



ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΨΥΧΟΛΟΓΙΑΣ – ΤΟΜΕΑΣ ΚΟΙΝΩΝΙΚΗΣ ΘΕΩΡΙΑΣ & ΕΡΕΥΝΑΣ
ΚΕΝΤΡΟ ΨΥΧΟ-ΚΟΙΝΩΝΙΟΛΟΓΙΚΗΣ ΕΡΕΥΝΑΣ ΤΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΤΩΝ ΔΥΝΗΤΙΚΩΝ ΚΟΙΝΟΤΗΤΩΝ – ΕΡΕΥΝΗΤΙΚΟ ΚΕΝΤΡΟ «ΩΜΕΓΑ».

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
**ΔΥΝΗΤΙΚΕΣ ΚΟΙΝΟΤΗΤΕΣ: ΚΟΙΝΩΝΙΟ-ΨΥΧΟΛΟΓΙΚΕΣ
ΠΡΟΣΕΓΓΙΣΕΙΣ ΚΑΙ ΤΕΧΝΙΚΕΣ ΕΦΑΡΜΟΓΕΣ**

ΣΕ ΣΥΜΠΡΑΞΗ ΜΕ ΤΟ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ
ΤΟΥ ΤΕΙ ΜΕΣΟΛΟΓΓΙΟΥ

ΚΑΙ ΣΕ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟ
ΕΡΕΥΝΗΤΙΚΟ ΑΚΑΔΗΜΑΪΚΟ ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ



ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**ΨΥΧΟ-ΚΟΙΝΩΝΙΟΛΟΓΙΑ ΤΗΣ ΚΥΡΙΑΡΧΙΑΣ:
ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ**

ΣΠΗΛΙΩΤΟΠΟΥΛΟΣ ΔΗΜΗΤΡΙΟΣ
ΑΜ: 6305Μ013

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

1. Αναπλ. Καθηγ. Κ. Κοσκινάς, Επιβλέπων
2. Αναπλ. Καθηγ. Ε. Κούρτη, Μέλος
3. Δρ. Α. Ξενάκης, Μέλος

ΙΟΥΝΙΟΣ 2008

ΠΕΡΙΛΗΨΗ

Ο σκοπός αυτής της εργασίας είναι να παρουσιάσει μια χαρτογράφηση (mapping) του φαινομένου του Κυβερνοπολέμου. Επίσης, θα προτείνει μια κατηγοριοποίηση των μορφών του νέου αυτού είδους πολέμου, σύμφωνα με το στόχο κάθε επίθεσης. Έτσι, θα χρησιμοποιήσουμε -για λόγους μεθοδολογίας- ένα οργανωτικό μοντέλο, το οποίο αναδεικνύεται, από τη μετάβαση στη Δυνητική Οργάνωση. Η τεκμηρίωση που θα χρησιμοποιηθεί θα αποτελεί μια σύνθεση της θεώρησης των επιστημών της Ψυχολογίας, της Κοινωνιολογίας και κυρίως του Διαδικτύου, για τη σχέση της ανθρώπινης συμπεριφοράς με το στοιχείο της Κυριαρχίας. Αξιοσημείωτο είναι το συμπέρασμα ότι ο Κυβερνοχώρος αναδύθηκε ως αποτέλεσμα του ανταγωνισμού ισχύος της ψυχροπολεμικής περιόδου, στις ΗΠΑ. Στο παρελθόν οι απειλές από το εξωτερικό, μπορούσαν να αντιμετωπιστούν στο εξωτερικό. Πλέον, τα γεωγραφικά όρια δεν διασφαλίζουν τη διατήρηση της απειλής έξω από τη χώρα.

Τα πιο «δεδεαστικά» χαρακτηριστικά της απόπειρας για εγκληματική ενέργεια στον κυβερνοχώρο είναι η αφανής ταυτότητα, το ελάχιστο κόστος και η ταχύτητα, στοιχεία που προσδίδουν πολύ χαμηλό ρίσκο σε όποια προσπάθεια. Κάθε συντονισμένη ενέργεια, η οποία αποσκοπεί να πλήξει την ισχύ ενός κράτους και για πεδίο μάχης χρησιμοποιεί τον κυβερνοχώρο, καλείται απειλή κυβερνοπολέμου. Άρα, από τη φύση του ο κυβερνοπόλεμος έχει μια τεράστια διαφορά από τον παραδοσιακό πόλεμο. Δεν υπακούει σε χρονοχωρικούς περιορισμούς, δηλαδή, δεν έχει επίσημη αρχή και τέλος, και δεν λαμβάνει χώρα σε συγκεκριμένη εδαφική έκταση. Ιστορικά, τα πρώτα σημάδια του διακρίνονται με την εμφάνιση του κυβερνοχώρου, στον οποίο μάλλον κινείται παράλληλα, σαν να είναι η σκιά του!

Σε αυτό το πλαίσιο, οι βιβλιογραφικές αναφορές προέρχονται από τρεις επιστημονικές περιοχές. Η πρώτη περιέχει συγγράμματα από τη νέα επιστήμη του διαδικτύου, η οποία επιχειρεί να καλύψει ένα μεγάλο κενό στο χώρο της ανθρώπινης γνώσης, ερμηνεύοντας τα διάφορα φαινόμενα – αποτέλεσμα που προκύπτουν από τις ΤΠΕ. Η δεύτερη περιλαμβάνει βιβλία από το χώρο των κοινωνικών επιστημών, επικεντρώνεται δε, στο πεδίο εκείνο των κοινωνιο-ψυχολογικών προσεγγίσεων για την επιρροή των Μέσων Μαζικής Ενημέρωσης (ΜΜΕ). Τέλος, κρίθηκε απαραίτητη η εμβάθυνση σε κάποια συγγράμματα ειδικών κλάδων της Πολιτικής Επιστήμης, όπως η Πολιτική Επικοινωνία, οι Διεθνείς Σχέσεις, η Γεωπολιτική ανάλυση και οι Στρατηγικές σπουδές.

ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ

Κυβερνοπόλεμος (Cyber warfare) / Πληροφοριακός Πόλεμος (Info War)

Ηλεκτρονικός και Δικτυακός Πόλεμος (Electronic and Net War)

Ψυχο-πόλεμος (Psycho War) / Προπαγάνδα (Propaganda)

Ψυχολογικές Επιχειρήσεις (Psychological Operations -PSYOP)

Στοχοθετημένη Πληροφόρηση (Targeted Information)

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ	ΚΕΦΑΛΑΙΟ	Τ Ι Τ Λ Ο Σ	ΣΕΛΙΔΑ
		Περίληψη	2
		Περιεχόμενα	3
	1	Εισαγωγή	5
	1.1	Ο ρόλος της τεχνολογίας στη σημερινή πραγματικότητα	5
	1.2	Ο Κυβερνοχώρος ως αποτέλεσμα του ανταγωνισμού Ισχύος	7
	1.3	Σκοπός, Βιβλιογραφική Ανασκόπηση και Μέθοδος	11
A'		Η ΘΕΩΡΙΑ	13
	2	Δυνητική Οργάνωση	14
	2.1	Το Νεότερικό και Δυνητικό Οργανωτικό Μοντέλο του Κράτους	14
	2.2	Τα Μέσα στην Παραδοσιακή Οργάνωση	16
	2.3	Τα Μέσα στην Δυνητική Οργάνωση	18
	2.4	Ηγεσία και Δυνητικές Κοινότητες	20
	3	Οργανωτικό Μοντέλο	22
	3.1	Οργανωτικό Μοντέλο και Μεθοδολογία	22
	3.2	Η εφαρμογή του Οργανωτικού Μοντέλου στο φαινόμενο της «Παγκοσμιοποίησης»	25
	4	Ορισμοί	27
	4.1	Οι θεμελιώδεις έννοιες	27
	4.2	Όροι Κοινωνικών επιστημών και της επιστήμης του Διαδικτύου	30
	4.3	Βασικές έννοιες Κυβερνοπόλεμου	32
	4.3.1	Πόλεμος των Πληροφοριών (War of Intelligences)	32
	4.3.2	Κυβερνοπόλεμος	32
	4.3.3	Πληροφοριακός Πόλεμος (Info war)	33
	4.3.4	Δικτυακός Πόλεμος (Net War)	34
	4.3.5	Ψυχο-πόλεμος (Psycho War) – Ψυχολογικές Επιχειρήσεις (Psychological Operations-PSYOP) – Στοχοθετημένη Πληροφόρηση (Targeted Information)	34
B'		Η ΠΡΑΞΗ	37
	5	Πληροφοριακός Πόλεμος	38
	5.1	Πόλεμος στο πρώτο Οργανωτικό Επίπεδο (Κυριαρχία στην Ηγεσία)	38
	5.2	Η αξιοποίηση των ΤΠΕ από τον Στρατιωτικό	42

		τομέα (C4ISR)	
	5.3	Παράδειγμα: Ανάλυση του Μοντέλου των ΗΠΑ	45
	5.3.1	Θεωρητικό υπόβαθρο	45
	6	Ηλεκτρονικός και Δικτυακός Πόλεμος (Electronic and Net War)	49
	6.1	Πόλεμος στο δεύτερο Οργανωτικό Επίπεδο (Κυριαρχία στα Μέσα)	49
	6.2	Μέθοδοι Κυβερνο-επίθεσης και Κυβερνο-άμυνας	51
	6.3	Διαστημική Τεχνολογία	53
	6.4	Κρυπτολογία (Κρυπτογραφία και Κρυπτανάλυση)	55
	7	Ψυχο-πόλεμος (Psycho War)	57
	7.1	Πόλεμος στο τρίτο Οργανωτικό Επίπεδο (Κυριαρχία στον Πληθυσμό)	57
	7.2	Ψυχολογικές Επιχειρήσεις (Psychological Operations-PSYOP) – Στοχοθετημένη Πληροφόρηση (Targeted Information)	64
	8	Μελέτη Περίπτωσης (Case Study) Α': Κυβερνοπόλεμος στις ΗΠΑ: Αντιμετώπιση	68
	8.1	Έκθεση στο Κογκρέσο για τον Κυβερνοπόλεμο	68
	8.2	Το ιστορικό των πρώτων κυβερνο-χτυπημάτων	71
	8.3	Κυβερνητικές Θέσεις και Έργα	73
	8.3.1	Το οργανόγραμμα	75
	8.3.2	Η Εθνική Στρατηγική για την Ασφάλεια του Κυβερνοχώρου	77
	9	Μελέτη Περίπτωσης (Case Study) Β': Ψυχο-Κοινωνιολογία της Κυριαρχίας στην Ελλάδα	79
	10.	<u>Επίλογος</u> : Η φύση του κυβερνο-εγκλήματος	84
Γ		ΠΑΡΑΡΤΗΜΑΤΑ	86
		Παράρτημα α: Η συλλογή πληροφοριών από Μη επανδρωμένα Αεροσκάφη (UAV)	87
		Παράρτημα β: Κατάλογος Κυβερνο-χτυπημάτων παγκοσμίως	88
		Παράρτημα γ: Κατάλογος Κυβερνο-χτυπημάτων στην Ελλάδα	92
		Παράρτημα δ: Αποκαλύψεις περί της Προπαγάνδας στο Διαδίκτυο	93
		Παράρτημα ε: Συζήτηση στο ελληνικό Κοινοβούλιο (Ιαν 2008)	96
		ΒΙΒΛΙΟΓΡΑΦΙΑ	99

Κεφάλαιο 1. Εισαγωγή

1.1 Ο ρόλος της τεχνολογίας στη σημερινή πραγματικότητα

Αποτελεί κοινή θέση ότι ο ταχύς ρυθμός προόδου των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ) οδήγησε την «παγκόσμια κοινότητα» σε ένα μεταβατικό στάδιο. Σε φιλοσοφικό επίπεδο, συνειδητοποιούμε ότι βρισκόμαστε σε οριακό σημείο. Κυρίως, όταν αναλογιστούμε την ανάγκη διανοητικής υπέρβασης που απαιτείται για να κατανοήσουμε τις νέες διαστάσεις, με τις οποίες προσλαμβάνει η αντίληψη μας τις έννοιες του Χώρου και του Χρόνου. Εδώ ξεκινάει η αποστολή της επιστημονικής σκέψης. Η παραδοχή της ανεπάρκειας των παλαιών διαχωρισμών σε θετικές και κοινωνικές επιστήμες ή «μάκρο και μικρο» προσεγγίσεις, επέβαλε μια μεταστροφή προς τη θεώρηση μιας νέας συνεργασίας. Το αποτέλεσμα θα κριθεί από το αν οι θέσεις του ενός κλάδου δεν αρκούν στις αντιθέσεις του άλλου. Πέρα της θέσης και αντίθεσης, οφείλουμε να κατανοήσουμε πως η ιστορία διδάσκει ότι κάθε καινοτομία υπήρξε αποτέλεσμα της σύνθεσης.

Ειδικότερα, η «μακρο-εκδοχή» μελετούσε έναν κόσμο διαιρεμένο σε αυτεξούσια κράτη. Αρχικά, κύρια αιτία πολέμου ήταν ο σεβασμός τού ζωτικού χώρου. Με άλλα λόγια, η έκταση που ανήκε στην επικράτεια καθενός, ταυτιζόταν με την ύπαρξη του. Κατόπιν, στην ιεράρχηση των προτεραιοτήτων τέθηκε η διασφάλιση των οικονομικών – ενεργειακών πόρων. Στις ημέρες μας, κάποιιοι προέβλεψαν ότι τα επόμενα αίτια σύγκρουσης θα εντοπίζονται στις πολιτισμικές διαφορές (Huntington, 1998). Ανεξάρτητα του βαθμού επαλήθευσης, είναι προφανής η αιτία. Η εξουσία ανέκαθεν μεριμνούσε για την εύρεση τρόπων ελέγχου της ανθρώπινης συμπεριφοράς. Σε αυτή τη φάση αυτό θα επιτευχθεί μέσω της πολιτισμικής ομογενοποίησης. Η προβολή κοινών προτύπων για όλους (παράδειγμα μέσω της μονομερούς τεχνολογικής εκπαίδευσης) δημιουργεί στερεοτυπικές, και άρα ευκολότερα προβλέψιμες, συμπεριφορές. [ΣΥΜΠΕΡΑΣΜΑ Α']

Εξετάζοντας τη «μικρο-εκδοχή», διακρίνουμε καταρχάς, ότι το νεότερο εγχείρημα κατέληξε σε έναν έντονο ατομικισμό στην κοινωνία, ο οποίος κατασκεύασε συναινετικά άτομα-δέκτες (Chomsky, 1994). Δηλαδή ανθρώπους με πρόβλημα εκδήλωσης τού λόγου, ο οποίος έχει μπλοκαριστεί στο διανοητικό ή θυμικό πεδίο. Αυτά τα άτομα επαφίενται να παρακολουθούν την καθημερινότητα (σε σχέση με το πρώτο συμπέρασμα, θα λέγαμε ότι αποκτούν το νέο τους πολιτισμό), μαθαίνοντας από τις πληροφορίες που έχουν σχεδιαστεί από ιθύνοντες των ΜΜΕ και δη, σε όσα από αυτά μπορούν να έχουν πρόσβαση. Έτσι, η

συμπεριφορά τους, μεταφορικά θα λέγαμε, ότι είναι θύμα των συμπεριφοριστών. Διότι είναι μάλλον αποτέλεσμα αντίδρασης στα εξωτερικά ερεθίσματα, παρά δράσης που παράγει η δική τους βούληση. [ΣΥΜΠΕΡΑΣΜΑ Β']

Αναζητώντας έναν τόπο σύνθεσης των παραπάνω συμπερασμάτων, διακρίνουμε ότι το νέο οικοδόμημα του πλανήτη δομείται με έναν ενιαίο οργανωτικό τύπο. Οι αποκλίνουσες γνώμες είναι αδύνατον να διατυπωθούν συγκροτημένα, συντονισμένα και εν τέλει, χρίζει μελέτης πόσο επίσημα... Ιδιαίτερα σήμερα, που εμφανίζονται απειλές συλλογικής ευθύνης, όπως η μόλυνση του περιβάλλοντος και η ανεπάρκεια της καθαρότητας του αέρα και των πηγών ύδατος, η ανάγκη μιας οικουμενικής προσπάθειας αυξάνεται' αλλά και παράλληλα αιτιολογεί (ή δικαιολογεί;) την ύπαρξη μιας παγκόσμιας κυβέρνησης, η οποία θα μεριμνήσει για όλα αυτά. Σε αυτό το πλαίσιο, όσοι διαφωνούν, έχουν βρει τρόπους να συγκροτήσουν, να συντονίσουν και να εκφράσουν (μάλλον ανεπίσημα) την αντίδραση τους. Αυτοί οι τρόποι βρήκαν διέξοδο σε έναν καινούριο χώρο, τον Κυβερνοχώρο. Από τη μια πλευρά, ήταν αποτέλεσμα των νέων ΤΠΕ. Από την άλλη όμως πλευρά -όπως θα δείξουμε- ήταν αποτέλεσμα της ανθρώπινης συνεχούς επιζήτησης της Κυριαρχίας.

Η υπεράσπιση ή διεύρυνση της Κυριαρχίας μέσω του Κυβερνοπολέμου είναι ο πυρήνας αυτής της έρευνας. Θα μελετηθεί σε επίπεδο ατόμου. Πόσο, για παράδειγμα, μπορεί να αυτορυθμίσει τη συμπεριφορά του στις συνθήκες συγκινησιακής φόρτισης και διανοητικής σύγχυσης, που δημιουργεί ο τεράστιος όγκος και η υψηλή ταχύτητα διακίνησης των πληροφοριών στην εποχή μας (Taylor, 2004). Σε επίπεδο κοινωνίας, αν η χαλάρωση των κανόνων συμπεριφοράς, που διαφαίνονται στη δυνητική κοινωνία, χαλαρώνουν και τις σχέσεις εξουσίας ή τις διαιωνίζουν θέτοντας τις σε ένα νέο πλαίσιο.

1.2 Ο Κυβερνοχώρος ως αποτέλεσμα του ανταγωνισμού Ισχύος

Τα περισσότερα επιστημονικά επιτεύγματα στην ιστορία της ανθρωπότητας, εφαρμόζονταν για πρώτη φορά (έστω και πιλοτικά) στον στρατό. Το ίδιο συνέβη και με την τεχνολογία, η οποία αποτελεί την «υλική υπόσταση» του κυβερνοχώρου, το διαδίκτυο. Η δημιουργία του έχει τις ρίζες της σε ένα ερευνητικό τμήμα του Υπουργείου Αμύνης των ΗΠΑ (DARPA - Defense Advanced Projects Research Agency). Εκεί, στις συνθήκες του ψυχρού πολέμου, με στόχο την αμυντική προετοιμασία της χώρας από την πυρηνική απειλή, κατασκευάστηκε ένα δίκτυο Ηλεκτρονικών Υπολογιστών (Η/Υ). Με αυτόν τον τρόπο προσπάθησαν να δημιουργήσουν έναν απρόσβλητο τρόπο επικοινωνίας και διακίνησης των πληροφοριών, σε ενδεχόμενο πόλεμο. Αργότερα, την δεκαετία του 1980, το σύστημα εξελίχθηκε και εξαπλώθηκε με την εμφάνιση δικτύων υπολογιστών που χρηματοδοτήθηκαν από τις πολιτείες, οδηγώντας στο Διαδίκτυο (Internet) και από εκεί στη μελέτη του κυβερνοχώρου (cyberspace), μέσα από τον οποίο αναδύθηκε ο κυβερνοπόλεμος (cyberwarfare).

Ο λόγος που οι κυβερνήσεις προσπαθούν να εκμεταλλευτούν οποιαδήποτε σύγχρονη τεχνολογία, είναι επειδή η τεχνολογική πρωτοπορία εξασφαλίζει ένα μεγάλο συγκριτικό πλεονέκτημα στον αέναο ανταγωνισμό για Κυριαρχία. Στο λεξικό μπορούμε να βρούμε τη διττή έννοια αυτού του όρου. Η πρώτη αφορά στη δυνατότητα ανεξαρτησίας και αυτοδιάθεσης ενός υποκειμένου. Η δεύτερη έννοια, υπονοεί την επιβολή της θέλησης ενός υποκειμένου σε ένα άλλο (Τεγόπουλος και Φυτράκης, 1995).

Η κοινωνιολογική όψη της προσέγγισης του όρου ανάγεται σε έναν από τους κλασικούς της επιστήμης, τον Μαξ Βέμπερ, ο οποίος χρησιμοποιούσε παράλληλα και τον όρο «Δύναμη» με την ίδια έννοια. Επίσης, θα μπορούσαμε να αναφέρουμε και έναν πιο σύγχρονο στοχαστή των κοινωνικών σχέσεων, το γάλλο Πιέρ Μπουρντιέ (P. Bourdieu)¹.

1. Η κοινωνιολογία του Πιέρ Μπουρντιέ θέτει ως κύριο στόχο της την αποκάλυψη και την ανάλυση των μηχανισμών κυριαρχίας που υπάρχουν μέσα στην κοινωνία. Η αποκάλυψη αυτή λειτουργεί ταυτόχρονα και ως "καταγγελία" των σχέσεων κυριαρχίας, προσδίδοντας έτσι στην κοινωνιολογική έρευνα μια άμεσα πολιτική διάσταση. Ο Μπουρντιέ καταδεικνύει ότι οι κοινωνικές σχέσεις στηρίζονται σε μια άνιση κατανομή όχι μόνο της οικονομικής δύναμης αλλά και των πολιτικών και των συμβολικών εξουσιών. Με την έννοια της κυριαρχίας ο Μπουρντιέ θέλει να φωτίσει την ίδια την ουσία των κοινωνικών σχέσεων που κρύβουν πάντοτε ασυμμετρίες και ανισότητες. Βρίσκουμε την κυριαρχία σε όλα τα πεδία της κοινωνικής ζωής, σε όλα τα επίπεδα, ακόμη και στις πιο συνηθισμένες περιπτώσεις της καθημερινότητας. Η κυριαρχία δεν βασίζεται πάντοτε στην ωμή βία. Στις περισσότερες περιπτώσεις, στηρίζεται στη συγκατάθεση των ιδίων των κυριαρχούμενων (<http://www.papaki.panteion.gr/teuxos9/bourdieu2.htm>, 2008).

Η ψυχολογική όψη της προσέγγισης σχετίζεται με τη δυνατότητα του ατόμου να αυτό-ρυθμίζει την συμπεριφορά του, ως αποτέλεσμα της παρακολούθησης και του ελέγχου των μεταγνωστικών διεργασιών (Ευκλείδη, 2005). Θα εξετάσουμε πώς αυτές οι δύο προσεγγίσεις λειτουργούν μέσα στα πλαίσια του κυβερνοπολέμου. Βεβαίως, εδώ αναδεικνύεται και η πολιτική όψη. Οι ηγετικές ομάδες συλλογικών φορέων, του σύγχρονου κράτους ή των αυτοκρατοριών του παρελθόντος, διατείνονταν πάντα, ότι ο σκοπός της αποστολής τους ήταν η προστασία των συμφερόντων του λαού. Άλλοτε οι ηγέτες ως αποκλειστικοί αντιπρόσωποι του Θεού, ήταν οι μόνοι που γνώριζαν το «καλό» (Μεσαίωνα). Άλλοτε, αυτοί ήταν υπεύθυνοι για την προστασία της ελεύθερης έκφρασης των πολιτών (Διαφωτισμός). Σήμερα αυτό διακηρύσσεται διαφορετικά.

Ο πρόεδρος των ΗΠΑ στο διάγγελμα του στο έθνος το 2002 διατύπωσε το γνωστό ως «Δόγμα Bush», το οποίο επρόκειτο να αποτελέσει νέα αφετηρία για τη διεθνή πολιτική. Τρία ήταν τα ουσιώδη σημεία για αυτήν (Taylor, 2004).

- Οι τρομοκράτες βλέπουν τον κόσμο ολόκληρο ως πεδίο μάχης, άρα και οι ΗΠΑ οφείλουν να χαράζουν παγκόσμια στρατηγική.
- Όποιος δεν είναι σύμμαχος σε αυτήν την «σταυροφορία», είναι εχθρός. Έτσι, διαμορφώνεται ο «άξονας του κακού», ο οποίος νομιμοποιεί τις όποιες επεμβάσεις.
- Σκοπός παραμένει η αδιαπραγμάτευτη προώθηση των φιλελευθέρων δημοκρατικών αξιών, σύμφωνα με το αμερικανικό μοντέλο.

Στην εργασία αυτή δεν μάς ενδιαφέρει η κριτική για τις παραπάνω πολιτικές θέσεις. Η χρησιμότητα της παράθεσης τους έγκειται στην ανάδειξη του στοιχείου της Κυριαρχίας στο δυνητικό περιβάλλον. Για να το δείξουμε αυτό θα εξετάσουμε το παγκόσμιο πολιτικό σύστημα διακυβέρνησης με έναν ολιστικό τρόπο σκέψης (Parker, 1998). Τυπικά, ο τρόπος οργάνωσης και διοίκησης του πλανήτη παραμένει ο ίδιος. Οι περίπου έξι δεκατομμύρια κάτοικοι αποτελεί, ο καθένας, μέλος ενός από τα 200 κράτη. Αυτά αποτελούν τη μοναδική οντότητα νόμιμης έκφρασης και επιβολής της βούλησης συλλογικοτήτων. Για αυτόν τον λόγο χαρακτηρίζονται κυρίαρχα. Οι ρίζες της οργανωτικής δομής ξεκινούν από τη συνθήκη της Βεσφαλίας το 1648 ως τα αποτελέσματα της γαλλικής επανάστασης το 1789. Ουσιαστικά στην εποχή της, είναι η πρώτη φορά που αμφισβητούνται τα όρια του δικαιώματος αυτόνομης δράσης, δηλαδή άσκησης ανεξάρτητης εξουσίας κάθε κράτους. Το κάθε κράτος, επικαλούμενο το συμφέρον του και αναλόγως την ισχύ που διαθέτει, δρα σε ένα πεδίο αλληλεπίδρασης, ενταγμένος σε ένα ανταγωνιστικό περιβάλλον διεθνών

σχέσεων (Βαρβαρούσης, 1998). Τέλος, σύμφωνα με αυτή την οπτική -των ισχυρών- καταγράφεται η ιστορική αφήγηση κάθε εποχής, τουλάχιστον τους δύο τελευταίους αιώνες. Η νοηματοδότηση θεμελιωδών εννοιών όπως η ελευθερία, δημοκρατία κ.λπ. διαμορφώνεται από τις νεαρές ηλικίες. Με αυτόν τον τρόπο, στα μέλη αυτών των δρώντων προσδίδεται μια ταυτότητα, θα λέγαμε με όρους «γραμμικούς» τυποποιώντας αρχέτυπα φυλής, έθνους, θρησκείας κ.λπ. Αξιοσημείωτο είναι ότι συχνά αντιτίθεται με την άποψη των προσώπων για τον εαυτό τους και την κοινωνία.

Στην εποχή μας, εμφανίζονται διάφοροι «επίσημοι οργανισμοί», οι οποίοι έμμεσα παρακάμπτουν, και άρα αμφισβητούν, την καθολική κυριαρχία των κρατών (όπως οι μη κυβερνητικές οργανώσεις και οι πολυεθνικές επιχειρήσεις). Αν αυτό το συνδυάσουμε με τα παραπάνω ζητήματα, γίνεται εύκολα αντιληπτό ότι η οργανωτική μορφή του πλανήτη μεταβάλλεται. Σημαντική ήταν η διαπίστωση του προέδρου των ΗΠΑ σε μια ομιλία του στο κογκρέσο για το σχεδιασμό της Στρατηγικής Εθνικής Ασφαλείας στον Κυβερνοχώρο, (The National Strategy to Secure Cyberspace, February 2003). Εκεί παραδέχθηκε ότι ο ιδιωτικός τομέας διαθέτει πιο εκσυγχρονισμένη τεχνολογία διαδικτύου από τον δημόσιο. Αυτοί λοιπόν, οι μη κρατικοί οργανισμοί αρχίζουν να κυριαρχούν στον κόσμο, να αλλάζουν το οργανωτικό μόντρωμα που επικρατούσε και το μυστικό της δύναμης τους κρύβεται στην τεχνογνωσία που διαθέτουν. Έτσι, πλέον, η διασπορά της πληροφορίας δεν μπορεί εύκολα να ελεγχθεί. Μελετητές θεώρησαν ότι η πρόσβαση σε αυτή την τεχνογνωσία έχει δύο προϋποθέσεις, α)την κατοχή των απαραίτητων υλικών πόρων (hardware & software) και β)τη γνώση διαχείρισης τους. Αυτό κρίθηκε ως τόσο σημαντικό, ώστε εκτιμήθηκε ότι η νέα ταξική διαίρεση στον κόσμο θα γίνει βάσει αυτών των κριτηρίων.

Σε αυτό το υπό διαμόρφωση καθεστώς έχουμε ήδη τις πρώτες οργανωμένες αντιδράσεις. Ο τρόπος δράσης τους βέβαια, δεν είναι ο παραδοσιακός. Η στρατηγική έννοια του «συμμετρικού» αρχίζει να εκλείπει και νέος κίνδυνος θεωρούνται οι ασύμμετρες απειλές².

2. Στη βιβλιογραφία, η χρήση των ΤΠΕ για την υπονόμευση της ισχύος των κρατών, θεωρείται ως ένα είδος -και μάλιστα το πιο πρόσφατο- των σύγχρονων προβλημάτων, τα οποία καλύφθηκαν από τον όρο «ασύμμετρες απειλές» (asymmetric threats). Ο όρος πρώτη φορά εμφανίζεται σε στρατιωτικά εγχειρίδια των Η.Π.Α. το 1997 και καταγράφει ως το πιο σημαντικό χαρακτηριστικό του την «αορατότητα» (invisible) της προέλευσης του κινδύνου. Στο περιεχόμενο του αναφέρονται οι ακόλουθες κατηγορίες: Θρησκευτικός Φονταμενταλισμός, Λαθρομετανάστευση, Τρομοκρατία, Οργανωμένο Έγκλημα (Όπλα-Ναρκοτικά-Σεξ), Ηλεκτρονικός Πόλεμος (Παραπλανήσεις Ηλεκτρονικού Φάσματος), Ψυχολογικές Επιχειρήσεις (Προπαγάνδα) και Κυβερνοπόλεμος.

Η κεντρική ιδέα της Εργασίας εστιάζεται στην ανάδειξη των κεντρικών σχεδιασμών επηρεασμού της συμπεριφοράς, και από την άλλη πλευρά της κοινής λογικής όσων προσπαθούν να (δι)αντιδράσουν μέσω του Κυβερνοχώρου.

- Πώς και σε ποιο βαθμό αντικαθιστά τα παραδοσιακά (ή φυσικά) πεδία μαχών ο κυβερνοχώρος;
- Πώς και σε ποιο βαθμό συνδέεται η Κυριαρχία στην Τεχνολογία, την Πληροφορία και της Επικοινωνίες με τον Κυβερνοπόλεμο;
- Τελικά, η κυβερνο-τρομοκρατία στη «Νέα Τάξη Πραγμάτων» αποτελεί τροχοπέδη ή την επιταχύνει, επιτυγχάνοντας μόνο την αποδόμηση του παλαιού καθεστώτος;

1.3 Σκοπός, Βιβλιογραφική Ανασκόπηση και Μέθοδος

Ο σκοπός της εργασίας είναι να παρουσιάσει μια χαρτογράφηση του φαινομένου του Κυβερνοπολέμου. Επίσης, να προτείνει μια κατηγοριοποίηση σύμφωνα με το στόχο κάθε επίθεσης. Η τεκμηρίωση που θα χρησιμοποιηθεί θα αποτελεί σύνθεση των θέσεων για την Κυριαρχία -κάτι που συνάδει με το πνεύμα των απόψεων της Εισαγωγής- των επιστημών της ψυχολογίας, της κοινωνιολογίας και του διαδικτύου.

Σε αυτό το πλαίσιο οι βιβλιογραφικές αναφορές προέρχονται από τρεις επιστημονικές περιοχές. Η πρώτη περιέχει συγγράμματα από τη νέα επιστήμη του διαδικτύου, η οποία επιχειρεί να καλύψει ένα μεγάλο κενό στο χώρο της ανθρώπινης γνώσης, ερμηνεύοντας τα διάφορα φαινόμενα – αποτέλεσμα των ΤΠΕ. Η δεύτερη περιλαμβάνει βιβλία από το χώρο των κοινωνικών επιστημών, επικεντρώνεται δε, στο πεδίο εκείνο των κοινωνιο-ψυχολογικών προσεγγίσεων για την επιρροή των Μέσων Μαζικής Ενημέρωσης (ΜΜΕ). Τέλος, κρίθηκε απαραίτητη η εμβάθυνση σε κάποιους ειδικούς κλάδους της Πολιτικής Επιστήμης, όπως η Πολιτική Επικοινωνία, οι Διεθνείς Σχέσεις, η Γεωπολιτική ανάλυση και οι Στρατηγικές σπουδές. Αυτό συνέβη διότι θεωρούμε ότι η εν γένει κυρίαρχη κατάσταση μιας ομάδας ανθρώπων σε ένα χρονοχωρικό πλαίσιο συνιστά κατεξοχήν πολιτικό γεγονός και σχετίζεται άμεσα με την ανάγκη του ανθρώπου να συνεργαστεί με τους ομόρους του.

Κατά αυτόν τον τρόπο δομήθηκαν και τα περιεχόμενα. Μετά την εισαγωγή, εξηγείται αμέσως ο τρόπος που μεταστοιχειώνεται το καθιερωμένο οργανωτικό μόρφωμα σε μια νέα Δυνητική Οργάνωση. Από αυτό το -κεντρικής σημασίας- κεφάλαιο προκύπτουν δύο ζητήματα. Το πρώτο αφορά τη μεθοδολογία (κεφάλαιο 3) της εργασίας, η οποία χρησιμοποιεί ως οδοδείκτη τον τρόπο διαμόρφωσης της Δυνητικής Οργάνωσης. Το δεύτερο ζήτημα αναδεικνύεται όταν διακρίνουμε την ανάδυση νέων εννοιών και κατά συνέπεια, την ανάγκη των επιστημόνων να τις οριοθετήσουν. Εξάλλου, η «ανάδυση» αποτελεί ένα φαινόμενο που θα εξηγηθεί σε αυτήν την εργασία, για την πληρέστερη κατανόηση του Κυβερνοπολέμου. Για αυτόν το λόγο στο επόμενο κεφάλαιο (4) παρατίθενται οι απαραίτητοι ορισμοί. Θα πρέπει εδώ να τονίσουμε ότι κατά τη διάρκεια του κειμένου, χρειάστηκε ο προσδιορισμός κάποιων λέξεων ή εκφράσεων, οι οποίες, δεν είχαν πρωτεύοντα ρόλο στη θεματολογία. Για παράδειγμα, στην τρίτη μορφή

κυβερνοπολέμου, αναπτύξαμε τη λειτουργία της προπαγάνδας στο διαδίκτυο. Εκεί ορίσαμε και τον όρο «προπαγάνδα».

Στη συνέχεια αναλύονται οι τρεις μορφές κυβερνοπολέμου (κεφάλαια 5,6 και 7). Επειδή, το φαινόμενο του Κυβερνοπολέμου δεν είχαμε στόχο να το μελετήσουμε μόνο θεωρητικά, περάσαμε στο δεύτερο μέρος της εργασίας, το οποίο αφορά την πράξη. Έτσι, χρησιμοποιήσαμε δύο, ακραίες περιπτώσεις έρευνας (case study). Η πρώτη αφορά τις ΗΠΑ, κράτος το οποίο πρωταγωνιστεί, για δύο λόγους. Επειδή δέχεται καθημερινά τις περισσότερες επιθέσεις και διότι, εξαιτίας αυτού του γεγονότος, συγκρότησε πρώτο -με εξαγγελίες μάλιστα του ίδιου του προέδρου του- την Κυβερνο-άμυνα του. Η δεύτερη μελέτη περίπτωσης αφορά την Ελλάδα. Η χώρα δέχεται μεν, άλλα ελάχιστες συγκριτικά, κυβερνο-επιθέσεις και η συνειδητοποίηση της ανάγκης για σχετική οργάνωση επαφίεται σε ορισμένους ακαδημαϊκούς. Πάντως, για την εξήγηση της κατάστασης έγινε μια σύντομη ιστορική αναδρομή στη δυναμική της συγκρότησης της «Κουλτούρα Εθνικοκρατικής Ασφαλείας» των Ελλήνων*. Η εργασία κλείνει με ορισμένα παραρτήματα, τα οποία καταγράφουν συγκεκριμένες επιθέσεις που έλαβαν χώρα κατά τη διάρκεια αυτού του ακήρυχτου πολέμου, στον οποίο μέχρι στιγμής κανένα κράτος δεν έχει ομολογήσει κυβερνο-επίθεση.

* Μία -εκ πρώτης όψεως- αντιφατική έκφανση της ψυχοσύνθεσης των ελλήνων είναι από τη μία πλευρά, το συχνό κατηγορώ του πληθυσμού έναντι της εκάστοτε ηγεσίας για έλλειψη στρατηγικού σχεδιασμού και από την άλλη, η γνωστή «αυτάρεσκη» συζήτηση επί θεμάτων στρατηγικού σχεδιασμού σε όλους τα μέσα και τους τόπους διαμόρφωσης της δημόσιας σφαίρας (π.χ. ΜΜΕ και καφενεία αντίστοιχα), καθώς και για όλα σχεδόν τα θέματα (ο καθένας παίρνει τη θέση του πρωθυπουργού, προπονητή, στρατηγού κοκ). Στο κεφάλαιο 9 θα επιχειρηθεί η καταγραφή μιας καινοτόμου μεθόδου εύρεσης των αιτιών συγκρότησης της λεγόμενης κουλτούρας ασφαλείας.

Α΄ ΜΕΡΟΣ

Η ΘΕΩΡΙΑ

Κεφάλαιο 2. Δυνητική Οργάνωση

2.1 Το Νεοτερικό και Δυνητικό Οργανωτικό Μοντέλο του Κράτους

Αρχικά, ο νεοτερικός τρόπος οργάνωσης επικράτησε στην Ευρώπη και στην Αμερική. Οι επιστήμονες εντοπίζουν την αφετηρία του τυπικά το 1648 και ουσιαστικά το 1789³. Πάντως, η εδραίωση του συγκεκριμένου οργανωτικού μορφώματος παρατηρείται σε ολόκληρο το 19^ο και 20^ο αιώνα. Τα κύρια χαρακτηριστικά του είναι τρία, (i) ο οντολογικός προσδιορισμός βάσει του χώρου και του χρόνου, (ii) η ορθολογικότητα στους κανόνες συλλογικής και ατομικής συμπεριφοράς και (iii) η ιεραρχία, καθώς και κατ'έκταση η εξουσία. Οριστικά μετά το δεύτερο παγκόσμιο πόλεμο ως δομική (μοναδιαία) οντότητα οργάνωσης και διοίκησης του πλανήτη θεωρείται το *κράτος* (Βέργος, 2004). Ακολουθεί η εφαρμογή των χαρακτηριστικών του νεοτερικού τρόπου οργάνωσης, σε μια σχηματική του παράθεση, αντίστοιχα με την αρίθμηση των τριών προαναφερθέντων χαρακτηριστικών:

i. Το κράτος συνίσταται από έναν συγκεκριμένο πληθυσμό, ο οποίος ορίζεται ως το σύνολο των ανθρώπων που κατοικούν σε μια περιοχή (χώρος) και σε μια ορισμένη περίοδο (χρόνος) ιστορικά (Τομαρά, 1998). Ως προς το χρόνο, η ίδρυση της κράτους επισημοποιείται με α) την δημόσια διακήρυξη των λόγων που συμβαίνει αυτό και των αξιών που πρεσβεύει (κάτι που είθισται να πραγματοποιείται με τη σύνταξη του Συντάγματος). Ωστόσο, ανεξαρτήτως των καταβολών που εικάζονται ως εθνικές ρίζες, η επίσημη ιστορία του καταγράφεται από εκείνη τη στιγμή και β) την αποδοχή από επαρκή αριθμό κρατών αυτού του γεγονότος. Ως προς το χώρο, δεν νοείται κράτος χωρίς τη δέσμευση ορισμένης έκτασης. Φυσικά, η έννοια του χώρου έχει και πιο αφηρημένες προεκτάσεις. Εδώ αναφερόμαστε μόνο στις ποικίλες εκφάνσεις που έχει κάθε διαλεκτική του σχέση με τον άνθρωπο (DeGruau, 1987).

ii. Πρωταρχική ανάγκη θεωρήθηκε η διασφάλιση της «επιβίωσης» του. Σε αυτή την κατεύθυνση ως θεμιτή συμπεριφορά κρίθηκε η ίδια ενίσχυση της ύπαρξης του κράτους (ορθολογικός τρόπος συμπεριφοράς). Γνώμονας δράσης συνεπώς, όπως διακηρύχθηκε από κοινή συμφωνία του συνόλου των χωρών στους διεθνείς οργανισμούς, είναι η ισορροπία μεταξύ του «εθνικού συμφέροντος» (national interest) και της διεθνούς συνεργασίας⁴.

3. Το 1648 υπογράφηκε η συνθήκη της Βεσφαλίας και συμβολικά, σήμανε της «κρατογεννήσεις» στην Ευρώπη. Το 1789, έτος της γαλλικής επανάστασης, συμβολίζει την επικράτηση του ορθολογισμού και γενικότερα, του νεοτερισμού.

4. Πολλά κινήματα και σχολές σκέψεις προασπίστηκαν τη μια από τις δύο, ως μοναδική ορθή πρόταση (Ρεαλιστική και Ιδεαλιστική Σχολή των Διεθνών Σχέσεων).

iii. Για την επίτευξη του άνω στόχου διαμορφώθηκε το οργανωτικό σχήμα που καθορίζει της κανόνες επικοινωνίας των ατόμων στο εσωτερικό των κρατών (του πληθυσμού), το οποίο θυμίζει πυραμίδα (ιεραρχικό) και απαρτίζεται από τρία επίπεδα.

ΤΑ ΤΡΙΑ ΕΠΙΠΕΔΑ ΤΟΥ ΟΡΓΑΝΩΤΙΚΟΥ ΜΟΝΤΕΛΟΥ



Στην κορυφή της πυραμίδας έχουμε το πρώτο οργανωτικό επίπεδο τους ιθύνοντες-λήπτες των αποφάσεων, τους οποίους θα καλούμε στο εξής «Ηγεσία». Βασικό καθήκον αυτού του επιπέδου είναι η διοίκηση και ο σχεδιασμός της πορείας του κράτους. Ακολουθεί το δεύτερο οργανωτικό επίπεδο, το οποίο περιέχει τα Μέσα υλοποίησης (τρόπους πραγματοποίησης) των αποφάσεων. Τα Μέσα βέβαια, διακρίνονται στα έμφυχα (γραφειοκρατία) και στα τεχνολογικά (ΤΠΕ). Τέλος, στη βάση της ιεράρχησης βρίσκεται το μεγάλο μέρος των μελών του κράτους και αποδεκτών των αποφάσεων, τους οποίους ονομάζουμε «Πληθυσμό». Σημειώνεται ότι το πλαίσιο του τρίτου οργανωτικού επιπέδου είναι ευρύτερο για να δειχθεί ότι αποτελεί και τη μήτρα εκπόρευσης των υπολοίπων, και άρα, και τη βάση της οργάνωσης (γι' αυτό είναι υπογραμμισμένο).

Το δεύτερο οργανωτικό επίπεδο, όπως φαίνεται και στο σχήμα, έχει μια κεντρική σημασία. Δίχως αυτό η Ηγεσία δεν υφίσταται, αφού δεν μπορεί να πραγματοποιήσει τη βούληση της. Το ιδιαίτερο σημείο που ενδιαφέρει τη μελέτη, αφορά στη μετάβαση που διαφαίνεται να πραγματοποιείται τις δύο τελευταίες δεκαετίες. Από την οργάνωση έντασης έμφυχων μέσων περάσαμε στην οργάνωση έντασης των ΤΠΕ (Rifkin, 1996). Το γεγονός αυτό αποτέλεσε τη γενεσιουργό αιτία της μετάβασης στο δυνητικό οργανωτικό μοντέλο. Για αυτό το λόγο θα ακολουθήσει μια σύντομη ανάλυση του τρόπου που διαδραματίστηκε αυτή η εξέλιξη.

2.2 Τα Μέσα στην Παραδοσιακή Οργάνωση

Σύμφωνα με το Ν. Μουζέλη (1991), δύο από τους πιο κλασικούς εκπροσώπους της οργανωτικής θεωρίας είναι ο Κ. Μαρξ και ο Μ. Βέμπερ. Στον πρώτο, το ζήτημα της οργάνωσης δεν ήταν κεντρικό στο έργο του. Το θέμα το μελέτησε στο πλαίσιο του καπιταλισμού, ιδιαίτερα επηρεασμένος από την εγελιανή θεωρία για το κράτος. Κατά το Χέγκελ, τα Μέσα της εξουσίας για την επίτευξη των σκοπών της, αποτελούνται από τη γραφειοκρατία, η οποία έχει το ρόλο της γέφυρας μεταξύ του κράτους και της πολιτικής κοινωνίας⁵. Τα ειδικά συμφέροντα των ομάδων του πληθυσμού κάθε κράτους προωθούνται από τους φορείς τους -από κάτω προς τα πάνω- και η ηγεσία του, με την αντίστροφη πορεία, θα πρέπει να προωθεί το γενικό συμφέρον. Ο Μαρξ εδώ, δεν συμφωνεί ότι το κράτος υπερασπίζεται το γενικό συμφέρον, αλλά το ειδικό συμφέρον της άρχουσας τάξης. Στην καπιταλιστική κοινωνία, η πραγματική λειτουργία της γραφειοκρατίας (η οποία στο οργανωτικό μας μοντέλο αποτελεί τα έμπνηχα μέσα) είναι να επιβάλει την τάξη πραγμάτων που εξυπηρετεί τα συμφέροντα της εξουσίας.

Κατά το Μ. Βέμπερ, η κοινωνική οργάνωση σχετίζεται, με το ζήτημα της εξουσίας. Καταρχάς, ορίζει τη Δύναμη ως τη δυνατότητα επιβολής της θέλησης του ατόμου στη συμπεριφορά άλλου (ή άλλων). Ειδικός τύπος της δύναμης είναι η εξουσία. Πρόκειται για ένα είδος κοινωνικής σχέσης, στην οποία και τα δύο μέρη (εξουσιαστής, που επιβάλει τη θέληση του και εξουσιαζόμενος, που προσαρμόζει τη συμπεριφορά του) πιστεύουν ότι δικαίως συμβαίνει αυτό. Αυτή λοιπόν, η νομιμοποίηση της δύναμης συντηρεί την κυριαρχία της ηγεσίας. Εδώ, διαδραματίζεται ο ρόλος των Μέσων. Όταν η εξουσία ασκείται σε έναν μεγάλο αριθμό ατόμων, χρειάζεται και έναν ισχυρό διοικητικό μηχανισμό (γραφειοκρατία), ο οποίος θα εκτελεί τις εντολές των εξουσιαστών προς τους εξουσιαζόμενους.

5. Η «πολιτική κοινωνία» περιλαμβάνει τα επαγγέλματα (και τα αντίστοιχα συνδικάτα) που διακατέχονται από τα ειδικά της συμφέροντα.

Το ενδιαφέρον στη βεμπεριανή θεωρία, ως προς τον εννοιολογικό προσδιορισμό των Μέσων, είναι η ανάλυση για τις ρίζες της γραφειοκρατίας. Η γραφειοκρατία εμφανίζεται με την εγκαθίδρυση της νομικής εξουσίας. Όπως αναφέρθηκε στην εισαγωγή, κύριο γνώρισμα της, είναι η πίστη στην ορθότητα του νόμου. Έτσι και η γραφειοκρατία χαρακτηρίζεται από την πίστη της στους απρόσωπους κανόνες της έννομης τάξης. Η οργάνωση της είναι ιεραρχική και η ύπαρξή της «ανήκει» στην κορυφή της ιεραρχικής οργάνωσης, την εξουσία, δεν αποτελεί ιδιοκτησία (όπως στο παρελθόν) κανενός. Στη σύγχρονη κοινωνία παρατηρούμε μια μεγέθυνση της «γραφειοκρατικοποίησης».

Ενδεχομένως το αντιπροσωπευτικότερο παράδειγμα είναι το πρότυπο της μεγάλης επιχείρησης, στην οποία επικράτησε το αμερικανικό σύστημα επιστημονικής διοίκησης, με κυρίαρχο τον ορθολογικό σχεδιασμό. Συμπερασματικά, διακρίνουμε στις αναλύσεις και των δύο κλασικών κοινωνικών επιστημόνων ότι η Ηγεσία χρειάζεται έναν τρόπο επικοινωνίας και πληροφόρησης από και προς τους πολίτες. Στα παραδοσιακά οργανωτικά σχήματα την ανάγκη αυτή κάλυπτε ένας εξειδικευμένος αριθμός ατόμων. Σταδιακά, αυτός ο αριθμός συσχετιζόταν αντιστρόφως ανάλογα με την εξέλιξη των τεχνολογικών μέσων. Δηλαδή, όσο αυξανόταν η παρουσία διαφόρων μηχανημάτων αυτοματισμού, τόσο μειωνόταν η εξάρτηση της ηγεσίας από τους ανθρώπινους πόρους. Στη σύγχρονη οργάνωση, εξαιτίας της εξέλιξης, τα τεχνολογικά Μέσα επικράτησαν σε τέτοιο βαθμό, ώστε να μιλάμε για μετασχηματισμό του οργανωτικού μορφώματος. Την τελευταία δεκαετία αναδύεται μία νέα μορφή, την οποία καλούμε Δυνητική Οργάνωση.

2.3 Τα Μέσα στην Δυνητική Οργάνωση

Ο ρόλος των Μέσων περιγράφεται με έμφαση στο γνωστό συγγραφικό έργο για το «Τέλος της Ιστορίας», όπου αναφέρει ότι η παγκόσμια πληροφοριακή τεχνολογία και οι στιγμιαίες επικοινωνίες προωθούν τα ιδανικά της δημοκρατίας, διότι η τεχνολογία είναι ουδέτερη και η χρήση της εξαρτάται από τον άνθρωπο (Fukuyama, 1992). Από το 1858, που ο πρόεδρος Buchanan και η βασίλισσα Βικτόρια γιόρτασαν την τοποθέτηση του υπερατλαντικού τηλεγραφικού καλωδίου. Το 1876, που ο Al. G. Bell δήλωσε -μετά την εφεύρεση του τηλεφώνου- ότι «οι επιχειρήσεις της χώρας πλέον, δεν θα έχουν πρόβλημα να επικοινωνούν από τη μια άκρη στην άλλη». Ως σήμερα, που στη δημόσια διοίκηση χρησιμοποιούμε τεχνολογίες, τις οποίες χθες θεωρούσαμε επιστημονική φαντασία, είναι βέβαιο ότι τα τεχνολογικά μέσα έχουν τη δική τους θέση στην οργάνωση των κρατών (Taylor, 2004). Σε αυτό το κεφάλαιο εξηγήσαμε πώς ο ορθολογικός τρόπος οργάνωσης των κρατών λειτουργεί μέσα από το σχήμα:

ΗΓΕΣΙΑ – Μέσα Επικοινωνίας και Πληροφορίας – ΠΛΗΘΥΣΜΟΣ
--

Η ανάπτυξη των ΤΠΕ δημιούργησε μια αμφισβήτηση για την αποδοτικότητα του ορθολογισμού. Ο χώρος και ο χρόνος γίνονται λιγότερο λειτουργικοί και τα όρια τους αμβλύνονται, με συνέπεια την αναγκαιότητα των οργανώσεων να προσαρμοστούν στα νέα δεδομένα. Οι δυνητικές οργανώσεις, οι οποίες επιχειρούν να καλύψουν αυτό το κενό, δομούνται στα νέα πλαίσια με περισσότερη ελευθερία και τα ακόλουθα χαρακτηριστικά:

- Της αύξησης της ταχύτητας επικοινωνίας,
- Της διεύρυνσης της διασποράς των πληροφοριών και
- Της μείωσης του κόστους χρήσης.

Οι έννοιες της επικοινωνίας και οργάνωσης υπήρξαν ανέκαθεν άρρηκτα συνδεδεμένες. Η κατάργηση της απόστασης και -κατά συνέπεια- η «ελαστικοποίηση» της οργάνωσης από τους αυστηρούς κανόνες της παραδοσιακής της μορφής, επέδρασαν στις κοινωνικές σχέσεις των ατόμων επιτρέποντας αμεσότερες διαντιδράσεις. Επιπροσθέτως, μια μεταβολή επέρχεται στην «οργανωσιακή μνήμη». Αναφερόμαστε στην κοινή βάση δεδομένων, όπου καταγράφονται οι δραστηριότητες κάθε οργάνωσης, η οποία πλέον, διατηρείται ευκολότερα και με μεγαλύτερη βεβαιότητα.

Τέλος, ίσως η πιο ανατρεπτική συνέπεια αυτής της μορφής οργάνωσης είναι η συνεχή επικράτηση της οριζόντιας οργάνωσης. Το χαρακτηριστικό της ιεραρχίας, που επέβαλε συγκεκριμένους κανόνες συμπεριφοράς των κατωτέρων στους ανώτερους αλλάζει. Η δυνητική επικοινωνία, για λόγους προσαρμογής, γίνεται πιο ευέλικτη στο συνεχώς εξελισσόμενο περιβάλλον. Καταληκτικά λοιπόν, τα θεμελιώδη στοιχεία που αλλάζουν διαρθρωτικά την οργάνωση είναι ο χώρος (απόσταση), ο χρόνος, η μνήμη και η χαλάρωση των κανόνων στις επικοινωνιακές σχέσεις.

Η δυνητική οργάνωση συνιστά ένα κοινωνικό δίκτυο συντονισμού, το οποίο καθίσταται εφικτό μέσω των ΤΠΕ. Κύριο χαρακτηριστικό του, όπως εξηγήσαμε, είναι η προσαρμογή. Αυτή η διάσταση προσάπτει κι ένα είδος νοημοσύνης, η οποία συμβάλλει καθοριστικά στη δυναμική της ενίσχυσης των κρατών. Αυτό έγινε γρήγορα κατανοητό από πολλά παραδοσιακά κράτη (ΗΠΑ, Καναδάς και χώρες της Ε.Ε.). Επιπροσθέτως, υπερδυνάμεις στην εφαρμοσμένη υψηλή τεχνολογία θεωρούνται και η Κίνα με τη Ρωσία. Τέλος, αξιοσημείωτο είναι ότι η ταχύτερα αναπτυσσόμενη χώρα σε αυτόν τον τομέα είναι η Ινδία (economist, 2007).

2.4 Ηγεσία και Δυνητικές Κοινότητες⁶

Η σχέση του πρώτου οργανωτικού επιπέδου (Ηγεσία) και των δυνητικών κοινοτήτων, οι οποίες διαδρούν στο δεύτερο και τρίτο οργανωτικό επίπεδο, φαίνεται σε ένα άρθρο των Bell και Kozlowski (digitalcommons, 2006). Οι συγγραφείς του άρθρου δηλώνουν εξαρχής τους τρεις στόχους, τους οποίους θέτουν. Ο πρώτος αφορά στη διάκριση των δυνητικών ομάδων από τις παραδοσιακές (συμβατικές). Ο Δεύτερος, τη διάκριση των διαφορετικών τύπων δυνητικών ομάδων μεταξύ τους. Και ο τρίτος, το ρόλο που καλείται να διαδραματίσει η Ηγεσία στο πλαίσιο αυτών των συσχετισμών. Ειδικότερα, αυτό το πλαίσιο χαρακτηρίζεται από τον κατακερματισμό της ομάδας στο χώρο, καθώς και την ασύγχρονη επικοινωνία των μελών των δυνητικών κοινοτήτων. Ολοκληρώνοντας, αναφέρεται ότι οι συνθήκες δυσχεραίνουν τον έλεγχο της ηγεσίας, η οποία αποσκοπεί:

- Να δημιουργήσει δομές και αυτοματισμούς που θα αναπληρώνουν την απουσία της «πρόσωπο με πρόσωπο» επικοινωνίας.
- Να δημιουργήσει αυτοδιοικούμενες ομάδες, παρέχοντας κατευθύνσεις, στόχους και στρατηγικές και να διευκολύνει τη συνοχή της ομάδας και τη συνεργασία των μελών.
- Να δημιουργήσει δομές που θα βοηθήσουν την ομάδα να διαχειριστεί τη λειτουργία της.
- Να παρέχει τις ανάλογες κατευθύνσεις και στόχους που θα βοηθήσουν τα μέλη της ομάδας να επιτύχουν τους επιμέρους σκοπούς και να προσαρμοστούν σε πιθανές αλλαγές συνθηκών.
- Να εξαλείψει διαφορές στη γλώσσα, τις παραδόσεις και την κουλτούρα γενικότερα, οι οποίες μπορούν να δυσκολέψουν την επικοινωνία.
- Να απλοποιεί τους σκοπούς ίδρυσης της κοινότητας. Όσο πιο πολύπλοκο είναι το έργο που έχει αναλάβει μια δυνητική ομάδα, τόσο καλύτερα είναι να μην παρακάμπτονται αυτά τα σύνορα. Όταν το έργο είναι πιο απλό, η παράκαμψη των συνόρων δεν επηρεάζει ιδιαίτερα.
- Στην εύρεση κοινών τόπων σχετικά με τις πολιτισμικές διαφορές. Η στελέχωση μιας δυνητικής ομάδας από άτομα διαφορετικής κουλτούρας δυσκολεύει τον έλεγχο.

6. Δυνητικές ονομάζουμε της κοινότητες, οι οποίες αλληλεπιδρούν στον Κυβερνοχώρο. Ο πλήρης ορισμός υπάρχει στο επόμενο κεφάλαιο.

Αυτό το άρθρο δείχνει δύο πράγματα. Το ένα είναι ότι στη δυνητική οργάνωση οι τρόποι διοίκησης και ελέγχου από την Ηγεσία είναι διαφορετικοί. Έτσι η κάθε ηγεσία προσπαθεί να προσαρμοστεί στο νέο περιβάλλον. Το δεύτερο, είναι ότι ενισχύει την ύπαρξη του διλήμματος που τέθηκε στην Εισαγωγή. Αν δηλαδή, η ομογενοποίηση των μελών μιας δυνητικά οργανωμένης ομάδας είναι αναγκαία για τον έλεγχο της.

Κεφάλαιο 3. Το Οργανωτικό Μοντέλο

3.1 Οργανωτικό Μοντέλο και Μεθοδολογία

Όπως εξηγήσαμε στο προηγούμενο κεφάλαιο, σκοπός της Ηγεσίας κάθε κράτους θα πρέπει να είναι ενίσχυση του σε όλους της τομείς (π.χ. τον οικονομικό και στρατιωτικό). Τα δύο πεδία δράσης για την επίτευξη αυτού του σκοπού χωρίζονται στο εσωτερικό (ενδοκρατικό) και το εξωτερικό (διεθνικών σχέσεων). Όσον αφορά το πρώτο, αυτό περιλαμβάνει τις εγχώριες διαδικασίες, μέσω των οποίων ενδυναμώνεται η ισχύς του κράτους, δια μέσω των επιπέδων του οργανωτικού σχήματος (Ηγεσία – Μέσα – Πληθυσμός), του οποίου την λειτουργία περιγράψαμε συνοπτικά στο προηγούμενο κεφάλαιο. Η έρευνα της αλληλεπίδρασης των τριών αυτών οργανωτικών επιπέδων, θα αποτελέσει τον οδηγό ανάπτυξης της εργασίας, για την εμβάθυνση στο φαινόμενο του κυβερνοπολέμου. Στη συνέχεια ακολουθεί μια πληρέστερη τεκμηρίωση της έννοιας της «ηγεσίας», η οποία θα υποδεικνύει και τη δόμηση (μεθοδολογία) της εργασίας.

Με όρους πολιτικής φιλοσοφίας, την κυρίαρχη ιδέα θεμελίωσης του σύγχρονου δυτικού κράτους⁷ την περιέγραψε ο Machiavelli. Βεβαίως, η προεργασία, στις κοινωνιο-ψυχολογικές συνθήκες είχε γίνει από την εποχή της Ρωμαϊκής Αυτοκρατορίας. Η συγγραφή του *Ηγεμόνα* το 16^ο αιώνα σηματοδότησε τις βασικές αξίες θεσμοθέτησης, άρα και τις αρχές πολιτικής οργάνωσης και διοίκησης, του σημερινού δυτικού κράτους. Το πλαίσιο που διαμορφώθηκε, όπως με ακρίβεια διατυπώθηκε, *εκπορεύθηκε από μια οντολογία και ανθρωπολογία της Ισχύος, ως θεσμικά διαμεσολαβούμενης έμμεσης ιστορικής κοινωνίας* (Λουδοβίκος, 2006).

Στο γνωστό ερώτημα του Μακιαβέλι αν τον ηγέτη θα πρέπει να τον αγαπούν ή να τον φοβούνται, προσπάθησαν να δώσουν απάντηση οι θεσμοί της εν γένει πολιτείας. Ειδικότερα στο επίπεδο της πολιτικής επικοινωνίας, η απάντηση όλων των πολιτικών πρωταγωνιστών⁸ θα ήταν ότι το ζητούμενο είναι η εμπιστοσύνη και όχι ο φόβος των πολιτών.

7. Αρχικά, ο όρος «δυτικός» αφορούσε κυρίως την Ευρώπη, τις τελευταίους δύο αιώνες περικλείει και την Αμερική. Συχνά δε, μόνο τη βόρεια.

8. Ο όρος «πολιτικοί πρωταγωνιστές» (Brian McNair – 1998) θα εξηγηθεί παρακάτω.

Παρόλα αυτά, όπως επισημαίνουν οι πολιτικοί επιστήμονες, και ιδιαίτερα αυτοί των διεθνών σχέσεων, το καθοριστικό κριτήριο είναι η Ισχύς. Από τις ελάχιστες εξαιρέσεις που αυτό ελέγχθη επίσημα ήταν σε μια συνέντευξη του προέδρου Νίξον στο περιοδικό Time (3/1/1972), η οποία συνοπτικά αναφέρει:

Πιστεύω σε έναν κόσμο με ισχυρές δυνάμεις, διότι μόνον αυτές εγγυώνται μεγάλες περιόδους ειρήνης (Κίσινγκερ, 1994).

Στις δύο προηγούμενες παραγράφους δείξαμε τη σημαντικότητα της έννοιας της ισχύος, για τη διατήρηση της πολιτικής κυριαρχίας και στα δύο πεδία δράσης. Το πρώτο, όπως αναφέραμε, αφορά το ενδοκρατικό πλαίσιο, εκεί όπου η εκάστοτε ηγεσία θεσμοθετεί, στοχοθετώντας στη διατήρηση του συστήματος εξουσίας της. Το δεύτερο αφορά την άσκηση εξωτερικής πολιτικής, όπου το σύστημα εξουσίας κάθε κράτους επιχειρεί τη συγκριτική υπεροχή του.

Σχετικά με το δεύτερο πεδίο δράσης, το οποίο περικλείει τις εκτός συνόρων αλληλεπιδράσεις μεταξύ των ίδιων των κρατών, το ενδιαφέρον βρίσκεται και εδώ στα μέσα επικοινωνίας, αλλά παράλληλα και διεκδίκησης για την άντληση ισχύος, τα οποία έχουν καθιερωθεί στο στίβο του διεθνούς ανταγωνισμού. Σύμφωνα με τη διεθνή βιβλιογραφία, κυρίως στη γνωστική περιοχή των πολιτικών επιστημών⁹, αποτελεί κοινό τόπο ότι αυτά τα μέσα διακρίνονται σε τέσσερις τομείς (Taylor, 2004)¹⁰, οι οποίοι τομείς είναι οι εξής:

- Πολιτικός (π.χ. διπλωματικά μέσα).
- Οικονομικός (Συμφωνίες για την εκμετάλλευση πηγών ενέργειας ή διόδων μεταφοράς της. Συναλλαγές για την προσφορά και τη ζήτηση πόρων κ.λπ.).
- Στρατιωτικός (Εδώ περικλείονται της οι διαδικασίες και δυνάμεις ασφαλείας).
- Πολιτισμικός¹¹ (Πρόκειται για τον τομέα με το μεγαλύτερο εύρος. Γενικότερα, εδώ περιλαμβάνονται θέματα επικοινωνίας μεταξύ των λαών, τέχνης, αναζήτησης κοινών μεθόδων συνεννόησης και πολλά άλλα).

9. Ειδικότερα, των Διεθνών Σχέσεων, της Γεωπολιτικής και Στρατηγικών Σπουδών.

10. Η βιβλιογραφική αναφορά είναι ενδεικτική. Σχεδόν όλα -τουλάχιστον τα κλασικά- έργα, κατηγοριοποιούν με αυτόν τον τρόπο τα μέσα επικοινωνίας και απόκτησης ισχύος μεταξύ των κρατών.

11. Για ορισμένους το τέταρτο επίπεδο αλληλοσχέτισης αποκαλείται «η κρυμμένη διάσταση» και περικλείει της δραστηριότητες των μυστικών υπηρεσιών (intelligence). Πρόκειται για τη συγκέντρωση (μυστικών) πληροφοριών για τη γνώση περί του επιπέδου ισχύος άλλου δρώντος (φίλου, ουδέτερου ή εχθρού). Το βιβλίο την υιοθετεί στο τέταρτο επίπεδο ψυχολογικής ή πληροφοριακής διάστασης (Taylor, 2004 – σ.76).

Ο τομέας που μας αφορά σε αυτήν την εργασία είναι ο στρατιωτικός. Η κυβερνοάμυνα, εφόσον αφορά ένα ιδιαίτερο είδος αντιμετώπισης του πολέμου, οργανώνεται κάτω από τις εντολές της στρατιωτικής ηγεσίας. Έστω και αν ο επιτιθέμενος είναι ένας απλός χάκερ ή ένας επικίνδυνος τρομοκράτης. Επίσης, έστω και αν ο στόχος επιζητά να πλήξει δομές του οικονομικού τομέα, η αντιμετώπιση, ο σχεδιασμός και η εγρήγορση είναι ευθύνη της στρατιωτικής ηγεσίας¹². Συμπερασματικά, η μεθοδολογία που θα ακολουθηθεί σε αυτή την εργασία, για την ανάλυση του φαινομένου του κυβερνοπολέμου, προκύπτει από την παραπάνω κατηγοριοποίηση.

Όπως αναλύσαμε στο προηγούμενο κεφάλαιο, το σύγχρονο κράτος οργανώνεται σε τρία επίπεδα. Βάσει αυτών, για τις ερευνητικές ανάγκες της εργασίας, θα χρησιμοποιήσουμε ένα οργανωτικό μοντέλο. Αυτό συνίσταται από τα τρία οργανωτικά επίπεδα και τον έναν από τους τέσσερις τομείς επικοινωνίας της Ηγεσίας με το κράτος (εσωτερικά με τον πληθυσμό του και εξωτερικά με τα άλλα κράτη). Πρόκειται για τον Στρατιωτικό. Εξάλλου, όπως έγραψε ο τότε διευθυντής του MIT Media Laboratory και αδελφός νυν υψηλόβαθμου στελέχους του Υπουργείου Εξωτερικών των ΗΠΑ, όταν εξετάζουμε την Επικοινωνία και τα Μέσα, οφείλουμε να θυμόμαστε ότι πάντα θα ελέγχονται από κάποιον. Ιδίως στην εποχή μας, που «οι δυνητικοί κόσμοι βιώνονται» (Negroponte, 1995). Οι εξελίξεις στα Μέσα ανέδειξαν ένα νέο είδος πολέμου, ο οποίος λαμβάνει χώρα στον Κυβερνοχώρο. Αυτός διεξάγεται σε όλα τα οργανωτικά επίπεδα και η αντιμετώπιση του, δηλαδή η Διοίκηση της Κυβερνοάμυνας είναι ευθύνη της Στρατιωτικής Ηγεσίας.

12. Υπενθυμίζεται πως στον Στρατιωτικό τομέα περιλαμβάνονται της οι Υπηρεσίες Ασφάλειας, όπως για παράδειγμα η Δίωξη Ηλεκτρονικού Εγκλήματος.

3.2 Η εφαρμογή του Οργανωτικού Μοντέλου στο φαινόμενο της «Παγκοσμιοποίησης»

Στόχος αυτού του κεφαλαίου είναι να δείξουμε τον τρόπο λειτουργίας του οργανωτικού μοντέλου που παρουσιάσαμε. Εκτιμήθηκε ως καλύτερο παράδειγμα εφαρμογής το φαινόμενο της «παγκοσμιοποίησης», για τρεις λόγους. Ο πρώτος είναι η επικαιρότητα του και οι συζητήσεις που έχουν ξεκινήσει στην ακαδημαϊκή κοινότητα για τη φύση του. Ο δεύτερος λόγος είναι ότι, αντίθετα από διάφορες υπεραπλουστευμένες αναλύσεις, δεν συμφωνούμε ότι έχει εισχωρήσει σε όλους τους κρατικούς τομείς. Ένα τελευταίο σημείο, που προσφέρεται από αυτό το παράδειγμα, είναι να δείξουμε τις αλληλεπιδράσεις μεταξύ των τομέων, στους οποίους έχει επικρατήσει.

Το μοντέλο θεωρεί -όπως και η ιδρυτική χάρτα του ΟΗΕ- ως μοναδικές οντότητες επίσημης συλλογικής έκφρασης¹³ των ατόμων τα κράτη (ΟΗΕ, 2008). Η ταχύτατη ανάπτυξη των ΤΠΕ δημιούργησε αλληλεξαρτήσεις σε όλα τα επίπεδα. Ορισμένα κράτη εισήγαγαν τόσο έντονα τις καινοτομίες στη δημόσια διοίκηση τους (e-Government), ώστε ορισμένοι να μιλούν για το εικονικό κράτος του μέλλοντος (Χουλιάρης, 2004). Έτσι, για παράδειγμα στην οικονομία, η διακύμανση των χρηματιστηριακών μεγεθών στην Άπω Ανατολή επηρεάζει άμεσα τη διακίνηση κεφαλαίων στη Νέα Υόρκη. Τα κράτη που ανήκουν στη συμμαχία του NATO, μπορούν να ανταλλάσουν στρατιωτικές πληροφορίες χωρίς να απαιτείται η φυσική παρουσία των ενδιαφερομένων. Οι ηγεσίες των κρατών που διέθεταν πρώτες την κατάλληλη τεχνογνωσία φρόντισαν να δημιουργήσουν διεθνείς οργανισμούς διακρατικών «συνεργασιών». Σε αυτούς πρόσφεραν, από τη μία πλευρά, μέρος από τα οφέλη των νέων τεχνολογιών στα άλλα κράτη-μέλη, τα οποία δεν τις κατείχαν. Από την άλλη πλευρά, απαιτούσαν την αναγνώριση της πρωτοκαθεδρίας τους σε αυτούς τους οργανισμούς. Άμεσο αποτέλεσμα ήταν η απόκτηση του ελέγχου. Αυτές είναι οι συνέπειες της παγκοσμιοποίησης, οι οποίες θυμίζουν χαρακτηριστικά ολοκληρωτικών καθεστώτων.

13. Επίσημης, διότι προϋποθέτει κοινή αποδοχή από τους υπόλοιπους. Αντιθέτως, δεν ισχύει στις εθνοτικές ομάδες, οι οποίες διεκδικούν την εθνικό-κρατική τους υπόσταση, η οποία δεν έχει ακόμη αναγνωριστεί (π.χ. Παλαιστίνιοι και Κούρδοι).

Συλλογικής, επειδή το κράτος εγγυάται ένα ολοκληρωμένο πλαίσιο έκφρασης και δράσης, για συγκεκριμένο χρόνο και σε ορισμένο χώρο, για έναν πληθυσμό. Κύρια μέριμνα του είναι η εξασφάλιση της εθνικής ομάδας ως σύνολο.

Εθνοτικότητα (ethnicity) συνιστούν ομάδες ατόμων που, εκτός των άλλων χαρακτηριστικών (γλώσσα-θρησκεία-ήθη-έθιμα), το μόνο απαραίτητο είναι η κοινή αντίληψη για το συμφέρον τους και κατά συνέπεια τι συνιστά για αυτό απειλή. Όταν καλύπτει ομοιογενώς το σύνολο μιας κοινωνίας και νομιμοποιεί ηγεσία και μέσα, καλείται «εθνικότητα» (nationality) (Μάζης, 2002).

Αν τώρα εξετάσουμε το παράδειγμα της Ευρωπαϊκής Ένωσης, θα δούμε ότι μετά από πολλά χρόνια προσπαθειών, δεν έχει επιτευχθεί η πολιτική ενοποίηση. Αντιθέτως, ο στόχος της οικονομικής ενοποίησης επιτεύχθη σύντομα και παρομοίως ακολούθησε και η στρατιωτική συνεργασία.

Εν κατακλείδι, σύμφωνα με το οργανωτικό μοντέλο, το φαινόμενο της παγκοσμιοποίησης λειτουργεί στον οικονομικό και στρατιωτικό τομέα, ενώ βρίσκεται ακόμα στο στάδιο των διαπραγματεύσεων για τον πολιτικό.

Κεφάλαιο 4. Ορισμοί

4.1 Οι Θεμελιώδεις έννοιες (Κυβερνοχώρος – Δυνητικό – Δυνητικοποίηση)

Εξαρχής θα πρέπει να επισημάνουμε ότι σε αυτό το κεφάλαιο δεν θα διατυπωθούν όλες οι έννοιες που χρίζουν ορισμού σε αυτήν την εργασία. Ορισμένοι όροι, επειδή θα πρέπει να εξηγηθούν αναλυτικότερα από όσο επιτρέπει ένας ορισμός, παρατίθενται στο αντίστοιχο κεφάλαιο αναφοράς τους. Τρεις κατηγορίες εννοιών θα προσδιοριστούν. Η πρώτη περικλείει τους εισαγωγικούς (θεμελιώδεις) όρους. Τα πρώτα «εργαλεία» των κοινωνικών επιστημόνων, για τη μελέτη των κοινωνικών σχέσεων στο διαδίκτυο. Η δεύτερη, θα λέγαμε ότι προκύπτει από την πρώτη, ως προς το γεγονός ότι θα ασχοληθούμε με τρεις κλασικές έννοιες των κοινωνικών επιστημών και τη μεταστοιχείωση τους στο διαδίκτυο. Η τρίτη περιέχει τους αναγκαίους βασικούς όρους, που παραβάλλονται κατά αντιστοιχία με τα είδη του κυβερνοπολέμου, βάσει της σχηματικής ανάλυσης του προηγούμενου κεφαλαίου.

Η μεγάλη ανάπτυξη των ΤΠΕ έδωσε στην ανθρωπότητα την ικανότητα να απεγκλωβιστεί σε έναν μεγάλο βαθμό από τις δεσμεύσεις του χώρου και του χρόνου. Βεβαίως, θα πρέπει να σημειώσουμε και τις επικρίσεις για αυτό το γεγονός, οι οποίες αντιθέτως, θεωρούν ότι η τεχνολογία εγκλωβίζει το άτομο. Αυτή η θέση προβάλλει τον αποξενωτικό χαρακτήρα των απρόσωπων σχέσεων που δημιουργούν οι πληροφοριακές επικοινωνίες (Heidegger, 1953). Παρόλα αυτά η διακίνηση της πληροφορίας και οι δυνατότητες επικοινωνίας διευρύνθηκαν, εξαιτίας της τεχνολογίας του διαδικτύου. Αυτός ο καινούριος -μη φυσικός- χώρος κοινωνικών σχέσεων ονομάστηκε Κυβερνοχώρος (Cyberspace)¹⁴.

14. Η λογοτεχνική απόδοση του όρου, μέσα από το βιβλίο που τον εισήγαγε είναι: *Κυβερνοχώρος. Μια συναινετική παραίσθηση (consensual hallucination) την οποία ζουν καθημερινά εκατομμύρια νόμιμοι χειριστές, σε κάθε χώρα, και παιδιά που μαθαίνουν τις μαθηματικές έννοιες... Μια γραφική αναπαράσταση των δεδομένων που προέρχονται από το σύνολο όλων των υπολογιστών του κόσμου. Αδιανόητη πολυπλοκότητα. Γραμμές φωτός που διασχίζουν τον α-χώρο, συμπλέγματα και αστερισμοί δεδομένων. Σαν τα φώτα της πόλης που τρεμοσβήνουν.*

Επίσης, πολύ περιγραφικός και μάλλον παραστατικός ορισμός είναι αυτός του Bruce Sterling (*Introduction to the Hacker Crackdown*): *Cyberspace is the place where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other's person phone, in some other city. The place between the phones.*

Τον όρο εμπνεύστηκε ο William Gibson, στο μυθιστόρημα επιστημονικής φαντασίας «Νευρομάντης» (Neuromancer), το οποίο εκδόθηκε το 1984. Ο συγγραφέας υπήρξε πρωτοπόρος του είδους της επιστημονικής λογοτεχνίας του «κυβερνοπάνκ» (cyberpunk) και ο «Νευρομάντης» έγινε το βιβλίο που θεμελίωσε αυτό το είδος τέχνης, του οποίου το ιδιαίτερο γνώρισμα ήταν η σχέση της ζωής με την υψηλή τεχνολογία (“high tech – low life”). Η υπόθεση εξελίσσεται σε ένα παγκόσμιο δίκτυο υπολογιστών που συνενώνει ανθρώπους και πληροφορία, μηχανές προγράμματα και δεδομένα, σχηματίζοντας το υλικό υπόβαθρο μέσα στο οποίο πραγματοποιείται η κίνηση (πλοήγηση) σε έναν αλληλεπιδραστικό δυνητικό κοινωνικό χώρο.

Το -εννοιολογικά καινοτόμο- στοιχείο του «δυνητικού» και κατά επέκταση της «δυνητικοποίησης», αφορούν έννοιες φιλοσοφικές, τις οποίες θα ορίσουμε (Levy, 1995). Οι τέσσερις τρόποι του *είναι* αποδίδονται ως:

- Δυνητικό (virtual)
- Ενεργά υπαρκτό (actual)
- Δυνατό (possible)
- Πραγματικό (real)

Το *δυνητικό* δεν είναι το *εικονικό*. Εικονικό εννοούμε το ψευδές, το φαινομενικά αληθινό, αλλά ουσιαστικά πλασματικό· το *εικονικό* δεν αφορά τρόπο του *είναι*! Το *δυνητικό*, ως τρόπος του *είναι*, προσφέρει χώρο για δημιουργία, διανοίγει προοπτικές. Υπάρχει, αλλά δεν γίνεται αντιληπτό από τις αισθήσεις. Το *πραγματικό* δηλώνει την υπόσταση του πράγματος, το *δυνατό* επικαλύπτει τις μορφές που δεν έχουν ακόμη εκδηλωθεί. Το *ενεργά υπαρκτό* επέρχεται κι αποτελεί την εκδήλωση του συμβάντος. Η *δυνητικοποίηση* (virtualization) επινοεί προβλήματα, «πυροδοτεί το γίγνεσθαι» και εν κατακλείδι, γίνεται πηγή. Όπως ξεκινά ο φιλόσοφος το έργο του:

Η δυνητικοποίηση επηρεάζει σήμερα όχι μόνο την πληροφόρηση και την επικοινωνία, αλλά εξίσου έντονα και το σώμα, την οικονομική λειτουργία και τη συλλογική νοημοσύνη. Η δυνητικοποίηση εγγίζει τους τρόπους κοινωνικής συνύπαρξης, όπως οι δυνητικές κοινότητες.

Εδώ λοιπόν, βρίσκονται οι απαρχές της αποεδαφικοποίησης (deterritorialisation)¹⁵, καθώς και υπέρβασης των χρονικών ορίων στις κοινωνικές σχέσεις. Είναι προφανές ότι αυτή η εξέλιξη θα επηρέαζε τους τρόπους οργάνωσης των ανθρώπινων δραστηριοτήτων. Έτσι, το οργανωτικό μόρφωμα μεταστοιχειώνεται. Στα θεμελιώδη χαρακτηριστικά που του

προσέδωσε ο ορθολογικός τρόπος κατανόησης των περασμένων αιώνων, όπως η ορθολογικότητα, η ιεραρχία, το κανονιστικό πλαίσιο και η εξουσία, κυρίαρχο ρόλο είχαν ο χώρος και ο χρόνος. Η δυνητική οργάνωση ανατρέπει αυτές τις σχέσεις (Αλεξιάς, 2007). Στις μέρες μας οι άνθρωποι διακινούν πληροφορίες και επικοινωνούν ανεξάρτητα από τις αποστάσεις που μάς χωρίζουν και το χρόνο που δύναται ο καθένας να ανταποκριθεί. Για παράδειγμα μπορούμε να εξετάσουμε την επικοινωνία μέσω ηλεκτρονικού μηνύματος (e-mail). Σε σχετικά μηδενικό χρόνο μπορεί να αποσταλεί και να καλύψει αποστάσεις μεταξύ ηπείρων. Επίσης, είναι δυνατόν ο ένας να το στείλει το πρωί και ο άλλος να το διαβάσει το βράδυ, ακυρώνοντας με αυτόν τον τρόπο την απαίτηση της άμεσης φυσικής παρουσίας. Πάντως δεν θα πρέπει να δοθεί η εντύπωση πως η δυνητική οργάνωση αποτελεί ένα ριζικά διαφορετικό μοντέλο από την παραδοσιακή (Mowshowitz, 2002). Σίγουρα συνιστά μια καινοτομία, η πραγματικότητα της όμως, δεν συνάδει με κάποιες ακραίες μεταμοντέρνες θεωρήσεις. Σε πιο ρεαλιστικό επίπεδο, θα πρέπει να μελετηθεί η σχέση ανθρώπου και μηχανής.

15. Σε έναν ελεύθερο εννοιολογικό προσδιορισμό, θα λέγαμε ότι ο όρος αποδίδει την υπέρβαση των «συνόρων» του χώρου, όπως έχει προσδιοριστεί στο προηγούμενο κεφάλαιο. Το αποτέλεσμα της διαλεκτικής σχέσης ανθρώπινης διαδραστικότητας (τεχνολογία) και φύσης.

4.2 Κοινωνικές Επιστήμες και Διαδίκτυο (Κοινωνία – Κοινότητα – Δυνητικές Κοινότητες)

Η μελέτη της σχέσης των όρων «Κοινωνία – Κοινότητα – Δυνητικές Κοινότητες» δείχνει ότι το στοιχείο της ορθολογικής διαχείρισης παραμένει εμφανές. Οι έρευνες έχουν εστιάσει την προσοχή τους σε αυτή τη σχέση, η οποία αποτελεί τη βάση για τον τρόπο που ο άνθρωπος οργανώνει το περιβάλλον του. Σήμερα μπορούμε να μιλάμε και για επιστήμη της «αλληλεπίδρασης ανθρώπου-υπολογιστή (HCI – Human Computer Interaction). Αντικείμενο της επιστήμης αποτελεί η μελέτη της διαδραστικότητας των υπολογιστικών συστημάτων, δηλαδή την αλληλεπίδραση με τους χρήστες τους (Συρμακέσης, 2006).

Κοινότητα. Η έννοια της χρησιμοποιείται με πολλούς διαφορετικούς τρόπους. Καταρχήν, θεωρούμε ότι καλύπτει βασικές ανάγκες του «ανήκειν» ή του «εμείς». Αποτελεί μια κοινότυπη έκφραση που χρησιμοποιείται σε καθημερινές συζητήσεις. Οι περισσότεροι πιστεύουν ότι ανήκουν τουλάχιστον σε μια κοινότητα. Ο όρος «κοινότητα» δεν είναι μόνο περιγραφικός, αλλά κοινωνικός και ιδεολογικός: μεταφέρει ένα βαρύ φορτίο μέσα του (Bell, 2001). Παρόλα αυτά μια επιστημονική προσέγγιση την θεωρεί ως μια ενότητα σταθερή και διαρκής, αποτελούμενη από ένα πυκνό δίκτυο κοινωνικής αλληλεπίδρασης υποστηριζόμενη από αισθήματα αμοιβαιότητας και κοινοχρηστικότητας, τα οποία καταφάσκονται στο πλαίσιο κοινών τελετουργιών και συμβόλων, ένα τοπικό κοινωνικό συμβόλαιο εμβαπτισμένο στο χώρο και ενεργό μέσω των διαπροσωπικών επαφών (Βατικιώτης, 2006). Εδώ, τα έθνη θεωρείται ότι συνιστούν φαντασιακές κοινότητες, τις οποίες χρησιμοποιούν συμβολικές αναφορές και πρακτικές. Η χρήση «αντικειμενικών παραστάσεων» ενώνει γύρω από μια κοινή ταυτότητα (σημαία, εθνικός ύμνος κ.λπ.). Αυτού του είδους οι κοινότητες υπάρχουν γιατί τα μέλη της πιστεύουν σε αυτές και τις διατηρούν μέσω κοινών πολιτισμικών πρακτικών.

Κοινωνία. Προέκυψε από την παραδοσιακή έννοια της κοινότητας, η οποία χάνεται -μέσω της αστικοποίησης- στο πλαίσιο της πυκνής ετερογένειας που χαρακτηρίζει την πόλη. Οι παλαιοί δεσμοί και κανόνες χάνουν τη δύναμή της και το κοινωνικό γίγνεσθαι αλλάζει δραστικά. Οι σχέσεις των ανθρώπων είναι επιφανειακές και διαμεσολαβημένες γιατί η πόλη είναι τεράστια. Η έννοια του κοινοτισμού γίνεται νοσταλγία (Βατικιώτης, 2006).

Δυνητική κοινότητα. Ο όρος αναφέρθηκε για πρώτη φορά από τον Howard Rheingold (1993), τον πιο ενθουσιώδη υποστηρικτή των ατομικών και κοινωνικών οφελών από

αυτές. Περιγράφει τη δυνητική κοινότητα σαν μια pub της γειτονιάς. Με αυτόν τον τρόπο προσδιορίζει τις διαδικτυακές συμπεριφορές (online cultures) εκείνων που εμπλέκονταν σε επικοινωνία διαμεσολαβημένη από τον ηλεκτρονικό υπολογιστή (Computer-Mediated Communication – CMC), εγκαθιστώντας «εναλλακτικά πλανητικά πληροφοριακά δίκτυα» (Flew, 2005). Στην ίδια συγγραφή διακρίνουμε τρία συσχετιζόμενα συστατικά της CMC:

- την κατασκευή κοινωνικών δικτύων και κοινωνικού κεφαλαίου,
- το μοίρασμα της γνώσης και της πληροφορίας και
- το σχηματισμό νέων μορφών δημοκρατικής συμμετοχής.

Αυτό το τελευταίο χαρακτηριστικό δηλώνει κάτι σημαντικό. Τα νέα μέσα είναι ελεύθερα για όλους. Οι χρήστες μπορούν να συνδεθούν από οποιαδήποτε τοποθεσία καθ' όλη τη διάρκεια της μέρας. Επικοινωνώντας σε αυτά τα online περιβάλλοντα, οι χρήστες μπορούν να συνεργαστούν και να δικτυωθούν σε πραγματικό ή μη χρόνο σε πολιτικά, επιχειρηματικά και κοινωνικά περιβάλλοντα (Hawkins et al., 1999). Μέσα σε αυτά τα περιβάλλοντα, τα οποία γενικά θα μπορούσαμε να χαρακτηρίσουμε ως περιβάλλοντα ηλεκτρονικής διακυβέρνησης, οι κοινωνικές δομές και κατά συνέπεια, η οργάνωση, η διοίκηση και ακόμη και ο τρόπος που πολεμούν τα κράτη αλλάζει.

Πριν την εμφάνιση του διαδικτύου οι κοινότητες αφορούν κυρίως ανθρώπους που ζουν ή εργάζονται μαζί. Όσοι έχουν πρόσβαση στο διαδίκτυο, διαθέτουν τη δυνατότητα να μοιράζονται με άλλα άτομα τα ίδια ενδιαφέροντα, ανεξαρτήτως πού βρίσκονται σαν φυσικές παρουσίες. Οι δυνητικές κοινότητες είναι αναπόφευκτα διαφορετικές, πιο ευέλικτες. Η συμμετοχή και αποχώρηση των ατόμων γίνεται με πιο χαλαρούς κανόνες. Μια τέτοια διαδικασία ανάπτυξης (online) κοινοτήτων είναι πλέον αναπόφευκτη για δύο λόγους: α) γιατί οι άνθρωποι τείνουν πάντα να πειραματίζονται με μια νέα τεχνολογία, ανατρέποντας παλιούς κοινωνικούς κώδικες, δημιουργώντας νέα είδη κοινοτήτων, β) αποτελούν φυσική απάντηση στην ανάγκη να ικανοποιηθεί η δίψα του κοινοτισμού σε μια εποχή που χαρακτηρίζεται από την αποσύνθεση των παραδοσιακών κοινοτήτων.

4.3 Οι βασικές έννοιες του Κυβερνοπολέμου

4.3.1 Πόλεμος Πληροφοριών (War of Intelligences)

Το ενδιαφέρον κάθε ηγεσίας να μαθαίνει τα ευαίσθητα και ισχυρά σημεία των αντιπάλων της είναι τόσο παλαιό, όσο και ο πολιτισμός του ανθρώπου στη γη. Δύο είναι οι τρόποι που μπορεί αυτό να επιτευχθεί (Αλειφαντής, 2002). Ο πρώτος αφορά την εκμετάλλευση στοιχείων από τις λεγόμενες ανοιχτές πηγές (open sources). Πρόκειται για τη μέθοδο συλλογής πληροφοριών από δημοσιοποιημένα δεδομένα. Σε αυτήν την περίπτωση δεν υπάρχει τίποτε παράνομο ή κρυφό. Ασφαλώς, όταν ξεκινά η επεξεργασία, τότε οι πληροφορίες διαβαθμίζονται και αυτός είναι ο λόγος που οι υπηρεσίες που τις διαχειρίζονται ονομάζονται μυστικές.

Ο δεύτερος τρόπος αφορά την εκμετάλλευση στοιχείων από τις λεγόμενες κλειστές πηγές (close sources). Εδώ περιέχονται οι απόρρητες πληροφορίες. Η ειδοποιός διαφορά από αυτή είναι ότι αντιθέτως, η εκμετάλλευση της θα απαιτεί τη διάθεση ειδικής εξουσιοδότησης και προφανώς, τον έλεγχο της πρόσβασης από οποιονδήποτε ενδέχεται να εξυπηρετεί ξένα συμφέροντα. Σε αυτές τις συνθήκες γεννήθηκε και η δραστηριότητα της επικαλούμενης κατασκοπείας και -του συστήματος προστασίας από αυτήν- της αντικατασκοπείας. Πρόκειται για τις μυστικές επιχειρήσεις (cover operations) συλλογής δεδομένων από απόρρητες πηγές.

Με την έναρξη της προσπάθειας εύρεσης τρόπων εκμετάλλευσης των ΤΠΕ από το Στρατό, άρχισαν να διαμορφώνονται οι επονομαζόμενες «μετά-νεοτερικές» μορφές μάχης (Taylor, 2004). Σε αυτές δόθηκαν κατά καιρούς διάφορες προσφωνήσεις, υπερπόλεμος (hyper war), δικτυοπόλεμος (net war) και εικονικός πόλεμος (virtual war). Ο τελευταίος για παράδειγμα, περιλαμβάνει την επίδραση των βίαιων εικόνων της τηλεόρασης κυρίως στον άμαχο πληθυσμό. Παρόλα αυτά ο όρος που καθιερώθηκε για οποιαδήποτε μορφή άσκησης πολεμικών επιχειρήσεων μέσω του διαδικτύου είναι ο Κυβερνοπόλεμος.

4.3.2 Κυβερνοπόλεμος (Cyberwar)

Κάθε συντονισμένη ενέργεια, η οποία αποσκοπεί να πλήξει την ισχύ του κράτους και για πεδίο μάχης χρησιμοποιεί τον κυβερνοχώρο, καλείται απειλή κυβερνοπολέμου. Άρα, από τη φύση του ο κυβερνοπόλεμος έχει μια τεράστια διαφορά από τον παραδοσιακό πόλεμο. Δεν υπακούει σε χρονοχωρικούς περιορισμούς, δηλαδή, δεν έχει αρχή και τέλος, και δεν λαμβάνει χώρα σε συγκεκριμένη εδαφική έκταση. Στο οργανωτικό επίπεδο, θα λέγαμε ότι

ξεκίνησε με την πρώτη εμφάνιση του κυβερνοχώρου, στον οποίο μάλλον κινείται παράλληλα, σαν να είναι η σκιά του!

Εφόσον πρόκειται ακριβώς για το αντικείμενο της εργασίας, θα αναλύσουμε περισσότερο αυτόν τον ορισμό, διότι όπως συμβαίνει και με τις έννοιες που χρίζουν ψυχοκοινωνιολογικής προσέγγισης, στην καθημερινότητα χρησιμοποιείται με ποικίλους τρόπους, κατά το δοκούν. Καταρχάς, πρόκειται για έναν πόλεμο ακήρυχτο, ασύμμετρο και δυνητικά συνολικό (ολοκληρωτικό).

- Ακήρυχτο, επειδή σε καμία περίπτωση (όπως θα αποδειχθεί και από τα παραρτήματα) δεν έχει ποτέ κανένα κράτος αποδεχτεί την ευθύνη κάποιας κυβερνοεπίθεσης.
- Ασύμμετρα ή μη-γραμμικά (non linear battlefields) ονομάζονται τα πεδία μάχης με κύριο χαρακτηριστικό τα «τυφλά» (invisible) χτυπήματα (Δρούγος, 2007), στα οποία συνεπώς η προέλευση παραμένει άγνωστη. Συνεπώς, εξ' ορισμού ο κυβερνοπόλεμος συνιστά την κλασική μορφή ασύμμετρης απειλής (asymmetric threat).
- Συνολικός είναι διότι εν δυνάμει καταφέρεται στο σύνολο των δομών της ηλεκτρονικής διακυβέρνησης -και κατ'επέκταση των αντίστοιχων αμυντικών εφαρμογών- του κράτους¹⁶.

4.3.3 Πληροφοριακός Πόλεμος (Info war)

Ο όρος «πληροφοριακός πόλεμος» διαφέρει από την έκφραση «Πόλεμος των Πληροφοριών». Καταρχάς, διενεργείται μόνο στον κυβερνοχώρο, σε αντίθεση με τον άλλον που έχει γενικό περιεχόμενο. Χρησιμοποιείται για να υποδηλώσει κάθε ενέργεια παρακολούθησης ή παρέμβασης στα ηλεκτρονικά και ψηφιακά συστήματα Διοίκησης και Ελέγχου (C4ISR¹⁷), της διαδικασίας λήψης αποφάσεων από τη στρατιωτική ηγεσία των κρατών.

16. Ένα γνωστό απόφευγα, που ειπώθηκε μετά το τέλος του ψυχρού πολέμου, λέει ότι ο τρίτος παγκόσμιος πόλεμος θα μπορεί να έχει δύο αιτίες. Α) Η πρώτη είναι «εξωσυστημική». Εδώ, «ενδοσυστημικό» θεωρείται οτιδήποτε μπορεί να εξολοθρευθεί από τον ανθρώπινο παράγοντα. Έτσι, δεν αποτελούν μέρος αμυντικού σχεδιασμού τα περιβαλλοντολογικά προβλήματα, όπως η έλλειψη υδάτινων πόρων. Β) Η δεύτερη, εκτιμά ότι όταν οι μεγάλες τουλάχιστον δυνάμεις θα έχουν οργανωθεί δυνητικά, σε τέτοιο σημείο, ώστε να εξαρτώνται αποκλειστικά από το διαδίκτυο, η μόνη παγκόσμιας εμβέλειας απειλή θα είναι ο κυβερνοπόλεμος.

17. Ορίζεται και αναλύεται στο επόμενο κεφάλαιο.

4.3.4 Δικτυακός Πόλεμος (Net war)

Το διαδίκτυο αποτελείται από μια συνένωση δικτύων Ηλεκτρονικών Υπολογιστών (Η/Υ). Ο Η/Υ είναι ένα αυτοματοποιημένο, ηλεκτρονικό και ψηφιακά προγραμματισμένο σύστημα, το οποίο επεξεργάζεται δεδομένα, βάσει του συνόλου οδηγιών που ονομάζονται προγράμματα (Παπαδάκης, 2002). Αποτελείται από δύο συστατικά μέρη. Το σύνολο των φυσικών εξαρτημάτων και τις κωδικοποιημένες εντολές, δηλαδή το «υλικό μέρος και το λογισμικό» (hardware & software).

Ο Δικτυακός Πόλεμος είναι ένας πόλεμος με στόχο τους Η/Υ του αντιπάλου. Οποιαδήποτε προσβολή αυτών των μερών του διαδικτύου, με σκοπό την αδρανοποίηση ή εν μέρει αλλοίωση του δικτύου του κράτους, μέσω του οποίου συμμετέχει στο παγκόσμιο διαδίκτυο ή υλοποιεί την εσωτερική του ηλεκτρονική διακυβέρνηση, συνιστά Δικτυακό πόλεμο.

4.3.5 Ψυχο-πόλεμος (Psycho war) και Ψυχολογικές Επιχειρήσεις (Psychological Operations – PSYOP) ή Στοχοθετημένη Πληροφόρηση (Targeted Information).

Διάφοροι χαρακτηρισμοί έχουν δοθεί στα όπλα που χρησιμοποιούνται σε αυτούς τους πολέμους, όπως «λεκτικά όπλα», «χάρτινες σφαίρες» και «πολεμοφόδια του μυαλού». Σε αυτή τη διάσταση του πολέμου, πυρήνας στο πεδίο της μάχης, δεν θεωρείται η χρήση βίας, αλλά οι σκέψεις και τα συναισθήματα που προκαλούνται από τη διακίνηση των πληροφοριών. Τυπικά, οι σχετικοί όροι περιγράφουν μια ψυχολογικής (συγκινησιακό-διανοητικής) έντασης μάχη, συγκριτικά με την παραδοσιακή (σωματικής έντασης), η οποία συνέχισε και ως «διαμεσολαβούμενη» μέσω των μηχανών που εξακολουθούσαν να στοχεύουν ύλη και όχι μυαλό ή καρδιά (Taylor, 2004).

Μια από τις αιτίες επιλογής αυτού του είδους μάχης αποτελεί το οικονομικό συμφέρον. Σίγουρα οι σφαίρες είναι πιο ακριβές από το χαρτί και τα αεροσκάφη από τον Η/Υ. Όσον αφορά το ζήτημα της ηθικής, σύμφωνα με την επιχειρηματολογία των υποστηρικτών αυτής της εξέλιξης, αναφέρει ότι είναι προτιμότερο να πεισθούν οι άνθρωποι να μην πολεμήσουν, από το να σκοτωθούν ή να σκοτώσουν¹⁸.

18. Ένα παράδειγμα που επικαλούνται είναι τα παιδικά βιβλία ζωγραφικής που μοιράστηκαν, καθώς και οι αυτοκόλλητες ετικέτες των IFOR (Implementation Force) για να προσέχουν τις νάρκες τα παιδιά της Βοσνίας.

Τέλος, θα πρέπει να υπογραμμιστεί και η στρατηγική διάσταση, δηλαδή ο σχεδιασμός και οι τακτικές επιλογές κατά την πραγματοποίηση, που έχουν καθοριστικό ρόλο.

Ο ορισμός που δίνουν τα στρατιωτικά εγχειρίδια των ΗΠΑ για τις Ψυχολογικές Επιχειρήσεις περιλαμβάνει τις σχεδιασμένες επιχειρήσεις παροχής επιλεγμένων πληροφοριών σε ξένα ακροατήρια με στόχο τον επηρεασμό των συναισθημάτων, του τρόπου σκέψης και τελικά, των κινήτρων συμπεριφοράς ξένων κυβερνήσεων, οργανισμών, ομάδων και ατόμων. Σκοπός είναι η πρόκληση στάσεων συμπεριφοράς ευνοϊκές στην πηγή. Αξιοσημείωτο είναι πως στις ΗΠΑ απαγορεύεται ο σχεδιασμός Ψυχολογικών Επιχειρήσεων στην αμερικανική επικράτεια, ενώ σε άλλες χώρες απαγορεύεται γενικώς στην ειρηνική περίοδο (π.χ. Ελλάδα).

Ενδιαφέρον έχει και ο ορισμός του NATO: Σχεδιασμένες ενέργειες σε καιρό ειρήνης και πολέμου που απευθύνονται σε εχθρικά, φιλικά και ουδέτερα ακροατήρια με σκοπό τον επηρεασμό των στάσεων και της συμπεριφοράς, για την επίτευξη πολιτικών και στρατιωτικών στόχων.

Η πρώτη, εμφανής, παρατήρηση είναι ότι αυτό αποτελεί προπαγάνδα. Παραδοσιακά θεωρείται ότι η προπαγάνδα απευθύνεται σε πολίτες και οι ψυχολογικές επιχειρήσεις σε στρατιώτες. Στην εποχή μας, σταδιακά, θεωρούνται συνώνυμα. Επαρκής ανάλυση για τη λειτουργία της προπαγάνδας και δη, στο διαδίκτυο ως μορφή κυβερνοπολέμου υπάρχει σε παρακάτω κεφάλαιο¹⁹.

Τέλος, για μια επαρκέστερη εικόνα παραθέτουμε τους αντίστοιχους ορισμούς από τα εγχειρίδια του NATO.

- Ψυχολογικές Επιχειρήσεις Σταθεροποίησης (PCA-Psychological Consolidation Activities) καλούνται οι ενέργειες, σε ειρήνη και πόλεμο, που έχουν στόχο τον άμαχο πληθυσμό περιοχών φιλικού ελέγχου, οι οποίες προετοιμάζουν τη συμπεριφορά του κοινού για την ενδεχόμενη στρατιωτική «παρουσία».
- Ψυχολογικές Δραστηριότητες Πεδίου Μάχης (BPA-Battlefield Psychological Activities) καλούνται οι ενέργειες σε περίοδο πολέμου, με σκοπό την άσκηση ψυχολογικής πίεσης στο στρατιωτικό και άμαχο προσωπικό.

- Στρατιωτικές Ψυχολογικές Δραστηριότητες (SPA-Strategic Psychological Operations) καλούνται οι ενέργειες, σε ειρήνη και πόλεμο, με σκοπό την αποθάρρυνση της εμπλοκής μη εχθρικών δυνάμεων.

Εξαιτίας της επιρροής των σύγχρονων ΤΠΕ, ο ρόλος της πληροφορίας έγινε κυρίαρχος στη νέα μορφή πολέμου. Θα λέγαμε ότι παρατηρήθηκε μια μετάβαση του ειδικού βάρους από το συγκινησιακό στο νοητικό επίπεδο. Συνεπεία αυτού, και στα πλαίσια της αναζήτησης του λιγότερο συναισθηματικά φορτισμένου όρου, άρχισε να χρησιμοποιείται η έκφραση «Στοχοθετημένη Πληροφόρηση» (Targeted Information). Οι υποστηρικτές της διατείνονται ότι με αυτόν τον τρόπο οι συγκρούσεις θα τελειώνουν πριν καν αρχίσουν. Έτσι, η Πολεμική Αεροπορία των ΗΠΑ (USAF) συγκρότησε την πρώτη Μοίρα Πολέμου Πληροφοριών (609) στην αεροπορική βάση του Shaw στη Νότια Καρολίνα.

19. Ο όρος «προπαγάνδα» προέρχεται από το λατινικό *propagare* χρησιμοποιήθηκε από την Καθολική εκκλησία για τη διάδοση της πίστης. Συγκεκριμένα, το 1662 ο Πάπας Γρηγόριος ΙΕ΄ εξέδωσε τη σχετική εγκύκλιο (*De Propagande Fide*).

ΜΕΡΟΣ Β΄
Η ΠΡΑΞΗ

Κεφάλαιο 5. Πληροφοριακός Πόλεμος

5.1 Πόλεμος στο πρώτο Οργανωτικό Επίπεδο (Ηγεσία)

Το χαρακτηριστικό γνώρισμα κάθε ηγεσίας είναι το καθήκον της λήψης αποφάσεων, κυρίως στις κρίσιμες στιγμές. Η στρατιωτική ηγεσία λαμβάνει αποφάσεις με αντικειμενικό σκοπό την ασφάλεια της χώρας. Οι προϋποθέσεις για την εύστοχη και έγκαιρη λήψη αποφάσεων είναι τρεις.

- Γνώση των πιθανών απειλών
- Γνώση των τρόπων που αυτές μπορούν να πλήξουν τη χώρα
- Γνώση του τρόπου εξουδετέρωσης της απειλής, αν είναι δυνατόν πριν την ενεργοποίηση της.

Απειλή συνιστά οτιδήποτε μπορεί να πλήξει την ισχύ του κράτους. Η έννοια της απειλής στο σύγχρονο περιβάλλον έχει διευρυνθεί. Παραθέτουμε στον παρακάτω πίνακα τις καταγεγραμμένες ως σημαντικότερες απειλές παγκοσμίως (Ντόκος και Τσάκωνας, 2005).

ΠΑΓΚΟΣΜΙΕΣ ΑΠΕΙΛΕΣ ΤΟΥ ΠΛΑΝΗΤΗ ΤΟΝ 21^ο ΑΙΩΝΑ

1	<u>Δημογραφικό:</u> Υπερπληθυσμός – Μεταναστεύσεις
2	Πρόβλημα επάρκειας και διανομής υδάτων και τροφίμων
3	Εξάπλωση μολυσματικών ασθενειών (AIDS –SARS)
4	Φαινόμενο θερμοκηπίου
5	Οργανωμένο έγκλημα
6	Διακοινοτικές (interethnic) Συγκρούσεις
7	Κυβερνοπόλεμος

Δύο συμπεράσματα μπορούμε να διεξάγουμε από τα παραπάνω στοιχεία. Το πρώτο, από την προηγούμενη παράγραφο, είναι ότι για κάθε ηγεσία είναι απαραίτητος ο μηχανισμός, που (με έμπυχους και τεχνολογικούς πόρους) μπορεί να παρέχει την κατάλληλη

πληροφόρηση για την εκτίμηση των απειλών και τους τρόπους αποτροπής τους. Το δεύτερο συμπέρασμα, το οποίο προκύπτει από τον πίνακα, είναι ότι η πρόοδος των ΤΠΕ έχει ήδη και τα αρνητικά της αποτελέσματα, τα οποία αναδεικνύουν την πιο πρόσφατη απειλή με παγκόσμιες διαστάσεις. Και τα δύο αυτά συμπεράσματα καταλήγουν στον κυβερνοπόλεμο.

Ο τρόπος που λειτουργεί ο κυβερνοπόλεμος, στο πρώτο οργανωτικό επίπεδο, αφορά στην παρακολούθηση (ψηφιακή κατασκοπεία) ή την αλλοίωση (παραπλάνηση με ψηφιακά μέσα) της πληροφοριακής ροής. Ο απώτερος σκοπός βεβαίως είναι η επίδραση στις αποφάσεις της αντίπαλης ηγεσίας ή η γνωστοποίηση των όσων γνωρίζει. Αυτό το είδος του κυβερνοπολέμου, είναι γνωστό ως πληροφοριακός πόλεμος ή πληροφοριοπόλεμος²⁰.

Όπως ήδη αναφέραμε, κάθε ηγεσία έχει ανάγκη από έναν μηχανισμό άντλησης πληροφοριών. Στο στρατιωτικό τομέα αυτό το ρόλο έχουν αναλάβει οι Υπηρεσίες Πληροφοριών. Στη συνέχεια του κεφαλαίου θα περιγραφεί ο τρόπος δόμησης και λειτουργίας του, ώστε να γίνει κατανοητό σε ποια στάδια μπορεί να διεξαχθεί αυτό το είδος του κυβερνοπολέμου.

Αν και οι πρώτες τεχνολογίες σχετικές με τους Η/Υ και τη δικτύωση τους εντοπίζονται στο δεύτερο παγκόσμιο πόλεμο, οι εμφανείς εφαρμογές τους απαντώνται στη δεκαετία του '70. Οι ανάγκες που αναδείχθηκαν από τις Υπηρεσίες Πληροφοριών για τη συλλογή, επεξεργασία και αρχειοθέτηση του τεράστιου όγκου δεδομένων, καθώς και η πρόοδος των πληροφοριακών και επικοινωνιακών συστημάτων έγινε προτεραιότητα των περισσότερων κυβερνήσεων. Στη βιβλιογραφία των στρατιωτικών ακαδημιών θεωρείται ότι είναι αδύνατος ο στρατηγικός σχεδιασμός οποιασδήποτε αμυντικής πολιτικής, χωρίς την επάρκεια του ηλεκτρονικού συστήματος διοικήσεως και ελέγχου στη διάθεση της Ηγεσίας (C4I). Σε αυτό το σύστημα περιλαμβάνονται τα μέσα, οι δυνατότητες χρήσης, η επιχειρησιακή ετοιμότητα και ενδεχόμενες τρωτότητες του συστήματος. Ο επίσημος ορισμός περιλαμβάνει: Ένα αυτοματοποιημένο σύστημα διοίκησης και ελέγχου, το οποίο αποτελείται από τους διευθύνοντες, τα μέσα, τις διαδικασίες και το ειδικό προσωπικό.

20. Ο πόλεμος των Πληροφοριών αποτελεί μια ευρύτερη έκφραση, μέρος της οποίας είναι ο πληροφοριακός πόλεμος. Στον τελευταίο έχει καθιερωθεί η πληροφορία να νοείται μόνο στην ψηφιακή της μορφή, η οποία είναι και ποσοτικώς μετρήσιμη.

Σκοπός είναι η συλλογή, επεξεργασία και ασφαλή διακίνηση (επικοινωνιακή ροή) της πληροφορίας, ώστε να μπορούν να γίνουν ορθές εκτιμήσεις και να ληφθούν οι κατάλληλες αποφάσεις για τους επιλεγμένους στόχους (Λεώνης, 2007). Από το σημείο της πρωτογενούς απόκτησης της πληροφορίας, ως την ολοκληρωμένη παρουσίαση της στην Ηγεσία, μεσολαβούν διαδοχικά τα παρακάτω στάδια.

A. Συλλογή. Πρόκειται για ένα από τα πιο ευαίσθητα στάδια, εξαιτίας δύο λόγων. Ο πρώτος έχει να κάνει με την υψηλή επικινδυνότητα. Ο δεύτερος λόγος συνεπάγεται από το γεγονός ότι η ελλιπής ή διαστρεβλωμένη πληροφόρηση οδηγεί όλο το κύκλωμα σε λάθος εκτιμήσεις. Τρεις είναι οι βασικοί τρόποι συλλογής.

i. Ο *φυσικός*. Αναφερόμαστε στη συλλογή πληροφοριών από την ίδια την ανθρώπινη παρουσία (HUMINT-Human Intelligence). Επικουρικά, χρησιμοποιούνται μέσα όπως φωτογραφικές μηχανές, μαγνητόφωνα, αεροσκάφη κ.τ.λ.

ii. Ο *διαμεσολαβούμενος*. Αναφερόμαστε στη συλλογή πληροφοριών από τα Μέσα Μαζικής Ενημέρωσης. Η ειδοποιός διαφορά είναι ότι εδώ συλλέγονται ήδη επεξεργασμένες πληροφορίες. Σε αυτή την κατηγορία περιλαμβάνονται τα έντυπα, το ραδιόφωνο και η τηλεόραση.

iii. Ο *ψηφιακός*. Αναφερόμαστε στη συλλογή πληροφοριών, στις οποίες δεν έχει παρέμβει άλλο πρόσωπο και έτσι, παραλαμβάνουμε την αυθεντική μορφή. Σε αυτόν τον τρόπο συλλογής ριζική αλλαγή έφερε η υψηλή τεχνολογία του διαδικτύου. Επίσης, συμπεριλαμβάνεται η διαστημική τεχνολογία, κυρίως δε, οι δορυφόροι, των οποίων ο ρόλος εξηγείται σε ειδικό υποκεφάλαιο.

B. Επεξεργασία. Η ανάλυση της πληροφορίας θεωρείται επαρκής όταν η παρουσίαση της είναι ικανή -με τρόπο απλό και κατανοητό- να δείξει αφενός, τα σημεία που ο στόχος είναι ανασφαλής και αφετέρου, τα σημεία που είναι επικίνδυνος για τον αμυνόμενο. Τις προηγούμενες δεκαετίες επρόκειτο μάλλον για μια τυποποιημένη διαδικασία αποκωδικοποίησης δεδομένων. Η διόγκωση της συλλογής με γεωμετρική πρόοδο, κυρίως λόγω του Διαδικτύου, αύξησε τις απαιτήσεις σε επίπεδο μηχανημάτων και εξειδικευμένου προσωπικού. Πλέον, η αυτοματοποιημένη αποκωδικοποίηση θεωρείται η ελάχιστη απαίτηση. Τέλος, το προσωπικό με ικανότητα χρήσης Η/Υ δεν αποτελεί «πρόσθετο προσόν», αλλά απαραίτητο εφόδιο.

Γ. Διακίνηση. Οι απαιτήσεις του σύγχρονου επιχειρησιακού περιβάλλοντος είναι υψηλές. Η αιτία είναι ότι αυτό πλέον διακρίνεται από την ψηφιοποίηση των οπλικών

συστημάτων και την ενοποίηση τους σε μια ενιαία διακλαδική δομή. Αυτό σημαίνει καταρχάς, ότι είναι αδύνατη πλέον, η διεξαγωγή των επιχειρήσεων χωρίς την εκμετάλλευση της ψηφιακής τεχνολογίας με τα χαρακτηριστικά της ακρίβειας και ταχύτητας που τη χαρακτηρίζουν. Κατόπιν, δεν μπορούν να ενεργούν αυτόνομα οι τρεις κλάδοι (στρατός ξηράς, ναυτικό και αεροπορία). Ο επιτελικός -σε πραγματικό χρόνο- συντονισμός της, που στις μέρες μας είναι εφικτός, λόγω των ΤΠΕ, συνιστά ένα μεγάλο «πολλαπλασιαστή ισχύος», κατά τη στρατιωτική ορολογία.

Δ. Προϊόν. Το αποτέλεσμα των παραπάνω τριών φάσεων είναι γνωστό ως πληροφοριακό προϊόν. Οι μορφές που μπορεί να πάρει είναι, είτε της εκτύπωσης σε μια κόλλα αναφοράς, είτε, αν είναι απαραίτητη η αμεσότερη και πληρέστερη (ήχος και εικόνα) ενημέρωση, σε μια οθόνη. Αξιοσημείωτο είναι ότι το προϊόν είναι πάντα ανάλογο του αιτήματος²¹. Το αίτημα θα πρέπει να διατυπώνεται με σαφήνεια, ακρίβεια και με οδηγίες ως προς τις προτιμήσεις της παρουσίασης.

Για να εξηγήσουμε πότε ο τρόπος διατύπωσης, από τους αρμόδιους, εκτιμάται ως ικανοποιητικός, θα χρησιμοποιήσουμε ένα παράδειγμα. Έστω λοιπόν, ότι ένα επιτελείο ζητά μια πληροφορία για την παρούσα κατάσταση σε μια θαλάσσια περιοχή. Θα πρέπει να διευκρινίζεται αν ενδιαφέρει

- τι γίνεται μόνο στη θαλάσσια ή και στην αντίστοιχη εναέρια περιοχή.
- επιπροσθέτως, αν ενδιαφέρει η παρουσία σκαφών σε αυτήν την περιοχή
- ή και όσο το δυνατόν περισσότερες λεπτομέρειες για το περιεχόμενο. Τέλος, αν η «έξοδος» της πληροφορίας θα είναι
 - σε μορφή εικόνας-ήχου,
 - αριθμητικών δεδομένων ή
 - γραφικών παραστάσεων.

Η ισορροπία, η οποία θα πρέπει να τηρηθεί, είναι μεταξύ της ποσότητας για την επάρκεια στη ζήτηση ικανοποιητικών στοιχείων και τη χρονική συνθήκη. Δηλαδή, όσο περισσότερα ζητούνται, τόσο περισσότερο θα καθυστερεί η απάντηση.

21. Θεμελιώδης Αρχή της Θεωρίας της Ανάκτησης Δεδομένων στο διαδίκτυο είναι ότι οι απαντήσεις (των μηχανών αναζήτησης) είναι ανάλογες της ακρίβειας της διατύπωσης των ερωτημάτων.

5.2 Η αξιοποίηση των ΤΠΕ από τον Στρατιωτικό τομέα (C4ISR) (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)

Η διεξαγωγή του κυβερνοπολέμου στο οργανωτικό επίπεδο της Ηγεσίας, εστιάζεται στον έλεγχο των πληροφοριών που έχει στη διάθεση του ο αντίπαλος. Οι τρόποι που μπορεί να συμβεί αυτό, καθώς και οι διαδικασίες που ακολουθούνται, θα αναλυθούν στη συνέχεια. Ένα συνηθισμένο φαινόμενο στην ιστορία της επιστήμης είναι ότι οι περισσότερες μεγάλες εφευρέσεις εφαρμόζονται πρώτα στον στρατιωτικό τομέα. Το ίδιο συνέβη και με τη ραγδαία ανάπτυξη των ΤΠΕ. Η συνειδητοποίηση του μεγίστου ρόλου της επικοινωνίας και πληροφορίας για τη διεξαγωγή των στρατιωτικών επιχειρήσεων οδήγησε τις ηγεσίες των χωρών να εντείνουν τις προσπάθειες τους για τη βελτίωση της αποτελεσματικότητας σε αυτόν τον τομέα. Αν εμβαθύνουμε στο ρόλο της στρατιωτικής ηγεσίας μιας μεγάλης δύναμης των τελευταίων δεκαετιών, των ΗΠΑ, τότε μπορούμε να παρατηρήσουμε την ακόλουθη διαδοχική διαδικασία. Η στρατιωτική ηγεσία γνωστοποιεί στην αντίστοιχη πολιτική ότι μέχρι την εποχή του ψυχρού πολέμου, συγκριτικό πλεονέκτημα είχαν τα κράτη που διέθεταν πυρηνικό οπλοστάσιο (εφαρμογή της υψηλής στρατηγικής της εκμηδένισης). Μετά την πτώση του «ανατολικού μπλοκ», αποδοτικότερη είναι η υψηλή στρατηγική της εξουθένωσης του αντιπάλου (Πλατιάς, 2000), που απαιτεί γνώση (επεξεργασμένες πληροφορίες) και αμεσότητα δράσης (διαλειτουργική επικοινωνία). Μετά από αυτή τη διάγνωση στον στρατιωτικό τομέα, η πολιτική ηγεσία αποφάσισε να ανταποκριθεί (θα το δείξουμε παρακάτω με τις ομιλίες του προέδρου στο κογκρέσο). Και τέλος, η οικονομική ηγεσία να επενδύσει σε αυτή την τεχνολογία.

Το αποτέλεσμα της διαδικασίας που περιγράψαμε ήταν το ολοκληρωμένο σύστημα για την υψηλής τεχνολογίας υποστήριξη στις αμυντικές υποθέσεις (C4ISR- Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Όπως προκύπτει και από την επωνυμία, ο αντικειμενικός του σκοπός συνίσταται από την υποστήριξη των λειτουργιών της Διοίκησης, του Ελέγχου, των Επικοινωνιών, των Υπολογιστών, των Πληροφοριών, της Επιτήρησης και της Αναγνώρισης. Ένα τελευταίο και εξίσου σημαντικό στοιχείο είναι ότι αυτές οι λειτουργίες θα πρέπει να είναι άριστα συντονισμένες (αναφερόμαστε στον αποφασιστικής σημασίας ρόλο της διαλειτουργικότητας).

Η διοίκηση των πληροφοριών αποτελεί πλέον το στοιχείο που δίνει το συγκριτικό πλεονέκτημα στο διεθνή ανταγωνισμό για τη στρατιωτική ισχύ. Αυτό οδηγεί στην προτροπή για υψηλή ειδίκευση των ανθρωπίνων πόρων και τη διάθεση μηχανημάτων σύγχρονης τεχνολογίας. Ειδικότερο ρόλο σε αυτόν τον τομέα έχουν η δορυφορική επισκόπηση, τα δίκτυα των ραντάρ και το διαδίκτυο (Πολυμενόπουλος, 2001).

Με τη χρήση των νέων ΤΠΕ ο στρατός δεν δρα μόνο στα στενά γεωγραφικά σύνορα. Η συμμετοχή στον Κυβερνοχώρο άλλαξε τους χωροχρονικούς περιορισμούς του παρελθόντος. Με τον κυβερνοπόλεμο ο αντίπαλος έχει τη δυνατότητα να πλήξει εγχώριες υποδομές από απόσταση. Κατά αυτόν τον τρόπο η έννοια της ασφάλειας διευρύνεται και ο ρόλος του στρατού αποκτά επιπλέον καθήκοντα. Οι κύριοι άξονες αυτών των καθηκόντων είναι τρεις.

- Η επικουρική λειτουργία στη λήψη αποφάσεων, ταξινομώντας και συνοψίζοντας την «άναρχη» διακίνηση της πληροφορίας μέσω διαφόρων εφαρμογών (data mining & data warehousing). Παράλληλα οφείλουν να φροντίζουν τη συνεχή αλληλεπίδραση με το χρήστη.
- Σημαντική παράμετρος είναι η επαγρύπνηση στην ασφάλεια των δικτύων, καθώς και η παρακολούθηση των διεργασιών που συντελούνται. Σε αυτή την κατεύθυνση συμβάλλουν οι κρυπτογραφικές τεχνικές (στο ρόλο των οποίων αφιερώνουμε ειδικό υποκεφάλαιο) και η υλοποίηση των πρωτοκόλλων συνεχούς ροής σε συνθήκες υπερφόρτωσης, για την αποφυγή διακοπής της σύνδεσης.
- Η διασύνδεση μέσω ενός εσωτερικού διαδικτυακού τόπου (Intranet).

Όπως επισημάναμε προηγουμένως, σε μια διάσταση υψηλής αξίας αναδεικνύεται η επίτευξη της διαλειτουργικότητας. Οι ανεπτυγμένες χώρες έχουν εκτιμήσει τη χρησιμότητα της, ώστε να την υπογραμμίζουν στο σχετικό αμυντικό τους Δόγμα. Στους ορισμούς του NATO η διαλειτουργικότητα ορίζεται ως «η ικανότητα των συστημάτων των δυνάμεων να παρέχουν και να δέχονται υπηρεσίες σε και από άλλα συστήματα ή δυνάμεις. Σκοπός είναι η αποδοτική ανταλλαγή τους» (<http://www.nato.int>, 2007).

Οι αρχές της αποδοτικής διαλειτουργικότητας είναι οι εξής:

- Χρήση προτύπων (standards)
- Συντονισμός ενεργειών
- Κοινή αντίληψη πληροφοριών
- Ομοιογενές πεδίο διεργασιών
- Σαφής διαχωρισμός ρόλων των αρμοδιοτήτων.

Η διαλειτουργικότητα μπορεί να είναι οριζόντια (παράδειγμα μεταξύ των τριών κλάδων, Στρατού Ξηράς, Ναυτικού και Αεροπορίας) ή κάθετη (παράδειγμα μεταξύ πολιτικής και στρατιωτικής ηγεσίας).

5.3 Παράδειγμα: Η Ανάλυση του Μοντέλου των ΗΠΑ

Οι ΗΠΑ θεωρούνται πρωτοπόρες σε αυτόν τον τομέα. Το συγκεκριμένο μοντέλο, που έχει επιλεγεί, ολοκληρώνεται σε πέντε κλίμακες πολυπλοκότητας.

- (0) Απομονωμένη. Χειρωνακτική ανταλλαγή (manual gateway-hard copies)
- (1) Συνδεδεμένη. Ηλεκτρονική σύνδεση (tactical data links, e-mail e.t.c.)
- (2) Λειτουργική. Κοινό περιβάλλον εργασίας (data with explanations...)
- (3) Διοικήσεις. Κοινά στοιχεία – χωριστές εφαρμογές (Common Data Bases)
- (4) Ηγεσία. Παρουσίαση διαλογικής ανάλυσης (High classification).

Αρχικός στόχος της διαβάθμισης των λειτουργιών είναι η υποβάθμιση της αβεβαιότητας, η εξοικονόμηση χρόνου μέσω της αποφυγής περιττών ενασχολήσεων και η διασφάλιση της διαρροής πληροφοριών. Αξιοσημείωτο είναι ότι έχει διαμορφωθεί ένας μηχανισμός εκτίμησης του εκάστοτε αποτελέσματος, ο οποίος παρατηρεί την απόκλιση των απαντήσεων (σε πιλοτικά ερωτήματα) από την πραγματικότητα.

Τα πιο σημαντικά οφέλη είναι:

- Δυνατότητα ακριβέστερων εντολών, λόγω της αναπαράστασης των γεγονότων σε πραγματικό χρόνο.
- Μείωση του χρόνου λήψης και διαβίβασης των αποφάσεων.
- Ταχύτερος κι ακριβέστερος εντοπισμός των βλαβών ή προβλημάτων συντονισμού, κατά τη διάρκεια της λειτουργίας.

5.3.1 Το θεωρητικό υπόβαθρο

Στη συνέχεια θα αναλύσουμε το θεωρητικό πλαίσιο, στο οποίο χρησιμοποιείται η προσομοίωση κυρίως για εκπαιδευτικούς λόγους. Τα πολύπλοκα συστήματα λοιπόν, έχουν εγγενή απροβλεψιμότητα. Οι γενικές βεβαιότητες του παρελθόντος για τη διεύθυνση και τον έλεγχο δεν ισχύουν. Μια εφαρμογή αποτελεί η ερμηνευτική των σύγχρονων οργανώσεων. Σύμφωνα με την Ομάδα της Σάντα Φε (1996) «η πολυπλοκότητα αναφέρεται στην κατάσταση του σύμπαντος, το οποίο αν και είναι ολοκληρωμένο, δεν μπορούμε να το κατανοήσουμε με εκείνον τον απλό τρόπο, ώστε να τον ερμηνεύσουμε με κοινούς (μηχανιστικούς ή γραμμικούς) νόμους. Η πολυπλοκότητα ασχολείται με τη φύση της αναδυτικότητας, της καινοτομίας, της μάθησης και προσαρμογής». Ένας από τους ιδρυτές της, ο νομπελίστας Μάρεϋ Γκελ-Μαν, δηλώνει πως κύριο χαρακτηριστικό της

είναι η απαίτηση για συνολική έρευνα του συστήματος, διότι η εξέταση των μερών του δεν οδηγεί σε ασφαλή συμπεράσματα.

Στην παραδοσιακή επιστήμη ένα σύστημα μπορεί να οριστεί όταν είναι δυνατός ο έλεγχος της συμπεριφοράς του (προβλεψιμότητα). Αυτό ακριβώς δεν μπορεί να γίνει στον άνθρωπο, τον καιρό και τους σεισμούς, που είναι πολύπλοκα συστήματα. Για να αντιμετωπιστεί αυτή η αδυναμία χρησιμοποιείται η προσομοίωση. Χαρακτηριστικά διατυπώθηκε από τον ειδικό Μάικλ ΜακΜάστερ «δεν αναφέρεται στον κλασικό τρόπο αναλυτικής προσέγγισης, αλλά δημιουργίας». Το πρώτο στάδιο αφορά τη μοντελοποίηση, δηλαδή την κατασκευή θεματικών μοτίβων, που λειτουργούν ως προγράμματα H/Y. Μια γνωστή εφαρμογή είναι η θεωρία των παιγνίων.

Επίκεντρο της παρατήρησης αποτελούν οι αναδύμενες συμπεριφορές που επαναλαμβάνονται στο πλαίσιο των βιολογικών, τεχνολογικών και ευρύτερα, συστημάτων της συμπεριφοράς. Η μελέτη της πολυπλοκότητας από την πλευρά της πληροφορίας (δηλαδή, πότε έχουμε έναν ικανό αριθμό για να μπορούμε να περιγράψουμε κάτι), οδηγεί στο συμπέρασμα ότι η επάρκεια στην έρευνα εξαρτάται από την πλευρά του παρατηρητή.

Όλα τα παραπάνω συνδέονται με το θέμα της οργάνωσης όταν αντιληφθούμε ότι διαχρονικά το αντικείμενο του μανάτζμεντ ήταν η αναζήτηση αιτιοκρατικών σχέσεων στα μέρη του συστήματος, με τη διαχείριση των οποίων θα διατηρείται ο έλεγχος. Η δυνητική οργάνωση ανέτρεψε αυτήν την προσδοκία, όπως εξηγήσαμε σε προηγούμενο κεφάλαιο. Η πολυπλοκότητα στις σχέσεις των σημερινών συστημάτων επέτρεψε την ανάδυση χαοτικών καταστάσεων. Χαοτική καλούμε την κατάσταση που δεν επιδέχεται πρόβλεψη (και άρα κατασκευή μοτίβων, δημιουργία προσομοίωσης και τελικά, έλεγχος). Το επόμενο βήμα ήταν η μελέτη συστημάτων προσαρμοζόμενα πολύπλοκων. Ο επιθετικός προσδιορισμός «προσαρμοζόμενα» υποδηλώνει την εξάρτηση του συστήματος από το περιβάλλον του και την τάση εναρμόνισης του με αυτό (μάθηση – αυτό-οργάνωση – προσαρμογή). Τέτοια συστήματα είναι τα πολιτικά, οικονομικά και πολιτισμικά (Μπάτραμ, 2001).

Για να δείξουμε πώς λειτουργεί το φαινόμενο της «Αναδυτικότητας» στην περίπτωση του κυβερνοπολέμου, θα δεχθούμε ως υπόθεση εργασίας ότι το σύνολο των κρατών αποτελούν ένα τέτοιο σύστημα. Κατανοούμε εξ αρχής ότι η δράση καθενός χωριστά μπορεί να εξυπηρετεί το συμφέρον του, αλλά η παγκόσμια τάση (στο σύστημα) αφορά μια ανάδυση των εν μέρει αλληλεπιδράσεων. Το σύστημα είναι πολύπλοκο προσαρμοζόμενο, διότι το

μερικό συμφέρον των συστατικών του στοιχείων εναρμονίζει τη συμπεριφορά του σε αυτή την κοινή συνισταμένη της παγκόσμιας τάσης. Και τέλος, όπως φαίνεται από μια στοχαστική αναδρομή στην ιστορία, δυναμική πορεία διαγράφουν οι «προσαρμοστικώς νοήμονες δρώντες» (Πριγκοζίν, 1996).

Στο στρατιωτικό τομέα έγινε γρήγορα κατανοητό ότι η δυνατότητα πρόβλεψης στο πεδίο της μάχης είναι κάτι πολύ σχετικό. Η κατανόηση για τη δυσχέρεια της πρόβλεψης επιδεινώθηκε ακόμα περισσότερο με τις σύγχρονες ΤΠΕ, οι οποίες δημιούργησαν τις συνθήκες εμφάνισης του κυβερνοπολέμου. Ο δρόμος ετοιμασίας για την άμυνα με αποτελεσματική αποτροπή πέρναγε αναμφισβήτητα από την ειδική εκπαίδευση των στελεχών. Η διαδικασία που ακολουθήθηκε λειτουργεί μέσα στα πλαίσια της πολυπλοκότητας που περιγράφηκε. Κυρίως, ακολουθεί τα στάδια της Μοντελοποίησης και Προσομοίωσης, εκτιμώντας τελικά, την επιχειρησιακή ετοιμότητα. Για να εξηγήσουμε πώς όλα αυτά πραγματοποιήθηκαν θα πρέπει πρώτα να ορίσουμε την έννοια του Συστήματος σε αυτήν τη διαδικασία.

Σύστημα καλούμε ένα σύνολο μερών, ένα «προσλαμβανόμενο όλο». Τα μέρη αλληλεπιδρούν στην κατεύθυνση επίτευξης κάποιου στόχου. Τα χαρακτηριστικά γνωρίσματα της συμπεριφοράς των μερών είναι η Δράση και η Αλληλόδραση. Ένα σύστημα, εξ ορισμού, υπάγεται σε ένα ευρύτερο σύστημα. Το ενδιαφέρον που παρουσιάζει η μεθοδολογία είναι το γεγονός ότι η δράση μεμονωμένων στοιχείων του συστήματος δημιουργεί σημαντικές επιδράσεις στο συνολικό επίπεδο του συστήματος. Πολύ περισσότερο αυτό ισχύει για την διαντίδραση των στοιχείων αυτών. Η εμπειρία έδειξε ότι τα περισσότερα συστήματα είναι προσαρμοστικά. Η μεθοδολογία παρουσιάζει ομοιότητες αλλά και σημαντικές διαφορές με τις μικρο (micro) εκδοχές των κοινωνικών κυρίως επιστημών. Ένα εξαιρετικό εύρημα αποτελεί το γεγονός ότι απλοί κανόνες για την ατομική δράση επιφέρουν σημαντικά αποτελέσματα σε μια ομάδα, ένα δίκτυο ή ένα σύστημα.

Η εμφάνιση πολύπλοκης, μη γραμμικής συμπεριφοράς έγινε στα στοιχεία της Δράσης, του Χρόνου και του Χώρου. Το βασικό χαρακτηριστικό της αλληλόδρασης είναι το γεγονός ότι η δράση κάθε ατόμου ενδέχεται να αποτελεί αντίδραση στη δράση άλλου ατόμου ή κατάστασης (Sequential or discrete process). Επίσης, το βασικό στοιχείο της δράσης είναι ότι οι αλληλεπιδράσεις που παράγονται τοπικά, έχουν και σημαντική επίδραση στο σύνολο (δίκτυο ή σύστημα). Συστατικά της είναι οι Ευφυείς Οντότητες, οι οποίες μπορεί

να είναι στοιχεία, άτομα, ενώσεις στοιχείων ή ατόμων (meta agents), ομάδες, επιχειρήσεις, ή και το κράτος.

Τα βασικά δομικά τους στοιχεία είναι:

α) η Δράση (action), οι σκόπιμες ενέργειες των ατόμων, οι οποίες διακρίνονται από τον περισσότερο ασαφή όρο συμπεριφορά.

β) η Αλληλόδραση (interaction) αναφέρεται στις σκόπιμες ενέργειες του ατόμου ως απόρροια της επίδρασης που δέχεται από ένα άλλο άτομο, ομάδα ή σύνολο ατόμων.

γ) οι Επιθυμίες (Desires) εκφράζουν μια έλξη ή προδιάθεση προς μια κατάσταση είτε ενεργητική είτε ουδέτερη

δ) οι Πεποιθήσεις (Beliefs) μπορούν να ορισθούν ως μια πρόταση για την κατάσταση του περιβάλλοντος την οποία ο φορέας της πεποίθησης θεωρεί αληθή.

ε) οι Ευκαιρίες (Opportunities) εκφράζουν το εύρος των εν δυνάμει εναλλακτικών δράσεων έναντι της αλληλεπίδρασης και υπάρχουν ανεξάρτητα από τις επιθυμίες και τις πεποιθήσεις.

Οι επιθυμίες, πεποιθήσεις και ευκαιρίες αποτελούν την αιτία εκδήλωσης δράσης. Στο βαθμό που επηρεάζονται από δράση τρίτου αποτελούν το σύνδεσμο ανάμεσα στη δράση και αλληλόδραση.

Κεφάλαιο 6. Ηλεκτρονικός Πόλεμος

6.1 Πόλεμος στο δεύτερο Οργανωτικό Επίπεδο (Μέσα)

Σε αυτό το κεφάλαιο θα δείξουμε τον τρόπο με τον οποίο δραστηριοποιούνται οι εμπλεκόμενοι σε έναν κυβερνοπόλεμο, όταν στόχο τους αποτελεί η προσβολή των μέσων του αντιπάλου. Με τον όρο «μέσα», προσδιορίσαμε σε προηγούμενο κεφάλαιο, όλα τα όπλα -σύγχρονης ή μη τεχνολογίας- που χρησιμοποιούνται σε μια μάχη. Άρα στον κυβερνοπόλεμο περιλαμβάνονται τα μέσα υψηλής τεχνολογίας, τα οποία εξυπηρετούν τη διάδραση στον κυβερνοχώρο. Ειδικότερα για τον ηλεκτρονικό πόλεμο, επιχειρώντας μια πιο αυστηρή διατύπωση, ορίζεται κάθε στρατιωτική κίνηση, η οποία απαιτεί ηλεκτρομαγνητική ενέργεια για τον έλεγχο του ηλεκτρομαγνητικού φάσματος²² (Πολυμενόπουλος, 2001).

Στον ηλεκτρονικό πόλεμο δύο είναι οι πιθανοί στόχοι. Ο πρώτος αφορά στην καταστροφή των οπλικών συστημάτων. Ένα συνηθισμένο είδος υλοποίησης του αποτελεί η χρήση λέιζερ (lasers) στο πεδίο της μάχης. Τα λέιζερ χαμηλής ισχύος εκπέμπουν λάμπες, με αποτέλεσμα τον αποπροσανατολισμό του εχθρού και την καταστροφή των αισθητήρων που διαθέτει. Τα λέιζερ υψηλής ισχύος μπορούν να καταστρέψουν σημαντικά μέρη ή ολοκληρωτικά το δίκτυο διασύνδεσης, με συνέπεια να καταστήσουν τον αντίπαλο εκτός κυβερνοχώρου (off line). Ο δεύτερος στόχος επιχειρεί την εισβολή και αλλοίωση του δικτύου, με στόχο τη διαστρέβλωση της διασποράς των πληροφοριών.

Ωστόσο είναι σημαντική η φροντίδα του οικείου εξοπλισμού. Συχνά ο φόβος της επίθεσης κατευθύνει την προσοχή στις κινήσεις του εχθρού και αυτό έχει ως συνέπεια τη μείωση της ετοιμότητας. Ειδικότερα στα μέσα, αυτό μπορεί να λάβει της ακόλουθες εκφάνσεις (Λεωνής, 2006).

- Οι επιχειρήσεις με αβέβαιο γεωγραφικό προσανατολισμό. Όταν το πεδίο ανάλυσης δεν είναι εξαρχής συγκεκριμένο, δημιουργούνται προβλήματα εστιασμού της αναπαράστασης. Κάποιες λύσεις έχουν δοθεί από τη συλλογή των χωρικών (spatial) και περιγραφικών (attribute) πληροφοριών, από τα Γεωγραφικά Συστήματα Πληροφοριών (G.I.S.- Geographical Systems Information) και ιδιαίτερα στη συνεργασία τους με τους δορυφόρους.

22. Ηλεκτρονικό φάσμα καλείται το εύρος των συχνοτήτων της ηλεκτρομαγνητικής ακτινοβολίας από το μηδέν ως το άπειρο.

- Η ενσωμάτωση ανασφαλών δορυφορικών συστημάτων εμποδίζει το συντονισμό των μερών (υποσυστήματα) του ολοκληρωμένου συστήματος, καθυστερεί τη ροή των δεδομένων και αυξάνει τους γεωγραφικούς περιορισμούς των επίγειων δικτύων.
- Η ταχύτητα εξέλιξης της σύγχρονης ΤΠΕ έχει ως συνέπεια ακριβά και μεγάλων επιδόσεων μηχανήματα να απαξιώνονται γρήγορα. Έτσι, η αρχική αρχιτεκτονική σχεδίαση για την επίτευξη της εν γένει στοχοθέτησης δεν αποδίδει. Βεβαίως, η αρχιτεκτονική σχεδίαση όλου του συστήματος είναι καθοριστικής σημασίας για την αποτελεσματικότητα των δικτύων.
- Ένα τελευταίο σημείο τρωτότητας είναι η έλλειψη του απαραίτητου εξοπλισμού. Τα βασικότερα εργαλεία, εκτός των συστημάτων γεωγραφικού προσανατολισμού κι απεικόνισης και της αξιοποίησης της διαστημικής τεχνολογίας, είναι οι επαρκώς ενημερωμένες βάσεις δεδομένων, οι υψηλής τεχνολογίας μηχανές, καθώς και τεχνικές κρυπτογράφησης και προσομοίωσης και τέλος, οι σύγχρονες μορφές τηλεπισκόπησης και ψηφιακής χαρτογράφησης.

6.2 Μέθοδοι Κυβερνο-επίθεσης και Κυβερνο-άμυνας

Άλλη μια περίπτωση που φαίνεται ότι μεταξύ των εκφράσεων «Ηλεκτρονικός πόλεμος και Δικτυακός πόλεμος» έχει επικρατήσει η πρώτη, αποτελεί το κινεζικό δόγμα των αντίστοιχων επιχειρήσεων. Η κινεζική στρατιωτική ηγεσία θεωρεί ενιαίες τις ενέργειες των επιχειρήσεων δικτύων (Computer Network Warfare) και του ηλεκτρονικού πολέμου (Electronic Warfare). Ειδικότερα, πέρα της θεωρητικής προσέγγισης, προχώρησαν στην υλοποίηση, δημιουργώντας και το πρώτο τάγμα δίκτυο-ηλεκτρονικών επιχειρήσεων. Αυτό αποτελείται από ένα Λόχο τηλεπικοινωνιών, ένα Λόχο επιχειρήσεων δικτύων Η/Υ και ένα Λόχο ηλεκτρονικού πολέμου²³. Εξάλλου στην εποχή μας τα όρια μεταξύ λογισμικού (software) και υλικών εξαρτημάτων (hardware) των Η/Υ είναι δυσδιάκριτα.

Σχετικά με τις κυβερνοεπιθέσεις, θα πρέπει να τονίσουμε ότι πρόκειται για τις εφαρμογές μιας τεχνολογίας σύνθετης και πολλαπλής ως προς τους τρόπους υλοποίησης της. Ωστόσο η λογική που ακολουθείται για την υπονόμηση των συστημάτων πληροφορίας και επικοινωνίας του κράτους, είναι απλή. Το γενικότερο πλαίσιο της κυβερνοεπίθεσης στο δεύτερο οργανωτικό επίπεδο συνοψίζεται στην αποστολή και ενσωμάτωση ειδικών προγραμμάτων στα ξένα συστήματα, με σκοπό την αφανή αλλοίωση των λειτουργιών ή την ολική καταστροφή τους. Συνήθως η έκφραση που χρησιμοποιείται για αυτά είναι «υποχθόνια λογισμικά»²⁴. Τα γνωστότερα είδη αυτών των λογισμικών είναι οι «ιοί» (computer viruses), τα «σκουλήκια» (computer worms), τα «τρωικά άλογα» (Trojan horses) και οι «λογικές βόμβες» (logical bombs).

Οι τρόποι εγκατάστασης περικλείουν από τους κλασικούς τρόπους ηλεκτρονικής επικοινωνίας (όπως το email) μέχρι τις πιο σύγχρονες μεθόδους εξουδετέρωσης των μέσων, όπως:

- με τη χρήση νανομηχανών (μικροσκοπικά ρομπότ, με ανάλογο προγραμματισμό).
- με τη χρήση μικροβίων (τα οποία «τρέφονται» με οτιδήποτε περιέχει πυρίτιο, συστατικό των ηλεκτρονικών συσκευών).
- με την τεχνική chipping (διαδικασία κατασκευής microchips. Αυτά απελευθερώνουν έναν ιό ή ένα «σκουλήκι», τα οποία αποθηκεύονται στη μνήμη ROM και εκεί προξενούν την καταστροφή).

23. Dai Qingmin (2002) *On Integrated Network Warfare and Electronic Warfare* China Military Science (pp.112-117).

24. Winn Schwarau (1996) *Information Warfare*. Thunder's Mouth Press.

- με τη χρήση όπλων ραδιοφωνικού σήματος υψηλής ενέργειας και βομβών ηλεκτρομαγνητικού παλμού. Η εκπομπή παλμών ισχύος δεκάδων δισεκατομμυρίων Watt (Terra Watt) προξενεί βλάβη σε ηλεκτρονικά κυκλώματα μεγάλων αποστάσεων.

Στην κυβερνοάμυνα, η προστασία των συστημάτων επιτυγχάνεται σε πέντε διαδοχικά μέρη.

- Πρόληψη. Θα μπορούσε να χαρακτηριστεί το σημαντικότερο μέρος, εφόσον η «θωράκιση» των οικείων συστημάτων με απρόσβλητους μηχανισμούς, εξυπηρετεί στην αποφυγή δέσμευσης πόρων (ανθρώπινων, οικονομικών κ.λπ.).
- Ανίχνευση προσβολής. Στην περίπτωση που το πρώτο μέρος δεν είναι επαρκές, θα πρέπει να υπάρχει εν ενεργεία υποδομή. Ο βασικός ρόλος θα είναι αυτός του συναγερμού, διότι ανεξαρτήτως της δυνατότητας αποτροπής της ζημιάς, η άμεση παύση, στον εφικτό βαθμό, των διεργασιών και οι απαραίτητες αποθηκεύσεις των δεδομένων είναι αναγκαία.
- Αποτροπή. Από τη στιγμή της σήμανσης του δεύτερου μέρους, σχεδόν ταυτόχρονα θα πρέπει να ενεργοποιηθούν οι διαδικασίες ανίχνευσης και ταυτοποίησης του τύπου της επίθεσης, για να εκτιμηθεί ο πιο αποτελεσματικός τρόπος εξουδετέρωσης.
- Προσαρμογή. Αποτελεί κοινή παραδοχή ότι η ταχύτατη εξέλιξη των ΤΠΕ αναδύει απρόβλεπτες δυσλειτουργίες σε όσους δεν μπορούν εγκαίρως να προσαρμοστούν. Είναι προφανείς οι κίνδυνοι που δημιουργούνται από έναν εχθρό ιδιαίτερος προηγμένο τεχνολογικά.
- Αντεπίθεση. Σε αντίθεση με το προηγούμενο μέρος, η υπεροχή στην εφαρμοσμένη τεχνολογία του κυβερνοπολέμου παρέχει το πλεονέκτημα του αιφνιδιασμού, εξάλλου όπως είναι γνωστό «καλύτερη άμυνα είναι ή επίθεση».

6.3 Διαστημική Τεχνολογία

Η εκμετάλλευση των τεχνολογικών επιτευγμάτων από το στρατό επιδρούσε ανέκαθεν στο θέμα της κυριαρχίας και της οργάνωσης. Ένα χαρακτηριστικό παράδειγμα αποτελεί η χρήση της πυρίτιδας στον πόλεμο. Η συγκεκριμένη επίδραση στο θέμα της κυριαρχίας ήταν η κατάκτηση της Κωνσταντινούπολης το 1453, από τους Οθωμανούς, οι οποίοι εξαιτίας της βελτιωμένης χρήσης πυρίτιδας²⁵ είχαν συγκριτικό πλεονέκτημα έναντι των βυζαντινών. Στο θέμα της οργάνωσης παρατηρήθηκε ότι μετά από αυτή την εξέλιξη, από τις μικρές πόλεις-κράτη συγκροτήθηκαν μεγάλα κράτη-αυτοκρατορίες (Κολοβός, 1995).

Την ανάλογη επίδραση στους διεθνούς ανταγωνισμούς κυριαρχίας είχε η εμφάνιση της πυρηνικής τεχνολογίας και η στρατιωτική εφαρμογή της στην ατομική βόμβα²⁶, στον προηγούμενο αιώνα. Στο νέο αιώνα τη σκυτάλη παραλαμβάνει ο έλεγχος της Πληροφορίας. Η υπεροχή στο κύκλωμα της πληροφοριακής ροής (το οποίο αναλύθηκε στο προηγούμενο κεφάλαιο), δημιουργεί νέο πλεονέκτημα στα ζητήματα κυριαρχίας. Διάφοροι μέθοδοι έχουν εφευρεθεί για αυτόν το σκοπό, όπως οι ανιχνευτές σε αεροπλάνα, μη επανδρωμένα οχήματα²⁷ και στους δορυφόρους.

Οι δορυφόροι έχουν τη δυνατότητα συλλογής πληροφοριών σε δυσχερείς καιρικές συνθήκες (παντός καιρού) από μεγάλες αποστάσεις. Σημαντική είναι η ικανότητα τους να εντοπίζουν, να αναγνωρίζουν και αποστέλλουν μια πλήρη ενημέρωση (δηλαδή, συντεταγμένες γεωγραφικής θέσης, χαρακτηριστικά και λειτουργία αντικειμένου) για ένα στόχο. Με αυτό τον τρόπο άρχισε η διεξαγωγή πολέμων από απόσταση, με πρόσφατα παραδείγματα στο Ιράκ, Βοσνία και Αφγανιστάν. Πλέον, παρατηρούμε την καθιέρωση των συρράξεων «χειρουργικής ακριβείας». Χαρακτηριστική είναι η δήλωση του πρώην υπουργού εθνικής άμυνας των ΗΠΑ σχετικά με τα συμπεράσματα από την «Καταιγίδα της Ερήμου»: *Οι ΗΠΑ ήρθαν αντιμέτωπες με έναν εχθρό σίγουρα κατώτερης ισχύος. Τον νίκησαν γρήγορα με χαμηλό κόστος πόρων. Δόθηκε το κίνητρο διατήρησης της δύναμης στην αναγνώριση και κρούση, η οποία λειτουργεί κι ως πυρηνική αποτροπή. Η «ομπρέλα των πληροφοριών» που θα παρέχουν οι ΗΠΑ στους συμμάχους τους, θα αποτελέσει τη μετάβαση από την «πυρηνική ομπρέλα» του παρελθόντος (Perry, 1998).*

25. Κύριο πλεονέκτημα στο πεδίο της μάχης ήταν η εκπόρθηση των επιβλητικών, αλλά αδύναμων πλέον, αμυντικά, κάστρων. Επίσης, ίδιο αποτέλεσμα είχε η χρήση της από τους Γάλλους έναντι των Ιταλών και από τους Ρώσους έναντι των Μογγόλων.

26. Αύγουστος 1945 στη Χιροσίμα και το Ναγκασάκι της Ιαπωνίας.

27. Πρόκειται για τα γνωστά UAV, των οποίων η περιγραφή ακολουθεί σε Παράρτημα.

Από το προηγούμενο απόφθεγμα είναι σαφές πόσο σημαντική αξιολογείται η δυνατότητα απόκτησης πληροφοριών για την κυριαρχία ενός κράτους. Η θέση της διαστημικής τεχνολογίας εδώ είναι καθοριστική. Μετά τους ιστορικούς διαδοχικούς ανταγωνισμούς ισχύος στην ξηρά, τη θάλασσα και τον αέρα, το διάστημα απετέλεσε το μεταβατικό στάδιο για την επιζήτηση της κυριαρχίας στον κυβερνοχώρο. Μια ενδιαφέρουσα προέκταση εδώ, είναι η ανάδυση από αυτήν την εξέλιξη της ανάγκης για συνεργασία. Σε πρώτη φάση των τριών παραδοσιακών κλάδων (στρατού ξηράς, ναυτικού και αεροπορίας), η οποία (όπως εξηγήθηκε) καλύπτεται από τον όρο «διαλειτουργικότητα».

Σε δεύτερη φάση, την ανάγκη για συνεργασία των κρατών, τα οποία κατανοούν ότι στο χώρο του διαστήματος, καθώς και στον κυβερνοχώρο, η έννοια της συνεργατικότητας²⁸ αποκτά καινούρια σημασία. Η πραγματική ενασχόληση του ανθρώπου με το Διάστημα διαδραματίζεται τον τελευταίο μισό αιώνα. Το πρώτο μέσο για να επικοινωνήσουμε με αυτόν τον άγνωστο χώρο ήταν οι δορυφόροι. Ένα δορυφορικό σύστημα συνίσταται, όπως και οι Η/Υ, από το υλικό (π.χ. επίγειοι σταθμοί δορυφόρων) και το λογισμικό (π.χ. έλεγχος κίνησης δορυφόρων). Τα τρία τμήματα του ολοκληρωμένου δορυφορικού συστήματος:

- Το επίγειο τμήμα. Σε γενικές γραμμές περιλαμβάνονται οι υποδομές (εγκαταστάσεις κ.λπ.) υποστήριξης της τροχιάς του δορυφόρου.
- Το τμήμα εκτόξευσης. Πρόκειται για τις διαδικασίες και τον απαραίτητο εξοπλισμό για την εκτόξευση του δορυφόρου.
- Το διαστημικό τμήμα. Αποτελείται από τον δορυφόρο ή δορυφόρους (πλέγμα ή σμήνος) και το φορτίο της συγκεκριμένης αποστολής.

Παράμετροι Συστήματος Δορυφορικής Τηλεπισκόπησης (Πολυμενόπουλος, 2001):

- Διαθεσιμότητα Δεδομένων (Data Availability)
- Ικανότητα Διάκρισης (Spatial Resolution)
- Επισκεψιμότητα Περιοχής (Revisit Frequency)
- Παρατήρηση σε συνθήκες φωτός-καιρού (Day-Night&AllWeather Capability)
- Φασματική Ανάλυση (Spectral Resolution)
- Παροχή Τρισδιάστατων Εικόνων (Stereo Images)
- Επεξεργασία και Διακίνηση Δεδομένων εδάφους (Data Processing and Dissemination).

28. Ο «ελεύθερος συνεργατισμός» έχει ως ιδεολογικό υπόβαθρο τον ανθρωπισμό. Βάσει του γερμανού θεωρητικού Zerche, αποτελεί ένα κράμα των κοινωνικών επιστημών, από την Οικονομική ως την Ψυχολογία. Προσδιορίζεται ως μια συγκεκριμένη μορφή συλλογικής ανθρώπινης δράσης. Οι δρώντες οφείλουν το δικό τους μερίδιο συμμετοχής, με αποτέλεσμα την αποφυγή της εκμετάλλευσης.

6.4 Κρυπτολογία

Μια μορφή του ηλεκτρονικού πολέμου αποτελεί και η υποκλοπή των πληροφοριών. Η επιστήμη που ερευνά τρόπους διασφάλισης της μεταφοράς δεδομένων και ευρύτερα της επικοινωνίας σε ευαίσθητα θέματα είναι η Κρυπτολογία. Η Κρυπτολογία χωρίζεται στην Κρυπτανάλυση και την Κρυπτογράφηση. Η κρυπτανάλυση είναι η μελέτη για την ανεύρεση μεθόδων που εξασφαλίζουν την κατανόηση του νοήματος της κρυπτογραφημένης πληροφορίας έχοντας σε άγνωστη ποσότητα τον κρυφό μετασχηματισμό για το κλειδί και το μήνυμα. Η Κρυπτογραφία είναι ο επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων (wikipedia, 2008). Θεωρητικά, για να υπάρξει πολιτισμός πρέπει να υπάρχει γλώσσα, στην οποία στηρίζεται η επικοινωνία και η συνεργασία των ανθρώπων. Με αυτήν την έννοια η γνώση της κρυπτολογίας αποτελεί μεγάλη δύναμη για ένα κράτος.

Περισσότερο σημαντικός είναι ο ρόλος της στον κυβερνοπόλεμο, όπου η ασφάλεια της μεταφοράς των δεδομένων είναι καθοριστικής σημασίας. Πρόκειται για μια επιστήμη – τέχνη. Αποτελεί σύνθεση γνωστικών αντικειμένων κυρίως, της γλωσσολογίας και των μαθηματικών. Ωστόσο, απαραίτητο προσόν για τον κρυπτολόγο θεωρείται ο ευφάνταστος στοχασμός για την αποκωδικοποίηση των σημάτων. Έτσι αρχικά χρησιμοποιήθηκε ο αναγραμματισμός για τη διασφάλιση του απορρήτου των πληροφοριών. Η μεταστοιχείωση σε έναν μυστικό κώδικα των γραμμάτων γίνεται σύμφωνα με έναν αλγόριθμο. Αλγόριθμος είναι ένα σύνολο από πράξεις που αν εκτελεστούν συντελούν στη λύση ενός προβλήματος.

Ο πιο δημοφιλής κώδικας χρησιμοποιήθηκε κατά το δεύτερο παγκόσμιο πόλεμο από τους γερμανούς ναζί, με την ονομασία “Enigma” (περιείχε τους αλγόριθμους πολλαπλών αναγραμματισμών). Σήμερα η κρυπτολογία θεωρείται από τα πιο αποδοτικά εργαλεία στην ασφάλεια των υπολογιστών. Έτσι, η εμπλοκή της επιστήμης της πληροφορικής και συναφών γνωστικών τομέων, όπως η τεχνητή νοημοσύνη και τα νευρωνικά δίκτυα, ήταν αναπόφευκτη. Σε κάθε περίπτωση, ειδικά αν πρόκειται για μυστικά εθνικής ασφαλείας, τα οποία συνήθως γίνονται στόχος κυβερνο-επιθέσεων, θα πρέπει να γίνεται εκτίμηση της απειλής (risk management). Δύσκολα θα μπορούσε κάποιος ειδήμονας να ισχυριστεί ότι υπάρχει διασφάλιση πλήρους εγγύησης (100%)²⁹.

Μια από της πιο σύγχρονες και γνωστές εφαρμογές αποτελεί η Ψηφιακή Υπογραφή. Οι Ψηφιακές Υπογραφές εφαρμόζονται σε διάφορους τομείς (όπως τον οικονομικό και τον στρατιωτικό). Μέχρι σήμερα, η νομική αυθεντικότητα πολλών εγγράφων εξαρτάται από την χειρόγραφο υπογραφή. Όσον αφορά στα φωτοαντίγραφα, αν δεν έχουν υπογραφή ως «γνήσιο αντίγραφο» δεν έχουν νομική ισχύ. Έτσι, η φυσική μεταφορά επίσημων εγγράφων (από χαρτί και μελάνι) σε συστήματα ηλεκτρονικής (ή ψηφιακής) αλληλογραφίας, μπορεί να γίνει μόνο με αυτόν τον τρόπο.

29. Χαρακτηριστικό είναι το κλασικό παράδειγμα, που επικαλείται «Κανόνας του 111» του Κλάουζεβιτς. Σε αυτό αναφέρεται ότι όταν κάποιος μυστικό το ξέρει ένας, είναι εν μέρει ασφαλές [Σημειώνοντας τον αριθμό ένα (1)]. Όταν το μάθουν δύο, η ανασφάλεια πολλαπλασιάζεται [Σημειώνοντας πάλι τον αριθμό ένα (1), έχοντας τώρα ένδεκα (11)]. Όταν το μάθει και τρίτος, τότε παύει να είναι μυστικό [Σημειώνοντας ξανά τον αριθμό ένα (1), όπου πλέον έχουμε εκατόν έντεκα (111)].

Κεφάλαιο 7. Ψυχο-πόλεμος

7.1 Πόλεμος στο τρίτο Οργανωτικό Επίπεδο (Πληθυσμός)

Στις δύο προηγούμενες μορφές του κυβερνοπολέμου περιγράψαμε τον τρόπο με τον οποίο ένα κράτος προσπαθεί να προσβάλλει το σύστημα της πληροφοριακής ροής του αντιπάλου κράτους. Σχηματικά, ορίσαμε αυτό το είδος της κυβερνο-επίθεσης ως «χτύπημα στο πρώτο επίπεδο οργάνωσης», την Ηγεσία. Η δεύτερη μορφή του κυβερνοπολέμου περιλαμβάνει όλους της τρόπους «προσβολής του δευτέρου επιπέδου οργάνωσης» των Μέσων. Επομένως, η τρίτη μορφή του κυβερνοπολέμου θα αφορά την «επίδραση στο τρίτο επίπεδο οργάνωσης», το οποίο ονομάσαμε Πλήθος. Η κοινωνιο-ψυχολογική διάσταση σε αυτό το επίπεδο είναι προφανής. Ο στόχος του αντιπάλου κράτους εστιάζεται σε έναν μεγάλο αριθμό -όχι απαραίτητα ομογενοποιημένου συνόλου- ανθρώπων, οι οποίοι (όπως αρχικά ορίσαμε) έχουν ως κοινό τη χωροχρονική τους συσχέτιση με μια νομική οντότητα, το κράτος.

Πολλοί ερευνητές ασχολήθηκαν με τη διαμόρφωση της κοινής γνώμης. Μια συνοπτική σύνθεση των ορισμών που έχουν διατυπωθεί από τους κοινωνιολόγους θα ήταν, ότι η κοινή γνώμη αποτελεί την εκφρασμένη άποψη ενός συγκεκριμένου πληθυσμού σε επίδικα θέματα του δημόσιου ενδιαφέροντος³⁰. Ειδικότερα, μας ενδιαφέρει το είδος του επηρεασμού με τα ακόλουθα χαρακτηριστικά.

- Η επίδραση στην κοινή γνώμη του πληθυσμού του κράτους, να γίνεται με σχεδιασμό άλλου κράτους. Σε διαφορετική περίπτωση δεν θα μιλάγαμε για πόλεμο.
- Το γεγονός της επίδρασης να μη βρίσκει σύμφωνη την εγχώρια ηγεσία. Αν η επίδραση, στην οποία συμφωνεί η ηγεσία, δημιουργεί πρόβλημα, τότε πρέπει να ελεγχθεί η ηγεσία και δεν έχουμε πόλεμο.
- Το σημαντικότερο βεβαίως είναι το μέσο της επίδρασης να είναι το Διαδίκτυο. Σε καιρό πολέμου, ο επηρεασμός των κατοίκων (στρατιωτικού ή άμαχου πληθυσμού) του εχθρού, αποτελεί μέρος της στρατηγικής από τα αρχαία χρόνια (Θουκυδίδης – Σουν Τζου). Στα πλαίσια του κυβερνοπολέμου, ο επηρεασμός νοείται μόνο στον κυβερνοχώρο, του οποίου τις ιδιαιτερότητες θα εξετάσουμε στη συνέχεια.

30. Ενδιαφέρον έχει η άποψη ότι δεν πρέπει να μιλάμε για ένα «κοινό» αλλά για «κοινά», η οποία υπογραμμίζει την ύπαρξη μιας πολυπλοκότητας και ανταγωνιστικότητας των δημόσιων σφαιρών (Fraser, 1992).

Το 18^ο αιώνα η κοινή γνώμη διαμορφώνεται κυρίως, από την κυκλοφορία του τύπου, η οποία διαμεσολαβεί στη συγκρότηση της δημόσιας σφαίρας (Habermas, 1962). Έτσι, προάγεται ο εκλογικευμένος διάλογος των ενεργών πολιτών, με την ελεύθερη επικοινωνία και την κυκλοφορία των πληροφοριών μέσω της ανταλλαγής γνώμων. Τη δεύτερη δεκαετία του 19^{ου} αιώνα άρχισαν τα έντυπα επιρροής της δημόσιας σφαίρας να παραδίδουν την πρωτοκαθεδρία στο ραδιόφωνο. Σταδιακά, ως τα μέσα του αιώνα επικράτησε η εμπορευματοποίηση του τύπου και η αυξανόμενη παρέμβαση του κράτους στις δημόσιες υποθέσεις, ώστε να μιλάμε για μετασχηματισμό της σχέσης από τη δημόσια στην ιδιωτική σφαίρα.

Η δημόσια ραδιοτηλεόραση είναι ένα πεδίο πραγματοποίησης των ιδανικών της δημόσιας σφαίρας. Αποτελεί το ιδεατό μέσο για την αντιπροσώπευση των διαφορετικών συμφερόντων της κοινωνίας των πολιτών στο δεδομένο γεωγραφικό πλαίσιο άρθρωσής τους (Garnham, 1990).

Κατά τη διάρκεια του Μεσοπολέμου άρχισαν να καθιερώνονται τα διεθνή ειδησεογραφικά πρακτορεία. Επρόκειτο για την απαρχή της συγκρότησης του παγκόσμιου δικτύου, το οποίο θα είχε τη δική του άποψη για το τι είναι είδηση και πως θα πρέπει να διανεμηθεί. Αυτή η διαδρομή οδήγησε σήμερα στις λεγόμενες, ψηφιακές λεωφόρους της ενημέρωσης (Negroponte, 1995).

Το μέγεθος των αλλαγών έκανε κάποιους επιστήμονες να μιλήσουν νωρίς για «επικοινωνιακή επανάσταση» (Briggs, 1966) και αργότερα, άλλοι για «πληροφοριακή επανάσταση» (Stonier, 1983). Ο όρος «επανάσταση», χρησιμοποιήθηκε για να δείξει τις διαστάσεις των μεταβολών που στην κοινωνιολογική προσέγγιση περιγράφηκε ως το πέρασμα από τη διυποκειμενική στη διαμεσολαβούμενη επικοινωνία. Πρόκειται για την πληροφόρηση από τρίτους, οι οποίοι ασκούν επιρροή στη δημόσια σφαίρα και χωρίς την οποία, δεν θα είχαμε άλλον τρόπο να αποκτήσουμε τις συγκεκριμένες πληροφορίες (Taylor, 2004). Βεβαίως, μαζί με την ταχύτητα στο ρυθμό της επικοινωνίας, αυξήθηκε υπερβολικά και η ποσότητα των πληροφοριών που καθημερινά γινόμαστε αποδέκτες. Το βαθύτερο πρόβλημα σε αυτό το «μποτιλιάρισμα» των ψηφιακών λεωφόρων, διατύπωσε ο επιφανής στοχαστής της μεταμοντέρνας σκέψης:

Υπάρχει όλο και περισσότερη σκέψη, αλλά λιγότερο νόημα (Baudrillard, 1983).

Οι αιτίες του μεγάλου μεγέθους των αλλαγών βρίσκονται στις κρίσεις της νεοτερικότητας. Κάθε έθνος, το οποίο θα οργανώνεται δυναμικά με τις επιταγές των σύγχρονων ΤΠΕ, περνάει τις ανάλογες κρίσεις. Όπως εύστοχα ειπώθηκε «το πρόβλημα δεν είναι ότι όσα περισσότερα μαθαίνεις, τόσο λιγότερα κατανοείς, αλλά ότι έτσι γίνεται αδύνατη η κατανόηση του κόσμου». Ο ρόλος του πλαισίου της ανθρώπινης επικοινωνίας είναι καθοριστικός για την αντίληψη και τελικά, τη συμπεριφορά της (Πουρκός, 1997). Από την προηγούμενη ανάλυση είναι φανερό ότι στο σύγχρονο περιβάλλον, του τεράστιου όγκου και των ταχέως διαδεδομένων πληροφοριών, επικρατεί η σύγχυση. Σε αυτές τις συνθήκες η ανθρώπινη αντίδραση εκπορεύεται από το συγκινησιακό και όχι το νοητικό πεδίο.

Σε αυτό το σημείο εισαγόμαστε στην περιοχή της Κοινωνικής και Γνωστικής Ψυχολογίας. Από τις αρχές του 19^{ου} αιώνα οι ηγεσίες των μεγάλων δυνάμεων, και κυρίως των ΗΠΑ, αντιλήφθηκαν ότι η ανάπτυξη των κοινωνικών επιστημών μπορεί να βοηθήσει στον έλεγχο της συμπεριφοράς του πλήθους. Από τη μια πλευρά, όπως εξήγησαν οι επιστήμονες-ερευνητές της γνωστής ως «Σχολή της Φραγκφούρτης»³¹, ο τρόπος ζωής στην καθημερινότητα της βιομηχανικής κοινωνίας ήταν εξαντλητικός. Σε γενικές γραμμές, το μεγαλύτερο μέρος της ημέρας κατείχε η εργασία και η αναγκαία ξεκούραση (όχι απαραίτητα ο ύπνος, αλλά και η ανάγκη ενασχόλησης με ανώδυνες υποθέσεις, σε επίπεδο νοητικό, θυμικό και σωματικό). Τις ελάχιστες ώρες που απόμεναν για ψυχαγωγία, διασκέδαση ή και εναλλακτική προσωπική καλλιέργεια οι «πολιτιστικές προτάσεις» ήταν συγκεκριμένες (Σαδικάς, 1986). Σε έναν εγκέφαλο του οποίου οι συνειδητές γνωστικές διεργασίες υπολειτουργούν (επειδή βρίσκονται σε χαλάρωση), είναι εύκολο να περάσεις πρότυπα και να επηρεάσεις πεποιθήσεις, που οδηγούν σε στερεοτυπικές συμπεριφορές (Maisonneuve, 2001).

Οι στερεοτυπικές συμπεριφορές έχουν ανάλογες αντιδράσεις σε παρόμοια ερεθίσματα. Με αυτόν τον τρόπο -και σύμφωνα με τη θεωρία των συμπεριφοριστών (Βοσνιάδου, 2000)- αν ενεργοποιηθούν συγκεκριμένα εξωτερικά ερεθίσματα, όπως κάποιο μήνυμα από ένα μέσο, μπορούμε να προβλέψουμε τις συμπεριφορές και άρα να τις ελέγξουμε. Οι στερεοτυπικές συμπεριφορές λειτουργούν μηχανιστικά.

31. Ιδρύθηκε στο διάστημα του Μεσοπολέμου στη Γερμανία με την ονομασία «Ινστιτούτο Κοινωνικών Ερευνών». Γνωστοί εκπρόσωποι του: Αντόρνο και Μαρκούζε.

Πρόκειται δηλαδή, για αυτορυθμιζόμενες³² εκδηλώσεις του εαυτού, χωρίς τη συμμετοχή έκδηλων μεταγνωστικών διεργασιών, οι οποίες επιτρέπουν στο άτομο να δρα συνειδητά (Ευκλείδη, 2005). Αυτός είναι θεωρητικά ο μηχανισμός που λειτουργεί η προπαγάνδα. Σχετικά με το πρακτικό κομμάτι, οι μέθοδοι υλοποίησης της επισυνάπτονται στο σχετικό παράρτημα.

Βεβαίως, ως προς τη νοηματοδότηση του όρου, υπάρχει η άποψη που υποστηρίζει ότι η προπαγάνδα δεν έχει, από μόνη της, ηθική απόχρωση.

...φαίνεται, ότι εκδικήθηκε τον εαυτό της, κατάφερε να ταυτιστεί με ό,τι χειρότερο έγινε στην ανθρωπότητα, στις συνειδήσεις του κόσμου! (Taylor, 2004).

Για τους περισσότερους αυτή η λέξη είναι συνώνυμη με την παραπλάνηση. Στη λαϊκή κουλτούρα εκπρόσωποι της θεωρήθηκαν πρόσωπα όπως ο Χίτλερ, ο Στάλιν και ο Μάο. Ενδεχομένως, στη συλλογική συνείδηση ως αντίθετη έννοια καταγράφηκε η Δημοκρατία. Πολλοί διατείνονταν ότι μόνον σε καιρό πολέμου νομιμοποιούνται να προπαγανδίσουν ιδέες. Ο εννοιολογικός προσδιορισμός είναι ότι η προπαγάνδα αποτελεί μια διαδικασία πειθούς, όπως στον οικονομικό τομέα είναι η διαφήμιση ή στον πολιτικό, ορισμένοι κομματικοί οργανισμοί χρησιμοποίησαν τον ευφημισμό «διαφώτιση». Σε αυτή την περίπτωση η ηθική της υπόσταση εξαρτάται από τον εμπνευστή του μηνύματος. Οι τεχνικές πειθούς είναι παντού όμοιες, αυτό που αλλάζει είναι ο στόχος. Θα μπορούσαμε να ισχυριστούμε ότι υπάρχει προπαγάνδα υπέρ της ειρήνης και προπαγάνδα υπέρ του πολέμου. Στην ιδανική περίπτωση που τα συμφέροντα του αποδέκτη και της πηγής συμπίπτουν, μιλάμε για «επιχείρηση σταθεροποίησης» (consolidation propaganda)³³.

Ασφαλώς, η πρώτη εντύπωση είναι ότι το μέσο από μόνο του είναι ένα απλό εργαλείο. Υπάρχει όμως και η κλασική άποψη ότι το μήνυμα είναι το ίδιο το μέσο (McLuhan, 1965). Στη συνέχεια ακολουθούν δύο αποφθέγματα αντιπροσωπευτικά των δύο ακραίων αντιλήψεων για το ρόλο των μέσων (του ραδιοφώνου, σε αυτήν την περίπτωση) και τις ευκαιρίες αξιοποίησης του.

32. Αυτό-ρύθμιση είναι η ικανότητα του ατόμου να παρακολουθεί και να τροποποιεί ή ελέγχει τη συμπεριφορά του, το γινώσκειν και το θυμικό του (Efklides, Niemivirta, & Yamauchi, 2002). Ο όρος «Αυτορύθμιση» γράφεται με μια λέξη όταν σημαίνει την αυτόματη ρύθμιση του συστήματος. Όταν αναφερόμαστε σε σχέση με τον εαυτό, τότε ο ορθός τρόπος γραφής είναι «Αυτό-ρύθμιση» (όπως, αυτό-αντίληψη και αυτό-αποτελεσματικότητα).

33. Βλ. Παράρτημα – Σχεδιάγραμμα.

Η δήλωση του πρώτου Γενικού Διευθυντή του BBC (Reith, 1932):

Το ραδιόφωνο είναι ένα από τα μεγάλα δώρα της Θείας Πρόνοιας στην ανθρωπότητα που πρέπει να το υπηρετούμε ταπεινά. Προσευχόμαστε να μη μειωθεί η αξία του.

Και στην άλλη άκρη, οι σκοπιμότητες που διέγινε ο Υπουργός Προπαγάνδας της Ναζιστικής Γερμανίας, Goebbels:

Η ραδιοφωνική εκπομπή είναι πραγματική προπαγάνδα. Προπαγάνδα σημαίνει να μάχεσαι σε όλα τα επίπεδα του πνεύματος, να παράγεις, να πολλαπλασιάζεις, να καταστρέφεις, να αφανίζεις, να κτίζεις και να χαλάς.

Το σημείο συμφωνίας και των δύο απόψεων είναι η πολιτισμική διάσταση των αλλαγών που έφεραν οι ΤΠΕ στην κοινωνία. Όχι μόνο διότι αφορούν της τεχνολογικές εξελίξεις, κάτι δηλαδή που είναι αποτέλεσμα ανθρώπινου επιτεύγματος. Κυρίως επειδή συμβάλλουν καθοριστικά στη μεταβολή των κοινωνικών σχέσεων.

Στην περίπτωση της προόδου του διαδικτύου, το οποίο επιτρέπει εξαιτίας της αλληλεπίδρασης των χρηστών τη διαμόρφωση νέων κοινωνικών σχέσεων μέσα στον κυβερνοχώρο, παρατηρούμε ότι ενώ μέχρι τώρα επικρατούσε το «μαζικό» στοιχείο, αυτό μεταβάλλεται στο «εξατομικευμένο». Άρα με τη συμμετοχή στον κυβερνοχώρο ξεκινά η «απομαζικοποίηση», την οποία επέβαλαν τα μέσα της βιομηχανικής επανάστασης (Taylor, 2004). Ο χρήστης και κοινωνός του διαδικτύου είναι απλά ένας μεταφορέας ιδεών, οι οποίες συνεχώς αναδιαμορφώνονται (βελτιώνονται ή αλλοιώνονται) από τους άλλους.

Την παράλληλη πορεία είχε και η εξέλιξη της προπαγάνδας, η οποία στην αρχή είχε χαρακτήρα της μαζικό. Στις μεταβιομηχανικές κοινωνίες η διεξαγωγή των ψυχολογικών επιχειρήσεων προπαγάνδας αποκτά ιδιαίτερο ενδιαφέρον. Στο σημερινό μεταβατικό στάδιο των πολλών τρόπων αποστολής του μηνύματος σε έναν ή πολλούς αποδέκτες, οι κύριες επιλογές άσκησης αυτής της μορφής κυβερνοπολέμου, η οποία στοχοθετεί τον επηρεασμό της συμπεριφοράς και της ψυχολογικής διάθεσης μιας καθορισμένης ομάδας ατόμων (target group) έχει τις ακόλουθες επιλογές.

- Τους ιστότοπους των κρατικών και λοιπών στρατευμένων φορέων.
- Τους ιστότοπους ελεύθερης διάδρασης (όπως τα forums, chat rooms κκ).
- Την αποστολή προσωπικών ηλεκτρονικών μηνυμάτων (e-mails).

Στην πρώτη επιλογή κύριο χαρακτηριστικό είναι η ομοιότητα με τον παραδοσιακό τρόπο μαζικής ενημέρωσης. Ο χρήστης παρακολουθεί σε τακτικά διαστήματα τα «επιλεγμένα

νέα του κόσμου». Η εικονική παρατήρηση των ειδήσεων, που δημιούργησε η τηλεόραση, είχε ως κύριο χαρακτηριστικό την αδράνεια των τηλεθεατών (παθητική σχέση με τα πολιτικά γεγονότα). Το κοινό είναι ικανοποιημένο όταν είναι πεπεισμένο ότι παρακολουθεί τις χειρότερες εκδηλώσεις της ανθρώπινης έκφρασης. Αυτό συμβαίνει για δύο λόγους. Ο πρώτος είναι ότι έχει την πεποίθηση ότι μαθαίνει όλη την αλήθεια, εφόσον αντικρίζει και τις πιο ακραίες καταστάσεις της πραγματικότητας. Ο δεύτερος είναι ότι εκ του ασφαλούς, αφού είναι μακριά από τον κίνδυνο, μπορεί να κατηγορεί γενικά τους υπεύθυνους και να παρηγορείται σκεπτόμενος ότι ποτέ δεν θα έκανε κάτι τέτοιο. Με αυτόν τον τρόπο επαληθεύεται η γνωστή ρήση:

Όσο ο κόσμος θα δίνει υψηλή ιεράρχηση στα ΜΜΕ, τόσο αυτά θα επιτυγχάνουν την κατασκευή της συναίνεσης (Chomsky, '88).

Βεβαίως οι διαφορές της παρακολούθησης των ειδήσεων από την τηλεόραση, σε σχέση με το διαδίκτυο, είναι οι διαφορές του μέσου. Ενδεικτικά αναφέρεται ότι τα πολυμέσα δίνουν τη δυνατότητα επιλογής του χρόνου και του τόπου ενημέρωσης, ο οποίος μπορεί να είναι διαφορετικός από την ώρα που εγγράφηκε η είδηση.

Ωστόσο ο πυρήνας της μετάβασης βρίσκεται στη δεύτερη επιλογή. Όπως αναφέραμε η πιο σημαντική καινοτομία της τεχνολογίας του διαδικτύου είναι η ανεξάρτητη, από τον τρόπο που αντιλαμβανόμασταν το χώρο και το χρόνο, επικοινωνία ή ευρύτερα, διασπορά της πληροφορίας. Οι περιορισμοί της απόστασης πλέον, δεν ισχύουν. Επιπροσθέτως, σε αυτήν την επιλογή ο χρήστης έχει τη σημαντική δυνατότητα της συμμετοχής. Έτσι, αν ένας φορέας επιθυμεί να προπαγανδίσει τις ιδέες του μέσω μιας επικοινωνίας σε πραγματικό χρόνο, στους κατοίκους σε οποιοδήποτε μέρος του κόσμου, θα πρέπει να πληρούνται τρεις νέες προϋποθέσεις.

- Η ομάδα στόχος να έχει πρόσβαση στο διαδίκτυο (κατοχή απαραίτητων πόρων, δηλαδή software – hardware).
- Τα μέλη της ομάδας να είναι ικανοί χρήστες (να γνωρίζουν τη μέθοδο διασύνδεσης με την αντίστοιχη ηλεκτρονική διεύθυνση).
- Ο φορέας εκπομπής των μηνυμάτων να μπορεί να ανταπεξέλθει άμεσα σε ενδεχόμενες (on line – real time) ερωτήσεις που θα του τεθούν.

Εδώ θα πρέπει να σημειωθεί και η πιο ακραία μορφή προπαγάνδας και απόλυτης λογοκρισίας, η δυνατότητα διακοπής του δικτύου θέτοντας έτσι τον αντίπαλο εκτός επικοινωνίας (off line).

Η τελευταία προϋπόθεση είναι ακριβώς η ειδοποιός διαφορά στη διαδικτυακή ενημέρωση. Για να κατανοηθεί καλύτερα το κεντρικό αυτό σημείο θα πρέπει να εξηγηθεί το θεωρητικό πλαίσιο. Η επικοινωνία στον κυβερνοχώρο μπορεί να είναι ασύγχρονη (ερωταπαντήσεις σε διαφορετικούς χρόνους) ή αντιθέτως σύγχρονη (παράλληλη). Σύμφωνα με τους Η. Βαρλάμη και Α. Γιανακουλόπουλο (2007) η ασύγχρονη επικοινωνία είναι ιδανική για εκτεταμένες συζητήσεις που απαιτούν βάθος σκέψης³⁴. Οι συμμετέχοντες αφιερώνουν το ανάλογο χρονικό διάστημα όταν μπορούν. Προβλήματα όπως η αργή πληκτρολόγηση δεν θεωρούνται ως μειονέκτημα. Τα μηνύματα μπορούν να ελεγχθούν από τους συντονιστές της συζήτησης και να δρομολογηθούν σε όσους αποφασίζουν. Ένα μέλος με ισχυρή άποψη που «μιλάει» πολύ μπορεί να επηρεάσει τα υπόλοιπα μέλη. Όσον αφορά την σύγχρονη επικοινωνία, συνυπάρχουν παράλληλα οι γνώμες όλων των μελών³⁵. Σίγουρα πλεονεκτεί στην εξοικονόμηση χρόνου, αλλά μόνο για όσους εξοικειωμένους μπορούν σε περιορισμένο χρόνο να δίνουν απαντήσεις σε πληθώρα ερωτήσεων. Μετά από αυτή την ανάλυση μπορούμε να διακρίνουμε τη δυσκολία άσκησης προπαγάνδας στη σύγχρονη επικοινωνία, η οποία απαιτεί άμεση κάλυψη ενδεχόμενων αποριών.

Ας εξετάσουμε την περίπτωση, για παράδειγμα, των διαφόρων ιστότοπων προβολής εθνικών ή θρησκευτικών θέσεων, με δυνατότητα τοποθετήσεων και συζητήσεων, με απώτερο στόχο τον προσηλυτισμό διαφόρων χρηστών δια του κυβερνοχώρου. Η συζήτηση ανάγεται συνήθως σε θέματα κουλτούρας και παρεμφερούς ενδιαφέροντος και συχνά, στην αναζήτηση των γενικών κατευθύνσεων της οργάνωσης και διοίκησης εθνικών ή θρησκευτικών ομάδων. Κατά τη μια πλευρά, αυτά τα στοιχεία συναποτελούν «φανταστικά συνεκτικά υλικά» για το άλλοθι της συνένωσης ατόμων και ομάδων (Δεμερτζής, 2005). Κατά την άλλη πλευρά πρόκειται για τη συγκυριακή πολιτισμική «κορύφωση του ανθρωπίνου πνεύματος» (Μάζης, 2006). Οι ερωτήσεις λοιπόν, των ανυποψίαστων, ή μη, μελών δεν ευνοούν πάντα την άμεση και εύστοχη απάντηση.

Τα ίδια χαρακτηριστικά ισχύουν και στην τρίτη επιλογή των ηλεκτρονικών μηνυμάτων. Η μόνη διαφορά είναι η προστασία του φορέα από την απαίτηση για άμεση ανταπόκριση σε τυχόν απορίες, στις οποίες θα μπορούν να ανταποκριθούν μετά από ένα χρονικό διάστημα.

34. Τα είδη ασύγχρονης επικοινωνίας είναι τα mailing lists, news groups και Web-based discussions.

35. Όσον αφορά την σύγχρονη επικοινωνία, τα είδη της είναι κυρίως τα online chats και τα instant messages.

7.2 Ψυχολογικές Επιχειρήσεις και Στοχοθετημένη Πληροφόρηση

Η έκφραση που χρησιμοποιούν στον στρατιωτικό τομέα για να περιγράψουν την εφαρμογή ενεργειών με σκοπό την προπαγάνδα είναι «Ψυχολογικές Επιχειρήσεις». Και εδώ η ραγδαία εξέλιξη των ΤΠΕ έπαιξε καθοριστικό ρόλο. Στο βαθμό που πολλοί μιλούν για την πραγματικά «Νέα Παγκόσμια Πληροφοριακή Τάξη Πραγμάτων» (Taylor, 2004). Αν και η φράση «Παγκόσμια Τάξη Πραγμάτων» χρησιμοποιήθηκε πρώτη φορά από τον H. G. Wells το 1944, στις ημέρες μας η αξία της έχει αναβαθμιστεί, εξαιτίας της σημασίας του ελέγχου της πληροφορίας στον πόλεμο, που συμβάλλει στην ανάδειξη του κυρίαρχου.

Το 1972 η UNESCO δήλωσε για πρώτη φορά ότι βρισκόμαστε υπό ένα νέο είδος αποικιοκρατίας, την «πολιτισμική νέο-αποικιοκρατία». Η βασική αιτία ήταν ότι το ισχύον σύστημα επικοινωνιών δεν πρόσφερε τις ίδιες ευκαιρίες σε όλους. Αυτό το γεγονός είχε παρόμοια εφαρμογή και στον πόλεμο. Όποτε ξεκινά ένας πόλεμος, στην πραγματικότητα έχουμε την παράλληλη έναρξη και ενός δευτέρου. Ο ένας, είναι ο πραγματικός (στρατιωτικός) και ο δεύτερος των Μέσων. Σε αυτόν το δεύτερο, για τους τηλεθεατές, τα πρωταγωνιστικά στοιχεία προβολής (π.χ. τραυματισμοί και θάνατος) είναι εικονικά. Όσον αφορά τους εμπλεκόμενους, τα πράγματα είναι διαφορετικά. Εκεί υπάρχει η ανάγκη ψυχολογικής υποστήριξης, η γνωστή «τόνωση του ηθικού».

Καταρχάς, υπάρχουν οι χώροι μάχης (battle spaces), το μέτωπο μάχης (battle front) και το εσωτερικό μέτωπο (home front). Αυτό το τελευταίο, εξαιτίας των ΤΠΕ έχει γίνει το λεγόμενο παγκόσμιο μέτωπο (global front), από το οποίο ενημερώνεται απευθείας το κοινό. Οι ερευνητές των στρατιωτικών υποθέσεων επικαλούνται τη μεταψυχροπολεμική αναθεώρηση του σκοπού των Ψυχολογικών Επιχειρήσεων. Υποστηρίζουν ότι μπορούν να συμβάλλουν στην εδραίωση της ειρήνης και να προτείνουν λύσεις στην κατεύθυνση της παγκόσμιας αλληλοκατανόησης, δίχως συγκρούσεις. Για να δειχθεί η δυσκολία να πείσουν οι συγκεκριμένοι επιστήμονες για αυτήν την άποψη, θα κάνουμε μια σύντομη ιστορική αναδρομή στην στρατιωτική χρήση της προπαγάνδας (Ψυχολογικές Επιχειρήσεις).

Η πρώτη φορά που διαμνηύθηκε ότι η μεγαλύτερη επιτυχία είναι να υποτάξεις τον εχθρό χωρίς πόλεμο, ήταν από τον Θουκυδίδη τον 5^ο αιώνα π.Χ. Στη σύγχρονη εποχή η θεωρία έγινε επίσημα πράξη το 1918, οπότε συστήθηκε το πρώτο βρετανικό τμήμα προπαγάνδας, με βάση του το Crewe House και επικεφαλής το Λόρδο Northcliffe. Οι Γερμανοί ίδρυσαν

το αντίστοιχο δικό τους στον πρώτο παγκόσμιο πόλεμο, τον Ψυχολογικό Υπό-Τομέα του G-2, με ένα τμήμα Προπαγάνδας, το οποίο υπαγόταν στο Στρατιωτικό Κλάδο Πληροφοριών (Military Intelligence Branch) των Γενικών Αρχηγείων. Για τους βρετανούς πάντως, πολιτικός πόλεμος σήμαινε «την πτυχή της πληροφόρησης-κατασκοπείας (intelligence), στην οποία οι πληροφορίες χρησιμοποιούνται επιθετικά για χειραγώγηση της κοινής γνώμης με διανοητικά μέσα»³⁶. Αρχικά οι Γερμανοί μιλούσαν για *Διανοητικό* πόλεμο, οι Βρετανοί για *Πολιτικό* και οι Αμερικανοί για *Ψυχολογικό* πόλεμο.

Ο πρώτος μεγάλος κλάδος ψυχολογικού πολέμου (PWB- Psychological Warfare Branches) ιδρύθηκε -με εντολή του ίδιου του Eisenhower- στη βόρεια Αφρική το Νοέμβριο του 1942 (άγγλο-αμερικανικό προσωπικό στρατιωτών και πολιτών). Το 1950, μετά τον πόλεμο της Κορέας, ο πρόεδρος Truman ίδρυσε το Συμβούλιο Ψυχολογικής Στρατηγικής (Psychological Strategy Board) στο Λευκό Οίκο. Επρόκειτο από τις πρώτες ενδείξεις της υψηλής θέσης που είχε στα κέντρα λήψης αποφάσεων, αυτό το είδους πολέμου.

Το 1952 ιδρύεται το κέντρο Ψυχολογικού Πολέμου (Psychological Warfare Centre). Οι παραδοσιακές μορφές ψυχολογικών επιχειρήσεων είναι τα φυλλάδια, οι μεγαφωνικές ανακοινώσεις και οι ραδιοφωνικές εκπομπές.

Νιώθεις πολύ απόκοσμα όταν ακούς ένα αεροσκάφος (C-47) να βουίζει ψηλά πάνω από το κεφάλι σου και μια τερατώδης «ουράνια» φωνή προστάζει τους αμαρτωλούς να μετανοήσουν (U.S. Special Operations Command H. Field, '94).

Οι βιετναμέζοι αμύνονταν χτυπώντας κατσαρόλια όταν εξέπεμπαν τα μεγάφωνα και έκοβαν τα χέρια όποιου διάβαζε τα φυλλάδια. Ψυχολογικές Επιχειρήσεις και Προπαγάνδα κορυφώνονται στον «Πόλεμο των Άστρων». Ωστόσο, μια πλήρως σχεδιασμένη επιχείρηση έχουμε για πρώτη φορά στον Πόλεμο του Κόλπου το 1991 (Καταιγίδα της Ερήμου). Συγκεκριμένα, ο σχεδιασμός είχε την κωδική ονομασία Φλεγόμενο Γεράκι (Burning Hawk). Η δαπάνη έφθασε τα 16m\$, με στόχο την αιχμαλωσία 87.000 Ιρακινών στρατιωτών και την αποτροπή σε εμπόλεμη εμπλοκή άλλων 160.000.

36. Τον όρο «διανοητικός πόλεμος» (Geistige Kriegführung) επινόησαν οι Γερμανοί, οι οποίοι θεωρούσαν ότι πρέπει να απευθύνονται στο κατώτερο μορφωτικά κοινό, μιας και οι διανοούμενοι θα μπορούσαν να το αντιληφθούν... Εξάλλου, η λογική πείθει και το συναίσθημα εξαναγκάζει.

Οι πρώτες συγκρίσεις δείχνουν μια εντυπωσιακή αναλογία. Με την κατανάλωση ποσοστού ύψους 0,03% των 60m\$ που κόστισε συνολικά ο πόλεμος στους συμμάχους, το 44% των Ιρακινών πείστηκε να εγκαταλείψει. Η υλοποίηση έγινε σε τρεις φάσεις:

- i) Προβολή σταθερότητας
- ii) Ενίσχυση συμμάχων και αποθάρρυνση αντιπάλων
- iii) Υποστήριξη της επιχειρήσεις και τόνωση διεθνούς κατανόησης.

Τα μέσα ασφαλώς, δεν κάλυψαν ολόκληρο τον πόλεμο. Η πρώτη φάση είχε να κάνει με τον, επί εβδομάδες, μαζικό βομβαρδισμό για την εξασθένιση του εχθρού. Εκεί οι ψυχολογικές επιχειρήσεις προσπάθησαν να πείσουν το μέτωπο ότι είναι θύματα του. Το 8^ο Ειδικό Απόσπασμα Ψυχολογικών Επιχειρήσεων συγκροτήθηκε το Σεπτέμβρη του 1990 κι έφθασε τα 650 άτομα. Σύνθημα της ήταν «κέρδισε το μυαλό – κέρδισε τη μάχη» (Win the Mind – Win the Day). Έτσι, φθάνουμε στο σημείο της αξιοποίησης των νέων ΤΠΕ. Η ηλεκτρονική ή ψηφιακή προπαγάνδα έχει αφετηρία στις αρχές της τελευταίας δεκαετίας του αιώνα στον πόλεμο της συμμαχίας της Δύσης έναντι του Ιράκ στο Κουβέιτ. Ένας προσωπικός υπολογιστής (PC) με επεξεργαστή Intel, συνδεδεμένος με ένα σαρωτή εικόνας (image scanner) και έγχρωμο λέιζερ εκτυπωτή, αποτέλεσε τον πρώτο εξοπλισμό (PAT-PSYOPS Analyst Terminal). Οι πρώτες ενδείξεις για την αποτελεσματικότητα ως προς το χρόνο, σε σχέση με το παρελθόν βέβαια, ήταν συγκλονιστικές. Αυτή η πρώτη αξιοποίησης των Η/Υ έγινε παράλληλα με την παραδοσιακή τεχνολογία. Ενδεικτικά, χρησιμοποιήθηκαν οι βόμβες φυλλαδίων M129, οι οποίες έχουν δυνατότητα «αποστολής» 60.000 συσκευασμένων φυλλαδίων και ρίπτονται από αεροσκάφη F-16 ή C-130. Ως το τέλος του πολέμου ρίφθηκαν 29 εκατομμύρια φυλλάδια. Αυτό το τελευταίο στοιχείο αποκτά ιδιαίτερη αξία αν αναλογιστούμε ότι τις τελευταίες εβδομάδες του πρώτου παγκοσμίου πολέμου ο αριθμός των αντίστοιχων φυλλαδίων έφθασε μόλις τα 5 εκατομμύρια.

Μετά την ολοκλήρωση, διενεργήθηκαν κάποια τεστ στους αιχμαλώτους πολέμου. Τα συμπεράσματα έδειξαν τα ακόλουθα (Taylor, 2004).

<u>Απόδοση ενέργειας</u>	ΦΥΛΛΑΔΙΑ	ΡΑΔΙΟΦΩΝΟ	ΜΕΓΑΦΩΝΟ
Ενημέρωση:	98	58	34
Επηρεασμός:	80	46	18
Αποτελεσματική:	70	34	16

Το σύγχρονο πρόβλημα είναι πώς θα εναρμονιστούν οι Ψυχολογικές Επιχειρήσεις με τις ΤΠΕ. Προς το παρόν δεν υπάρχει ενδεδειγμένη μέθοδος. Από τη μία πλευρά, οι παραδοσιακές ρίζες της ναζιστικής και σοβιετικής κληρονομιάς. Από την άλλη, η αναζήτηση του σύγχρονου ρόλου μιας ενιαίας (Μυστικής) Υπηρεσίας Πληροφοριών. Στη στρατιωτική αργκό οι Ψυχολογικές Επιχειρήσεις θεωρούνται «πολλαπλασιαστής της πολεμικής ισχύος». Αυτός προσαυξάνεται με την αποδοτική διαχείριση των πληροφοριών του διαδικτύου. Το πιο ανεπτυγμένο ενημερωτικό σύστημα στον κόσμο το έχουν οι ΗΠΑ. Αυτές γίνονται καθημερινά, στόχος των γνωστών ως «πληροφοριο-βομβιστών» (info-bombers). Ειδικότερα, αυτοί αποσκοπούν στην υπονόμευση των κρίσιμων (οι οποίες αναλύονται σε επόμενο κεφάλαιο) υποδομών ή στην υποκλοπή βασικών στοιχείων για τη λήψη αποφάσεων (κυβερνοπόλεμος στο πρώτο επίπεδο οργάνωσης, την Ηγεσία). Εδώ οι Ψυχολογικές Επιχειρήσεις αναλαμβάνουν ως αποστολή την επίλυση αυτού του προβλήματος. Βεβαίως, πλέον στις απειλές δίνεται υπέρ-εθνικός χαρακτήρας, αφού το διαδίκτυο μπορεί να απευθυνθεί σε όποιον έχει πρόσβαση σε αυτό, ανεξαρτήτως χωρικών συνόρων. Έτσι, δικαιολογείται η αυτόκλητη αποστολή των ΗΠΑ, ως «παγκόσμιου αστυνόμου της προάσπισης των αξιών της ελευθερίας και του σεβασμού της ανθρώπινης προσωπικότητας». Καταληκτικά, στο θεωρητικό πλαίσιο, οι Ψυχολογικές Επιχειρήσεις είναι επικοινωνία και επομένως καλύπτουν όλο το φάσμα της ανθρώπινης δραστηριότητας³⁷.

37. William Daugherty [American Institutes for Research in the Behavioral Science] (1976) *The Art and Science of Psychological Operations*. Washington: Department of the Army.

Κεφάλαιο 8. Κυβερνοπόλεμος της ΗΠΑ

8.1 Έκθεση στο Κογκρέσο για τον Κυβερνοπόλεμο³⁸

Ο έλεγχος της παραγωγής, διασποράς και ανατροφοδότησης της πληροφορίας αποτελεί μια βασική επιδίωξη για τη διεύρυνση της κυριαρχίας των κρατών. Στην εποχή μας αυτό το γεγονός έχει γίνει κοινή συνείδηση. Ένα από τα στοιχεία που το επιβεβαιώνουν είναι η σχετική εισήγηση του -σημερινού νομπελίστα και τότε- αντιπροέδρου των ΗΠΑ Al Gore. Το Μάρτιο του 1994 στο Μπουένος Άιρες προτάθηκε η συγκρότηση της Παγκόσμιας Υποδομής Πληροφοριών (GII-Global Information Infrastructure) στο συμπόσιο της Διεθνούς Τηλεπικοινωνιακής Ένωσης (ITU-International Telecommunications Union). Ανεξάρτητα από τις αποφάσεις για διεθνή συνεργασία σε αυτό το θέμα, παρομοίως έπραξε και ο Κλίντον, ο οποίος έθεσε το αίτημα για την υλοποίηση της Εθνικής Πληροφοριακής Υποδομής (National Information Infrastructure). Ένα επιπρόσθετο στοιχείο είναι η πρόβλεψη του υπεύθυνου της κοινοπραξίας του INTELSAT, η οποία έχει μέλη πάνω από 135 χώρες και με ιδιοκτησία περίπου 20 δορυφόρους, ότι:

Η πληροφορία θα γίνει τον 21^ο αιώνα, τόσο σημαντική, όσο και το πετρέλαιο. Θα πάψει να είναι ιδιοκτησία των λίγων της εξουσιαστικής ελίτ (Goldstein, 1995).

Ο Κυβερνοπόλεμος αναδεικνύεται σε ύψιστο θέμα για την προστασία του εθνικού συμφέροντος. Με την έκφραση αυτή υποδηλώνεται τα πολλά στρατιωτικά ζητήματα για τους νέους τρόπους επίθεσης και άμυνας με στόχο τα δίκτυα, τις πληροφορίες και τον επηρεασμό της συμπεριφοράς στον Κυβερνοχώρο. Μια από τις σημαντικότερες δυσκολίες είναι ο προσδιορισμός της ταυτότητας του επιτιθέμενου. Συχνά δε, σημειώνεται και μεγάλη καθυστέρηση στον εντοπισμό του ίδιου του προβλήματος, που δημιουργήσε η επίθεση. Για παράδειγμα, η «κυβερνο-κατασκοπεία», βάσει της οποίας, έχεις τη δυνατότητα να παρακολουθείς τη διαδικτυακή διακίνηση της πληροφορίας. Σε αυτήν την περίπτωση ο επιτιθέμενος δεν παρεμβαίνει, συνεπώς αυτός που υπόκειται στην παρακολούθηση είναι ιδιαίτερα δύσκολο να αντιληφθεί το πρόβλημα, ακόμη πιο δύσκολο να ανακαλύψει το πρόγραμμα-κατάσκοπο και τώρα, γίνεται κατανοητό ότι ο εντοπισμός αυτού που το εγκατέστησε είναι σχεδόν αδύνατος.

38. Steven A. Hildreth (June 19, 2001) *Specialist in National Defense* CRS Report for Congress.

Ένας μεγάλος αριθμός κρατών ενσωμάτωσαν την προετοιμασία για την αντιμετώπιση της κυβερνο-απειλής ως βασικό μέρος του στρατιωτικού τους δόγματος. Ορισμένες από τις ισχυρότερες δυνάμεις του πλανήτη, οι οποίες αναδιοργανώνονται σε αυτή την κατεύθυνση είναι η Κίνα, η Ρωσία, η Γερμανία, η Γαλλία, το Ηνωμένο Βασίλειο και η Ινδία. Πρώτο κράτος ήταν οι ΗΠΑ, του οποίου τα πρώτα βήματα κατασκευής μιας ασπίδας σε μελλοντικές κυβερνο-επιθέσεις αξίζει να μελετήσουμε στη συνέχεια.

Για να δείξουμε το βαθμό σημαντικότητας, που εκτίμησαν οι αρμόδιοι, ότι αποκτά ο Κυβερνοπόλεμος, παραθέτουμε την ακόλουθη δήλωση του επίσημου εκπροσώπου του Υπουργείου Άμυνας των ΗΠΑ, για αυτό το θέμα στο Κογκρέσο:

Μπορούμε να πούμε πλέον, ότι είμαστε σε συνεχή πόλεμο. (John Hamre, 11/2/2001)

Το κύριο επιχείρημα για αυτήν τη δήλωση ήταν η αναφορά της Κεντρικής Υπηρεσίας Πληροφοριών (Central Intelligence Agency) ότι οι «νούμερο ένα» κυβερνο-απειλές θεωρούνται η Ρωσία και η Κίνα (*G. Tenet, 24/6/1998*).

Σήμερα η ίδια υπηρεσία αναφέρει ότι περισσότερες από 20 χώρες έχουν προετοιμάσει διάφορα είδη Επιχειρήσεων Πληροφοριών (IO-Information Operation) που στοχοθετούν τις ΗΠΑ. Ορισμένες από αυτές είναι η Κούβα, η Β. Κορέα, η Λιβύη, η Συρία και το Ιράν. Έτσι, καταληκτικά, προτάθηκε να εισαχθεί στο δόγμα η διοργάνωση της Κυβερνο-άμυνας. Τα βασικότερα σημεία-ερωτήματα της εισήγησης είναι τα ακόλουθα.

- Τα υπολογιστικά συστήματα του Πενταγώνου και άλλοι στρατιωτικοί ιστότοποι δέχονται επιθέσεις χιλιάδες φορές το χρόνο. Αυτό το γεγονός άραγε, μπορεί να χαρακτηριστεί πόλεμος;
- Συχνά αυτές οι επιθέσεις γίνονται από εφήβους-κατοίκους των ΗΠΑ και λιγότερο συχνά του εξωτερικού. Το ζητούμενο είναι πότε οι στρατιωτικοί ιθύνοντες θα πρέπει να ανησυχούν πραγματικά.
- Θα πρέπει να δούμε τι είναι κυβερνο-επίθεση και τελικά πώς καθορίζεται η νίκη σε μια τέτοια μάχη.
- Η συνεχής επίθεση του έθνους στην περιοχή του κυβερνοχώρου, όπου διακινούνται πληροφορίες σχετικά με αμερικανικές οικονομικές υποθέσεις συνιστά κυβερνοπόλεμο;

Τα πιο «δεδεαστικά» χαρακτηριστικά της απόπειρας για εγκληματική ενέργεια στον κυβερνοχώρο είναι η ταχύτητα και η αφανής ταυτότητα, στοιχεία που προσδίδουν πολύ χαμηλό ρίσκο σε όποια προσπάθεια. Αυτά τα χαρακτηριστικά τα κάνει να επικαλούνται

και ασύμμετρα (αόρατα). Βεβαίως υπάρχουν πολλά είδη εγκληματικής δράσης στον κυβερνοχώρο. Ενέργειες όπως το χάκιν (hacking), κυβερνο-προσβολή (cyber mischief), κυβερνο-χουλιγκανισμός (cyber hooliganism) και πώληση παράνομων ειδών του γνωστού «οργανωμένου εγκλήματος», του οποίου κυριότερα θεωρούνται τα ναρκωτικά, πορνογραφικά προϊόντα και τα πολιτιστικά ευρήματα περιεχομένου αρχαιοκαπηλίας.

8.2 Το ιστορικό των πρώτων κυβερνο-χτυπημάτων

Air Force Rom Lab (1994)

Η πρώτη περίπτωση αφορά την επίθεση που δέχτηκαν οι αεροπορικές δυνάμεις (USA Air Force) στο εργαστήριο της στη Νέα Υόρκη το Μάρτιο του 1994. Το πρώτο πλήγμα πραγματοποιήθηκε σε έναν παροχέα του διαδικτύου (Internet Service Provider) πρώτα στη Νέα Υόρκη, μετά στο Σιάτλ, Ουάσιγκτον, όπου το δίκτυο ολοκληρωνόταν. Οι επιτιθέμενοι χρησιμοποιούσαν γραμμές dial-up. Όταν έγιναν αντιληπτοί και άρχισαν να παρακολουθούνται, δύο χάκερ που συνεργάζονταν αναγνωρίστηκαν. Ο ένας από αυτούς μάλιστα, καυχόταν που μπόρεσε να εισέλθει στα αμερικανικά στρατιωτικά συστήματα. Πληροφοριοδότες ενημέρωσαν για αυτή τη φήμη στη Μ. Βρετανία και συνελήφθη από την αστυνομία (Scotland Yard). Ο δράστης είχε καταφέρει να υποκλέψει τηλεφωνικές εταιρίες μεταξύ της Κολούμπια και Χιλής και με αυτόν τον τρόπο να εισέλθει ανώνυμα στο εργαστήριο. Μετά έγινε γνωστό ότι είχε καταφέρει παρόμοια πλήγματα στα κεντρικά γραφεία του NATO, στο Αεροδιαστημικό Κέντρο και στην αεροπορική βάση Wright-Patterson. Για να επιτύχει αυτές τις επιθέσεις ενέπλεξε στο διαδίκτυο οκτώ κράτη.

Τέλος, ενδιαφέρον έχει ότι πρόκειται για ένα 16χρονο αγόρι (DataStream Cowboy) βρετανό μαθητή. Ο μέντοράς του (Kuji) είναι ένας 22χρονος ισραηλινός τεχνικός. Και οι δύο αθώωθηκαν, διότι οι νόμοι της εποχής δεν προέβλεπαν παρόμοιο αδίκημα.

Eligible Receiver (1997)

Η ονομασία «Νόμιμος Αποδέκτης» (Eligible Receiver) δόθηκε στην πρώτη άσκηση πληροφοριακού πολέμου (IW-Info Warfare) στις ΗΠΑ. Στη γνωστή ως Κόκκινη Ομάδα (Red Team) συμμετείχαν 35 άτομα, τα οποία επί τρεις μήνες χρησιμοποιούσαν τη διαθέσιμη τεχνολογία και λογισμικό. Το σενάριο ήταν ότι ένας επιτήδειος (rogue) αγνόησε τους κανονισμούς των ΗΠΑ και επιτίθεται στο σύστημα πληροφοριών των ΗΠΑ. Οι στόχοι του επιτήδειου ήταν να αποκρύψει την ταυτότητα του, καθώς και να ακυρώσει οποιαδήποτε αμερικανική προσπάθεια για στρατιωτική επιχείρηση. Ένας αριθμός από επιτιθέμενους σε προσομοίωση προγραμματίστηκαν για να δράσουν ενάντια στην επικοινωνιακή ισχύ των δικτύων των Oahu, Low Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, DC, Fayetteville και Tampa.

Τα αποτελέσματα ήταν δυσάρεστα για τις κυβερνητικές αρχές. Σε αρκετούς κόμβους παραβιάστηκαν τα μέτρα ασφαλείας. Το μήνυμα που διεξήχθη από τα τελικά συμπεράσματα, ήταν η μεγάλη ανάγκη για περισσότερα χρήματα στην κατεύθυνση της κυβερνο-άμυνας. Χαρακτηριστική ήταν η δήλωση του υπεύθυνου του Πενταγώνου:

Αυτή η άσκηση μας έδειξε σαφέστατα τις ελλείψεις μας στη διαλειτουργικότητα σε φυσικές και κυβερνο-επιθέσεις στις σχετικές υποδομές (G.Campbell, 1998).

Ο κυβερνητικός εκπρόσωπος, μετά τα αποτελέσματα, δήλωσε:

Επρόκειτο για μία σημαντική άσκηση, η οποία μάς δίδαξε ότι οφείλουμε να οργανωθούμε καλύτερα, διότι οι δυνητικές επιθέσεις επέκειτο (K. Bacon, 1998).

Solar Sunrise (1998)

Ένας αριθμός αμυντικών υπηρεσιών, οι οποίες είναι αρμόδιες για τα δίκτυα, δέχθηκαν επίθεση το Φεβρουάριο του 1998. Οι δράστες εκμεταλλεύθηκαν τα τρωτά σημεία του υπολογιστικού συστήματος Solaris (UNIX-based). Το επίτευγμα ήταν η εγκατάσταση ενός προγράμματος συλλογής δεδομένων, το οποία (δεδομένα) κατόπιν συνέλεξαν στα δικά τους συστήματα. Πολλοί ενεπλάκησαν στην εξέταση αυτού του γεγονότος, όπως το Harvard University. Τελικά εντοπίστηκαν οι δράστες, δύο μαθητές από την Καλιφόρνια και ένας 18χρονος ισραηλινός που τους επέβλεπε. Όλοι συνελήφθηκαν και καταδικάστηκαν. Από το Πεντάγωνο χαρακτηρίστηκε ως η πιο συστηματικά οργανωμένη επίθεση. Παρόλα αυτά, τα πρώτα μέτρα από τις προηγούμενες εμπειρίες άρχισαν να αποδίδουν. Όπως δήλωσε η δικαστική υπηρεσία «καμία διαβαθμισμένη πληροφορία δεν εκλάπη».

8.3 Κυβερνητικές Θέσεις και Έργα

Μετά από αυτά τα πλήγματα οι ιθύνοντες προβληματίστηκαν για το πόσο επαρκή είναι η εθνική ασφάλεια στις δυνητικές απειλές (κυβερνο-επιθέσεις). Στο προηγούμενο κεφάλαιο δείξαμε τα πρώτα στάδια που χρειάστηκαν, ώστε να συνειδητοποιήσουν οι κυβερνήσεις το μέγεθος του κινδύνου. Εδώ, θα δούμε τις προσεγγίσεις που έγιναν για τη θεραπεία αυτού του προβλήματος. Το σημαντικότερο όλων είναι ότι πριν την αρχή του νέου αιώνα τέθηκε σε προτεραιότητα, πλέον και επίσημα, ο όρος «κυβερνοπόλεμος»³⁹.

Η κατανόηση του κινδύνου οδήγησε σε δύο βασικές απόψεις. Η πρώτη πρόταση υποστηρίζει ότι η κυβερνο-απειλή συνιστά ύψιστη προτεραιότητα για την εθνική ασφάλεια. Όπως στο παρελθόν, έτσι και τώρα θα πρέπει η αμερικανική στρατιωτική και διπλωματική ισχύ να συνεργαστούν για να προστατέψουν το εθνικό συμφέρον. Η άλλη άποψη, συμφωνεί ότι το μέγεθος της απειλής είναι μεγάλο και προτείνει την αντιμετώπιση του προβλήματος από τις εκπαιδευτικές αρχές του τόπου. Ο κύριος λόγος που συμβαίνει αυτό αφορά ότι ο σεβασμός των προσωπικών ελευθεριών θέτει όρια, εντός των οποίων, δύσκολα μπορεί να κινηθεί ο στρατός⁴⁰. Στο παρελθόν οι απειλές από το εξωτερικό, μπορούσαν να αντιμετωπιστούν στο εξωτερικό. Πλέον, τα γεωγραφικά όρια δεν διασφαλίζουν τη διατήρηση της απειλής έξω από τη χώρα.

Πολλές προτάσεις έχουν γίνει για την κατάρτιση του σχεδίου αντιμετώπισης του προβλήματος. Η πιο πρόσφατη αφορά μία έκθεση της Εθνικής Στρατηγικής Ασφαλείας (National Security Strategy) για τον Λευκό Οίκο⁴¹, η οποία σημείωνε ότι «βρισκόμαστε υπό την απειλή υπονόμησης κρίσιμων εθνικών υποδομών, η οποία δύναται να είναι παρεμφερούς ισχύος με τις απειλές πραγματικών επιθέσεων από τρομοκρατικά ή γενικότερες εγκληματικές ομάδες». Στην πραγματικότητα έχει δοθεί εντολή σε πολλά τμήματα να παρουσιάσουν οδηγούς πρόληψης ή επίλυσης των προβλημάτων.

39. Χαρακτηριστικό γνώρισμα είναι ότι η πληροφορία που διακινείται, δεν έχει τις ιδιότητες των παραδοσιακών αγαθών, όπως την άπαξ κατανάλωση και ιδιοκτησία. Όσο δηλαδή κι αν καταναλώνουμε-αποκτούμε μια πληροφορία, δεν έχουμε απαραίτητα και την αποκλειστικότητα της (Stonier, 1983).

40. Γενικότερα, πάντως, τα πράγματα στις ΗΠΑ είναι πιο ελαστικά, από ό,τι στην Ευρώπη για παράδειγμα, σε αυτό το θέμα (Drumheller, 2007).

41. The White House. A National Security Strategy for a new century. (Dec. 1999).

Για παράδειγμα η Διεύθυνση Δόγματος των Πληροφοριακών Επιχειρήσεων⁴², παρουσίασε στοιχεία για το πώς οι Ένοπλες Δυνάμεις των ΗΠΑ δραστηριοποιούνται σε συνθήκες κυβερνοπολέμου. Η τετραετής έκθεση για τις ασύμμετρες απειλές (asymmetric threats) και κυρίως τον πληροφοριακό πόλεμο ανέφερε:

Όπως συμπεραίνεται από τις πληροφορίες για τις εχθρικές δυνατότητες επίθεσης στον κυβερνοχώρο, είναι άμεση η ανάγκη σχεδίασης στρατηγικών κυβερνο-άμυνας (Department of Defense, Report of the Quadrennial Review. May '97).

Παρόλα αυτά η κυβέρνηση Μπους δεν θεωρείται ότι έχει ένα έτοιμο ή επαρκές πλάνο για αυτήν την προοπτική της (κυβερνο)τρομοκρατίας. Από την άλλη πλευρά η εκτίμηση της απειλής είναι κοινή για τις αρμόδιες επιτροπές των δύο μεγάλων κομμάτων. Έτσι, μόνο για την ταξινόμηση, διαβάθμιση και ηλεκτρονική αρχειοθέτηση στοιχείων δόθηκαν \$50m.

42. Joint Doctrine for Information Operations 3-13, October 9, 1998.

8.3.1 Το οργανόγραμμα

Η θέση του Εθνικού Συντονιστή Ασφαλείας (National Coordinator Security) για τις υποθέσεις αντι-τρομοκρατίας ήταν ότι, καταρχάς, θα πρέπει να προσδιοριστούν οι ευαίσθητοι τομείς-στόχοι υποδομών (critical infrastructure), οι οποίοι είναι:

- οι εγκαταστάσεις που παρέχουν ροή πληροφοριών και επικοινωνίας,
- τα χρηματο-οικονομικά συστήματα και οι τράπεζες,
- οι περιοχές και οι αγωγοί υδάτινων πόρων,
- οι μεταφορικοί σταθμοί και οι δίοδοι (αεροδρόμια, κεντρικές λεωφόροι καθώς και κεντρικοί άξονες μαζικής μεταφοράς, μετρό κ.λπ.),
- τα κτίρια λήψης αποφάσεων και έδρας σωμάτων ασφαλείας,
- οι μονάδες υγείας και
- Οι χώροι αποθήκευσης και διακίνησης ενέργειας (κυρίως ηλεκτρισμού-πετρελαίου).

Στο βαθμό λοιπόν, που τα άνω θα εξαρτώνται από την ηλεκτρονική ή ψηφιακή τεχνολογία, η απειλή του κυβερνοπολέμου θα αποκτά μείζονα σημασία, ιδίως εξαιτίας της ασύμμετρης μορφής του (τρομοκρατία). Η επίλυση αυτού του ζητήματος προϋποθέτει την ανάπτυξη ενός διαλειτουργικού δικτύου διακυβέρνησης μέσω των Η/Υ. Ένας από τους πολλούς όρους που χρησιμοποιήθηκαν ήταν ο «CAN» (Computer Network Attack). Ο αμυντικός σχεδιασμός πάντως, εντάσσεται στο αντιτρομοκρατικό πρόγραμμα. Η πρώτη Υπηρεσία με αυτό το αντικείμενο ιδρύθηκε στη Βιρτζίνια τον Αύγουστο του 1999, με την ονομασία Joint Task Force – Computer Network Defense (JTF-CND) (spacecom, 2007).

Μια άλλη οργανωτική διάσταση της κανονικοποίησης του τρόπου συμμετοχής στον κυβερνοχώρο -απαραίτητα κατάλοιπα ενδεχομένως του ορθολογικού καθεστώτος- είναι το νομικό πλαίσιο. Για να επισημοποιηθούν οι εντολές υλοποίησης μια στρατηγικής σχεδίασης κυβερνοάμυνας, θα έπρεπε πρώτα να προσδιοριστεί τι θεωρείται κυβερνοέγκλημα. Ήδη έχουμε έτοιμο ένα σύνολο κανόνων, οι οποίοι προσπαθούν να «ελέγξουν» τη ροή των πληροφοριών. Οι πρώτες νομοθετήσεις έγιναν σε ΗΠΑ και ΕΕ. Αξιοσημείωτο είναι ότι αφετηρία ήταν οι διατάξεις για την Προστασία των Προσωπικών Δεδομένων, αποτέλεσμα των πιέσεων των κινημάτων της «ελεύθερης διακίνησης στον κυβερνοχώρο» (FOIA-Freedom of Information Act). Ενδεικτικά, τον Ιανουάριο του 2000, ο πρόεδρος Κλίντον ανακοίνωσε ένα πρόγραμμα 10 σημείων, το οποίο πριμοδότησε με 2 δισεκατομμύρια δολάρια.

Σκοπός του ήταν να προστατέψει τη δημόσια διοίκηση από τις επιθέσεις σε (δίκτυα και διαδίκτυο) Η/Υ και Κυβερνοχώρο. Τα βασικά σημεία αυτού του προγράμματος περιλάμβαναν τις εξής κατευθύνσεις:

- εντοπισμό και σύλληψη των εγκληματιών δρώντων
- έρευνα των τρωτών σημείων του συστήματος
- καταγραφή μεθόδων κυβερνοπειρατίας.

Σε αυτή την κατεύθυνση αναζητήθηκε η εμπειρία κρατών που έχει δραστηριοποιηθεί σε αυτόν τον τομέα, με μόνη προϋπόθεση για τη συνεργασία οι χώρες να ανήκουν στο σύμφωνο του ΝΑΤΟ. Οι τρεις πιο εξειδικευμένες ήταν η Βρετανία, η Γερμανία και η Γαλλία.

8.3.2 Η Εθνική Στρατηγική των ΗΠΑ για την Ασφάλεια του Κυβερνοχώρου. The National Strategy to Secure Cyberspace

Το ακόλουθο απόσπασμα από την ομιλία του προέδρου George Bush στο Λευκό Οίκο, για την ανάγκη χάραξης Εθνική Στρατηγική Ασφάλειας του Κυβερνοχώρου, το Φεβρουάριο του 2003 (The National Strategy to Secure Cyberspace), αποτελεί ένα ακόμη σημείο που δείχνει την προτεραιότητα που έδωσαν οι ΗΠΑ σε αυτόν τον τομέα, από πολύ νωρίς.

Οι κρίσιμες υποδομές των ΗΠΑ περιλαμβάνουν:

- Αγροτική Παραγωγή
- Τροφίμων
- Νερού
- Δημόσιας Υγείας
- Πολιτικής Προστασίας
- Δημόσιας Διοίκησης
- Βιομηχανίας
- Τηλεπικοινωνιών
- Χρηματοπιστωτικών
- Αμυντικής
- Ενέργειας
- Μεταφοράς

Ο χαρακτηρισμός που δίδεται στον Κυβερνοχώρο είναι ότι αποτελεί το νευρικό σύστημα ελέγχου αυτών των τομέων, από το οποίο εξαρτάται η ασφάλεια της χώρας. Πιο συγκεκριμένα το κείμενο αναφέρει ότι ο Κυβερνοχώρος συνιστά το δίκτυο εκατοντάδων χιλιάδων διασυνδεδεμένων υπολογιστών και συναφών μηχανημάτων (routers, servers and switches). Η λειτουργία χωριστά της κάθε μιας και η διαλειτουργικότητα όλων μαζί, εξαρτάται από την ασφαλή πληροφοριακή ροή του κυβερνοχώρου. Αυτός είναι ο λόγος που αυτή η «τεχνολογική περιοχή» αποτελεί αναπόσπαστο μέρος της Στρατηγικής Εθνικής Ασφαλείας. Η σπουδαιότητα αυτού του γεγονότος για τις κρίσιμες υποδομές της χώρας, οδήγησε στην Εθνική Στρατηγική Ασφαλείας του Κυβερνοχώρου (National Strategy to Secure Cyberspace). Σκοπός είναι η συνεχή παροχή ασφαλούς πλοήγησης των αμερικανών στον κυβερνοχώρο. Αποτελεί μια ιδιαίτερη πρόκληση για τον δημόσιο τομέα, τον ιδιωτικό τομέα, αλλά και κάθε αμερικανό πολίτη χωριστά. Η οργάνωση της πολιτικής καταρχάς, στόχευσης θα πρέπει να γίνει προτεραιότητα. Τα βήματα της κυβερνοασφάλειας (cybersecurity) θα πρέπει να είναι σαφή.

Τα δύο βασικά χαρακτηριστικά του κυβερνοεγκλήματος, του οποίου το σημαντικότερο μέρος είναι η κυβερνοτρομοκρατία, προκύπτουν από τη φύση του κυβερνοχώρου και είναι δύο. Η ταχύτητα και η ανωνυμία των επιθέσεων. Παρόλα αυτά, όσο εξαλείφονται τα τρωτά σημεία του εγχώριου δικτύου, τόσο ελαττώνονται οι δυνατότητες παράνομης εισβολής σε αυτό. Τα βασικά αντικείμενα της στρατηγικής είναι τρία.

- i) Η προστασία των κρίσιμων αμερικανικών υποδομών
- ii) Συνεχή αντιμετώπιση των εθνικών τρωτών σημείων
- iii) Αντιμετώπιση των καταστροφών σε όσο το δυνατόν λιγότερο χρόνο.

Η αμερικανική οικονομία εξολοκλήρου εξαρτάται από την ομαλή λειτουργία των ΤΠΕ. Το διαδίκτυο βρίσκεται στον πυρήνα των ΤΠΕ. Επρόκειτο για ένα σύστημα που σχεδιάστηκε από επιστήμονες για συγκεκριμένη λειτουργία, η οποία θα κάλυπτε εθνικές υποθέσεις. Το ίδιο το διαδίκτυο είναι που πλέον διασυνδέει εκατομμύρια ανθρώπους παγκοσμίως. Από αυτό το δίκτυο Η/Υ εξαρτάται η λειτουργία μεταφοράς ηλεκτρικής ενέργειας, των τρένων, των ραντάρ κι άλλων πολλών υπηρεσιών. Σε αυτό το χώρο ελεύθερης πρόσβασης, πολλοί κακόβουλοι θα μπορούσαν να εισέλθουν, με σκοπό να διαπράξουν εγκληματική ενέργεια. Οι αρμόδιες για την ασφάλεια του διαδικτύου υπηρεσίες θα πρέπει να βρίσκονται σε συνεχή επαγρύπνηση. Εδώ εντοπίζεται και ο ρόλος της κυβέρνησης. Αν και αποτελεί κοινή παραδοχή ότι ο ιδιωτικός τομέας είναι αρτιότερα τεχνολογικά εξοπλισμένος.

Κεφάλαιο 9. Η Ψυχο-κοινωνιολογία της Κυριαρχίας στην Ελλάδα και ο Κυβερνοπόλεμος στην τεχνολογική αιχμή

Η άποψη ορισμένων επιστημόνων είναι ότι αν θα έπρεπε να διακρίνουμε μόνο ένα κριτήριο για να χαρακτηρίσουμε μια ομάδα ως εθνοτική, πέρα του χρονοχωρικού προσδιορισμού της (έτος ίδρυσης και εδαφική έκταση), της κοινής γλώσσας και των υπολοίπων στοιχείων (ήθη και έθιμα), αυτό θα ήταν η κοινή αντίληψη του συλλογικού κινδύνου της ομάδας ως προς το κοινωνικοπολιτικό της περιβάλλον (Μάζης, 2006)⁴³. Άμεσο αντίκτυπο αυτής της κοινής συνισταμένης, όταν πρόκειται για έθνος-κράτος, είναι η ανάγκη οικοδόμησης μιας εσωτερικής «στρατηγικής κουλτούρας»⁴⁴ (Ντόκος και Τσάκωνας, 2005). Η έννοια αυτή αφορά τις αξίες, παραδόσεις και στάσεις που διαμορφώνουν τη κοινή γνώμη του κράτους για τα θέματα ασφάλειας. Ένα επιπλέον σημαντικό στοιχείο είναι οι ιδιαίτεροι τρόποι προσαρμογής του στο εκάστοτε διεθνές περιβάλλον. Πηγές της στρατηγικής κουλτούρας είναι η ιστορία, η γεωγραφία και η πολιτική νοοτροπία. Τέλος, μια εννοιολογική οριοθέτηση προσδίδει και το ακόλουθο απόφθεγμα ενός ειδικού.

Με την ανάλυση της στρατηγικής κουλτούρας μπορούν να εντοπιστούν και να διακριθούν τάσεις, όχι καθοριστικοί παράγοντες (Gray, 1986).

Στην ελληνική περίπτωση, για να εμβαθύνουμε στην έκφανση της στρατηγικής κουλτούρας, η οποία αφορά στο συλλογικό αίσθημα ασφάλειας των Ελλήνων, θα πρέπει να εξετάσουμε και συνθέσουμε τα ιδιαίτερα στοιχεία που διαμορφώνουν το κοινωνιο-ψυχολογικό πλαίσιο συμπεριφοράς στα σχετικά θέματα.

- Στοιχείο του Χρόνου. Το διάστημα που, από η συνείδηση μέλους μιας εθνοτικής ομάδας μετατράπηκε σε συνείδηση μέλους του εθνικό-κρατικού μορφώματος είναι 176 χρόνια. Η αξία αυτού του γεγονότος είναι διττή. Πρώτον, θα πρέπει να λάβουμε υπόψη μας ότι το περί ασφαλείας αίσθημα είναι πιο σφριγηλό όταν η ανάγκη του «ανήκειν» καλύπτεται από ένα κράτος, σε σύγκριση με τη στήριξη μιας εθνοτικής -υπό ξένης κυριαρχίας- ομάδα. Δεύτερον, αυτό το διάστημα σημαίνει για τους κοινωνικούς επιστήμονες περίπου επτά γενιές (Τομαρά, 1999). Έτσι γίνεται σαφές ότι η συλλογική μνήμη δεν έχει διαποτιστεί, για επαρκή περίοδο, με το χαρακτηριστικό της σταθερότητας.

43. Σύμφωνα με το συγγραφέα, πρόκειται για έναν όρο κοινωνικού περιεχομένου.

44. Χρησιμοποιείται και ο όρος «Στρατηγική Αγωγή» και ευρύτερα «Πολιτική εθνικής κουλτούρας» (National Defense Policy).

- Στοιχείο του Χώρου. Ένα, ακόμη στοιχείο που δεν συνάδει με το χαρακτηριστικό της σταθερότητας είναι οι πολλές μεταβολές του μεγέθους της εδαφικής έκτασης. Σημαντικό φυσικά, είναι ότι σε γενικές γραμμές αυτό έγινε σε όφελος της χώρας. Εξαιρέση αποτελούν οι περιπτώσεις του 1897 και 1922 (κι ενδεχομένως και του 1973). Αυτή η τελευταία περίπτωση φορτίστηκε έντονα συγκινησιακά, ώστε να μπορούμε να εκτιμήσουμε ότι ακόμη σήμερα είναι νοπή στη συλλογική μνήμη. Κυρίως αυτό συμβαίνει επειδή επρόκειτο για μια τραγωδία με μεγάλες κοινωνικές προεκτάσεις.
- Στοιχείο του «αντιπάλου» πληθυσμού. Αν συνδέσουμε το γεγονός της Μικρασιατικής καταστροφής με την έντονη αντιπαράθεση του τελευταίου μισού αιώνα με το γειτονικό κράτος, θα συμπεράνουμε ότι το αίσθημα περί της εγγύτητας της απειλής παγιώνεται στο μέσο έλληνα. Σε αυτό συνηγορούν και οι πρόσφατες ανακατατάξεις ή όπως τιτλοφορήθηκε τα γεγονότα «αποδόμησης των Βαλκανίων» (Βερέμης, 2002).

Το συμπέρασμα των τριών προαναφερθέντων στοιχείων είναι ότι το πλαίσιο στο οποίο διαμορφώνεται το αίσθημα ασφάλειας των Ελλήνων το διακατέχει υψηλή τρωτότητα. Βεβαίως, υπήρξαν γεγονότα που επηρέασαν θετικά, όπως η εισδοχή της χώρας στην Ευρωπαϊκή Ένωση. Πάντως, αποτελεί κοινή παραδοχή ότι αυτό δεν δικαιολογεί εφησυχασμό. Αυτή η κατάσταση αντανακλάται στη συχνή εκδήλωση υψηλών απαιτήσεων από την εν γένει ηγεσία. Αυτό όμως, μπορεί να γίνει αντικείμενο εκμετάλλευσης από αυτήν. Έτσι, διαπιστώνουμε δύο αντίρροπες πιέσεις, η μία αφορά στη «φωνή του λαού» περί εξασφάλισης και η δεύτερη, η ανάγκη της Ηγεσίας να διατηρήσει τις ισορροπίες της συγκυρίας (αυτές μπορεί να είναι γεωπολιτικές ή και εξυπηρέτησης του ίδιου συμφέροντος). Η κοινή συνισταμένη αυτών των πιέσεων κατευθύνεται στην κάλυψη των ακολούθων -πραγματικών ή φοβικών- αναγκών.

- Διατήρηση του στρατιωτικού εξοπλισμού σε ικανοποιητικό επίπεδο. Αρκεί να αναφέρουμε ότι σύμφωνα με τα στοιχεία της έκθεσης που δόθηκε στη δημοσιότητα στις 26/12/2007 από την Ερευνητική Επιτροπή του Κογκρέσου των ΗΠΑ, για το διάστημα 1999-2006 η Ελλάδα κατατάσσεται στην έκτη θέση αγοράς οπλικών συστημάτων από τις ΗΠΑ⁴⁵, παγκοσμίως. Ακολουθεί ο σχετικός πίνακας.

45. Σε σχέση με το Ακαθάριστο Εθνικό Προϊόν αντιστοιχεί σε ποσοστό περίπου 2%, όταν το σύνολο των αμυντικών δαπανών είναι περίπου 3%.

A	ΧΩΡΑ	b\$	A	ΧΩΡΑ	b\$
1	Σαουδική Αραβία	13,3	5	Νότιο Κορέα	5,6
2	Ταϊβάν	9,9	6	Ελλάδα	5,0
3	Αίγυπτος	9,6	7	Ιαπωνία	3,7
4	Ισραήλ	8,5	8	Βρετανία	3,2

- Συνεχής προσαρμογή στις τεχνολογικές εξελίξεις, των οποίων η ταχύτητα και το μέγεθος έχουν σημαντική επίπτωση στην ασφάλεια της χώρας. Η ελληνική πραγματικότητα στο χώρο της τεχνολογίας άρχισε να αλλάζει από τη δεκαετία του '90 και με γεωμετρική πρόοδο επιχείρησε να συγκλίνει στην ευρωπαϊκή πραγματικότητα τη δεκαετία που διανύουμε. Το πρώτο δείγμα της τάσης των ελλήνων να πορεύονται παράλληλα με την αιχμή της τεχνολογίας το διακρίναμε με τη χρήση των κινητών τηλεφώνων. Τα ποσοστά χρήσης σε ώρες συνομιλίας, καθώς και τα κέρδη των τριών εταιριών παροχής κινητής τηλεφωνίας (Vodafone, Wind και αργότερα Cosmote)⁴⁶ το αποδεικνύουν περίτρανα.

Παρόλα αυτά, άξιο μελέτης είναι ότι ο ενθουσιασμός δεν ήταν ο ίδιος στη χρήση του διαδικτύου. Το 73% των Ελλήνων δεν έχει χρησιμοποιήσει ποτέ το Διαδίκτυο. Το εντυπωσιακό αυτό ποσοστό είναι το υψηλότερο στην Ευρώπη, σύμφωνα με τα στοιχεία της Ευρωπαϊκής Στατιστικής Υπηρεσίας (Eurostat). Πιο αναλυτικά, τα στοιχεία δείχνουν πως μόλις το 22% των νοικοκυριών έχει πρόσβαση στο Διαδίκτυο. Η Ευρωπαϊκή Επιτροπή έχει επικρίνει αρκετές φορές την Ελλάδα για τη μη διάδοση των ευρυζωνικών συνδέσεων, οι οποίες, σύμφωνα με τη Στρατηγική της Λισαβόνας, αποτελούν το σημαντικότερο εργαλείο για τη μετάβαση στην Κοινωνία της Πληροφορίας (in, 2008).

Σύμφωνα με ορισμένα πιο αναλυτικά στοιχεία από τα αποτελέσματα έρευνας, η συντριπτική πλειοψηφία των ερωτηθέντων (72,5%) απαντά ότι χρησιμοποιεί το Internet για αναζήτηση πληροφοριών. Το 36,4% λέει ότι το χρησιμοποιεί για να στέλνει και να δέχεται e-mails, το 20,2% για να «κατεβάζει» μουσική, το 9,7% για να παίζει online παιχνίδια, το 8,6% για να επικοινωνεί μέσω των διαφόρων εργαλείων chatting, το 2,2% για να κατεβάζει προγράμματα και μόλις το 1,9% για να πραγματοποιεί online αγορές.

46. Η εμφάνισή τους στην ελληνική αγορά, την προηγούμενη δεκαετία έγινε με διαφορετικές επωνυμίες (Panafon και Telestet αντίστοιχα).

Όσον αφορά στη διείσδυση του διαδικτύου ανά ηλικιακή ομάδα, το μεγαλύτερο ποσοστό εντοπίζεται στις ηλικίες 13 – 17 ετών. Υψηλά ποσοστά εντοπίζονται και της ηλικίες 18 – 24 ετών (66% και 66,3%), καθώς και στις ηλικίες 25 – 34 ετών (50% και 49%), ενώ τα ποσοστά αυτά μειώνονται -αν και παραμένουν αυξημένα- στην ηλικιακή ομάδα 35 – 44 ετών (40,7% και 37,7%).

Το ενδιαφέρον των άνω στοιχείων, ως προς το θέμα του κυβερνοπολέμου, έγκειται στον εξής συλλογισμό. Ένα κράτος για να είναι ευάλωτο σε κυβερνοεπιθέσεις οποιασδήποτε εκ των τριών μορφών που περιγράψαμε, αλλά κυρίως στην τρίτη (κυβερνοπόλεμος στην ευρεία μάζα των πολιτών), θα πρέπει να έχει ευρύ φάσμα συμμετοχής στις υπηρεσίες του διαδικτύου. Αυτό μπορεί να συμβαίνει, είτε υπό την ενίσχυση της Ηλεκτρονικής Διακυβέρνησης⁴⁷, είτε με τη μεγάλη χρήση από τους πολίτες του διαδικτύου, για τη μεταξύ τους επικοινωνία και ανταλλαγή πληροφοριών. Είναι προφανές ότι τα άτομα που δεν χρησιμοποιούν το διαδίκτυο, δεν μπορούν να γίνουν στόχος στον πόλεμο του κυβερνοχώρου.

Παρόλα αυτά δεν είναι λίγα τα ηλεκτρονικά εγκλήματα στην ελληνική κοινωνία. Όπως μπορούμε να ενημερωθούμε από την ηλεκτρονική σελίδα εφημερίδας (Καθημερινή, 31/1/08):

Στόχος ηλεκτρονικών επιθέσεων έχουν γίνει τα υπουργεία Εσωτερικών και Αγροτικής Ανάπτυξης. Άγνωστοι παραβίασαν τα δίκτυα υπολογιστών και «ανέβασαν» στις ιστοσελίδες προκήρυξη με μηνύματα εναντίον της Αστυνομίας και συμπαράστασης υπέρ των προσφύγων. Οι δράστες, που χρησιμοποίησαν το ψευδώνυμο «ψηφιακή αναρχία» («cyber anarchy») είναι οι ίδιοι που στις 14 Νοεμβρίου έθεσαν εκτός λειτουργίας την ιστοσελίδα του υπουργείου Δικαιοσύνης. Τα αρμόδια τμήματα των υπουργείων κατάλαβαν την επίθεση μόλις το μεσημέρι της ίδιας ημέρας. Το ΥΠΕΣ απομόνωσε το τμήμα της ιστοσελίδας που επλήγη (Γραφείο Τύπου), ενώ το απόγευμα απενεργοποιήθηκε ολόκληρη η σελίδα του υπουργείου Αγροτικής Ανάπτυξης.

47. Ηλεκτρονική Διακυβέρνηση (e-Governance) ορίζεται ο μετασχηματισμός διαδικασιών, οργανωτικών δομών, δραστηριοτήτων και στόχων των Δημόσιων Οργανισμών, καθώς και του τρόπου επικοινωνίας με τους πολίτες, με βάση τις δυνατότητες που παρέχουν οι ΤΠΕ και με στόχο την αύξηση της αποδοτικότητας και της αποτελεσματικότητάς τους (Αποστολάκης, 2006).

Με αφορμή αυτό το τελευταίο συμβάν, ανώτατο στέλεχος της Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ) προανήγγειλε, μέσω της «Καθημερινής» την έναρξη λειτουργίας του Κέντρου Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CERT) σημειώνοντας χαρακτηριστικά: «Η ηλεκτρονική τρομοκρατία είναι απειλή του σήμερα, όχι του αύριο. Είναι επομένως πρόδηλο ότι οι επιθέσεις στους οργανισμούς και υπηρεσίες του Δημοσίου απασχολούν σοβαρά τις ευρωπαϊκές και ελληνικές υπηρεσίες πληροφοριών». Το Κέντρο Αντιμετώπισης Ηλεκτρονικών Επιθέσεων θεσμοθετείται με το νέο σχέδιο νόμου για την αναδιάρθρωση της ΕΥΠ.

Μέχρι σήμερα η Ελλάδα ήταν η μόνη χώρα της Ευρωπαϊκής Ένωσης που δεν διαθέτει αντίστοιχη ομάδα δράσης («Task Force») και οι προσπάθειες προστασίας των κρίσιμων υποδομών από ηλεκτρονικές απειλές να γίνονται δίχως τη συνεργασία των αντίστοιχων υπηρεσιών του εξωτερικού. Τα μέλη του Κέντρου Αντιμετώπισης Ηλεκτρονικών Επιθέσεων θα μπορούν να εντοπίζουν την ταυτότητα των δραστών πριν από την εκδήλωση της επίθεσης (με τη μέθοδο του sniffing), ενώ θα παρέχουν τεχνική υποστήριξη για την αντιμετώπιση τρομοκρατικών επιθέσεων και επιθέσεων υποκλοπής. Το CERT θα απαρτίζεται από την ΕΥΠ, την ΕΛ.ΑΣ. και την ειδική διεύθυνση του Λιμενικού Σώματος. Στο διάστημα από το 2003 ως το 2006 καταγράφηκαν 6.000 ηλεκτρονικές επιθέσεις: το 70% σε νομικά πρόσωπα ιδιωτικού δικαίου, το 20% σε μεγάλες ιδιωτικές εταιρείες και το 10% σε υπουργεία και δημόσιες υπηρεσίες. Στο 90% των περιπτώσεων, δράστες είναι Αλβανοί και Τούρκοι, ενώ το 10% των επιθέσεων εξαπολύονται από servers κρατικών φορέων ξένων χωρών και πραγματοποιούνται στο πλαίσιο του ελέγχου της τρωτότητας των συστημάτων Η/Υ.

Κεφάλαιο 10. Επίλογος: Η φύση του κυβερνο-εγκλήματος

Ο Γουίλλυ Σάτεν (ένας αμερικανός ληστής τραπεζών) απάντησε όταν ερωτήθηκε γιατί επιλέγει τις τράπεζες για κλοπή: Διότι εκεί βρίσκονται τα χρήματα! Πρόκειται για την επιβεβαίωση της βασικής αρχής της εγκληματολογίας, ότι «το έγκλημα αναζητά τις ευκαιρίες» (Grabosky & Smith, 1998).

Στο συγκεκριμένο βιβλίο υποστηρίζεται η άποψη ότι οι σημερινές «ευκαιρίες» για διάπραξη εγκλήματος βρίσκονται -ή ίσως μπορούν να δημιουργηθούν- στις εφαρμογές των σύγχρονων ΤΠΕ. Σε αυτήν την εργασία αναπτύχθηκε, πέραν των πρακτικών προσεγγίσεων, μια επιστημονική σκέψη για το κυβερνο-έγκλημα στο στρατιωτικό τομέα. Αν επιχειρούσαμε να καταγράψουμε μια συζήτηση (αντί επιλόγου) για τις γενικότερες μορφές εγκλήματος που έχουν εμφανισθεί στον κυβερνοχώρο, θα διαπιστώναμε ότι οι αποκλίσεις, σε σχέση με τις μορφές του κυβερνοπολέμου, είναι πολύ μικρές. Σε μια ευρύτερη περιγραφή του κυβερνοχώρου θα λέγαμε ότι περιλαμβάνει διεργασίες από όλους τους τομείς του φυσικού κόσμου, όπως για παράδειγμα τον οικονομικό. Είναι πλέον δημοφιλείς οι εκφράσεις: ηλεκτρονικό κατάστημα – ηλεκτρονικό επιχειρείν – ψηφιακές συναλλαγές κοκ. Και εδώ οι καινοτομίες των ΤΠΕ άλλαξαν τόσο πολύ την κυρίαρχη κατάσταση, ώστε να μιλάμε για «νέα οικονομία». Χρήσιμη είναι η παράθεση του ορισμού που διατυπώθηκε από την Ένωση Επαγγελματιών του Ιντερνέτ, ώστε να γίνει κατανοητός ο τρόπος αλληλεπίδρασης στον οικονομικό τομέα, αλλά και ευρύτερα.

Νέα οικονομία ονομάζουμε το σύνολο όσων επιχειρηματικών δραστηριοτήτων υλοποιούνται, βασισμένες πάνω στην αμφίδρομη ψηφιακή επικοινωνία. Γι' αυτό και σχεδόν πάντοτε οι δράσεις αυτές αξιοποιούν (σε διαφορετικές αναλογίες) τα χαρακτηριστικά της συσσώρευσης, της εξειδίκευσης και του αυτοματισμού. Θα μπορούσαμε με άλλα λόγια να παρομοιάσουμε την νέα οικονομία με ένα οίκημα χτισμένο πάνω σε ένα δίκτυο. Το δίκτυο αποτελείται από της νέους τρόπους με τους οποίους επικοινωνούν μεταξύ τους ιδιώτες με επιχειρήσεις, επιχειρήσεις με άλλες επιχειρήσεις και ιδιώτες με άλλους ιδιώτες (συνήθως μέσω του Internet), ενώ το οίκημα αποτελείται από όσες εφαρμογές αξιοποιούν επιχειρηματικά αυτή την επικοινωνία (Επιτήδειος, 2000).

Σε αυτό το νέο περιβάλλον αλληλεπίδρασης, μέσω της διαδικτυακής επικοινωνίας, παρατηρούμε ότι τα είδη του εγκλήματος παραμένουν ίδια (κλοπή, πορνογραφία κ.λπ.).

Αυτό που αλλάζει μόνο είναι οι τρόποι πραγμάτωσης. Πιο συγκεκριμένα, η καταγεγραμμένη κατηγοριοποίηση περιλαμβάνει (Grabosky & Smith, 1998):

1. Ηλεκτρονικός βανδαλισμός και Τρομοκρατία
2. Κλοπή σε τηλεπικοινωνιακές υπηρεσίες
3. Κυβερνο-πειρατεία
4. Πορνογραφία και συναφή
5. Απάτες από της τηλεδιαφημίσεις
6. Εγκλήματα σε μεταφορές κεφαλαίων μέσω του κυβερνοχώρου
7. Διαδικτυακό «ξέπλυμα» χρήματος

Σήμερα, ένα τεράστιο κεφάλαιο που ανοίγει για συζήτηση στην ακαδημαϊκή κοινότητα, στην πολιτική και στρατιωτική ηγεσία, τις εθνικές υπηρεσίες ασφαλείας κ.τ.λ. είναι αυτό της «Κυβερνο-Τρομοκρατίας». Οποιαδήποτε κίνηση στον κυβερνοχώρο αποσκοπεί στην πίεση της ομάδας-στόχου για πρόκληση φοβικών αντιδράσεων (σε όλα τα οργανωτικά επίπεδα) συνιστά κυβερνοτρομοκρατική ενέργεια. Απάντηση μπορεί να εγγυηθεί μόνο μια συνεργατική προσπάθεια με κύριο αίτημα τον πραγματικό εκδημοκρατισμό του διαδικτύου, ο οποίος προαπαιτεί τον ανθρωποκεντρικό χαρακτήρα του κυβερνοχώρου (Δερτούζος, 2001).

Γ' ΜΕΡΟΣ
ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Α΄

ΜΗ ΕΠΑΝΔΡΩΜΕΝΑ ΟΧΗΜΑΤΑ UAV

Οι πληροφορίες είναι απαραίτητες πριν και κατά τη διεξαγωγή μιας στρατιωτικής επιχείρησης. Βάσει αυτών επιλέγονται οι στόχοι και ακόμα πιο συγκεκριμένα, τα ευάλωτα σημεία της. Τον 21^ο αιώνα, η ανάπτυξη των Τεχνολογιών Πληροφορίας και Επικοινωνίας ήταν αναμενόμενο να επηρεάσουν και τους αμυντικούς σχεδιασμούς. Αυτό επέδρασε σε τέτοιο σημείο, ώστε να μιλάμε για επανάσταση στις στρατιωτικές υποθέσεις (RMA – Revolution in Military Affairs). Τα σύγχρονα στρατιωτικά δόγματα θεωρούν ότι θα πρέπει να ελαττωθεί το διάστημα που μεσολαβεί από τον εντοπισμό ως την καταστροφή του στόχου. Αυτό μπορεί να πραγματοποιηθεί με την ταχύτατη ανταλλαγή δεδομένων εντοπισμού και προσβολής στόχου (Sensor to Shooter).

Στον 1^ο πόλεμο του Κόλπου το παραπάνω διάστημα διαρκούσε από δύο ώρες και σε ορισμένες περιπτώσεις ξεπερνούσε την ημέρα. Στο 2^ο πόλεμο του Κόλπου το διάστημα είχε μέγιστη διάρκεια τη μία ώρα. Και τέλος, στις επιχειρήσεις στο Αφγανιστάν μειώθηκε κάτω της μισής. Σήμερα, στα νέα πλαίσια που διαμορφώνονται από την αξιοποίηση των νέων τεχνολογικών επιτευγμάτων «ζεύξης δεδομένων» (data-link-sat Com), ο χρόνος διάρκειας περιορίζεται σε μονοψήφιο αριθμό λεπτών.

Σε όλη αυτή την απαίτηση για ταχεία και ακριβή συλλογή πληροφοριών συνέβαλαν σημαντικά και τα συστήματα συλλογής πληροφοριών μέσω μη επανδρωμένων αεροσκαφών, γνωστά ως UAVs (Unmanned Aerial Vehicles). Πρόκειται για κατευθυνόμενα αεροσκάφη, τα οποία μπορούν να εξοπλιστούν με κάμερα και αισθητήρες (κυρίως εικόνας) και να συλλέγουν δεδομένα σε δύσκολες καιρικές συνθήκες ημέρας και νύχτας (<http://www.fas.org/irp/program/collect/uav.htm>). Επιπλέον, αν χρειαστεί, έχουν τη δυνατότητα καταστροφής στόχων με πυραύλους (Hellfire και Spike) και κατευθυνόμενες με Laser βόμβες (LGB), τις οποίες φέρουν κάτω από τα πτερύγια τους.

Μια από τις πρώτες χώρες που τα χρησιμοποίησαν ήταν το Ισραήλ. Στις επιχειρήσεις εναντίον της Hezbollah στο Λίβανο το 2006, η συμβολή τους αξιολογήθηκε από τους εμπειρογνώμονες ως ιδιαίτερα αποδοτική. Βεβαίως η διοίκηση και ο έλεγχος τους επιτυγχάνεται με ψηφιακά συστήματα (double data link και συμβατά του Hunter).

ΠΑΡΑΡΤΗΜΑ Β΄

Περιπτώσεις κυβερνο-επιθέσεων παγκοσμίως

1. Ο αμερικανός υφυπουργός Άμυνας Μάικλ Ουάιν ανακοίνωσε ότι στις υφιστάμενες υπηρεσίες κυβερνοπολέμου, η Πολεμική Αεροπορία θα ιδρύσει, με προγραμματισμό υλοποίησης ενός έτους την τρίτη Διοίκηση Κυβερνο-διαστήματος, η οποία θα αναλάβει ηλεκτρονικές επιχειρήσεις σε όλο τον κόσμο, συνδυασμένες με συμβατικές επιχειρήσεις. Την αιτία αποτελούν οι κυβερνοεπιθέσεις εναντίον της Εσθονίας και οι ανακοινώσεις για κινεζικές ηλεκτρονικές επιθέσεις εναντίον δυτικών στόχων. Αντικείμενο της είναι η εκπαίδευση και ο εξοπλισμός δυνάμεων για επιχειρήσεις διαμέσου του κυβερνο-διαστήματος (Γαλλικό Πρακτορείο Ειδήσεων, 18/9/07).

2. Πληροφοριακά συστήματα παραβιάστηκαν στο Λονδίνο, Βερολίνο και Παρίσι, μετά από ηλεκτρονικές επιθέσεις, ενδεχομένως από την Κίνα, η οποία το αρνείται κατηγορηματικά, μέσω του ΥΠΕΞ Jiang Yu.

Ο γενικός γραμματέας του γαλλικού υπουργείου Εθνικής Άμυνας Φράνσις Ντελόν επιβεβαίωσε ανάλογο δημοσίευμα της Monde. Ύποπτοι για κυβερνοεπιθέσεις σε αμερικανικό στόλο αεροπλανοφόρων, είναι δύο χάκερς-μέλη του Λαϊκού Απελευθερωτικού Στρατού της Κίνας. Η Κίνα διεκδικεί μια θέση ανάμεσα στους κύριους ανταγωνιστές στην «κατάκτηση του κυβερνοχώρου», που θεωρούνται οι ΗΠΑ, η Ρωσία και η Βρετανία. Επιδίωξη του Πεκίνου είναι η ηλεκτρονική κυριαρχία ως το 2050 (Times 8/9/2007).

3. Για ενδορωσικό πληροφοριακό πόλεμο κατηγορείται η κυβέρνηση πριν τις πρόσφατες εκλογές, με σκοπό να πλήξει τα υπόλοιπα υποψήφια κόμματα. Η δήλωση ανήκει στον Όλεγκ Πανφίλοφ του Κέντρου Δημοσιογραφίας. Η απάντηση του προέδρου Πούτιν ήταν ότι άγνωστοι χάκερς (με χρήση botnets) χρησιμοποιούν ψευδείς διαδικτυακές διευθύνσεις (IP), οι οποίες φαίνεται ότι ανήκουν στο Κρεμλίνο (Associated Press, 1/7/07).

4. Αξιωματούχοι των Δυνάμεων Ασφαλείας της Αρμενίας κατήγγειλαν ότι Αζέροι ομόλογοι τους διαπράττουν κατασκοπεία με τη χρήση ηλεκτρονικών ιών. Συγκεκριμένα, εντοπίστηκε ο ιός «Perfect Key» σε απεσταλμένα ηλεκτρονικά μηνύματα σε δημόσιες υπηρεσίες του Nagorno-Karabakh. Αυτός ο ιός μετατρέπει τον Η/Υ σε πηγή παροχής των πληροφοριών που διακινεί στο Διαδίκτυο (Ειδησεογραφικό πρακτορείο Regnum, 6/12/07).

5. Πρωτοφανή επίθεση δέχτηκε η ιστοσελίδα του γενικού γραμματέα του ΟΗΕ, Μπαν Κι Μουν. Υπαίτιοι θεωρούνται μάλλον ένας τούρκος και δύο άραβες χάκερ, οι οποίοι διαμαρτύρονταν για την υποστηρικτική πολιτική των ΗΠΑ στο Ισραήλ. Το αποτέλεσμα στην οθόνη ήταν το ακόλουθο μήνυμα:

Αυτή είναι μια ηλεκτρονική διαμαρτυρία ενάντια στο Ισραήλ και των ΗΠΑ. Σταματήστε να σκοτώνετε τα παιδιά και τους αθώους πολίτες. Ειρήνη για πάντα, όχι στον πόλεμο!

Την προκήρυξη υπέγραφαν οι «Karem 125 – Mosted – Gsy». Το ίδιο κείμενο εμφανίστηκε και σε ιστοσελίδες, που αναφέρονταν σε δηλώσεις του νοτιοκορεάτη ιθύνοντα του ΟΗΕ (www.un.org, 12/8/07).

6. Η Γερμανία προσπαθεί να αντιμετωπίσει το κυβερνοέκλημα με την εγκατάσταση «δούρειων ίππων», σε όσους Η/Υ θεωρούνται ύποπτοι για τρομοκρατία. Στην αναζήτηση επιστημόνων του διαδικτύου, οι οποίοι θα μπορούν να ανακαλύψουν τον τρόπο που χρησιμοποιούν οι κυβερνο-τρομοκράτες τις ΤΠΕ, ανακοίνωσε πως κατευθύνονται οι γερμανικές αρχές ασφαλείας ο ΥΠΕΣ Βολφγκάγκ Σόιμπλε. Αυτός ο ιός μπορεί να λειτουργήσει στα πλαίσια της «αντιπληροφόρησης», κατασκοπεύοντας κατασκόπους. Πάντως για τη χρήση του αναμένεται ψήφισμα από το κρατίδιο της Βόρειας Ρηνανίας Βεστφαλίας. Οι χώρες που ήδη έχουν εφαρμόσει αυτό το μέτρο είναι η Ισπανία, η Ρουμανία, η Σλοβενία, η Λιθουανία και η Κύπρος (Deutsche Welle, 4/9/07).

7. Βίντεο με οδηγίες στα αραβικά για την κατασκευή πυροκροτητή εκρηκτικού μηχανισμού, εντοπίστηκε στη δημοφιλή ιστοσελίδα «You Tube». Οι εκφράσεις κλειδιά (key-words) που ανακτούσαν το συγκεκριμένο ιστοχώρο από τη μηχανή αναζήτησης ήταν:

- *Πυροκροτητής από απόσταση*
- *Βομβιστές Αυτοκτονίας*
- *Μαρτυρικός Θάνατος.*

Οι θεατές έβλεπαν στο βίντεο ένα άτομο με χακί παντελόνι, λευκό πουκάμισο και πλαστικά γάντια. Ύποπτος θεωρήθηκε ένας αιγύπτιος φοιτητής στη Νότιο Καρολίνα (Stratfor, 9/10/07).

8. Η βρετανική Υπηρεσία Πληροφοριών αναζητά νέους πράκτορες στο διαδίκτυο, (όπως δηλώθηκε στις 19/10/07). Συγκεκριμένα, από τα κεντρικά γραφεία της στο Cheltenham της δυτικής Αγγλίας, ο κλάδος Αντικατασκοπίας της ΜΙ6 «GCHQ»

ανακοίνωσε ότι έχει προβεί σε αγγελίες στον κυβερνοχώρο και σε video games (Tom Clancy's Splinter Cell: Double Agent, Need for Speed Carbon κ.άλ.).

9. Οπαδοί της Al Qaeda ανακοίνωσαν σε ισλαμική ιστοσελίδα προειδοποίηση για επιθέσεις στη Σουηδία. Στην ιστοσελίδα διατίθεται προβολή βίντεο, στο οποίο διακρίνονται άνδρες με όπλα που φορούν μάσκες. Αυτοί κάνουν διάφορα σχόλια για το γελοιογράφο Lars Vilks και το βασιλιά της Σουηδίας Carl XVI Gustaf (Forum "Al Ekhlas", 4/10/07).

10. Η Al Qaeda αναζητεί υψηλά εξειδικευμένα πρόσωπα, τα οποία να έχουν προηγμένες γνώσεις σε H/Y, επιπέδου διδακτορικού διπλώματος. Θεωρείται δεδομένο ότι το επικοινωνιακό τμήμα της, η As Sahab, έχει στη διάθεση του εξοπλισμό υψηλής τεχνολογίας. Ο εκπρόσωπος της οργάνωσης Mohammed Yussuf, δήλωσε ότι το μορφωτικό επίπεδο είναι υψηλό και μεταξύ άλλων βρίσκονται πολλοί καθηγητές. Τέλος, ο ίδιος υπογράμμισε ότι η οργάνωση διαθέτει μεγάλο αρχείο σε ψηφιακή μορφή.

Για το ίδιο θέμα αναφέρεται ότι τα βίντεο της προβάλλονται σε δύο γλώσσες (αραβική με αγγλικούς υπότιτλους). Το 2006 ανεστάλησαν 16 τέτοια βίντεο, ενώ το 2007, 74 (IntelCenter, 2008*).

11. Ο πρόεδρος Πούτιν και το επιτελείο του, ενώ επί χρόνια προτιμούσαν να προπαγανδίσουν τις θέσεις τους με τα παραδοσιακά μέσα (έντυπα, ραδιόφωνο και τηλεόραση), τώρα επικεντρώνονται στο διαδίκτυο. Διάφοροι υποστηρικτές δημιουργούν φιλοκυβερνητικές ιστοσελίδες, αγοράζουν ιστότοπους και διαμορφώνουν ένα δίκτυο από μπλογκς (Washington Post, 31/10/07).

12. Ιδιαίτερη ανάπτυξη παρατηρείται στη ρώσικη τεχνογνωσία του κυβερνοχώρου. Η βρετανική GUARDIAN έγραψε πως οι ρωσικές Υπηρεσίες Ασφαλείας (FSB) έχουν ξεκινήσει ένα εγχείρημα για τη εγκαθίδρυση τύπου διαδικτύου με βασική γλώσσα την κυριλλική, το οποίο θα είναι ανεξάρτητο από τον παγκόσμιο ιστό (WWW). Ο πυρήνας του ζητήματος βρίσκεται στο αν οι ρωσικές Αρχές θα αποφασίσουν να αποχωρήσουν από την «Διαδικτυακή Εταιρεία Ονοματοδοσίας και Αριθμοδότησης» (ICANN), δημιουργώντας μια αντίστοιχη ρωσόφωνη για τον έλεγχο της διακίνησης των πληροφοριών στον κυβερνοχώρο.

* Ιδιωτική αντιτρομοκρατική οργάνωση των ΗΠΑ.

Το σημαντικότερο πρόβλημα που θα παρουσιαστεί είναι η δυσχέρεια στις μηχανές αναζήτησης, οι οποίες δεν θα μπορούν να ανακτούν δεδομένα με λατινικούς χαρακτήρες. Έτσι, θα πρέπει εξαρχής να προβλεφθεί η «κατασκευή μιας γέφυρας» για το αλφάβητο ASCII (AXIS GLOBE, 14/1/08).

12. Ειδικοί στα θέματα διαδικτυακής ασφάλειας των κρατικών αρχών εκτιμούν ότι το 2008 ίσως να αναδειχθεί σε έτος κατασκοπείας στον κυβερνοχώρο. Όπως τονίζουν αυτό αποτελεί κίνδυνο, όχι μόνο για το δημόσιο, άλλα και για τον ιδιωτικό τομέα. Ενδεικτικά, η εταιρεία MCAFEE προειδοποίησε ότι ενδεχόμενες κυβερνοεπιθέσεις μπορούν να κατευθυνθούν ενάντια ακόμα και σε διεθνείς οργανισμούς, όπως το NATO και το FBI. Τέλος, υπογραμμίζουν ότι βασικός στόχος των hackers θα είναι τα Πανεπιστήμια (www.netzeitung.de, 5/12/07).

ΠΑΡΑΡΤΗΜΑ Γ΄

Περιπτώσεις κυβερνο-επιθέσεων στην Ελλάδα

1. Ανθελληνικοί ιστότοποι με ιστορικές ανακρίβειες από τα Σκόπια έχουν κατακλύσει το διαδίκτυο. Ορισμένα αξιοσημείωτα στατιστικά στοιχεία είναι:

- Με λέξη-κλειδί αναζήτησης στο Google τη «Macedonia» τα αποτελέσματα είναι περίπου 73 εκατομμύρια.
- Από τα δέκα (10) πρώτα αποτελέσματα, μόλις τα (3) αναφέρονται σε ελληνικούς ιστότοπους.
- Οι περισσότεροι ιστότοποι περιέχουν σε εμφανείς θέσεις χάρτες, οι οποίοι ταυτίζουν τη χώρα με όλη τη γεωγραφική περιοχή της Μακεδονίας, η οποία στο μεγαλύτερο μέρος ανήκει στην Ελλάδα και σε μικρότερο στη Βουλγαρία.
- Στο παιχνίδι «Age of Empires» υπάρχει ιστορική αναφορά σε χώρα «Macedonia».
- Στα περισσότερα διεθνή λογισμικά στις λίστες με τις γλώσσες για τις γραμματοσειρές, υπάρχει η επιλογή της «Macedonia» (Εφημερίδα Πολιτών, 7/8/07).

2. Τούρκοι χάκερς ανάρτησαν της διευθύνσεις των δικών της ιστοσελίδων, εγκαθιστώντας σχετική μουσική υπόκρουση και φωτογραφίες των τουρκικών Ενόπλων Δυνάμεων και με φόντο μια τουρκική σημαία.

Πιο συγκεκριμένα, την 1^η Νοεμβρίου του 2007 «ψηφιακή εισβολή» δέχτηκε ο έλληνας βουλευτής Σερρών Μάρκος Μπόλαρης. Στην πρώτη σελίδα που εμφανίζεται στον ιστότοπο του βουλευτή ήταν αναρτημένη η φωτογραφία ενός νεκρού κούρδου αντάρτη, με το πρόσωπο πολτοποιημένο. Αργότερα εμφανιζόταν ένας τούρκος μεταμφιεσμένος σε ιάπωνα ειδικό πολεμιστή (νίντζα). Τονίζουμε το πρωτοφανές γεγονός οι κυβερνοπειρατές να αφήνουν και τα στοιχεία της ηλεκτρονικής τους διεύθυνσης (Μακεδονία 2/11/07).

3. Προβολή των θέσεων του ως πρόεδρος της αυτοαποκαλούμενης «Ευρωπαϊκής Ομοσπονδίας Τούρκων Δυτικής Θράκης (ΑΒΤΤΦ)» έκανε ο Χαλίτ Χαμπίπογλου μέσω της διαδικτυακής εφημερίδας με ηλεκτρονική διεύθυνση <http://www.trakyanethaber.com>.

4. Ολόκληρη ιστοσελίδα αφιέρωσαν οι τούρκοι για να προπαγανδίσουν τις απόψεις τους ενάντια του Οικουμενικό Πατριαρχείο της Κωνσταντινούπολης. Σημαντικό είναι ότι τα υπερκείμενα είναι στην ελληνική γλώσσα, στα οποία το Πατριαρχείο χαρακτηρίζεται «εικονικό». <http://www.bulgarmak.org/patriarchate.htm>

ΠΑΡΑΡΤΗΜΑ Δ΄

Αποκαλύψεις περί Προπαγάνδας

Δι. Τεχνική της Προπαγάνδας

Με τον όρο «Προπαγάνδα» επικαλούμαστε μια διαδικασία πειθούς, με σκοπό τον έλεγχο της κοινής γνώμης. Στην κατακριτέα μορφή της έχει γενικό σκοπό να «θολώσει» τις γνωστικές διεργασίες, ώστε το άτομο να μη χρησιμοποιεί τη λογική του, για αυτόν το λόγο χαρακτηρίστηκε διανοητικός πόλεμος*. Η ομάδα που σχεδιάζει τον τρόπο προβολής των επιχειρημάτων της, μπορεί να επιλέξει τα ακόλουθα μέσα επικοινωνίας με την ομάδα στόχο (target group):

- Διαπροσωπική επαφή
- Μοίρασμα έντυπου υλικού ή
- Εκπομπή μηνυμάτων από μεγάφωνο
- Μέσα Μαζικής Ενημέρωσης και
- Διαδίκτυο

Ενδεικτική Μέθοδος

- Κολακεία στόχου. Στο πρώτο βήμα επιχειρείται να κερδηθεί η εμπιστοσύνη του στόχου, δημιουργώντας κλίμα συμπάθειας.
- Γνωστική – Συγκινησιακή Σύγχυση. Στο δεύτερο βήμα αποσπάται η προσοχή του ατόμου, ώστε η πρόταση που θα ακολουθήσει, ή να αιφνιδιάσει ή να λυτρώσει.
- «Πέρασμα» Μηνύματος. Η επιτυχία της τεχνικής εξαρτάται κυρίως από το πλαίσιο παρουσίασης. Πρόκειται για ένα «παιχνίδι» με τις αισθήσεις (κατάλληλες εικόνες και μουσική).

Παράδειγμα

Έστω ότι ο σκοπός είναι ένα μήνυμα εναντίον των μεταναστών που κατοικούν στη χώρα. Καταρχάς, ξεκινάει μια αφήγηση για τις παραδόσεις και τα κατορθώματα του λαού (κολακεία). Κατόπιν, προβάλλονται απότομα συνθήκες εισβολής από το «ξένο στοιχείο» (σύγχυση), το οποίο υπονοείται ότι είναι η αιτία του κακού. Τέλος, προτείνεται ένας διαφορετικός κόσμος παρόμοιος με τον παραδοσιακό, ως η λύση του προβλήματος.

* Τον όρο «διανοητικός πόλεμος» (Geistige Kriegführung) επινόησαν οι Γερμανοί, οι οποίοι θεωρούσαν ότι πρέπει να απευθύνονται στο κατώτερο μορφωτικά κοινό, μιας και οι διανοούμενοι θα μπορούσαν να το αντιληφθούν... Εξάλλου, η λογική πείθει και το συναίσθημα εξαναγκάζει.

Δii. Διαδικτυακή προπαγάνδα

Ενδιαφέρον έχει η δημοσίευση που ανακτήθηκε από την ηλεκτρονική σελίδα <http://syrizavrona.pblogs.gr/2007/12/paihnidia-toy-myaloy.html> (ΓΑΛΕΡΑ, 12/2007).

Η διαρκής ανάπτυξη του διαδικτύου δημιουργεί διαφορετικά δεδομένα ως προς τις νέες μορφές των ψυχολογικών επιχειρήσεων. Οι δυνατότητες του νέου μέσου ξεδιπλώθηκαν ως ένα βαθμό στην περίπτωση του βομβαρδισμού της Σερβίας από το ΝΑΤΟ. Μετά την καταστροφή από πύραυλο του κτιρίου της σερβικής κρατικής τηλεόρασης στο κέντρο του Βελιγραδίου, επειδή είχε θεωρηθεί όργανο της προπαγάνδας του Μιλόσεβιτς, η κυβέρνηση των ΗΠΑ «μεγαλόψυχα» αποφάσισε να μην «κόψει» την πρόσβαση των Σέρβων στο διαδίκτυο. Θεώρησε ότι με αυτό τον τρόπο θα είχαν τη δυνατότητα να πληροφορηθούν για τα εγκλήματα ενάντια στην ανθρωπότητα που ετοιμάζε το καθεστώς Μιλόσεβιτς στο Κόσσοβο. Υπό αυτή την έννοια, ο πόλεμος στο Κόσσοβο μπορεί να θεωρηθεί ως ο πρώτος «πόλεμος του διαδικτύου».

Στα νέα μέσα που έχουν εμπλουτίσει το «οπλοστάσιο» της μαζικής επικοινωνίας (διαδίκτυο, sms, δορυφόροι, ιπτάμενες πλατφόρμες μετάδοσης εκπομπών) και τα οποία λειτουργούν με έναν πιο εκλεπτυσμένο και αδιαφανή τρόπο ο στόχος των ψυχολογικών επιχειρήσεων παραμένει ο ίδιος. Η καλλιέργεια κλίματος αναστάτωσης και εξέγερσης στο εσωτερικό του εχθρού, αλλά και η απόκτηση ηθικού πλεονεκτήματος (*εμείς είμαστε οι καλοί*) ώστε να νομιμοποιηθεί στα μάτια της παγκόσμιας κοινής γνώμης η προετοιμαζόμενη πολεμική επιχείρηση.

Στις 16 Οκτωβρίου ο υπουργός Άμυνας των ΗΠΑ, προλογίζοντας ουσιαστικά τις «αποκαλύψεις» του Μπους Τζούνιορ περί Τρίτου Παγκοσμίου Πολέμου, δήλωνε ότι όλα τα ενδεχόμενα για την αντιμετώπιση του Ιράν πρέπει να μείνουν ανοικτά («Reuters»: «Gates says all options on table for Iran»). Τον χορό της προετοιμασίας της διεθνούς κοινής γνώμης για τον νέο «μπαμπούλα» που ακούει στο όνομα Ιράν τον είχαν ανοίξει τα γεράκια της αμερικανικής εξωτερικής πολιτικής. Στην περίπτωση βέβαια αυτή έδαφος για ευνοϊκότερο κλίμα ως την ανάπτυξη ψυχολογικών επιχειρήσεων (PSYOPS) προσφέρουν αναμφίβολα οι λαϊκιστικές δηλώσεις της πρόεδρου Αχματινετζάντ, ο οποίος ταυτίζει το Ισραήλ με τον σατανά.

Όπως υπογραμμίζει ο καθηγητής επικοινωνίας Phil Taylor, «η αμερικανική κυβέρνηση του Τζορτζ Μπους Τζουνιόρ δεν κάνει πλέον διάκριση ανάμεσα σε μία συνέντευξη Τύπου και μια στρατιωτική ψυχολογική καμπάνια». Έτσι, τέσσερα χρόνια μετά τη συμμαχική επέμβαση στο Ιράκ και ενώ οι κατηγορίες εναντίον του για την ύπαρξη πυρηνικών και χημικών οπλοστασίων δεν έχουν ακόμα αποδεχθεί, οι ΗΠΑ ετοιμάζουν προληπτική επίθεση σε μία ακόμα χώρα από τον περίφημο Άξονα του Κακού. Οι όροι «Άξονας του Κακού, Σοκ, Δέος και Τρίτος Παγκόσμιος Πόλεμος» χρησιμοποιούνται καθαρά στο πλαίσιο των Ψυχολογικών Επιχειρήσεων.

Δiii. Μέθοδος Διαδικτυακής Προπαγάνδας

Έχουμε το στόχο, ο οποίος συνίσταται από το άθροισμα των ατόμων που επιθυμούμε να επηρεάσουμε. Αναλόγως με το μέσο που χρησιμοποιείται ο στόχος καλείται κοινό (για το έντυπο), ακροατήριο (για το ραδιόφωνο), τηλεθεατές (για την τηλεόραση) και τέλος, χρήστες (για το διαδίκτυο). Ο στόχος διακρίνεται στον εσωτερικό (εγχώριος) και στον εξωτερικό. Ο εξωτερικός στόχος διακρίνεται σε φίλιος, ουδέτερος και εχθρικός.

Οι αλλαγές που έφεραν οι ΤΠΕ στη διακίνηση της πληροφορίας, διαμόρφωσαν νέες απαιτήσεις στο στρατηγικό σχεδιασμό ψυχολογικών επιχειρήσεων. Τα βήματα είναι:

Α. Η δημιουργία μιας κεντρικής βάσης δεδομένων (data base), σχετικά με άτομα σε «θέσεις-κλειδιά», σύνολα ατόμων συντονισμένα σε έναν θυμικό σκοπό (π.χ. εθνικές και θρησκευτικές πεποιθήσεις) και τέλος, επιλεγμένα κράτη. Η κεντρική ιδέα εδώ, είναι η στόχευση συλλογής διαβαθμισμένων πληροφοριών για την κουλτούρα (κίνητρα συμπεριφοράς) των πιθανών στόχων. Σκοπός είναι η κατασκευή ενός μοντέλου-οδηγού των χρήσιμων πληροφοριών για τους λήπτες αποφάσεων.

Β. Εκτός της επεξεργασίας, το παραπάνω αρχείο θα πρέπει να έχει και συνεχή ενημέρωση (update), ώστε τα δεδομένα να βρίσκονται πάντα σε «πραγματικό χρόνο».

Γ. Η επιτυχής επίτευξη του στόχου, κατά τη διενέργεια των επιχειρήσεων, προϋποθέτει την προηγούμενη εξασφάλιση της διαλειτουργικότητας.

Δ. Η διατήρηση μιας ιστοριογραφίας σχετικά με τις τεχνικές και υλοποιήσεις άλλων κρατών, κατά το παρελθόν, ώστε να εξετάζεται τι προσαρμόζεται.

Ε. Το πιο σημαντικό στοιχείο στη λήψη αποφάσεων σε κρίσιμες περιόδους (με το χαρακτηριστικό της αβεβαιότητας) είναι ο Χρόνος. Όλα τα άνω το εξουδετερώνουν.

ΠΑΡΑΡΤΗΜΑ Ε΄

Η΄ ΑΝΑΘΕΩΡΗΤΙΚΗ ΒΟΥΛΗ - ΠΕΡΙΟΔΟΣ ΙΒ΄ - ΣΥΝΟΔΟΣ Α΄
ΕΙΔΙΚΗ ΔΙΑΡΚΗΣ ΕΠΙΤΡΟΠΗ ΕΥΡΩΠΑΪΚΩΝ ΥΠΟΘΕΣΕΩΝ
ΔΙΑΡΚΗΣ ΕΠΙΤΡΟΠΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ, ΤΑΞΗΣ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗΣ
11 Ιανουαρίου 2008, ημέρα Παρασκευή και ώρα 11.10

"Εξέταση της πρότασης απόφασης - πλαισίου του Συμβουλίου σχετικά με την τροποποίηση της απόφασης - πλαισίου 2002/475/ΔΕΥ για την καταπολέμηση της τρομοκρατίας".

ΕΛΙΣΑΒΕΤ (ΕΛΣΑ) ΠΑΠΑΔΗΜΗΤΡΙΟΥ (Α΄ Αντιπρόεδρος της Βουλής και Προεδρεύουσα των Επιτροπών): Το λόγο έχει η κυρία Παπακώστα.
ΑΙΚΑΤΕΡΙΝΗ ΠΑΠΑΚΩΣΤΑ (Εισηγήτρια της Πλειοψηφίας): Μετά τις δηλώσεις της Κυβέρνησης, μπορούμε να τοποθετηθούμε υπεύθυνα πάνω στο θέμα που συζητούμε σήμερα. Ξεκινάμε από την παραδοχή ότι η τρομοκρατία αποτελεί μια από τις σοβαρότερες απειλές της Δημοκρατίας, της ελεύθερης άσκησης των ανθρωπίνων δικαιωμάτων και των ατομικών ελευθεριών και της κοινωνικής και οικονομικής ανάπτυξης. Η παραδοχή αυτή δεν επιδέχεται καμία αμφισβήτηση.

Η ραγδαία ανάπτυξη των ηλεκτρονικών μέσων, όπως είναι ο κυβερνοχώρος και η δυνατότητα πρόσβασης σε οποιοδήποτε αρχείο ηλεκτρονικού συστήματος, "εγκαινιάζει" μια νέα παράμετρο στα ζητήματα ασφάλειας και δίνει μια επιπλέον διάσταση στην έννοια της τρομοκρατίας.

Όλοι γνωρίζουμε πως οι σύγχρονες τεχνολογίες, στον τομέα της πληροφορίας και τεχνολογίας, διαδραματίζουν πολύ σημαντικό ρόλο στη διάδοση της τρομοκρατικής απειλής, για την οποία συζητάμε σήμερα. Ειδικότερα, το διαδίκτυο είναι φθινό, γρήγορο, εύκολα προσβάσιμο και σχεδόν παγκόσμιας εμβέλειας. Αντιλαμβάνεσθε ότι όλα αυτά τα πλεονεκτήματα, που τα απολαμβάνουν οι πολίτες των δημοκρατικών κρατών του κόσμου, είναι πλεονεκτήματα από τα οποία επωφελούνται καθημερινά από τον κυβερνοχώρο και οι τρομοκράτες εξίσου.

Οι τελευταίοι χρησιμοποιούν το διαδίκτυο, κυρίες και κύριοι συνάδελφοι, για να διαδώσουν την προπαγάνδα τους, με στόχο την κινητοποίηση και τη στρατολόγηση, καθώς και οδηγίες χρήσης και εγχειρίδια σε ηλεκτρονική μορφή, που προορίζονται για την εκπαίδευση τρομοκρατών ή τον σχεδιασμό επιθέσεων, που απευθύνονται σε υποστηρικτές τόσο υπάρχοντες όσο και δυνητικούς. Άρα, μιλούμε για στρατολόγηση μέσω του διαδικτύου.

Ο κυβερνοχώρος, το διαδίκτυο αποτελεί κατά τον τρόπο αυτό, επομένως, μια από τις βασικές δυνάμεις πυροδότησης διαδικασιών ριζοσπαστικοποίησης και στρατικοποίησης, στρατολόγησης, καθώς επίσης χρησιμεύει και ως πηγή πληροφοριών σχετικά με τα τρομοκρατικά μέσα και τις μεθόδους, λειτουργώντας περίπου ως οιωνοί εικονικών στρατοπέδων εκπαίδευσης.

Θα σας αναφέρω ένα παράδειγμα, για να γίνουμε πιο πρακτικοί. Οι βομβιστικές επιθέσεις, όπως εκείνη της Μαδρίτης, πραγματοποιήθηκαν με τη χρήση εκρηκτικών υλών, που διατίθενται στο εμπόριο μέσω του διαδικτύου. Η διάδοση, λοιπόν, της προπαγάνδας και της τεχνογνωσίας των τρομοκρατών, μέσω του διαδικτύου, συμπληρώνει και ενισχύει την παραδοσιακή, ιδεολογική, μέσα σε εισαγωγικά ή έξω από εισαγωγικά, χειραγώγηση και εκπαίδευση και συμβάλει στην ανάπτυξη ενός ισχυρότερου και ευρύτερου δικτύου ενεργών τρομοκρατών και υποστηρικτών τους.

Μια Έκθεση των Η.Π.Α., για παράδειγμα, αναφέρει χαρακτηριστικά ότι ακραίες τρομοκρατικές ομάδες κάνουν τόσο εκτεταμένη, αλλά και συστηματική χρήση του κυβερνοχώρου, έχοντας καταστήσει το πληκτρολόγιο του υπολογιστή εξίσου σημαντικό

με ένα καλάζνικοφ. Αυτή είναι η παρομοίωση. Συγκεκριμένα χρησιμοποιούν το internet με διάφορους τρόπους. α) Τα μηνύματα e - mail, που δεν στέλνονται αλλά αποθηκεύονται σε συγκεκριμένα σημεία, ώστε να διαβάζονται απ' όσους έχουν πρόσβαση στα συγκεκριμένα δίκτυα. β) Τα εγχειρίδια εκπαίδευσης, που βρίσκονται καλά κρυμμένα σε φαινομενικά αθώους καταλόγους του διαδικτύου. γ) Η έρευνα για πιθανούς στόχους. δ) Η εξεύρεση πόρων μέσω διαδικτυακών ανώνυμων προσφορών. ε) Τα chat rooms.

Όπως αντιλαμβάνεσθε, αυτό είναι ένα γεγονός που κάνει τον εντοπισμό των τρομοκρατών ακόμη δυσκολότερο. Μέσα από το διαδίκτυο, οι τρομοκράτες μπορούν να διαδώσουν ανενόχλητοι την προπαγάνδα τους για την σύγκρουση των πολιτισμών. Η πιο θανάσιμη εφαρμογή του internet δεν είναι η αναμετάδοση, κυρίες και κύριοι συνάδελφοι, των πληροφοριών, αλλά η χρήση τους ως μέσα επικοινωνίας μεταξύ ανθρώπων στο κυβερνοχώρο, οι οποίοι συντονίζουν μέσα από τον κυβερνοχώρο τις πράξεις τους και αναλαμβάνουν τη δράση, στη συνέχεια, στον πραγματικό κόσμο. Αυτά αναφέρει η Έκθεση.

Θα πρέπει, λοιπόν, να σας πω ότι η πρόληψη μιας τέτοιας αυξανόμενης απειλής αποτελεί πολιτική προτεραιότητα σε ευρωπαϊκό, αλλά και σε διεθνές επίπεδο. Η Ε.Ε. πρέπει να καταπολεμήσει τη σύγχρονη τρομοκρατία και το νέο τρόπο λειτουργίας της με την ίδια αποφασιστικότητα που επέδειξε για την καταπολέμηση της παραδοσιακής τρομοκρατίας. Άρα, καταλήγοντας, λέμε πως είναι αναγκαίο να προσαρμοσθούν, στο νέο modus operandi των τρομοκρατών, οι σημερινές συμπληρωματικές προσπάθειες για την καταπολέμηση της τρομοκρατίας, τόσο σε εθνικό επίπεδο όσο και σε επίπεδο Ε.Ε..

Αναφέρω χαρακτηριστικά πως βίαιες τρομοκρατικές επιθέσεις σημειώθηκαν, τα τελευταία χρόνια, στο έδαφος της Ένωσης, στη Μαδρίτη το Μάρτιο του 2004, στο Λονδίνο τον Ιούλιο του 2005. Πολλά άλλα τρομοκρατικά σχέδια εξουδετερώθηκαν πρόσφατα στην Αυστρία, στη Δανία, στη Γαλλία, στη Γερμανία και στο Ηνωμένο Βασίλειο. Η προτεινόμενη τροποποίηση της απόφασης - πλαισίου του Συμβουλίου της 13ης Ιουνίου του 2002, που εξετάζουμε, στοχεύει στην εναρμόνιση των εθνικών διατάξεων σχετικά με τη δημόσια πρόκληση για τέλεση τρομοκρατικών εγκλημάτων, τη στρατολόγηση και την εκπαίδευση τρομοκρατών, κατά τρόπο ώστε οι συμπεριφορές αυτές να είναι αξιόπινες σε όλη την Ε.Ε., περιλαμβανομένων και εκείνων που διαπράττονται μέσω του διαδικτύου και να υπάρξουν, παράλληλα, εγγυήσεις ότι οι ισχύουσες διατάξεις, σχετικά με τις ποινές, την ευθύνη των νομικών προσώπων, καθώς και τη δικαιοδοσία και την άσκηση ποινικών διώξεων απέναντι σε τρομοκρατικά εγκλήματα, θα εφαρμόζονται, επίσης, σε τέτοιου είδους συμπεριφορές.

Η Ελλάδα συντάσσεται με τις προσπάθειες κατά της τρομοκρατίας και σε διεθνές επίπεδο, κάτω από την ηγεσία των Ηνωμένων Εθνών και συνεργάζεται στενά με τα κράτη - μέλη της Ε.Ε. για την καταπολέμηση της τρομοκρατίας. Η πρόταση συμφωνεί με τη στρατηγική και το σχέδιο δράσης της Ε.Ε. σχετικά με τη ριζοσπαστικοποίηση και στρατολόγηση τρομοκρατών, ενημερώνει και συμπληρώνει το αντιτρομοκρατικό νομικό πλαίσιο της Ε.Ε. και τηρεί - εδώ είναι πάρα πολύ σπουδαίο να το υπογραμμίσουμε - το χάρτη θεμελιωδών δικαιωμάτων της Ε.Ε., ενώ υπογραμμίζει, παράλληλα, τη σημασία της διεθνούς συνεργασίας, στο πλαίσιο των υπάρχοντων οργανώσεων και μηχανισμών συνεργασίας.

Κυρίες και κύριοι συνάδελφοι, θέλω να υπογραμμίσω πώς στόχος μας είναι να παραμείνει η διατήρηση, η κατοχύρωση, η θωράκιση και η εξασφάλιση της κατάλληλης ισορροπίας μεταξύ του θεμελιώδους δικαιώματος ασφάλειας των πολιτών, του δικαιώματος στη ζωή και των άλλων θεμελιωδών ατομικών δικαιωμάτων, περιλαμβανομένης και της προστασίας της ιδιωτικής ζωής και των δικονομικών δικαιωμάτων. Χαίρομαι πολύ που η Κυβέρνηση σήμερα, απευθυνόμενη στο νομοθετικό Σώμα, στην Εθνική μας Αντιπροσωπεία, απολύτως αποσαφήνισε πως αυτό είναι κορυφαίο ζήτημα.

Άρα, λοιπόν, όπως τονίζεται και στην αιτιολόγηση της πρότασης, αφού λειτουργούμε με

αυτό τον τρόπο, είναι σημαντικό να περιληφθούν τα εγκλήματα αυτά και στην απόφαση - πλαίσιο για την καταπολέμηση της τρομοκρατίας, για τους εξής λόγους. Διότι, πρέπει να αιτιολογήσουμε γιατί ζητούμε να συμπεριληφθούν αυτά τα εγκλήματα στην απόφαση - πλαίσιο και γιατί ζητείται από την Ε.Ε. να τα συμπεριλάβουμε.

Πρώτον, υπάρχουν τα πλεονεκτήματα ενός πιο ολοκληρωμένου θεσμικού πλαισίου της Ε.Ε. και, ιδίως, αποφεύγουμε τις μακροχρόνιες διαδικασίες υπογραφής και επικύρωσης, όπως για τις συμβάσεις του Συμβουλίου της Ευρώπης. Έχουμε εφαρμογή καταλλήλων μηχανισμών παρακολούθησης και κοινή ερμηνεία από το δικαστήριο, που είναι πάρα πολύ σημαντική. Δεύτερο πλεονέκτημα είναι ότι η απόφαση - πλαίσιο προβλέπει ένα ειδικό νομικό καθεστώς, ιδίως όσον αφορά στο είδος, το επίπεδο των ποινικών κυρώσεων, καθώς και τους υποχρεωτικούς κανόνες δικαιοδοσίας, που θα εφαρμόζονται, επίσης, στις νεοσυσταθείσες αξιόποινες πράξεις. Η απόφαση - πλαίσιο αποτελεί βασικό μέσο της αντιτρομοκρατικής πολιτικής της Ε.Ε.. Επομένως, η ρητή ενσωμάτωση των ειδικών αυτών προπαρασκευαστικών πράξεων προωθεί τους μηχανισμούς συνεργασίας της Ε.Ε.

Κυρίες και κύριοι συνάδελφοι, η προστιθέμενη αξία της ενσωμάτωσης της δημόσιας πρόκλησης για τέλεση τρομοκρατικών εγκλημάτων, καθώς και της στρατολόγησης και εκπαίδευσης τρομοκρατών στην έννοια της τρομοκρατίας - ευρωπαϊκής έννοιας αναλύεται στο κεφάλαιο που αναφέρεται στην αξιολόγηση των επιπτώσεων. Η παρούσα πρόταση, που θα εξετάσουμε εδώ, περιλαμβάνει την αξιολόγησή της σε ευρωπαϊκό και διεθνές επίπεδο, παρουσιάζει τις ισχύουσες διατάξεις, στον τομέα της πρότασης, τη συνοχή τους, την εναρμόνισή τους με τις άλλες πολιτικές και στόχους της Ένωσης. Στο δεύτερο μέρος περιλαμβάνει τη διαβούλευση των ενδιαφερομένων μερών, μέσα από τρία ερωτηματολόγια και τέλος, στο τρίτο μέρος, τη νομική βάση της τροποποίησης της απόφασης - πλαισίου, η οποία -αυτό είναι θεμελιώδες - είναι σύμφωνη με τις αρχές της επικουρικότητας και της αναλογικότητας.

Κυρίες και κύριοι συνάδελφοι, πρέπει να πω, κλείνοντας, ότι θέλω να δώσω μεγαλύτερη σημασία στη νομική βάση, στα νομικά στοιχεία της πρότασης. Για τη νομική βάση, θα έλεγα το εξής: η αρχή της επικουρικότητας στη δράση της Ένωσης εφαρμόζεται. Οι στόχοι, λοιπόν, της πρότασης δεν μπορούν να πραγματοποιηθούν με ικανοποιητικό τρόπο, εκ μέρους των κρατών - μελών, για τους ακόλουθους λόγους.

Η σύγχρονη τρομοκρατία αποτελεί έντονο παγκόσμιο φαινόμενο, οι πολιτικές της Ένωσης για την καταπολέμηση της τρομοκρατίας, καθώς και την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο δεν θα πετύχουν το στόχο τους, παρά μόνο εάν τα κράτη - μέλη συντονίσουν τις προσπάθειές τους και επιτύχουν συνεργασία σε διεθνές επίπεδο και εάν δεν προσαρμόσουμε, στο νέο *modus operandi* των τρομοκρατών, τις σημερινές συμπληρωματικές προσπάθειές μας για την καταπολέμηση της τρομοκρατίας, τόσο σε εθνικό όσο και σε επίπεδο Ε.Ε..

Κατά συνέπεια κυρίες και κύριοι βουλευτές, αυτή συμφωνεί με την αρχή της επικουρικότητας. Η πρόταση τηρεί την αρχή της αναλογικότητας για τους εξής λόγους. Ως απόφαση πλαίσιο δεσμεύει τα κράτη μέλη ως προς το επιδιωκόμενο αποτέλεσμα μεν, αλλά αφήνει την οριοθέτηση του πεδίου εφαρμογής στις εθνικές αρχές ως προς τη μορφή, αλλά και τις μεθόδους εφαρμογής. Οι διατάξεις της Οδηγίας σχετικά με το ηλεκτρονικό εμπόριο και με την διατήρηση των δεδομένων παραμένουν αμετάβλητες, έτσι ώστε δεν υπάρχει καμία νέα υποχρέωση για τους παρόχους υπηρεσιών τηλεπικοινωνιών ή τους φορείς εκμετάλλευσης. Έχει επίσης, μόνο ως αποτέλεσμα την αυξημένη χρήση των υπαρχόντων μηχανισμών που προβλέπονται στις οδηγίες για το ηλεκτρονικό εμπόριο και για την διατήρηση των δεδομένων.

Κυρίες και κύριοι συνάδελφοι, ως προς την επιλογή των μέσων, προτεινόμενα μέσα είναι η απόφαση πλαίσιο που βασίζεται στο άρθρο 34 παρ. 2 σημείο β' της Συνθήκης της Ε.Ε.. Επειδή ο στόχος είναι η προσέγγιση των νομοθεσιών, τα άλλα μέσα δεν είναι κατάλληλα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνικές Αναφορές

- Αλειφαντής Σ. (2002) *Το Σύστημα Διαχείρισης Δεδομένων Crisis Eval*, Αθήνα: Εκδόσεις Φλώρου.
- Αλεξιάς Γ. (2006) *Παραδόσεις στο μάθημα «Δυνητική Οργάνωση» του ΜΠΣ: Δυνητικές Κοινότητες – Τμ. Ψυχολογίας, Πάντειο Π. Αθήνα.*
- Βαρβαρούσης Π. (1998) *Στρατηγική των Παιγνίων*, Αθήνα: Εκδόσεις Παπαζήση.
- Βαρλάμης Η. και Γιαννακουλόπουλος Α. (2007) *Παραδόσεις στο μάθημα «Διαχείριση Δυνητικών Κοινοτήτων» του ΜΠΣ: Δυνητικές Κοινότητες – Τμ. Ψυχολογίας, Πάντειο Π. Αθήνα.*
- Βατικιώτης (2005) *Παραδόσεις στο μάθημα «Δυνητική Πραγματικότητα» του ΜΠΣ: Δυνητικές Κοινότητες – Τμ. Ψυχολογίας, Πάντειο Π. Αθήνα.*
- Βέργος Κ. (2004) *Γεωπολιτική των εθνών και της παγκοσμιοποίησης. Για μια ιστορία της γεωγραφίας και μια γεωγραφία της ιστορίας*, Αθήνα: Εκδόσεις Παπαζήση.
- Βοσνιάδου Σ. (1992) *Σκέψη*, Αθήνα: Εκδόσεις Gutenberg.
- Βερέμης Θ. (2004) *Βαλκάνια – Δόμηση και Αποδόμηση κρατών*, Αθήνα: Εκδόσεις Πατάκη.
- Δερτούζος, Μ. (2001). *Η ανολοκλήρωτη επανάσταση*. Μτφρ. Χ. Καψάλης. Αθήνα: Εκδόσεις Λιβάνης.
- Δρούγος Α. (2007) *Στρατηγική αντιμετώπισης επικείμενων απειλών*. Αθήνα: ΓΕΣ/Στρατιωτική Επιθεώρηση.
- Ευκλείδη Α. (2005) *Μεταγνωστικές Διεργασίες και Αυτό-ρύθμιση*, Αθήνα: Εκδόσεις Ελληνικά γράμματα.
- Κολοβός Α. (1995) *Διάστημα και Εθνική Ασφάλεια*, Αθήνα: Εκδόσεις Ποιότητα.
- Λεώνης Ν. (2007) *Στρατηγική αντιμετώπισης επικείμενων απειλών*, Αθήνα: ΓΕΣ/Στρατιωτική Επιθεώρηση.
- Λουδοβίκος Ν. (2006) *Ορθοδοξία και Εκσυγχρονισμός*, Αθήνα: Εκδόσεις Αρμός.
- Μουζέλης Ν. (1991) *Οργάνωση και Γραφειοκρατία [αναθεωρημένη έκδοση]*, Αθήνα: Εκδόσεις Μαθιουδάκη.
- Μάζης Ι. (2002) *Γεωπολιτική – Η θεωρία και η πράξη*, Αθήνα: Εκδόσεις Παπαζήση.
- Ντόκος, Θ. και Τσάκωνας Π. (2005) *Στρατηγική εθνικής ασφαλείας*, Αθήνα: Εκδόσεις Παπαζήση.
- Παπαδάκης Σ. και Χατζηπέρης Ν. (2002) *Εισαγωγή στην Πληροφορική*, Αθήνα: Εκδόσεις Μεταίχμιο.
- Πλατιάς Α. (2000) *Διεθνείς Σχέσεις και Στρατηγική στο Θουκυδίδη*, Αθήνα: Βιβλιοπωλείο της Εστίας.
- Πολυμενόπουλος Α. (2001) *Ο ψηφιακός κόσμος στην εθνική άμυνα [Επιτελείο Υπεθα]*, Αθήνα: Ελληνικά γράμματα.
- Πούρκος Μ. (1997) *Ο ρόλος του πλαισίου στην ανθρώπινη επικοινωνία, την εκπαίδευση και την κοινωνικο-ηθική μάθηση*, Αθήνα: Gutenberg.

- Σαρίκας Γ. (1984) *Τέχνη και μαζική κουλτούρα*, Αθήνα: Εκδόσεις Ύψιλον.
- Συρμακέσης, (2006) *Παραδόσεις στο μάθημα «Αλληλεπίδραση Ανθρώπου-Μηχανής και Ηλεκτρονικές Μαθησιακές Κοινότητες»* του ΜΠΣ: Δυνητικές Κοινότητες – Τμ. Ψυχολογίας, Πάντειο Π. Αθήνα.
- Τεγόπουλος και Φυτράκης (2005) *Ελληνικό Λεξικό*, Αθήνα: Εκδόσεις Ελευθεροτυπία.
- Τομαρά Μ. (1998) *Ιστορική Δημογραφία (από τις δημογραφικές διαδικασίες στις συλλογικές συμπεριφορές*, Αθήνα: Εκδόσεις Παπαζήση.
- Χουλιάρας Α. (2004) *Γεωγραφικοί μύθοι της Διεθνούς Πολιτικής*, Αθήνα: Εκδόσεις Ροές.

Αναφορές Ξενόγλωσσων Συγγραφέων

- Batram A (2001) *Χάος Πολυπλοκότητα και μάνατζμεντ* Αθήνα: Καστανιώτης.
- Baudrillard J (1983) *In the Shadow of the Silent Majorities*, New York: Semiotext.
- Briggs A (1966) *The Communications Revolution*, Leeds: Leeds University Press.
- Brzezinski Z (2005) *Η Επιλογή – Κυριαρχία ή Ηγεσία*, Αθήνα: Εκδόσεις Λιβάνης.
- Bell D. (2001) *An Introduction to Cybercultures*. London: Routledge.
- Chomsky, N. (1994) *Ο Έλεγχος των Μ.Μ.Ε. Τα Θεαματικά Επιτεύγματα της Προπαγάνδας*, Αθήνα: Ελευθεριακή Κουλτούρα.
- Daugherty W. (1976) *The Art and Science of Psychological Operations*, Washington: Department of the Army.
- Derruau M. (1987) *Geography Humaine*, Αθήνα: Μορφωτικό Ίδρυμα Εθνικής Τράπεζας.
- Drumheller T. (2007) *Η μυστική διπλωματία των ΗΠΑ*, Αθήνα: Ενάλιος.
- Flew T. (2005). *New Media: An Introduction*, South Melbourne: Oxford University Press.
- Garnham N. (1990) *Capitalism and Communication: Global Culture and the Economics of Information*, London: Sage.
- Gray C. (1986) *Nuclear Strategy and National Style*, Hamilton Press: Art Books.
- Fukuyama F. (1993) *The end of History and the Last Man*, New York: Penguin.
- Grabosky P. & Smith R. (1998) *Crime in the Digital Age*, Annandale: The Federation Press (National Library of Australia).
- Hawkins R., Mansell R. & Steinmueller, W.E. (1999) *Toward Digital Intermediation in the Information Societ - In Journal of Economic Issues*
- Habermas J. (1989) *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*, England: Polity (Original work published 1962).
- Heidegger M. (1953/1993) *The Question Concerning Technology*, London: Routledge.
- Huntington S. (1998) *The Class of Civilizations and the Remaking of World Order*, New York: Simon and Schuster.
- Kissinger H. (1994) *Diplomacy*, New York: Simon and Schuster.
- Levy P. (1995) *Δυνητική Πραγματικότητα. Η Φιλοσοφία του Πολιτισμού και του Κυβερνοχώρου*, Αθήνα: Κριτική.
- Maisonneuve J. (2001) *Εισαγωγή στην Ψυχο-Κοινωνιολογία*, Αθήνα: Τυπωθήτω.

- McLuhan, M. (1965) *Understanding Media: The extensions of Man*. London: Routledge.
- Mc Nair, B. (1998) *Εισαγωγή στην πολιτική επικοινωνία*. Αθήνα: Κατάρτι.
- Morgenthau H. (1978) *Politics among Nations: The Struggle for Power and Piece*, New York: Knopf.
- Mowshowitz A. (2002) *Virtual Organization*, Westport Connecticut: Quorum books.
- Negroponte N. (1995) *Being Digital*, London: Hodder and Stoughton.
- Parker G. (1998) *Geopolitics – past, present and future*, Αθήνα: Ροές.
- Perry William (1998) *Το πλεονέκτημα των πληροφοριών: Η μη πυρηνική αποτροπή της Αμερικής*.
- Rifkin J. (1996) *The end of the work*, Αθήνα: Εκδοτικός Οργανισμός Λιβάνη – Νέα Σύνορα.
- Prigogine I. (1996) *Οι νόμοι του Χάους*, Αθήνα: Εκδοτικός Οίκος Τραυλός.
- Stonier T. (1983) *The wealth of information*, London: Thames Methuen.
- Taylor P. (2004) *Global Communications, international affairs and the media since 1945*, London, New York: Routledge.

Αναφορές με πηγή ανακτημένη από τον Παγκόσμιο Ιστό (WWW):

- The National Strategy to Secure Cyberspace (2003) <http://www.whitehouse.gov/pcipb/>
- Rheingold H. (2000) *The Virtual Community: Homesteading on the Electronic Frontier*. Online Available at: <http://www.rheingold.com/vc/book/> (accessed on November 2005).
- Bell, B.S. & Kozlowski, S.W.J. (2002) *A Typology of Virtual Teams. Group and Organization Management*. Sage Publishing.
- Επιτήδειος Γ. (2000) <http://www.eeei.gr/interbiz/articles/newecon.htm>
- www.economist.com
- <http://digitalcommons.ilr.cornell.edu/hrpubs/8/>
- <http://www.un.org>
- www.spacecom.af.mil/usspace/rel15-00.htm
- <http://assets.in.gr/dGenesis/assets/Content5/Photo/697181b.jpg>
- www.in.gr/news/article.asp?lngEntityID=697181&lngDtrID=252
- http://news.kathimerini.gr/4dcgi/w_articles_ell_0_31/01/2008_257557
- <http://www.papaki.panteion.gr/teuxos9/bourdieu2.htm>
- <http://www.un.org/aboutun/unhistory/>
- <http://syriaza-vyrona.pblogs.gr/2007/12/paihnidia-toy-myaloy.html>
- http://www.nato.int/science/nato_funded_activities/topics_supported.htm
- http://www.media.uoa.gr/people/demertzis/pages_gr/articles/docs/2003/nat_ident_Internet.php
- <http://www.fas.org/irp/program/collect/uav.htm>