts Richard, *Enemies of Intelligence. Knowledge and Power in American National Security*, Columbia University Press, New York, 2007
- Betts R., “Analysis, war, and decision: why intelligence failures are inevitable” στο *Intelligence Theory: Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, UK, 2009
- Bill A. James, *The Eagle and the Lion: The Tragedy of American-Iranian Relations*, Yale University Press, 1988
- Bimfort T. Martin, “A Definition of Intelligence” στο *Studies in Intelligence*, Volume 2, Number 4, 1958

Booth Ken, “War, security and strategy: toward a doctrine for stable peace” στο *New Thinking About Strategy and International Security*, επιμ. Booth Ken, Harper Collins Academic, UK, 1991

Born H., “Parliamentary and External Oversight” στο *Democratic Control of Intelligence Services. Containing Rogue Elephants*, επιμ. Born Hans, Caparini Marina, Ashgate Publishing, 2007

Bostdorf D., *Proclaiming the Truman Doctrine: The Cold War Call to Arms*, Texas A&M University Press, USA, 2008

Bouzis Kathleen, “Countering the Islamic State: US Counterterrorism Measures” στο *Studies in Conflict and Terrorism*, Volume 38, Issue 10, 2015

Bowyer J., *Cheating*, New York, St. Martin’s, 1980

Bowyer J., “The armed struggle and underground intelligence: An overview” στο *Studies in Conflict and Terrorism*, Volume 17, Issue 2, 1994

Boylan Brandon “Sponsoring Violence: A Typology of Constituent Support for Terrorist Organizations” στο *Studies in Conflict and Terrorism*, Volume 38, Issue 8, 2015

Braddock Kurt, “Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism” στο *Studies in Conflict and Terrorism*, Volume 39, Issue 5, 2016

Brian Greene, *Rethinking Strategic Surprise. Defence Planning Under “Bounded Uncertainty”*, Defence R&D Canada / Centre for Operational Research & Analysis, Canada, 2010

Bridgeman Vincent, “Defense Counterintelligence” στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, Washington, D.C., 2009

Brope Reginald, “Russia” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Brown A., *Bodyguard of Lies*, Harper and Row, New York, 1975

Brown Bradford, *Introduction to Defense Acquisition Management*, Defense Acquisition University Press, Fort Belvoir / Virginia, Αύγουστος 2010

Bruneau T., “Democracy and Effectiveness: Adapting Intelligence for the Fight Against Terrorism” στο *International Journal of Intelligence and CounterIntelligence*, Volume 21, Issue 3, 2008

Buckley John, *Managing Intelligence. A Guide for Law Enforcement Professionals*, CRC Press, Florida, 2014

- Bures Oldrich, “Ten Years of EU’s Fight against Terrorist Financing: A Critical Assessment” στο *Intelligence and National Security*, Volume 30, Number 2-3, 2015
- Byman Daniel, *A High Price: The Triumphs and Failures of Israeli Counterterrorism*, Oxford University Press, Oxford, 2011
- Cambone Stephen, *A New Structural for National Security Policy Planning*, CSIS, Washington, D.C., 1998
- Campana Aurélie, Ducol Benjamin, “Voices of the ‘Caucasus Emirate’: Mapping and Analyzing North Caucasus Insurgency Websites” στο *Terrorism and Political Violence*, Volume 27, Issue 4, 2015
- Campbell St., “A Survey of the U. S. Market for Intelligence Education” στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 2, 2011
- Carter A., Deutch J., Zelikow P., “Catastrophic Terrorism: Tackling the New Danger”, *Foreign Affairs*, Νοέμβριος / Δεκέμβριος 1998
- Carter L. David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, U.S. Department of Justice, 2004
- Carter David, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, U. S. Department of Justice / Office of Community Oriented Policing Services, USA, 2009
- Cavelty Myriam, “Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate”, *Journal of Information Technology & Politics*, Volume 4, Issue 1, 2007
- Cepik Marco, “Structural change and democratic control of intelligence in Brazil” στο *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, επιμ. Bruneau C. Tomas., Boraz C. Steven, University of Texas Press, Austin, 2007
- Cha D. V., “Globalization and the Study of International Security” στο *Journal of Peace Research*, Volume 37, Number 3, 2000
- Chalk Peter, “Canada” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009
- Chalk Peter, “Australia” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009
- Charters A. D., “Eyes of the Underground: Jewish Insurgent Intelligence in Palestine, 1945-47” στο *Intelligence and National Security*, Volume 13, Number 4, 1998

Charvat J., “Cyber Terrorism: A New Dimension in Battlespace” στο *The Virtual Battlefield: Perspectives on Cyber Warfare*, επιμ. Czosseck Christian, Geers Kenneth, Ios Press, Amsterdam, 2009

Churchill W., *The World Crisis: 1915*, Charles Scribner's Sons, New York, 1923

Clapper R. J. “Luncheon Remarks, Association, of Former Intelligence Officers” στο *The Intelligence*, AFIO newsletter, McLean, Virginia, 1995

Clark J. Ransom, *Intelligence and National Security. A Reference Handbook*, Praeger Security International, USA, 2007

Clark Robert, *Intelligence Analysis: A Target-Centric Approach*, CQ Press, Washington, D.C., 2003

Clarke Richard, *Against All Enemies: Inside America's War on Terror*, Free Press, New York, 2004

von Clausewitz, Carl, *On War*, Princeton University Press, USA, 1975

van Cleave, Michelle, *Counterintelligence and National Security*, National Defense University Press, Washington, D.C., 2007

van Cleave, Michelle, “Guide to the Study of Intelligence. What is Counterintelligence? A Guide to Thinking and Teaching about CI” στο *The Intelligence Journal of U.S. Intelligence Studies*, Volume 20, Number 2, 2013

Clough D. H., Margulies A. R., “The Corporate Competitive Intelligence / Counterintelligence Team: A Symbiotic Design for the Future” στο *Competitive Intelligence Review*, Volume 5, Number 3, 1994

Clutterbuck L., “The United Kingdom” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009

Codevilla A., *Informing Statecraft: Intelligence for a New Century*, The Free Press, USA, 1992

Collins A. Pamela, Baggett K. Ryan, “Private Security Intelligence and Homeland Security” στο *Homeland Security and Intelligence*, επιμ. Logan G. Keith, Praeger, California, 2010

Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council, *Cybersecurity. Today and Tomorrow. Pay Now or Pay Later*, National Academy Press, Washington, D.C., 2002

Conetta Carl, *The New Warfare and the New American Calculus of War*, Project on Defense Alternatives, Brief Memo Number 26, September 2002

Conway Maura, “Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research” στο *Studies in Conflict and Terrorism*, Volume 40, Issue 1, 2017

Cooper J., “Another View of the Revolution in Military Affairs” στο *Conference Proceedings of the Fifth Annual Conference on Strategy*, Strategic Studies Institute, U.S. Army War College, HPIA, 1994

Cordesman H. Anthony, *The Instant Lessons of the Iraq War*, Executive Summary, Fourth Working Draft, April 2003

Coyne John, Bell Peter, *The Role of Strategic Intelligence in Law Enforcement*, Palgrave Macmillan, 2015

van Creveld, M., *Technology and War. From 2000 B.C. to the Present*, The Free Press, USA, 1991

Crosston M., “Occam’ s Follies: Real and Imagined Biases Facing Intelligence Studies” στο *Journal of Strategic Security*, Volume 6, Number 3, 2013

Cruickshank Charles, *Deception in World War II*, Oxford University Press, New York, 1980

Cukier Neil Kenneth, Mayer-Schoenberger Viktor, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, Boston, 2013

Cullison Allan, “Inside Al-Qaeda’s Hard Drive” στο *The Atlantic Monthly*, Σεπτέμβριος 2004

Intelligence and Counterintelligence. Spy Agencies, Intelligence Operations, and the People Behind Them, επιμ. Curley Rob, Britannica Educational Publishing, Rosen Educational Services, New York, 2013

Dahl J. Erik, “Missing the Wake-up Call: Why Intelligence Failures Rarely Inspire Improved Performance” στο *Intelligence and National Security*, Volume 25, Number 6, 2010

Daniel D, Herbig K., *Strategic Military Deception*, Pergamon, N. Υόρκη, 1982

Daniel D., Herbig K., “Propositions on Military Deception” στο *Strategic Military Deception*, επιμ. Daniel D., Herbig K, Pergamon, New York, 1982

Daun Anna, “Germany” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Davies Phillip, “Theory and intelligence reconsidered” στο *Intelligence Theory. Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, UK, 2009

Davis Jack, “The Kent-Kendall Debate of 1949” στο *Studies in Intelligence*, Volume 35, Number 5, 1992

Davis Jack, “Paul Wolfowitz on Intelligence-Policy Relations” στο *Studies in Intelligence*, Volume 39, Number 1, 1995

Davis Jack “Sherman Kent’s Final Thoughts on Analyst-Policymaker Relations” στο *Occasional Papers: Volume 2, Number 3*, Central Intelligence Agency, The Sherman Kent Center for Intelligence Analysis, Washington, June 2003

Deakin F., Storry G., “The Journalist: Richard Sorge, the Spy Who Tricked Hitler”, *Famous Soviet Spies: The Kremlin’s Secret Weapon*, επιμ. Newman J., US News & World Report, Ουάσινγκτον, 1973

Deane Philip, *I Should Have Died*, Athenaeum Publishers, New York, 1977

Degaut Marcos, “Spies and Policymakers: Intelligence in the Information Age” στο *Intelligence and National Security*, Volume 31, Number 4, 2016

Den Boer, Monica, “Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis” στο *Intelligence and National Security*, Volume 30, Number 2-3, 2015

Denécé E., Arboit G., “Intelligence Studies in France” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 4, 2010

Denning Dorothy, *Information Warfare and Security*, ACM Press, USA, 1999

Denning Dorothy, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” στο *Networks and Netwars: The Future of Terror, Crime, and Militancy*, επιμ. Arquilla John, Ronfeldt David, RAND, Santa Monica, 2001

Devin D. Jessee, “Tactical Means, Strategic Ends: Al Qaeda’s Use of Denial and Deception” στο *Terrorism and Political Violence*, Volume 18, Issue 3, 2006

Diaz-Matey, G., *Intelligence studies at the dawn of the 21st century: New possibilities and resources for recent topic in international relations*, Research Unit on International Security and Cooperation (UNISCI), Madrid, 2005

Diaz-Matey, G., *Methodological Approaches to the Concept of Intelligence Failure*, UNISCI Discussion Papers, 2005

Donovan Michael, “National intelligence and the Iranian revolution” στο *Eternal Vigilance? 50 Years of the CIA*, επιμ. Jeffreys-Jones R., Andrew Christopher, Frank Cass, London, 1997

Dorando P., “For College Courses in Intelligence” στο *Studies in Intelligence*, Volume 4, Number 3, 1960

Dorn, A. Walter, “United Nations Peacekeeping Intelligence” στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson Loch, Oxford University Press, Oxford, 2010

Douglas Bernhardt, *Competitive Intelligence. How to acquire and use corporate intelligence and counter-intelligence*, Pearson Education Limited, UK, 2003

Dover Robert, Goodman Michael, “Introduction” στο *Why Intelligence Needs the Media, Why the Media Needs Intelligence*, επιμ. Dover Robert, Goodman Michael, Columbia University Press, New York, 2009

Dujmovic Nicholas, “Intelligence in Recent Public Literature. Enemies of Intelligence: Knowledge and Power in American National Security” στο *Studies in Intelligence*, Volume 51, Number 4, 2007

Dujmovic Nicholas, “Enemies of Intelligence: Knowledge and Power in American National Security” στο *Studies in Intelligence*, Volume 51, Number 4, 2007

Dumaine C., “Intelligence in the New Millennium”, CIA Directorate of Intelligence, AFCEA Spring Intelligence Conference, April 18, 2001

Dunn Myriam, *Information Age Conflict. A Study of the Information Revolution and a Changing Operating Environment*, Center for Security Studies, Ζυρίχη, 2002

van Duyne, Petrus C., “Organized Crime, Corruption and Power”, *Crime, Law and Social Change*, 26, 1997

Duyvesteyn Isabelle, “Intelligence and Strategic Culture: Some Observations” στο *Intelligence and National Security*, Volume 26, Number 4, 2011

Dycus Stephen, “The role of military intelligence in homeland security” στο *Louisiana Law Review*, 64, 2004

Eftimiades Nicholas, *Chinese Intelligence Operations*, Toppan Company, Tokyo, 1995

Eftimiades Nicholas, “China” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Ehrman John, “What are We Talking About When We Talk about Counterintelligence?” στο *Studies in Intelligence*, Volume 53, Number 2, 2009

Ekstedt V., Parkhouse T., Clemente D., “Commitments, Mechanisms and Governance” στο *National Cyber Security. Framework Manual*, επιμ. Klimburg Alexander, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2012

Elisan C. C., *Malware, Rootkits and Botnets: A Beginning Guide*, McGraw Hill, New York, 2013

Ember Carol, Ember Melvin, *Cross-Cultural Research Methods*, AltaMira Press, Βρετανία, 2009

Erbschloe M, *Information Warfare. How to Survive Cyber Attacks*, The McGraw-Hill Companies, USA, 2001

Evans Joseph, “U.S. Business Competitiveness and the Intelligence Community” στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 3, 1994

Evans G., Newnham J., *The Penguin Dictionary of International Relations*, Penguin Books, 1998

Evans G., “Rethinking military intelligence failure -Putting the wheels back on the intelligence cycle” στο *Defense Studies*, Volume 9, Number 1, 2009

Fägersten Björn, “Bureaucratic Resistance to International Intelligence Cooperation: The Case of Europol” στο *Intelligence and National Security*, Volume 25, Number 4, 2010

Felix Christopher, *A Short Course in the Secret War*, Madison Books, Lanham / Maryland, 2001

Finckenauer James, Waring Elin, *Russian Mafia in America*, Northeastern University Press, Boston / USA, 1998

Fink Steven, *Sticky Fingers. Managing the Global Risk of Economic Espionage*, Dearborn Trade Publishing, USA, 2002

Fischhoff B., “For those Condemned to Study the Past: Reflections on Historical Judgment” στο *New Directions for Methodology of Behavioural Science: Fallible Judgments in Behavioural Research*, επιμ. Shweder A. R., Fiske W. D., Jossey-Bass, San Francisco, 1980

Fitsanakis Joseph, “State-Sponsored Communications Interception: Facilitating Illegality” στο *Information, Communication and Society*, Volume 6, Number 3, 2003

Fitsanakis Joseph, “National Security Agency: The Historiography of Concealment” στο *The History of Information Security*, επιμ. de Leeuw, K. και Bergstra, J., Elsevier BV, Άμστερνταμ, 2006

Flood Brian, “Strategic Aspects of the UK National Intelligence Model” στο *Strategic Thinking in Criminal Intelligence*, επιμ. Ratcliffe Jerry, Federation Press, Σύδνεϋ, 2003

Flynn Michael, Pottinger Matt, Batchelor Paul, “Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan” στο *Voices from the Field* series, Center for a New American Security, Washington, D.C., Ιανουάριος 2010

Ford H., *Estimative Intelligence. The Purposes and Problems of National Intelligence Estimates*, Defense Intelligence College, Maryland, 1989

Ford Harold, “The US Government’s Experience with Intelligence Analysis: Pluses and Minuses” στο *Intelligence and National Security*, Volume 10, Number 4, 1995

Fort Randall, “Economic Espionage” στο *U.S. Intelligence at a Crossroad*, επιμ. Godson R., May E., et al., Brassey's UK Ltd, ΗΠΑ, 1995

Foryst A. C., “Rethinking National Security Strategy Priorities” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 3, 2010

Fowler C., Nesbit R., “Tactical Deception in Air-Land Warfare” στο *Journal of Electronic Defense*, Ιούλιος 1995

Freedman Lawrence, *The Revolution in Strategic Affairs* στο *Adelphi Paper*, Volume 38, Issue 318, 1998

Freedman Lawrence, *The Transformation of Strategic Affairs* στο *Adelphi Paper*, Volume 45, Issue 379, 2006

Freilich D. Charles, “Israel Counter-Terrorism Policy: How Effective?” στο *Terrorism and Political Violence*, Volume 29, Issue 2, 2017

French Geoffrey, Kim Jin, “Acknowledging the Revolution: The Urgent Need for Cyber Counterintelligence” στο *National Intelligence Journal*, Volume 1, Number 1, 2009

Fry M., Hochstein M., “Epistemic communities: Intelligence studies and international relations” στο *Intelligence and National Security*, Volume 8, Number 3, 1993

Galvan Robert, “The Role of American Intelligence in the Global Economy: Business and Industrial Spying” στο *International Journal of Intelligence and CounterIntelligence*, Volume 8, Issue 3, 1995

McGarvey P., “DIA: Intelligence to please” στο *Readings in American Foreign Policy*, επιμ. Halperin M., Kanter A., Little Brown, Boston, Massachusetts, USA, 1973

Gearson John, “Deterring Conventional Terrorism: From Punishment to Denial and Resilience” στο *Contemporary Security Policy*, Volume 33, Issue 1, 2012

Gentry John, “Intelligence Failure Reframed” στο *Political Science Quarterly*, Volume 123, Number 2, 2008

Gentry J., “The ‘Professionalization’ of Intelligence Analysis: A Skeptical Perspective” στο *International Journal of Intelligence and CounterIntelligence*, Volume 29, Issue 4, 2016

Gentry John, "Toward a Theory of Non-State Actors' Intelligence" στο *Intelligence and National Security*, Volume 31, Number 4, 2016

Gentry J., Spencer D., "Colombia's FARC: A Portrait of Insurgent Intelligence" στο *Intelligence and National Security*, Volume 25, Number 4, 2010

George Z. Roger, Kline D. Robert, "Introduction: Teaching Intelligence" στο *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, επιμ. George Z. Roger, Kline D. Robert, Rowman & Littlefield Publishers, Inc., USA, 2006

George Z. Rogert, "Beyond Analytic Tradecraft" στο *International Journal of Intelligence and Counterintelligence*, Volume 23, Issue 2, 2010

Gill Peter, Phythian Mark, *Intelligence in an Insecure World*, Polity Press, USA, 2012²

Gleghorn E. T., *Exposing the Seams: The Impetus for Reforming U.S. Counterintelligence* (διατριβή κατατεθειμένη στο Naval Postgraduate School), Monterey / California, 2003

Godson R., "Intelligence and Policy: An Introduction" στο *Intelligence Requirements for the 1980s: Intelligence and Policy*, επιμ. Godson R., Lexington Books, Lexington / Massachusetts, 1986

Godson R., "Intelligence: an American View" στο *British and American Approaches to Intelligence*, επιμ. Robertson G. K., Royal United Services Institute, USA, 1987

Godson R., *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, Transaction Publishers, N. Jersey / HPIA, 2001

Godson R., Wirtz J., "Strategic Denial and Deception" στο *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 4, 2000

Goldman Jan, *Words of Intelligence. A Dictionary*, The Scarecrow Press, Inc., USA, 2006

Goodman M., "Studying and Teaching About Intelligence: The Approach in the United Kingdom" στο *Studies in Intelligence*, Volume 50, Number 2, 2006

Goodman Michael, "The United Kingdom" στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Grabo C., "Strategic Warning: The Problem of Timing" στο *Studies in Intelligence*, Volume 16, Number 2, 1972

Grabo C., *Anticipating Surprise. Analysis for Strategic Warning*, University Press of America, Inc., USA, 2004

- Gross J., “Trouble in Paradise”, *British Journal of Criminology*, 43, 2003
- Gross L. M., “Fighting by Other Means in the Mideast: a Critical Analysis of Israel’s Assassination Policy”, *Political Studies*, Volume 51, Issue 2, 2003
- Grove Andrew, *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career*, Doubleday, New York, 1996
- Gunaratna Rohan, *Inside Al Qaeda: Global Network of Terror*, Berkeley Books, New York, 2003
- Haggerty Kevin, Ericson Richard, “The militarization of policing in the information age” στο *Journal of Political and Military Sociology*, 27, 1999
- Haines G., “An Emerging New Field of Study: US Intelligence” στο *Diplomatic History*, Volume 28, Number 3, 2004
- Halevy Efraim, *Man in the Shadows: Inside the Middle East Crisis with a Man Who Led the Mossad*, St. Martin’s Press, New York, 2006
- Hammond T., “Intelligence Organizations and the Organization of Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 4, 2010
- Hampton C., *A history of camouflage, concealment and deception*, εργασία κατατεθειμένη στο Air War College, Alabama / USA, 1988
- Hamrah Satgin, “The Role of Culture in Intelligence Reform”, *Journal of Strategic Security*, Volume 6, Number 3, 2013
- Handel Michael, “Intelligence and the problem of strategic surprise” στο *Journal of Strategic Studies*, Number 7, 1984
- Handel M., *War, Strategy, and Intelligence*, Frank Cass & Co. Ltd., UK, 1989
- Handel M., “Intelligence and Deception” στο *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, επιμ. George Roger, Kline Robert, Rowan & Littlefield Publishers, Inc., USA, 2006
- Harber Justin, “Unconventional Spies: The Counterintelligence Threat from Non-State Actors” στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 2, 2009
- Harel Amos, Issacharoff Avi, *34 Days: Israel, Hezbollah, and the War in Lebanon*, Palgrave Macmillan, New York, 2008
- Hastedt Glenn, “The Politics of Intelligence and the Politicization of Intelligence: The American Experience” στο *Intelligence and National Security*, Volume 28, Number 1, 2013

Hathaway E. Melissa, Klimburg Alexander, “Preliminary Considerations: On National Cyber Security“ στο *National Cyber Security. Framework Manual*, επιμ. Klimburg Alexander, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2012

Hatlebrekke A., K., Smith, M. L. R., “Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure” στο *Intelligence and National Security*, Volume 25, Number 2, 2010

Hayden F. J. “Economic Intelligence” στην Select Committee on Intelligence, U.S. Senate, 103rd Congress, Συνεδρία 1^η, 5 Αυγούστου 1993

Hazelton L. Jacqueline, “Drone Strikes and Grand Strategy: Toward a Political Understanding of the Uses of Unmanned Aerial Vehicle Attacks in US Security Policy” στο *Journal of Strategic Studies*, Volume 40, Number 1-2, 2017

Healey Jason, van Bochoven, Leendert, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, D.C, 2011

Healey Jason, Jordan Tothova Klara, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, D.C, 2014

Heickerö Roland, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency, Στοκχόλμη, 2010

Heidenrich John, “The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence” στο *Studies in Intelligence*, Volume 51, Number 2, 2007

Herman Michael, *Intelligence Power in Peace and War*, The Royal Institute of International Affairs, Cambridge University Press, 1996

Herman Michael, *Intelligence Services in the Information Age*, Frank Cass Publishers, Λονδίνο, 2001

Hillebrand Claudia, “The Role of News Media in Intelligence Oversight ” στο *Intelligence and National Security*, Volume 27, Number 5, 2012

Hilsman Roger, “Intelligence and Policy-Making in Foreign Affairs” στο *World Politics*, Volume 5, Issue 1, 1952

Hjortdal Magnus, “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence” στο *Journal of Strategic Security*, Volume 4, Number 2, Article 2, 2011

Høffding Simon, Rønn Kira, “The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence” στο *Intelligence and National Security*, Volume 28, Number 5, 2013

Hollis M., Smith St., *Explaining and Understanding International Relations*, Oxford University Press, Βρετανία, 1990

Honig Arthur Or, “A New Direction for Theory-Building in Intelligence Studies” στο *International Journal of Intelligence and CounterIntelligence*, Volume 20, Issue 4, 2007

Hughes G., “Intelligence in the Cold War” στο *Intelligence and National Security*, Volume 26, Number 6, 2011

Hulnick S. Arthur, *Fixing the Spy Machine*, Praeger Publishers, USA, 1999

Hulnick S. Arthur, “What’s Wrong With The Intelligence Cycle?” στο *Strategic Intelligence*, Volume 2, επιμ. Johnson Lock, USA, 2007

Hulnick Arthur, “Intelligence theory: seeking better models” στο *Understanding the Intelligence Cycle*, επιμ. Phythian Mark, Βρετανία, 2013

Hundley O. R., Anderson H. R., “Emerging Challenge: Security and Safety in Cyberspace” στο *In Athena’s Camp. Preparing for Conflict in the Information Age*, επιμ. Arquilla J., Ronfeldt D., National Defense Research Institute, RAND, Santa Monica, 1997

Hutchinson William, “Information Warfare and Deception” στο *Informing Science*, Volume 9, 2006

Successful Law Enforcement Using Analytic Methods, International Association of Law Enforcement Intelligence Analysts, Florida, 1996

Ilardi Gaetano, “Al-Qaeda’s Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control” στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 2, 2009

Ilardi Gaetano, “Irish Republican Army Counterintelligence”, *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 1, 2010

Ilardi Gaetano, “Irish Republican Army Counterintelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 1, 2010

Ishengoma Frederick, “Online Social Networks and Terrorism 2.0 in Developing Countries” στο *International Journal of Computer Science & Network Solutions*, Volume 1, Number 4, 2013

Jackson P., “Historical Reflections on the Uses and Limits of Intelligence” στο *Intelligence and Statecraft: The Use and Limits of Intelligence in International Society*, επιμ. Jackson P. Siegel J., Praeger, USA, 2005

Jackson Peter, “On Uncertainty and the Limits of Intelligence” στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson L., Oxford University Press, Inc., New York, 2010

The Challenge of Domestic Intelligence in a Free Society. A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency, επιμ. Jackson A. Brian, RAND, Santa Monica, 2009

Jalil Sh., *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?*, SANS Institute, 2003

James Adrian, *Examining Intelligence-Led Policing. Developments in Research, Policy and Practice*, Palgrave Mcmillan, 2013

Jensen Carl, McElreath David, Graves Melissa, *Introduction to Intelligence Studies*, Taylor & Francis Group, USA, 2013

Jensen M. Joan, *Army Surveillance in America, 1775-1980*, Yale University Press, USA, 1991

Jensen Mark, “Intelligence Failures: What Are They Really and What Do We Do about Them?” στο *Intelligence and National Security*, Volume 27, Number 2, 2012

Jervis R., *Perception and Misperception in International Politics*, Princeton University Press, USA, 1976

Jervis Robert, “Reports, Politics, and Intelligence Failures: The Case of Iraq” στο *Journal of Strategic Studies*, Volume 29, Number 1, 2006

Jervis R., *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*, Cornell University Press, Ithaca, 2010

Johnson J., “Bricks and Mortar for a theory of Intelligence” στο *Comparative Strategy*, Volume 22, Issue 1, 2003

Johnson Loch, *America’s Secret Power: The CIA in a Democratic Society*, Oxford University Press, New York, 1989

Johnson L., *Secret Agencies U.S. Intelligence in a hostile world*, Yale University Press, HIA, 1996

Johnson L., “Analysis for a New Age” στο *Intelligence and National Security*, Volume 11, Number 4, 1996

Johnson L., “Sketches for a theory of strategic intelligence” στο *Intelligence Theory: Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, UK, 2009

Johnson L., “National Security Intelligence” στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson Loch, Oxford University Press, New York, 2010

Johnson L., “National Security Intelligence in the United States: A Performance Checklist” στο *Intelligence and National Security*, Volume 26, Number 5, 2011

Johnson L., Shelton A., “Thoughts on the State of Intelligence Studies: A Survey Report” στο *Intelligence and National Security*, Volume 28, Number 1, 2013

Johnson R. W., “Clandestinity and Current Intelligence” στο *Studies in Intelligence*, Volume 20, Number 3, 1976

Johnson R. W., *Thwarting Enemies at Home and Abroad. How to Be a Counterintelligence Officer*, Georgetown University Press, Washington, D.C., 2009

Jones Garret, “It’s a Cultural Thing: Thoughts on a Troubled CIA” στο *Secret Intelligence*, επιμ. Aldrich R., Andrew C., Wark W., Routledge, London, 2009

Jordan Javier, “The Effectiveness of the Drone Campaign against Al Qaeda Central: A Case Study” στο *Journal of Strategic Studies*, Volume 37, Number 1, 2014

Kalaris G., McCoy L., “Counterintelligence for the 1990s” στο *International Journal of Intelligence and CounterIntelligence*, Volume 2, Issue 2, 1988

Kalugin Oleg, *Spymaster: My 32 Years in Intelligence and Espionage Against the West*, Basic Books, London, 2009

Karabacak Bilge, Tatar Ünal, “Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection” στο *Critical Infrastructure Protection*, επιμ. Edwards Matthew, Ios Press, Amsterdam, 2014

Kass L., London Ph., “Surprise, Deception, Denial and Warning: Strategic Imperatives” στο *Orbis*, Volume 57, Number 1, 2013

Keegan J., *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, Hutchinson, London, 2003

Keithy M. D., “Intelligence Fundamentals” στο *Homeland Security and Intelligence*, επιμ. Logan G. K., Praeger, California, 2010

Kessler Ronald, *The CIA at War*, St. Martin’s Press, New York, 2004

Kenedli Tamás, Béres János, “Is the cyberterror exaggerated?” στο *AARMS*, Volume 7, Number 1, 2008

Kierman K., “Counterintelligence and Law Enforcement” στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, USA, 2009

Kirchofer P. Charles, “Managing Non-State Threats with Cumulative Deterrence-by-Denial” στο *Perspectives on Terrorism*, Volume 11, Issue 2, 2017

Kirby Aidan, “Domestic Intelligence Agencies After September 11, 2001: How Five Nations Have Grappled with the Evolving Threat” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009

Kirkpatrick Lyman, Jr., “Intelligence” στο *Encyclopedia of US Foreign Relations*, Volume 2, επιμ. Jentelson Bruce, Paterson Thomas, Oxford University Press, New York, 1997

Klehr H., *VENONA: Decoding Soviet Espionage in America*, Yale University Press, USA, 2000

Klimburg Alexander, Tirmaa-Klaar Heli, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU*, European Parliament, Belgium, 2011

Knight Amy, *Spies Without Cloaks: The KGB's Successors*, Princeton University Press, Princeton / New Jersey, 1996

Konstantopoulos J., Doga A., “The (R)evolution of Intelligence as an Academic Discipline: Challenges and Constraints” στο *Journal of Mediterranean and Balkan Intelligence*, Volume 5, Number 1, 2015

Konstantopoulos Ioannis, “Democracy and Ethics vs Intelligence and Security: From WikiLeaks to Snowden” στο *Democracy and an Open-Economy World Order*, επιμ. Bitros George, Kyriazis Nicholas, Springer, 2017

Kostopoulos K. George, *Cyberspace and Cybersecurity*, Taylor and Francis Group, LLC, USA, 2013

Krieger Wolfgang, “German Intelligence History: A Field in Search of Scholars” στο *Intelligence and National Security*, Volume 19, Number 2, 2004

Kuloglu G., Gül Z., Erçetin S., “Counter-Intelligence as a Chaotic Phenomenon and Its Importance in National Security” στο *Chaos Theory in Politics*, επιμ. Banerjee Santo, Erçetin Sefika, Tekin Ali, Springer, 2014

Lahneman William, “Is a Revolution in Intelligence Affairs Occurring?” στο *International Journal of Intelligence and CounterIntelligence*, Volume 20, Issue 1, 2007

Lahneman W., “The Need for a New Intelligence Paradigm” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 2, 2010

Lambakis S., Kiras J., Kolet K., *Understanding “Asymmetric” Threats to the United States*, National Institute for Public Policy, USA, 2002

Lance Peter, *1000 Years for Revenge: International Terrorism and the FBI-The Untold Story*, Regan Books, New York, 2003

Laqueur Walter, *A World of Secret. The Uses and Limits of Intelligence*, Basic Books, N.Y., 1985

Larsdotter Kersti, “Regional Support for Afghan Insurgents: Challenges for Counterinsurgency Theory and Doctrine” στο *Journal of Strategic Studies*, Volume 37, Number 1, 2014

Larson Eric, Eaton Derek, κ. ά., *Assessing Irregular Warfare. A Framework for Intelligence Analysis*, RAND, Santa Monica, 2008

Latimer J., *Deception in Warfare*, Overlook Press, Woodstock, New York, 2001

Lee Newton, *Counterterrorism and Cybersecurity. Total Information Awareness*, Springer, USA, 2013

Lefebvre Stéphane, “The Difficulties and Dilemmas of International Intelligence Cooperation” στο *International Journal of Intelligence and CounterIntelligence*, Volume 16, Issue 4, 2003

Lemieux Frédéric, “Financing Terrorism: Entrepreneurship, Business Strategies, and Moral Issues” στο *Protecting the Homeland from International and Domestic Terrorism Threats: Current Multi-Disciplinary Perspectives on Root Causes, the Role of Ideology, and Programs for Counter radicalization and Disengagement*, επιμ. Fenstermacher Laurie, Rieger Tom, κ. ά., 2010

Lequesne Christian, “French foreign and security challenges after the Paris terrorist attack”, *Contemporary Security Policy*, Volume 37, Issue 2, 2016

Encyclopedia of Espionage, Intelligence, and Security, Volume 1, επιμ. Lerner K., Lerner B., Gale, HHA, 2004

Leslau Ohad, “The Effect of Intelligence on the Decisionmaking Process” στο *International Journal of Intelligence and CounterIntelligence*, Volume 23, Issue 3, 2010

Lewis A. James, Timlin Katrina, *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization*, Center for Strategic and International Studies, Washington, D.C., 2011

Liaropoulos Andrew, *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm*, Research Paper No 100, RIEAS, Athens, 2006

Liaropoulos Andrew, “A Review of: ‘The Three Foes of Intelligence’” στο *International Journal of Intelligence and CounterIntelligence*, Volume 21, Issue 2, 2008

Liaropoulos Andrew, “The transformation of warfare in the information age” στο *Themata. Policy and Defence*, τεύχος 28, Απρίλιος 2009

Liaropoulos Andrew, Konstantopoulos Ioannis, “Reforming the Greek National Intelligence Service: Untying the Gordian Knot” στο *Journal of Mediterranean and Balkan Intelligence*, Volume 3, Number 1, 2014

Libicki M., *Illuminating Tomorrow's War*, Institute for National Strategic Studies, National Defense University, ΗΠΑ, 1999

Libicki M., *Cyberdeterrence and Cyberwar*, RAND, Santa Monica, 2009

Lillbacka R., “Realism, Constructivism, and Intelligence Analysis” στο *International Journal of Intelligence and CounterIntelligence*, Volume 26, Issue 2, 2013

Lim K., “Big Data and Strategic Intelligence” στο *Intelligence and National Security*, Volume 31, Volume 4, 2016

Lockhart B. John, “Intelligence: a British View” στο *British and American Approaches to Intelligence*, επιμ. Robertson G. K., Royal United Services Institute, USA, 1987

Lockhart B. John, “Intelligence: A British View” στο *Approaches to Intelligence*, επιμ. Robertson K., Macmillan, London, 1987

Lowenthal M., *Intelligence. From Secrets to Policy*, CQPress, Washington, D. C., 2003²

Lowenthal M., *Intelligence: From Secrets to Policy*, CQPress, Washington, D.C., ΗΠΑ, 2008⁴

Lucas Scott, “Recognizing Politicization: The CIA and the Path to the 2003 War in Iraq” στο *Intelligence and National Security*, Volume 26, Number 2-3, 2011

Luijff Eric, Healey Jason, “Organisational Structures & Considerations” στο *National Cyber Security. Framework Manual*, επιμ. Klimburg Alexander, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2012

Macdonald Sc., *Propaganda and Information Warfare in the Twenty-First Century*, Routledge, UK, 2007

McGrory Daniel, Jenkins Russell, “Fears of Terror Mole in UK Defence” στο *The Weekend Australian*, 3 Φεβρουαρίου 2007

McIntosh Christopher, “Counterterrorism as War: Identifying the Dangers, Risks, and Opportunity Costs of U.S. Strategy Toward L Qaeda and Its Affiliates” στο *Studies in Conflict and Terrorism*, Volume 38, Issue 1, 2015

McKenzie, Kenneth F., Jr., “The Revenge of the Melians: Asymmetric Threats and the Next QDR”, *McNair Paper*, 62, Carlisle Barracks / Pennsylvania, Νοέμβριος 2000

Mahnken T., “War in the Information Age” στο *Joint Force Quarterly*, τεύχος 10, 1995

Manget Frederick, “Intelligence and Law Enforcement” στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson L., Oxford University Press, Inc., USA, 2010

Maniscalco M. Luisa, “Living in the Cyber Era: Reflections on Security in a Hybrid World” στο *Mediterranean Council for Intelligence Studies Yearbook*, 2012

Manwaring Max, *Internal Wars: Rethinking Problem and Response*, Strategic Studies Institute / U.S. Army War College, Pennsylvania, 2001

Marrin Stephen, “Preventing Intelligence Failures by Learning from the Past” στο *International Journal of Intelligence and CounterIntelligence*, Volume 17, Issue 4, 2004

Marrin St., “The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis” στο *Intelligence and National Security*, Volume 26, Number 2-3, 2011

Marrin St., “Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful” στο *Intelligence and National Security*, Volume 27, Number 3, 2012

Marin St., “Guide to the Study of Intelligence: Why Teach About Intelligence” στο *The Intelligencer Journal of U.S. Intelligence Studies*, Volume 20, Number 1, 2013

Marrin St., “Rethinking Analytic Politicization” στο *Intelligence and National Security*, Volume 28, Number 1, 2013

Marrin St., “Revisiting Intelligence and Policy: Problems with Politicization and Receptivity” στο *Intelligence and National Security*, Volume 28, Number 1, 2013

Marrin Stephen, “The United States” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Masse Todd, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, Order Code RL31920, Report to Congress, Μάιος 2013

Max Boot, “More Small Wars” στο *Foreign Affairs*, Volume 93, Number 6, 2014

May E., “The importance of interchange. Studying and Teaching Intelligence” στο *Studies in Intelligence*, Volume 38, Number 5, 1995

Mazumadar Keshav, *Actionable Intelligence*, RIEAS, RIEAS e-Book No 5, Αθήνα, Σεπτέμβριος 2013

Metz St., *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*, Strategic Studies Institute, USA, 2000

Metz St., “Lessons from the Military Experience: The US Military and the IR: The Pitfalls of Uneven Adaptation” στο *The Information Revolution and National Security*, επιμ. Copeland Thomas, Strategic Studies Institute, ΗΠΑ, 2000

Michal Kr., “Business counterintelligence and the role of the U.S. intelligence community” στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 4, 1994

Monar Jörg, “The EU as an International Counter-terrorism Actor: Progress and Constraints” στο *Intelligence and National Security*, Volume 30, Number 2-3, 2015

Morag Nadav, “Foreign Intelligence and Counterterrorism: An Israeli Perspective” στο *Homeland Security and Intelligence*, επιμ. Logan G. Keith, Praeger, Santa Barbara / California, 2010

Moravej K., Díaz G., “Critical Issues in Contemporary Counter-Intelligence” στο *UNISCI Discussion Papers*, Number 13, Ιανουάριος 2007

Morgan Gareth, *Images of Organization*, Sage Publications, Inc., Thousand Oaks / California, 1997

Morse P. G., *America Twice Betrayed: Reversing Fifty Years of Government Security Failure*, Bartleby Press Inc, USA, 1995

Mottram Richard, “Protecting the Citizen in the Twenty-first Century: Issues and Challenges” στο *The New Protective State. Government, Intelligence and Terrorism*, επιμ. Hennessy Peter, Continuum Books, Mile End Institute, New York, 2007

Muller D., “Improving Futures Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 3, 2009

Mullins Sam, Dolnik Adam, “Relations between Violent Non-State Actors and Ordinary Crime” στο *Protecting the Homeland from International and Domestic Terrorism Threats: Current Multi-Disciplinary Perspectives on Root Causes, the Role of Ideology, and Programs for Counter radicalization and Disengagement*, επιμ. Fenstermacher Laurie, Rieger Tom, et al., 2010

Murphy Jr., J. F., “Michael Collins and the Craft of Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 17, Issue 2, 2004

Mowbray Joel , “How They Did It: An ‘Evil One’ Confesses, and Boasts” στο *National Review*, Volume 54, Number 24, 2002

Nasheri H., *Economic Espionage and Industrial Spying*, Cambridge University Press, N. York, HIA, 2005

Nathan Laurie, “The Intelligence Requirement of International Mediation” στο *Intelligence and National Security*, Volume 29, Number 2, 2014

National Intelligence Council, *Global Trends 2015*, National Intelligence Council, Washington, D.C., Δεκέμβριος 2000

Naylor T. R., “Mafias, Myths and Markets” στο *Transnational Organized Crime*, 3(3), 1997

- Newman Graeme, Clarke Ronald, *Policing Terrorism: An Executive's Guide*, US Department of Justice / Office of Community Oriented Policing Services, Brief 23
- Nicander Lars, "Understanding Intelligence Community Innovation in the Post 9-11 World" στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 3, 2011
- Nichiporuk Brian, Builder H. Carl, *Information Technologies and the Future of Land Warfare*, RAND, Santa Monica, 1995
- Nolte William, "Valuing Intelligence: Opening a Conversation" στο *Intelligence and National Security*, Volume 26, Number 5, 2011
- Nomikos John, "The Internal Modernization of the Greek Intelligence Service (NIS-EYP)" στο *International Journal of Intelligence and CounterIntelligence*, Volume 17, Issue 3, 2004
- Nomikos John, Liaropoulos Andreas, "Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernization of the Greek National Intelligence Service" στο *Journal of Policing, Intelligence and Counter Terrorism*, Volume 5, Number 1, 2010
- Nye Joseph, Owens William, "America's information edge", *Foreign Affairs*, Volume 75, Number 2, 1996
- Omand David, "The Cycle of Intelligence" στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, Βρετανία, 2014
- Orlov Alexander, "The Theory and Practice of Soviet Intelligence" στο *Studies in Intelligence*, Volume 7, Number 2, 1963
- Owens William, "The Emerging System of Systems" στο *Military Review*, Volume 75, Number 3, 1995
- Papp Daniel, Alberts David, "The Impacts of the Information Age on International Actors and the International System" στο *The Information Age: An Anthology on Its Impact and Consequences*, επιμ. Alberts D., Papp D., CCRP Publication Series, 1997
- Papp D., Alberts D., "War in the Information Age Military" στο *Information Age Anthology: The Information Age Military*, επιμ. Alberts D., Papp D., CCRP Publication Series, 2001
- Papp D., Alberts D., "The Future of Defence Policy: Information Age Trends" στο *Information Age Anthology: The Information Age Military*, επιμ. Alberts D., Papp D., CCRP Publication Series, 2001
- Pascovich Eyal, "Military Intelligence and Controversial Political Issues: The Unique Case of the Israeli Military Intelligence" στο *Intelligence and National Security*, Volume 29, Number 2, 2014

Perkovich George, *India's Nuclear Bomb: The Impact on Global Proliferation*, University of California Press, Berkeley, 1999

Perrow Charles, *Normal Accident: Living with High-Risk Technology*, Basic Books, New York, 1984

Perrow Charles, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*, Princeton University Press, Princeton, 2007

Petersen Martin, "The Challenge for the Political Analyst" στο *Studies in Intelligence*, Volume 47, Number 1, 2003

Phythian M., "Intelligence theory and theories of international relations: shared worlds or separate worlds?" στο *Intelligence Theory: Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, UK, 2009

Phythian Mark, "Beyond the Intelligence Cycle?" στο *Understanding the Intelligence Cycle*, επιμ. Phythian Mark, Routledge, Βρετανία, 2013

Phythian Mark, "Cultures of national intelligence" στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Pillar Paul, "The Perils of Politicization" στο *The Oxford Handbook of National Security Intelligence*, επιμ. Johnson L., Oxford University Press, N. York, 2010

Πλακούδας Σπυρίδωνας, "Strategy in Counter-Insurgency: A Distilled Approach" στο *Studies in Conflict and Terrorism*, Volume 38, Issue 2, 2015

Pollard Neal, Sullivan John, "Counterterrorism and Intelligence" στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Porteous S., "Economic & Commercial Interests and the World's Intelligence Services: A Canadian Perspective" στο *International Journal of Intelligence and CounterIntelligence*, Volume 8, Issue 3, 1995

Posner A. Richard, *Remaking Domestic Intelligence*, Hoover Institution Press Publication, USA, 2005

Posner A. Richard, "We Need Our Own MI5", *The Washington Post*, 14 Αυγούστου 2006

Posner A. Richard, "Counterintelligence, Counterterrorism, Civil Liberties, and the Domestic Intelligence Controversy" στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, USA, 2009

Potter Gary, *Criminal Organizations: Vice Racketeering and Politics in an American City*, Waveland Press, Illinois / USA, 1993

Rovner Joshua, “Is Politicization Ever a Good Thing?” στο *Intelligence and National Security*, Volume 28, Number 1, 2013

Powner D., “Critical Infrastructure Protection. DHS Needs to Better Address its Cybersecurity Responsibilities” στο *Cybersecurity, Cyberanalysis and Warning*, επιμ. Norwood Kerry, Catwell Sandra, Nova Science Publishers, Inc, New York, 2009

Prunckun Hank, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, The Scarecrow Press, Inc., UK, 2010

Prunckun Hank, *Counterintelligence. Theory and Practice*, Rowman & Littlefield Publishers, USA, 2012

Quiggin Thomas, *Seeing the Invisible. National Security Intelligence in a Uncertain Age*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2007

Reagan Mark, *Introduction to U.S. Counterintelligence. “CI 101--A Primer”*, 2005

Terms & Definitions of Interest for Counterintelligence Professionals, επιμ. Reagan M., 2014

Reddick Christopher, *Homeland Security Preparedness and Information Systems. Strategies for Managing Public Policy*, IGI Global, USA, 2010

Redmond J. Paul, “The Challenges of Counterintelligence” στο *The Oxford Handbook of National Security Counterintelligence*, επιμ. Johnson Loch, Oxford University Press, New York, 2010

van Reijn, Joop, “Intelligence and Strategic Culture: Essays on American and British Praxis since the Second World War” στο *Intelligence and National Security*, Volume 26, Number 4, 2011

Reiner Robert, *The Politics of the Police*, OUP, Oxford, 2000²

Richards Julian, “Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy” στο *Intelligence and National Security*, Volume 27, Number 5, 2012

Richter Andrew, “Lessons From the Revolution: What Recent US Military Operations Reveal About the Revolution in Military Affairs and Future Combat” στο *Journal of Military and Strategic Studies*, Volume 7, Issue 3, 2004

Rid Thomas, “The Nineteenth Century Origins of Counterinsurgency Doctrine” στο *Journal of Strategic Studies*, Volume 33, Number 5, 2010

van Riper, P., Hoffman E., “Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare” στο *National Security Studies Quarterly*, Volume 4, Number 3, 1998

Rittinghouse W., John, Hancock M., William, *Cybersecurity Operations Handbook*, Elsevier, Inc., USA, 2003

Robinson Colin, *Military and Cyber-Defense: Reactions to the Threat*, Center for Defense Information Terrorism Project, Washington, D.C., 2002

Rogan Hanna, *Jihadism Online: A Study of How al-Qaeda and Radical Islam Groups Use the Internet for Terrorist Purposes*, Norwegian Defence Research Establishment, Norway, 2006

Rokosz F. Ronald, Hash H. Charles, “Army Antiterrorism Force Protection” στο *Joint Force Quarterly*, Φθινόπωρο / Χειμώνας 1997-1998

Romm Joseph, *Defining National Security: The Nonmilitary Aspects*, Council of Foreign Relations Press, New York, 1993

Rosenau James, “The Information Revolution: Both Powerful and Neutral” στο *The Information Revolution and National Security*, επιμ. Copeland Th., Strategic Studies Institute / US Army War College, Pennsylvania, 2000

Roth P. Mitchel, *Crime and Punishment: A History of the Criminal Justice System*, Wadsworth Publishing, Belmont / California, 2004

Rovner J., “Intelligence in the Twitter Age” στο *International Journal of Intelligence and CounterIntelligence*, Volume 26, Issue 2, 2013

Rudner M., “Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand” στο *International Journal of Intelligence and CounterIntelligence*, Volume 22, Issue 1, 2009

Sageman Marc, “The Next Generation of Terror” στο *Foreign Policy*, Μάρτιος / Απρίλιος 2008

Sanchez E. S., “Spider Web: Al-Qaeda’s Link to the Intelligence Agencies of the Major Powers” στο *International Journal of Intelligence and CounterIntelligence*, Volume 28, Issue 3, 2015

Sanderson Th., “Transnational Terror and Organized Crime: Blurring the Lines”, *SAIS Review*, Volume 24, Number 1, 2004

Scales R., *Future Warfare Anthology*, US Army War College, Pennsylvania, 2000

Schein Edgar, *Organizational Culture and Leadership*, Jossey Bass, San Francisco, 2010

Schiattareggia H. M., “Counterintelligence in Counterguerrilla Operations”, *Studies in Intelligence*, Volume 6, Number 3, 1962

Schoomaker P., *The Way Ahead: Our Army at War ... Relevant and Ready. Moving from the Current Force to the Future Force ...Now!*, Army Strategic Communications, USA, November 2003

Schreier Fred, *Transforming Intelligence Services. Making Them Smarter, More Agile, More Effective and More Efficient*, National Defence Academy, Austrian Ministry of Defence and Sports, Geneva Centre for the Democratic Control and Armed Forces, Βιέννη, 2010

Schreier Fred, *On Cyberwarfare*, DCAF Horizon 2015, Working Paper No 7

Schulze, K. E., “Camp David and the Al-Aqsa intifada: an assessment of the state of the Israeli-Palestinian peace process July-December 2000”, *Studies in Conflict and Terrorism*, Volume 24, Issue 3, 2001

Schweizer P., *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal our Secrets*, Atlantic Monthly Press, USA, 1993

Schweizer P., “The Growth of Economic Espionage: America Is Target Number One” στο *Foreign Affairs*, Volume 75, Number 1, 1996

Scott L., “Sources and Methods in the Study of Intelligence: A British View” στο *Intelligence and National Security*, Volume 22, Number 2, 2007

Scott L., Jackson P., “The Study of Intelligence in Theory and Practice” στο *Intelligence and National Security*, Volume 19, Number 2, 2004

Shelton Christina, “The Roots of Analytic Failures in the U.S. Intelligence Community” στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 4, 2011

United States District Court, *United States of America v. Ali Mohamed*, Southern District of New York, 20 Οκτωβρίου 2000

Senge Peter, *The Fifth Discipline: The Art and Practice of the Learning Organization*, Random House, Sydney, 1992

Shpiro Shlomo, “Israeli Intelligence and al-Qaeda” στο *International Journal of Intelligence and CounterIntelligence*, Volume 25, Issue 2, 2012

Shulsky A., Schmitt G., *Silent Warfare. Understanding the World of Intelligence*, Brassey's, Inc., Washington, D.C., HPIA, 2002³

Shulsky A., “Elements of Strategic Denial and Deception” στο *Strategic Denial and Deception*, επιμ. Godson R., Wirtz J, Transaction Publishers, New Brunswick / New Jersey, 2002

Sick Gary, *All Fall Down: America's Tragic Encounter With Iran*, Penguin, New York, 1986

Sims J., *Understanding Friends and Enemies: The Context for American Intelligence Reform*, Georgetown University Press, Washington, D.C., 2005

Sims J., “Twenty-first-Century Counterintelligence. The Theoretical Basis for reform” στο *Vaults Mirrors and Masks. Rediscovering U.S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, Washington, D.C., 2009

Sims J., “Defending adaptive realism. Intelligence theory comes of age” στο *Phythian Mark*, Routledge, UK, 2009

Singer W. P., Friedman Allan, *Cybersecurity and Cyberwar. What Everyone Needs To Know*, Oxford University Press, USA, USA, 2014

Skogan Wesley, “Why Reforms Fail?”, *Policing and Society*, 18, 1, March 2008

Skoudis E., Liston T., *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Pearson Education, Inc., New Jersey, 2006²

Šmíd Tomáš, Mareš Miroslav, “‘Kadyrovtsy’: Russia’s Counterinsurgency Strategy and the Wars of Paramilitary Clans” στο *Journal of Strategic Studies*, Volume 38, Number 5, 2015

Smith, W. Thomas, Jr., *Encyclopedia of the Central Intelligence Agency*, Facts On File, Inc., New York, 2003

Slapper G., Tombs S., *Corporate Crime*, Harlow, London, 1999

Sloan Stephen, “Terrorism: How Vulnerable is the United States?” στο *Terrorism: National Security Policy and the Home Front*, επιμ. Pelletiere Stephen, Strategic Studies Institute, USA, 1995

Speckhard A., Yayla A., *ISIS Defectors: Inside Stories of the Terrorist Caliphate*, Advances Press / LLC, McLean / Virginia, 2016

Speckhard A., Yayla A., “The ISIS Emni: Origins and Inner Working s of ISIS’s Intelligence Apparatus” στο *Perspectives on Terrorism*, Volume 11, Issue 1, 2017

Stafford Th., “Assessing current intelligence studies” στο *International Journal of Intelligence and CounterIntelligence*, Volume 2, Issue 2, 1988

Steele Robert, “National Intelligence and Open Source: From School House to White House”, *American Intelligence Journal*, Volume 14, Number 2 / 3, 1993

Steele Robert, “The Importance of Open Source Intelligence to the Military”, *International Journal of Intelligence and Counterintelligence*, Volume 8, Issue 4, 1995

Steele Robert, “Crafting Intelligence in the Aftermath of Disaster”, *International Journal of Intelligence and Counterintelligence*, Volume 15, Issue 2, 2002

- Stein G., “Information Warfare” στο *Air Power Journal*, Volume 9, Number 1, 1995
- Steinberg J., “The policymaker’s Perspective: Transparency and Partnership” στο *Analyzing Intelligence. Origins, Obstacles, and Innovations*, επιμ. George Roger, Bruce James, Georgetown University Press, Washington, D. C., 2008
- Steinmeyer Walter, “The Intelligence Role in Counterinsurgency”, *Studies in Intelligence*, Volume 9, Number 4, 1965
- Stephan R., *Stalin’s Secret War. Soviet Counterintelligence Against the Nazis, 1941-1945*, University Press of Kansas, Lawrence / Kansas, 2004
- Steven Graeme, Gunaratna Rohan, *Counterterrorism. A Reference Handbook*, ABC-CLIO, Inc., Santa Barbara / California, 2004
- Stime Britta, “Counterinsurgency Agent Networks and Noncombatant-Targeted Violence” στο *Intelligence and National Security*, Volume 32, Number 1, 2017
- Stoll Clifford, “Stalking the Willy Hacker”, *Communication of the ACM*, Volume 31, Number 5, 1988
- Stoll Clifford, *The Cuckoo’s Egg: Tracking a Spy through the Maze of Computer Espionage*, Doubleday, New York, 1989
- Strategic Survey 2003 / 2004. An Evaluation and Forecast of World Affairs*, International Institute for Strategic Studies / Oxford University Press, Oxford, 2004
- Strong T., “Tilting with Machiavelli: Fighting Competitive Espionage in the 1990s” στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 2, 1995
- Sulc L., *Law Enforcement Counterintelligence*, Varro Press, Kansas / USA, 1996
- Sulick J. Michael, “Counterintelligence in the War Against Terrorism”, *Studies in Intelligence*, Volume 48, Number 4, 2004
- Sulick Michael, *American spies: espionage against the United States from the Cold War to the present*, Georgetown University Press, USA, 2013
- Sun Tzu, *The Art of War*, μτφρ. Griffith B. Samuel, Oxford University Press, New York, 1973
- Svendsen Ad., “Connecting Intelligence and Theory: Intelligence Liaison and International Relations” στο *Intelligence and National Security*, Volume 24, Number 5, 2009
- Taylor A. Stan, “Definitions and Theories of Counterintelligence” στο *Strategic Intelligence*, Volume 4, επιμ. Johnson K. Loch, Praeger Security International, 2007

Tenet G., “The CIA and Security Challenges of the New Century”, *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 2, 2000

Titus James, “Review of ‘Henry L. Stimson: The First Wise Man’ by David F. Schmitz” στο *Aerospace Power Journal*, Volume XVI, Number 2, 2002

Toffler Al., *Powershift. Knowledge, Wealth and Violence at the Edge of the 21st Century*, Bantam Books, New York, 1990

Touhill J. G., Touhill J. C., *Cybersecurity for Executives. A Practical Guide*, John Wiley & Sons, Inc., Hoboken / New Jersey, 2014

Treverton Gregory, *Reshaping National intelligence for an Age of Information*, Cambridge University Press, New York, 2003

Toward a Theory of Intelligence. Workshop Report, επιμ. Treverton Gregory, Jones Seth, Boraz Steven, Lipsky Phillip, RAND, Santa Monica, 2006

Treverton Gregory, *Reorganizing U.S. Domestic Intelligence. Assessing the Options*, RAND, Santa Monica, 2008

Treverton Gr., “Intelligence Analysis: Between ‘Politicization’ and Irrelevance” στο *Analyzing Intelligence. Origins, Obstacles, and Innovations*, επιμ. George Roger, Bruce James, Georgetown University Press, Washington, D. C., 2008

Tucker David, *The End of Intelligence. Espionage and State Power in the Information Age*, Stanford University Press, USA, 2014

Turbiville Graham, Jr., *Guerrilla Counterinsurgency. Insurgent Approaches to Neutralizing Adversary Intelligence Operations*, Joint Special Operations University Press, Florida, 2009

Turner Michael, “Understanding CIA’s Role in Intelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 4, Issue 3, 1990

Turner Michael, *Historical Dictionary of United States Intelligence*, The Scarecrow Press, Inc., USA, 2006

Ucko David, “‘The People are Revolting’: An Anatomy of Authoritarian Counterinsurgency” στο *Journal of Strategic Studies*, Volume 39, Number 1, 2016

Ulph Stephen, “New Online Book Lays out al-Qaeda’s Military Strategy” στο *Terrorism Focus*, Volume 2, Issue 6, 2005

United Nations Convention against Transnational Organized Crime, United Nations Office of Drugs and Crime, UN, Geneva, 2000

U.S. President, *National Security Strategy*, Washington, D.C., Μάιος 2010

U.S. President, *National Security Strategy*, Washington, D.C., Φεβρουάριος 2015

Uneri Mert, Karabacak Bilge, “Securing Networks in the Information Age” στο *Cyberwar-Netwar. Security in the Information Age*, επιμ. Carvalho Fernando, daSilva Eduardo, Ios Press, Amsterdam, 2006

Varouhakis Miron, “An Institution-Level Theoretical Approach for Counterintelligence” στο *International Journal of Intelligence and CounterIntelligence*, Volume 24, Issue 3, 2011

Varouhakis M., “What is Being Published in Intelligence? A Study of Two Scholarly Journals” στο *International Journal of Intelligence and CounterIntelligence*, Volume 26, Issue 1, 2013

Vellone Luigi, “From Data to Knowledge: How Intelligence and Security Tools Can Help” στο *Cyberwar-Netwar. Security in the Information Age*, επιμ. Carvalho Fernando, daSilva Eduardo, Ios Press, Amsterdam, 2006

Modernizing Intelligence: Structure and Change for the 21st Century, επιμ. Victory C. B., National Institute for Public Policy, 2002

Wallace P., “A Time for Counterespionage” στο *Vaults, Mirrors and Masks. Rediscovering U. S. Counterintelligence*, επιμ. Sims J., Gerber B., Georgetown University Press, USA, 2009

Waller Michael, *Secret Empire: The KGB in Russia Today*, Westview Press, Oxford, 1994

Walters Vernon, *Silent Missions*, Doubleday, Garden City / N.Y., 1978

Waltz Edward, *Information Warfare, Principles and Operations*, Artech House, Inc, ΗΠΑ, 1998

Waltz Edward, *Knowledge Management in the Intelligence Enterprise*, Artech House, Inc, Μασαχουσέτη / ΗΠΑ, 2003

Wark Wesley, “The Intelligence Revolution and the Future” στο *Studies in Intelligence*, Volume 37, Number 4, 1993

Wark Wesley, “Introduction: The Study of Espionage: Past, Present, Future?” στο *Espionage: Past, Present, Future?*, επιμ. Wark K. Wesley, Frank Cass & Co. Ltd., Great Britain, 1994

Warner M., “Wanted: A Definition of ‘Intelligence’” στο *Studies in Intelligence*, Volume 46, Number 3, 2002

Warner M., “Sources and methods for the study of intelligence” στο *Handbook of Intelligence Studies*, επιμ. Johnson L., Routledge, Βρετανία, 2007

Warner M., “Intelligence as Risk Shifting”, *Intelligence Theory. Key questions and debates*, επιμ. Gill Peter, Marrin Stephen, Phythian Mark, Routledge, London, UK, 2009

Warner M., “Reflections on Technology and Intelligence Systems” στο *Intelligence and National Security*, Volume 27, Number 1, 2012

Warner M., “Fragile and Provocative: Notes on Secrecy and Intelligence” στο *Intelligence and National Security*, Volume 27, Number 2, 2012

Warner M., “Cybersecurity: A Pre-History” στο *Intelligence and National Security*, Volume 27, Number 5, 2012

Warner M., “Theories of intelligence: the state of play” στο *Routledge Companion to Intelligence Studies*, επιμ. Dover Robert, Michael S. Goodman, Hillebrand Claudia, Routledge, UK, 2014

Warner William, “International technology transfer and economic espionage” στο *International Journal of Intelligence and CounterIntelligence*, Volume 7, Issue 2, 1994

Warnes Richard, “France” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009

Warnes Richard, “Germany” στο *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, επιμ. Jackson Brian, RAND, Santa Monica, 2009

Wasemiller C. A., “The Anatomy of Counterintelligence” στο *Studies in Intelligence*, Volume 13, Number 1, 1969

Watt Donald, “Intelligence Studies: The Emergence of the British School” στο *Intelligence and National Security*, Volume 3, Number 2, 1988

Webb M. J., “Intelligence in Public Literature. Intelligence Theory: Key Questions and Debates” στο *Studies in Intelligence*, Volume 53, Number 2, 2009

Webster Fr., “What Information Society?” στο *The Information Society*, Volume 10, Number 1, 1994

Wege A. Carl, “Hizballah’s Counterintelligence Apparatus” στο *International Journal of Intelligence and CounterIntelligence*, Volume 25, Issue 4, 2012

Wei Jincheng, “New Form of People’s War” στο *Foreign Broadcast Information Survey -CHI*, Number 159, 1996

Weimann Gabriel, “Cyberterrorism: The Sum of All Fears?” στο *Studies in Conflict & Terrorism*, Volume 28, Issue 2, 2005

Wellman Carl, *Terrorism and Counterterrorism. A Moral Assessment*, Springer, 2013

West N., *Historical Dictionary of British Intelligence*, The Scarecrow Press, Inc., HΠΑ, 2005

West N., *Historical Dictionary of International Intelligence*, The Scarecrow Press, Inc., HΠΑ, 2006

Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992, επιμ. Westerfield B. H., Yale University Press, New Haven, 1995

Wettering Frederick, "Counterintelligence: The Broken Triad" στο *International Journal of Intelligence and CounterIntelligence*, Volume 13, Issue 3, 2000

Whaley B., *Stratagem: Deception and Surprise in War*, Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, USA, 1969

Whaley B., "Toward a General Theory of Deception" στο *Military Deception and Strategic Surprise*, Frank Cass and Co. Ltd, London, 1982

Whaley B., *Stratagem: Deception and Surprise in War*, Artech House, Inc., Norwood / Massachusetts, 2007

Williams R. D., "Is the West's Reliance on Technology the Panacea for Future Conflict or its Achilles heel?" στο *Defence Studies*, Volume 1, Number 2, 2001

Williams Phil, "Transnational Criminal Networks" στο *Networks and Netwars: The Future of Terror, Crime, and Militancy*, επιμ. Arquilla John, Ronfeldt David, RAND, Santa Monica, 2001

Williams Phil, Dunlevy Casey, Shimeal Tim, "Intelligence Analysis for Internet Security" στο *Contemporary Security Policy*, Volume 23, Issue 2, 2002

Williams P., Godson R., "Anticipating Organized and Transnational Crime", *Crime, Law and Social Change*, 37, 2002

Wilner Alex, "Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism" στο *Journal of Strategic Studies*, Volume 34, Number 1, 2011

Wimmer Bruce, *Business Espionage. Risks, Threats, and Countermeasures*, Elsevier Inc., 2015

Winterfeld Steve, Andress Jason, *The Basics of Cyber Warfare. Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Elsevier, Inc., USA, 2013

Wirtz James, "Theory of Surprise" στο *Intelligence Theory. Key questions and debates*, επιμ. Gill P., Marrin St., Phythian M., Routledge, U.K., 2009, σ. 73

Wirtz James, Rosenwasser John, "From Combined Arms to Combined Intelligence: Philosophy, Doctrine and Operations" στο *Intelligence and National Security*, Volume 25, Number 6, 2010

Wolfers Arnold, “National Security as an Ambiguous Symbol” στο *Discord and Collaboration*, Johns Hopkins, Baltimore, 1962

Woodward Bob, *Plan of Attack*, Simon & Schuster, London, 2004

Woodard N., “Testing the Forbidden Fruit: Unlocking the Potential of Positive Politicization” στο *Intelligence and National Security*, Volume 28, Number 1, 2013

Wright Jeffrey, “Intelligence and Economic Security” στο *International Journal of Intelligence and CounterIntelligence*, Volume 5, Issue 2, 1991

Zegart Amy, *Spying Blind: The CIA, the FBI and the Origins of 9/11*, Princeton University Press, Princeton, 2007

Zegart Amy, “Cloaks, Daggers, And Ivory Towers” στο *Strategic Intelligence*, Volume 1, επιμ. Johnson K. Loch, Praeger Security International, 2007

ΕΚΔΟΣΕΙΣ, ΕΓΧΕΙΡΙΔΙΑ, ΠΡΑΞΕΙΣ ΘΕΣΜΩΝ, ΟΡΓΑΝΙΣΜΩΝ, ΥΠΗΡΕΣΙΩΝ

National Security Act of 1947, (Chapter 343; 61 Stat. 496; approved July 26, 1947), [As Amended Through P.L. 110–53, Enacted August 3, 2007]

Association of Chief Police Officers (ACPO), *Introduction to Intelligence-Led Policing*, Centre for Policing Excellence, UK, 2007

Air Force Doctrine Document 2-5, *Information Operations*, U.S. Air Force, 1998

Air Force Instruction 71-101, Volume 4, *Special Investigations, Counterintelligence*, Department of the Air Force, Νοέμβριος 2011

Air Force Policy Directive 71-1, *Special Investigations, Criminal Investigations and Counterintelligence*, Ιανουάριος 2010

Report of the Inquiry into Australian Intelligence Agencies, Australian Government, Ιούλιος 2004

Army Regulation (AR) 381-14, *Technical Surveillance Countermeasures*, Headquarters, Department of the Army, Washington, D.C., Οκτώβριος 1986

AR 381-12, *Subversion and Espionage Directed Against the US Army*, DoD, 15 Ιανουαρίου 1993

AR 381-20, *Military Intelligence. The Army Counterintelligence Program*, Headquarters, Department of the Army, Washington, D.C., Νοέμβριος 1993

AR 380-5, *Department of the Army Information Security Program*, Headquarters, Department of the Army, Washington, D.C., Σεπτέμβριος 2000

AR 381-14, *Technical Counterintelligence*, Headquarters, Department of the Army, Washington, D.C., Σεπτέμβριος 2002

AR 381-14, *Technical Surveillance Countermeasures*, Headquarters, Department of the Army, Washington, D.C., Φεβρουάριος 2015

AR 381-12, *Threat Awareness and Reporting Program*, Headquarters, Department of the Army, Washington, D.C., Ιούνιος 2016

Standards for Law Enforcement Accreditation, Commission on Accreditation of Law Enforcement Agencies, Washington, D.C., 2002

Making Intelligence Smarter: Report of an Independent Task Force, Council on Foreign Relations, New York, 1996

Federal Broadcast Information Service (CIA), “BKA Registers Less Damaged Caused by Gangs”, *Frankfurter Rundschau*, 13 Ιουλίου 1998

U.S. GAO (2005a), *Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, May 2005

GAO (2005b), *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, (GAO Publication No. GAO-05-231), Government Printing Office, Washington, D.C., 2005

U.S. Government Accountability Office, “Cyber Analysis and Warning. DHS Faces Challenges in Establishing a Comprehensive National Capability” στο *Cybersecurity, Cyberanalysis and Warning* στο *Cybersecurity, Cyberanalysis and Warning*, επιμ. Norwood Kerry, Catwell Sandra, Nova Science Publishers, Inc, New York, 2009

National Criminal Intelligence Sharing Plan, Global Intelligence Working Group, Office of Justice Programs, Washington, D.C., 2003

National Military Strategic Plan for the War on Terrorism, Chairman of the Joint Chiefs’ of Staff, Washington, D.C., 2006

JP 3-13, *The U.S. Joint Doctrine for Information Operations*, Joint Chiefs of Staff, 1998

JP 3-13, *Information Operations*, Joint Chiefs of Staff, 2012

JP 3-13.4, *Military Deception*, Joint Chiefs of Staff, 2006

JP 3-58, *The U.S. Joint Doctrine for Military Deception*, Joint Chiefs of Staff, 1996

Central Intelligence Agency, Office of Public Affairs, *A Consumer’s Guide to Intelligence. Gaining Knowledge and Foreknowledge of the World around Us*, Washington, D.C., 1999

“CIA Opens Center on Climate Change and National Security”, CIA, 25 Σεπτεμβρίου 2009

National Security and the Accelerating Risks of Climate Change, CNA Military Advisory Board, Alexandria / Virginia, Μάιος 2014

Department of the Army, *U.S. Army Counterintelligence Handbook*, Skyhorse Publishing, Inc., 2013

MCWP 2-14, *Counterintelligence*, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., Σεπτέμβριος 2000

Cornerstones of Information Warfare, Department of the Air Force, Washington, D.C., 1995

Air Force Policy Directive 71-1, *Special Investigations, Criminal Investigations and Counterintelligence*, Department of the Air Force, Ιανουάριος 2010

The Department of Defense Strategy for Counterintelligence in Cyberspace, DoD, Αύγουστος 2009

DoD, *Quadrennial Defense Review Report*, Φεβρουάριος 2010

Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, DoD, Washington, D.C., Ιανουάριος 2013

2014 Climate Change Adaptation Roadmap, DoD, 2014

The DoD Cyber Strategy, DoD, Απρίλιος 2015

DoD Directive 5000.01, *The Defense Acquisition System*, Μάιος 2003

Department of Defense Directive (DoDD) O-5240.02, *Counterintelligence*, 2007

DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, Οκτώβριος 2008

DoDI 5240.05, *Technical Surveillance Countermeasures (TSCM)*, Department of Defense, Απρίλιος 2014

DoDD 5240.02, *Counterintelligence*, Μάρτιος 2015

Department of Defense Directive Instruction (DoDI) 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, Αύγουστος 2007

DoDI 5240-16, *Counterintelligence Functional Services*, US DoD, 27 Αυγούστου 2012

Department of Defense, CI Functional Services Integrated Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services*, Φεβρουάριος 2009

Department of Defense Instruction (DoDI), *Counterintelligence Functional Services*, 5240.16, Αύγουστος 2012

Terms & Definitions of Interest for DoD Counterintelligence Professionals, Defense Intelligence Agency, 2011

Global Justice Information Sharing Initiative, *Navigating Your Agency's Path to Intelligence-Led Policing*, US Department of Justice, Washington, D.C., 2009

ICS 700-1, *Glossary of Security Terms, Definitions, and Acronyms*, ODNI, Απρίλιος 2008

ICD 702, *Technical Surveillance Countermeasures*, ODNI, Φεβρουάριος 2008

Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, 10 Μαρτίου 2009

ICD 700, *Protection of National Intelligence*, Office of the Director of National Intelligence, 7 Ιουνίου 2012

Vision 2015. A Globally Networked and Integrated Intelligence Enterprise, ODNI, Washington, D.C., 2008

National Intelligence. A Consumer's Guide, ODNI, 2009

The National Intelligence Strategy of the United States of America, ODNI, Αύγουστος 2009

U.S. National Intelligence. An Overview, ODNI, 2013

The National Intelligence Strategy of the United States of America, ODNI, 2014
DNI Unveils 2014 National Intelligence Strategy, ODNI, Σεπτέμβριος 2014

National Counterintelligence Strategy of the United States of America, National Counterintelligence and Security Center, ODNI, 2016

Fundamental Elements of the Counterintelligence Discipline. Universal Counterintelligence Competencies, National Counterintelligence Institute, Office of the National Counterintelligence Executive, Office of the Director of National Intelligence, 2006

Executive Order 12333--United States Intelligence Activities, Δεκέμβριος 1981, παράγραφος 1.4

Executive Order 12292 “Further Amendment to Executive Order 12958, as Amended, Classified National Security Information”, Μάρτιος 2003

The European Union’s Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness, European Parliament, Brussels, Ιανουάριος 2017

FM 1-02, *Operational Terms and Graphics*, Department of the Army, Marine Corps Combat Development Command. Department of the Navy, Washington, D.C., 21 Σεπτεμβρίου 2004

FM 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2004

FM 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2010

FM 2-0, *Intelligence*, Headquarters, Department of the Army, Washington, D.C., 2014

FM 2-22.2, *Counterintelligence*, Headquarters, Department of the Army, Washington, D.C., Οκτώβριος 2009

FM 2-22.3, *Human Intelligence Collector Operations*, Headquarters, Department of the Army, Washington, D.C., Σεπτέμβριος 2006

FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques and Procedures*, Headquarters, Department of the Army, Washington, D.C., 2003

FM 3-24 / FMFM 3-24, *Counterinsurgency*, Headquarters, Department of the Army, Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., June 2006

FM 3-24 / MCWP 3-33.5, *Counterinsurgency*, Headquarters, Department of the Army, Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Washington, D.C., December 2006

FM 34-7 *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations*, Headquarters, Department of the Army, Washington, D.C., 1993

FM 34-60, *Counterintelligence*, Headquarters, Department of the Army, Washington, D.C., Οκτώβριος 1995

FM 34-130, *Intelligence Preparation of the Battlefield*, Headquarters, Department of the Army, USA, July 1994

Report of the Commission on Government Security, US Government Printing Office, Washington, D.C., 1957

The Threat of Foreign Economic Espionage to U.S. Corporations, U.S. Government Printing Office, Washington, D.C., 1992

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 Απριλίου 2001 (as amended through 17 October 2007)

JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 16 July 2014)

JP 1-02, *Dictionary of Military and Associated Terms*, DoD, Νοέμβριος 2010 (as amended through 15 February 2015)

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, DoD, November 2010 (as amended through February 2016)

JP 2-0, *Joint Intelligence*, Joint Chiefs of Staff, Οκτώβριος 2013

JP 2-01, *Joint and National Intelligence Support to Military Operations*, 2012

JP 2-01.2, *CI & HUMINT in Joint Operations*, DoD, Μάρτιος 2011

JP 3-13, *The U.S. Joint Doctrine for Information Operations*, 1998JP 3-13, *Information Operations*, Νοέμβριος 2012 (Incorporating Change 1 November 2014)

JP 3-13.4, *Military Deception*, 2006

JP 3-26, *Counterterrorism*, Joint Chiefs of Staff, Νοέμβριος 2009

JP 3-58, *The U.S. Joint Doctrine for Military Deception*, 1996

Joint Security Commission II Report, Αύγουστος 1999

Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Φεβρουαρίου 1994

Joint Test Publication 2-0, *Doctrine for Intelligence Support to Joint Operations*, The Joint Staff, Washington, D.C., June 1991

NCIX Publication 2005-10007, *The National Counterintelligence Strategy of the United States*, Office of the National Counterintelligence Executive, Washington, D.C., Μάρτιος 2005

Foreign Economic Collection and Industrial Espionage, 2005, NCIX, Αύγουστος 2006

The National Counterintelligence Strategy of the United States, Office of the National Counterintelligence Executive, Μάρτιος 2005

The National Counterintelligence Strategy of the United States of America, Office of the National Counterintelligence Executive, 2007

The National Counterintelligence Strategy of the United States of America, Office of the National Counterintelligence Executive, 2008

The National Counterintelligence Strategy of the United States of America, Office of the National Counterintelligence Executive (NCIX-2010-002), 2009

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008, ONCIX, Ιούλιος 2009

US Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage*, 2009-2011, Οκτώβριος 2011

Protecting Key Assets: A Corporate Counterintelligence Guide, ONCIX, 2012

NSCID No 5, *U.S. Espionage and Counterintelligence Activities Abroad*, Απρίλιος 1958

Presidential Decision Directive 63, *Critical Infrastructure Protection*, Μάιος 1998, τμήμα II

U.S. President Executive Order “United States Intelligence Activities, Executive Order 12333”, *Federal Register* 46, number 59941, 4 Δεκεμβρίου 1981

Secretary of the Navy Instruction (SECNAVINST) 3850.2C, Department of the Navy Counterintelligence, 20 Ιουλίου 2005

SECNAVINST 3850.4A, *Technical Surveillance Countermeasures Program*, Department of the Navy, Washington, D.C., Αύγουστος 2014

Senate Report # 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, US Government Printing Office, Washington, D.C., Απρίλιος 1976

United States District Court, *United States of America v. Mokhtar Haouari*, Southern District of New York, 3 Ιουλίου 2001

Cyber Security Strategy for Germany, German Federal Ministry of the Interior, Βερολίνο, 2011

Critical Infrastructure Protection: Threats, Attacks and Countermeasures, επιμ. Montarani Luca, Querzoni Leonardo, Tenace Prin Project, Italian Ministry of Education, University and Research, Μάρτιος 2014

National Intelligence Machinery, The Stationary Office, UK, Απρίλιος 2000

Security Service Act 1989, The Stationary Office, UK, 1989, Chapter 5
HM Government. Countering International Terrorism: The United Kingdom's Strategy, The Stationary Office, Ιούλιος 2006, παράγραφος 65

HM Government. *Pursue, Prevent, Protect, Prepare. The United Kingdom's Strategy for Countering International Terrorism*, The Stationary Office, Μάρτιος 2009, παράγραφος 8.03

The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, UK Cabinet Office, 2011

ΜΕΛΕΤΕΣ / ΔΙΑΤΡΙΒΕΣ

Bhalla R., *Finding Virtue in Strategic Denial and Deception*, (διατριβή κατατεθειμένη στο Graduate School of Arts and Sciences of Georgetown University), ΗΠΑ, 2011

Blanks Kenneth, *An Effectiveness Analysis of the Tactical Employment of Decoys*, μελέτη κατατεθειμένη στο U.S. Army Command and General Staff College, Κάνσας, 1994

Elder James, *The Operational Implications of Deception at the Battle of Kursk* για το School of Advanced Military Studies / U.S. Army Command and General Staff College, Κάνσας, 1989

Hull George, *The Information Revolution and the Environment of Future Conflict*, μονογραφία κατατεθειμένη στο School of Advanced Military Studies / United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1997

Martin Charmaine, *Military Deception Reconsidered* (διατριβή κατατεθειμένη στο Naval Postgraduate School), Monterey / California, 2008

Pistilli D., *Start Making Sense. Managing The Command's Information*, μονογραφία κατατεθειμένη στο School of Advanced Military Studies / United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1995

ΔΙΑΔΙΚΤΥΟ

<http://ethos.bl.uk/Home.do>: βρετανικό αποθετήριο ακαδημαϊκών διατριβών

<http://www.universityworldnews.com/article.php?story=2009011717424810>: Rudner M., "CANADA: Intelligence studies in higher education", *University World News*

<http://www.intelligence.senate.gov/davidlborennationalsecurityact.pdf>: πληροφορίες περί της αμερικανικής εκπαιδευτικής πολιτικής σε σχέση με τα προγράμματα σπουδών στην πληροφόρηση κατά το έτος 1991

http://www.upm.ro/facultati_departamente/stiinte_litere/conferinte/situl_integrare_europeana/Lucrari3/istorie/98_Tanase_Tiberiu.pdf: Tiberiu Tanase, "The study of Intelligence in the Euro-Atlantic area"

<http://www.tandfonline.com/doi/pdf/10.1080/02684527.2014.952932>:
Marrin St., “Improving Intelligence Studies as an Academic Discipline”

<https://babel.hathitrust.org/cgi/pt?id=mdp.39015012152321;view=1up;seq=6>:
Commission on Organization of the Executive Branch of the Government [the Hoover Commission], *Intelligence Activities*

<http://www.liberal.gr/arthro/54589/amyna--diplomatia/2016/pliroforisi-Intelligence-kai-ypsili-stratigiki-i-periptosi-tis-elladas.html>:
Κωνσταντόπουλος Ιωάννης, «Πληροφόρηση (Intelligence) και Υψηλή Στρατηγική: Η περίπτωση της Ελλάδας»

<http://openjurist.org/title-50/us-code/section-401-a/definitions>: 50 USC 401a

<https://www.ncsc.gov/training/resources/nsaact1947.pdf>: *National Security Act of 1947* [(chapter 343; 61 Stat. 496; approved July 26, 1947) As Amended Through P.L. 110-53, Enacted August 3, 2007]

<https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2011/08/Aspin-Brown-Report-on-the-Intelligence-Community-1996.pdf>: Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of US Intelligence* [the "Brown-Aspin Report"], Government Printing Office

<https://www.fbi.gov/about-us/intelligence/defined>: Federal Bureau of Investigation, “Intelligence Defined”

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no2/html/v02i2a09p_0001.htm: Random R., “Intelligence as a Science” στο *Studies in Intelligence*, Volume 2, Number 2

<https://www.fbi.gov/about-us/intelligence/intelligence-cycle>: “Intelligence Cycle”

https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf: *U.S. National Intelligence. An Overview 2013*, ODNI

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/page_46.pdf: “The Traditional Intelligence Cycle”

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm: Orlov Alexander, “The Theory and Practice of Soviet Intelligence”, *Studies in Intelligence*, Volume 7, Number 2

http://c.ymcdn.com/sites/www.cicentre.com/resource/resmgr/reports/ci_101_primer_july_2005.pdf: Reagan Mark, *Introduction to U.S. Counterintelligence. “CI 101--A Primer”*

http://wais.stanford.edu/Governments/gov_ciajamesatleton.htm: “CIA: James Angleton”

<http://fas.org/irp/offdocs/eo12333.htm>: U.S. President Executive Order “United States Intelligence Activities, Executive Order 12333”, *Federal Register* 46, number 59941

<http://www.intelligence.senate.gov/nsaact1947.pdf>: *National Security Act of 1947*

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol13no1/html/v13i1a02p_0001.htm: Wasemiller C. A., “The Anatomy of Counterintelligence” στο *Studies in Intelligence*, Volume 13, Number 1

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a06p_0001.htm: Timm W. Eric, “Countersabotage--a Counterintelligence Function” στο *Studies in Intelligence*, Volume 7, Number 2

<https://fas.org/irp/news/2005/03/ncix030505.pdf>: *The National Counterintelligence Strategy of the United States*: NCIX Speech (CI for the 21st Century Conference)

http://www.bbc.co.uk/history/worldwars/wwtwo/mi5_ww2_01.shtml: West N., “Double Cross - MI5 in World War Two”

<http://fas.org/irp/dni/icd/icd-700.pdf>: ICD 700, *Protection of National Intelligence*, Office of the Director of National Intelligence

<http://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap15-sec401a.pdf>: 50 USC 401a

<http://www.state.gov/m/ds/terrorism/c8653.htm>:
US Department of State, “Counterintelligence Investigations”

http://www.soft-vision.com/ao_vets/pdf/sub_esp_against%20USArmy.pdf: AR 381-12, *Subversion and Espionage Directed Against the US Army*, DoD

http://www.eliamep.gr/wp-content/uploads/2008/07/apostolidies_eyp_gr.pdf:
Αποστολίδης Παύλος, «Οι Υπηρεσίες Πληροφοριών στο Εθνικό Σύστημα Ασφαλείας. Η περίπτωση της ΕΥΠ»

<https://archives.fbi.gov/archives/news/stories/2004/july/szady072004>:
“Focus on Counterintelligence” (συνέντευξη με τον βοηθό διευθυντή του FBI Dave Szady)

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm: “Counterintelligence for National Security” στο *Studies in Intelligence*, Volume 2, Number 4

<http://www.prim.osd.mil/init/dcipcadat.html>: “Department of Defense, Defense Critical Infrastructure Program (DCIP)/ Characterization and Dependency Analysis Tool (CADAT)”

<http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1114-dni-unveils-2014-national-intelligence-strategy?tmpl=component&format=pdf> : *DNI Unveils 2014 National Intelligence Strategy*, ODNI

<https://www.fbi.gov/about/faqs/what-is-the-fbis-foreign-counterintelligence-responsibility>: “What is the FBI’s foreign counterintelligence responsibility?”

<http://www.archives.gov/federal-register/codification/executive-order/12333.html#3.6>: *Executive Order 12333 United States Intelligence Activities*, 4 Δεκεμβρίου 1981, παράγραφοι 1.8, 1.14

<https://www.intelligencecareers.gov/icprotecting.html>: “Protecting America”

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/260780/4779.pdf: *British Security Service Act 1989*, The Stationery Office

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/250868/0114301808.pdf: *National Intelligence Machinery*, The Stationery Office

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf: *National Intelligence Machinery*, Cabinet Office

<http://www.csse.monash.edu.au/courseware/cse468/2006/cornerstones-iw.html>: *Cornerstones of Information Warfare*, Department of the Air Force, Washington, D.C.

<http://www.c4i.org/cornerstones.html>: “Cornerstones of Information warfare”

<https://fas.org/irp/doddir/army/ar380-5.pdf>: AR 380-5, *Department of the Army Information Security Program*, Headquarters, Department of the Army, Washington, D.C.

<http://www.au.af.mil/au/awc/awcgate/ssi/deception.pdf>: Caddell J., *Deception 101-Primer on Deception*

<https://www.hsdl.org/?view&did=7443>: Joint Military Intelligence College, *Intelligence Warning Terminology*

<http://www.e-ir.info/2012/11/08/are-intelligence-failures-inevitable/>: Morgan Trujillo “Are Intelligence Failures Inevitable?”

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art12.html>: CIA, “What Are Cognitive Biases?”

https://www.cia.gov/news-information/speeches-testimony/1995/dci_speech_51195.html: DCI John Deutch, “Remarks at CIA Town Meeting”

http://www.cato.org/pubs/pas/pa-265.html#FOOTNOTE_11: Kober Stanley, “Why Spy? The Uses and Misuses of Intelligence”

<http://www.datapacrat.com/True/INTEL/CSIS/COM46E.HTM>: Porteous Samuel, “Economic Espionage II”, *Commentary*, Number 46

http://www.cato.org/pubs/pas/pa-265.html#FOOTNOTE_11: Kober Stanley, “Why Spy? The Uses and Misuses of Intelligence”

<http://www.iwar.org.uk/ecoespionage/resources/senate/echearingmarch98/torrence.htm>: “Cybercrime, Transnational Crime and Intellectual Property Theft”, (κατάθεση του Larry E. Torrence στη Joint Economic Committee του αμερ. Κογκρέσου στις 24 / 3 / 1998)

http://www.ncsc.gov/publications/reports/fecie_all/FECIE_2005.pdf: *Foreign Economic Collection and Industrial Espionage, 2005*, NCIX

http://www.ncsc.gov/publications/reports/fecie_all/ProtectingKeyAssets_CorporateCI_Guide.pdf: *Protecting Key Assets: A Corporate Counterintelligence Guide*, ONCIX

<http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf>: *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, McAfee, Inc.

https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf: *Unsecured Economies: Protecting Vital Information*, McAfee, Inc.

<http://foreignpolicy.com/2009/10/26/web-of-influence/>: Drezner W. Daniel, Farrell Henry, “Web of Influence”

<https://www.ncsc.gov/training/resources/nsaact1947.pdf>: *National Security Act of 1947*, (Chapter 343; 61 Stat. 496; approved July 26, 1947), [As Amended Through P.L. 110–53, Enacted August 3, 2007]

http://www.lancsresilience.org.uk/Documents/Bcm/Protecting_Against_Terrorism.pdf: Security Service MI5, *Protecting Against Terrorism*

<http://www.dailymail.co.uk/news/article-4265870/Images-Syrian-strike-new-kind-drone-exist.html>: “US forces deploy deadly new drone: Images reveal how Al Qaeda leader was killed with deadly accurate strike -which didn’t even break his car’s windows”, *Mail Online*

<https://www.theguardian.com/world/2017/mar/13/predator-drone-retire-reaper-us-military-obama>: Helmore Edward, “US retires Predator Drones after 15 years that changed ‘the war on terror’”, *The Guardian*

<http://blog.ihs.com/game-of-drones-the-uses-of-uavs-by-militant-groups-in-iraq-and-syria>: “Game of ‘Drones’: the uses of UAVs by militant groups in Iraq and Syria”, *HIS Markit*

<https://www.theguardian.com/commentisfree/2017/mar/17/defeat-terrorists-terrorism>: Searle Nicholas, “To defeat terrorists we have to get inside their minds”, *The Guardian*

[http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU\(2017\)583124_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf): *The European Union’s Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness*, European Parliament, Brussels

[http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Insurgent%20Principles%20and%20Practices/MiniManual%20of%20the%20Urban%20Guerrilla%20%20Carlos%20Marighella%20\(1969\).pdf](http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Insurgent%20Principles%20and%20Practices/MiniManual%20of%20the%20Urban%20Guerrilla%20%20Carlos%20Marighella%20(1969).pdf): Marighella Carlos, *Minimanual of the Urban Guerrilla*

<http://www.latinamericanstudies.org/bayo.htm>: Giroud Alberto, *One Hundred Fifty Questions for a Guerrilla*

<http://www.outpost-of-freedom.com/opf980830a.htm>: Osama bin Laden, *A Declaration of War Against the Americans Occupying the Land of the Two Holy Places: A Message from Osama bin Muhammad bin Laden unto his Muslim brethren all over the world generally, and toward the Muslims of the Arabian Peninsula specifically*

http://www.au.af.mil/au/awc/awcgate/terrorism/alqaida_manual/manualpart1_3.pdf: Al-Qaeda, *Declaration of Jihad against the Country’s Tyrants, Military Series*, (Ninth Lesson, “Security Plan”)

<https://www.washingtonpost.com/archive/politics/2001/12/09/a-terrorists-guide-to-infiltrate-west/2bb6d717-d9a0-4cdf-ba8c-9ab13710eb37/>: Glasser Susan, “A Terrorist’s Guide to Infiltrate West” στο *The Washington Post*

https://fas.org/irp/congress/2002_hr/091902wolfowitz.pdf: Wolfowitz P., “Prepared Testimony of Deputy Secretary of Defense Paul Wolfowitz for the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence: Joint Inquiry Hearing on Counterterrorist Center Customer Perspective”

http://www.au.af.mil/au/awc/awcgate/terrorism/alqaida_manual/manualpart1_2.pdf: Al-Qaeda, *Declaration of Jihad against the Country’s Tyrants, Military Series*, (Fifth Lesson, “Means of Communication and Transportation”)

<http://www.freerepublic.com/focus/news/807903/posts?page=3>: Mownbray Joel, “How They Did It”

http://www.jamestown.org/programs/tm/single/?tx_ttnews%5Btt_news%5D=27713&tx_ttnews%5Bba#.V7suZKIRPZ4: “New online book lays out al-Qaeda’s military strategy”

<https://azelin.files.wordpress.com/2010/08/abu-bakr-naji-the-management-of-savagery-the-most-critical-stage-through-which-the-umma-will-pass.pdf>: Naji Abu, *The Management of Savagery: The Most Critical Stage Through Which the Umma Will Pass*, μετάφραση στην αμερικανική γλώσσα από τον William McCants υπό τη χορηγία του John M. Olin Institute for Strategic Studies / Harvard University

<https://www.theguardian.com/world/2003/dec/13/politics.alqaida>: “Al-Qaeda Plot to Bomb Embassy in Yemen Foiled” στο *World News*

<http://www.scotsman.com/news/world/al-qaeda-plot-to-blow-up-british-embassy-1-1297039>: “Al-Qaeda Plot to Blow Up British Embassy” στο *The Scotsman*

<http://www.abc.net.au/4corners/content/2004/s1132151.htm>: “Testimony: Melanie Brown”, *Four Corners*

<http://nypost.com/2006/02/25/qaeda-claim-we-infiltrated-uae-govt/>: Lathem Niles, “Qaeda Claim: We ‘Infiltrated’ UAE Gov,t”

<https://bsimmons.wordpress.com/2007/02/04/uk-officials-suspect-jihadist-mole-in-ministry-of-defense/>: “UK officials suspect jihadist mole in Ministry of Defence”

<http://www.economist.com/node/16478792>: “War in the fifth domain”, *The Economist*

http://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/infor_war.html: RAND Organization Research Review, *Information Warfare: A Two-Edged Sword*

<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>: “Information Security”

<http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/>: Lee M. Robert, “Cyber Counterintelligence: From Theory to Practice”, *The State of Security*

http://fas.org/irp/world/china/docs/iw_mg_wang.htm: Pufeng Wang, “The challenge of information warfare”

http://zeenews.india.com/news/world/us-china-russia-have-cyber-weapons-mcafee_579965.html: *US, China, Russia have ‘cyber weapons’: McAfee*

<http://blog.executivebiz.com/2010/03/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/>: *What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare*

<http://fas.org/irp/gao/aim96084.htm>: GAO, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84

<http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf>: *Information Operations: The Hard Reality of Soft Power*

https://en.wikisource.org/wiki/US_v_Gary_McKinnon_Indictment: Department of Justice, U.S. District Court for the Eastern District of Virginia, Alexandria Division, Indictment, *United States of America v. Gary McKinnon*

<http://www.dailytech.com/USB+Stick+Led+to+Worst+Cyber+Attack+on+US+Military+Russia+Suspected/article19458.htm>: Mick Jason, “USB Stick Led to Worst Cyber Attack on U.S. Military; Russia Suspected”, *Daily Tech*

<http://www.ft.com/cms/s/0/82343fba-491a-11e0-af8c-00144feab49a.html#axzz3sdXtN2G5>: Menn Joseph, “US probes Anonymous plans for attack on marines”, *FT. com*

<http://www.computerworld.com/article/2559195/security0/guard-against-titan-rain-hackers.html>: Winkler Ira, “Guard against Titan Rain hackers”, *Computerworld*

<http://www.theguardian.com/technology/2010/jan/14/google-hacking-china-cyberwar>: Arthur Charles, “Google the latest victim of Chinese ‘state-sponsored’ cyberwar”, *The Guardian*

<http://content.time.com/time/nation/article/0,8599,1098371,00.html>: Thornburgh Nathan, “Inside the Chinese hack Attack”, *Time*

<http://www.telegraph.co.uk/news/worldnews/wikileaks/8181619/Top-Chinese-officials-ordered-attack-on-Google-Wikileaks-cables-claim.html>: Sawyer Patrick, “Top Chinese officials ordered attack on Google, Wikileaks cables claim”, *The Telegraph*

<http://www.techwatch.co.uk/2011/02/17/cyber-crime-costs-uk-economy-27-billion-per-year/>: Allan Darren, “Cyber-crime costs UK economy £27 billion per year”, *Techwatch*

<http://www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm>: Fact File U.S. Strategic Command Public Affairs, 901 SAC Blvd, Suite 1A1, Offutt AFB NE 68113-6020, *Joint Task Force Computer Network Operations*

<http://www.globalsecurity.org/military/ops/eligible-receiver.htm>: Global Security.org, “Eligible Receiver”

<https://www.ausa.org/SiteCollectionDocuments/ILW%20WebExclusivePubs/Background%20Briefs/bb96.pdf>: *Space, Missile Defense and Computer Network Operations Challenges: Computer Network Operations: A Critical Element of Current and Future Military Operations in Combating the Asymmetrical Threat*

<http://www.economist.com/node/16478792>: “Cyberwar. War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?”, *The Economist*

<https://www.theguardian.com/commentisfree/2011/dec/16/al-shabab-tweets-terrorism-twitter>: Burke Jason, “Al-Shabab’s Tweets Won’t Boost its Cause”

<http://www.pcworld.com/article/109819/article.html>: Evers Joris, “Does Cyberterrorism Pose a True Threat?”, *PC World*

<http://www.computerworld.com/article/2581635/security0/cyberterror-threat-overblown--say-experts.html>:

“Cyberterror threat overblown, say experts”, *Computerworld*

<http://www.usip.org/sites/default/files/sr119.pdf>: Weimann Gabriel, *Special Report-Counterterrorism: How Real is the Threat?*, United States Institute of Peace, Washington, D.C.

<http://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/>: “Is the cyber threat overblown?”, *Foreign Policy*

https://www.ida.liu.se/~johsi32/docs/EISIC2013_Sigholm_Bang.pdf: Sigholm Johan, Bang Martin, “Toward Offensive Cyber Counterintelligence. Adopting a Target-Centric View on Advanced Persistent Threats”, 2013 European Intelligence and Security Informatics Conference

<http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/>:

Lee M. Robert, “Cyber Counterintelligence. From Theory to Practice”

<http://www.gao.gov/new.items/d08588.pdf>: U.S. Government Accountability Office, “Cyber Analysis and Warning. DHS Faces Challenges in Establishing a Comprehensive National Capability” στο *Cybersecurity, Cyberanalysis and Warning* στο *Cybersecurity, Cyberanalysis and Warning*

http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf: “Public Law 107-296, 107th Congress”

<https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf>: ιστοσελίδα του White House

https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf: U.S. President, *The National Strategy to Secure Cyberspace*

<http://www.gao.gov/new.items/d05434.pdf>: U.S. GAO (2005a), *Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*

http://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf: *The Homeland Security Act of 2002*

<http://www.dhs.gov/federal-information-security-management-act-fisma>: *The Federal Information Security Modernization Act*

https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf: Executive Office of the President of The U.S., *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*

<https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>: Executive Office of the President of The U.S., *The Comprehensive National Cybersecurity Initiative*

<http://acqnotes.com/acqnote/careerfields/cyberspace>:
“Information Technology. Cyberspace”

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, European Commission

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf: *Convention on Cybercrime*, Council of Europe, European Treaty Series

<http://fas.org/irp/offdocs/pdd/pdd-63.htm>: *Presidential Decision Directive / NSC-63*, The White House

<https://www.hsdl.org/?abstract&did=441950>: “Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection”

https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf: *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*

<http://www.bizjournals.com/dallas/stories/2003/09/15/daily21.html>: “Sprint Inks Outsourcing Pacts with EDS, IBM”, *Dallas Business Journal*

<http://www.tatvasoft.com/outsourcing/2005/05/programming-jobs-are-heading-overseas.html>: “Programming Jobs are Heading Overseas by the Thousands. Is there a Way for the U.S. to Stay on Top?”

<http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf>: Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, DoD, Washington, D.C.

<http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-050.pdf>: *Strategy for Operating in Cyberspace*, DoD, Washington, D.C.

<https://ccdcdoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf>: *Defending the Networks. The NATO Policy on Cyber Defense*, NATO

http://www.nato.int/cps/en/natohq/topics_78170.htm:
North Atlantic Treaty Organization, “Cyber security”

http://www.nato.int/cps/en/natolive/news_124868.htm?selectedLocale=en: North Atlantic Treaty Organization, “Experts put to the test during NATO’s largest annual cyber defence exercise”

<http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html>: Abrial St éphane, “NATO Builds its Cyberdefenses”, *The New York Times*

<https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf>: “Cyber Crime - A Growing Challenge for Governments” στο *Issues Monitor*

http://www.fincen.gov/about_fincen/wwd/faqs.html#money: ιστοσελίδα του United States Department of the Treasury

<http://www.fincen.gov/>: ιστοσελίδα του United States Department of the Treasury
<https://www.ncjrs.gov/pdffiles1/Photocopy/134434NCJRS.pdf>: Carter David, *Law Enforcement Intelligence Operations*

<http://www.9-11commission.gov/report/911Report.pdf>: *The 9 / 11 Commission Report*

<http://fas.org/irp/agency/doj/fbi/websterreport.html>: Commission for Review of FBI Security Programs, *A Review of FBI Security Programs*, U.S. Department of Justice

<https://fas.org/sgp/crs/intel/RL34279.pdf>: Bazan B. Elizabeth, CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*

http://www.au.af.mil/au/awl/wastage/do/Nat_cram_Intel_share_plan2005.puff: *The National Criminal Intelligence Sharing Plan*, U.S. Department of Justice

<http://www.usembassy-israel.org.il/publish/peace/archives/2002/february/021301.html>:
Transcript: Defense Department Briefing, February 12, 2002

<http://users.clas.ufl.edu/zselden/Course%20Readings/Jones.pdf>: Jones Garret, “It’s a Cultural Thing: Thoughts on a Troubled CIA”

http://www.bbc.co.uk/radio4/history/spies_cia.shtml: BBC Radio 4, *Spies R Us*

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record.html>: MacEachin D., “Predicting the Soviet invasion of Afghanistan: the intelligence community’s record”

<https://www.cia.gov/library/kent-center-occasional-papers/vol2no2.htm>: Davis J., *Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence*

<https://www.cia.gov/library/readingroom/docs/CIA-RDP86B00269R001100100010-7.pdf>: “Report on a Study of Intelligence Judgments”

<http://www.nytimes.com/1998/06/03/world/cia-study-details-failures-scouring-of-system-is-urged.html>: Weiner Tim, “CIA Study Details Failures; Scouring of System Is Urged”

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/vietnam.html>: Ford P. H., “Why CIA Analysts Were So Doubtful About Vietnam”, *Studies in Intelligence*, 1997

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/ford.htm>: Ford P. H., “Thoughts Engendered by Robert McNamara’s In Retrospect”, *Studies in Intelligence*, 1996

<http://www.nytimes.com/2001/01/20/us/political-memo-keeping-cia-chief-puts-pressure-on-relationship.html>: Risen James, “Keeping CIA. Chief Puts Pressure on Relationship”

<http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060200905.html>: Pincus Walter, “Before War, CIA Warned on Negative Outcomes”

<http://www.politico.com/story/2009/05/panetta-warns-against-politicization-022676>: Gerstein Josh, “Panetta Warns Against Politicization”

<https://www.theguardian.com/uk/2009/nov/24/iraq-war-chilcot-inquiry>: Norton-Taylor Richard, “Iraq war inquiry: Britain heard US drumbeat for invasion before 9/11”

<https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/volume-36-number-1/pdf/v36i1a01p.pdf>: Gates R., “Guarding Against Politicization”

<https://www.foreignaffairs.com/articles/iraq/2006-03-01/intelligence-policy-and-war-iraq>: Pillar Paul, “Intelligence, Policy, and the War in Iraq”

<http://www.fpri.org/2017/02/politicization-intelligence-community-extremely-dangerous/>: Bakos Nada, “Politicization of the Intelligence Community is Extremely Dangerous”

<https://fas.org/sgp/library/pccip.pdf>: The Report of the President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructure*, Οκτώβριος 1997

<http://www.unz.org/Pub/WashingtonMonthly-1970jul-00068>: McGarvey P., “DIA: Intelligence to please”

<http://fas.org/irp/offdocs/pdd/pdd-63.pdf>: Presidential Decision Directive / NSC-63, *Critical Infrastructure Protection*, Μάιος 1998

http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/107.pdf:
Alston Anthony, et al., *Implementing Edge Organizations: Exploiting Complexity*, Paper Number #107, 10th International Command and Control Research & Technology Symposium, McLean, Virginia, Ιούνιος 2005

<http://www.e-ir.info/2013/11/08/importance-of-intelligence-to-international-security/>:
Kupcikas Karolis, “The Importance of Intelligence to International Security”

<http://www.au.af.mil/au/awc/csat/2025/volume3/vol3ch03.pdf>: Stein George,
Information Attack: Information Warfare in 2025

<http://www.antiwar.com/orig/shaw.php?articleid=3054>: Shaw Martin, *Risk Transfer Militarism and Legitimacy of War after Iraq*, 2004

<http://www.naftemporiki.gr/story/764635/gia-themata-asfaleias-sunedriase-to-symboulio-pliroforion-tis-eyyp>: «Για θέματα ασφαλείας συνεδρίασε το Συμβούλιο Πληροφοριών της ΕΥΠ», *Naftemporiki.gr*, 11 Φεβρουαρίου 2014

<http://policenet.gr/article/η-ιστορική-διαδρομή-της-εθνικής-υπηρεσίας-πληροφοριών>:
«Πώς έφτασε η ΕΥΠ στη σημερινή της μορφή. Η ιστορική διαδρομή της Εθνικής Υπηρεσίας Πληροφοριών»

<http://policenet.gr/article/η-ιστορική-διαδρομή-της-εθνικής-υπηρεσίας-πληροφοριών>:
«Η ιστορική διαδρομή της Εθνικής Υπηρεσίας Πληροφοριών»

<http://www.nis.gr/portal/page/portal/NIS/History/Diktatoria/>: ΕΥΠ, «Ιστορικό»

<https://www.newsbeast.gr/greece/arthro/233219/pos-ginetai-kapoios-praktoras-stin-eyyp>: «Πώς γίνεται κάποιος πράκτορας στην ΕΥΠ;»

http://www.onalert.gr/stories/Ellhnes_se_kindynooi_Ellhnikes_EDhtan_panta_ekeiDy_o_istorikes_epixeirhseis/3473: «Έλληνες σε κίνδυνο: Οι ελληνικές ένοπλες δυνάμεις ήταν πάντα εκεί. Δύο ιστορικές επιχειρήσεις»

<http://www.tovima.gr/relatedarticles/article/?aid=167438>: «Ποιος κάρφωσε τον Στίβεν Λάλας»

<http://www.in.gr/2005/11/13/greece/i-krisi-twn-imiwn-kai-o-rol-os-tis-eyyp-tis-cia-kai-tis-kybernis/>: «Η κρίση των Ιμίων και ο ρόλος της ΕΥΠ, της CIA και της κυβέρνησης»

<http://www.tovima.gr/politics/article/?aid=169407>: «Τι συνέβη τη νύχτα των Ιμίων» του Αλέξη Παπαχελά

<http://e-amyna.com/ίμια-1996-το-λεπτομέρες-χρονικό-της-κρίσης/>: «Ιμια 1996: το λεπτομέρες χρονικό της κρίσης»

<http://www.onalert.gr/stories/h-krish-imiwn-ti-mas-dida3e-ti-exoume-pra3ei/62625>: «Η κρίση των Ιμίων: Τι μας δίδαξε και τι έχουμε πράξει» του αντιστρατήγου ε. α. Λάμπρου Τζούμη

<https://www.youtube.com/watch?v=9AggJ3miNrM>: Συνέντευξη του ταγματάρχη ε. α. Σάββα Καλεντερίδη στο 98,4 RADIO

<https://www.protothema.gr/stories/article/618489/upothesi-otsalan-to-thriller-tis-apagogis-pou-arhise-stin-athina-kai-teleiose-sto-imrali/>: «Υπόθεση Οτσαλάν: Το θρίλερ της απαγωγής που άρχισε στην Αθήνα και τέλειωσε στο Ίμραλι» του Διονύση Θανάσουλα

<http://www.tovima.gr/politics/article/?aid=108257>: «Το πραξικόπημα της ΕΥΠ. Το άγνωστο παρασκήνιο της υπόθεσης Οτσαλάν» του Νίκου Μαράκη

<http://www.news247.gr/politiki/ypoklopes-kata-karamanli-to-schedio-pythia-i-vodafone-oi-rosoi-kai-i-asimenia-drachmi.6461776.html>: «Υποκλοπές κατά Καραμανλή: Το Σχέδιο Πυθία, η Vodafone, οι Ρώσοι και η ασημένια δραχμή» του Χρήστου Δεμέτη

<http://www.tovima.gr/books-ideas/article/?aid=186449>: «Οι τρύπες των μυστικών υπηρεσιών» του Θάνου Ντόκου

<http://www.rieas.gr/researchareas/homeland-security/2211-does-greece-need-a-department-of-homeland-security>: “Does Greece Need a Department of Homeland Security?” του Ιωάννη Νομικού

<https://www.newsbeast.gr/weekend/arthro/788812/ta-fanera-erga-kai-oi-skoteines-imeres-tis-eup>: «Τα φανερά έργα και οι σκοτεινές μέρες ημέρες της ΕΥΠ»

<http://www.rizopoulospost.com/h-ne-a-yphresia-plhroforiwn/>: «Η νέα Υπηρεσία Πληροφοριών» του Γιάννη Νικήτα

<http://www.onalert.gr/stories/stratiotiki-ypiresia-pliroforion-erxetai-gia-na-kalyfthei-to-keno>: «Στρατιωτική Υπηρεσία Πληροφοριών: Έρχονται χακί κατάσκοποι να καλύψουν το κενό της ΕΥΠ»

<https://www.militaire.gr/στρατιωτική-υπηρεσία-πληροφοριών-αλ/>: «Στρατιωτική Υπηρεσία Πληροφοριών, αλλά με τι στελέχη;» του Πάρι Καρβουνόπουλου

<https://www.militaire.gr/υπηρεσία-στρατιωτικών-πληροφοριών/>: «Σώμα Στρατιωτικών Πληροφοριών: Η εισήγηση του ΓΕΕΘΑ και γιατί είναι επείγον να ‘περάσει’»

<http://e-amyna.com/επιτακτική-ανάγκη-η-συγκρότηση-σώματ/>: «Επιτακτική ανάγκη η συγκρότηση Σώματος Στρατιωτικών Πληροφοριών»

<https://nomoi.info/%CE%A6%CE%95%CE%9A-%CE%91-180-1999-%CF%83%CE%B5%CE%BB-19.html>: Νόμος 2738/1999, ΦΕΚ Α 180, σ. 19

<https://www.hellenicparliament.gr/Koinovouleftikes-Epitropes/CommitteeDetailView?CommitteeId=2b188390-2f24-4d95-b867-912d485fa8cf>: «Κοινοβουλευτικές Επιτροπές: Ειδική Μόνιμη Επιτροπή Θεσμών και Διαφάνειας»

<https://akrivopoulouchristina.wordpress.com/2010/03/02/ανεξάρτητες-αρχές-χαρακτηριστικά-κα/>: «Οι Ανεξάρτητες Αρχές»

<http://www.idis.gr/?p=3036>: «Κοινοβουλευτική Επίβλεψη Υπηρεσιών Πληροφοριών στις Σύγχρονες Δημοκρατίες και η Ευρωπαϊκή Εμπειρία» του Ιωάννη Κωνσταντόπουλου