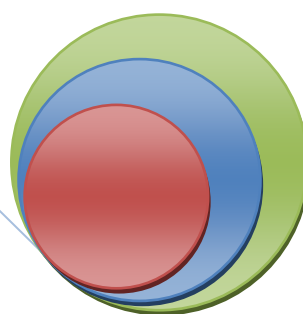
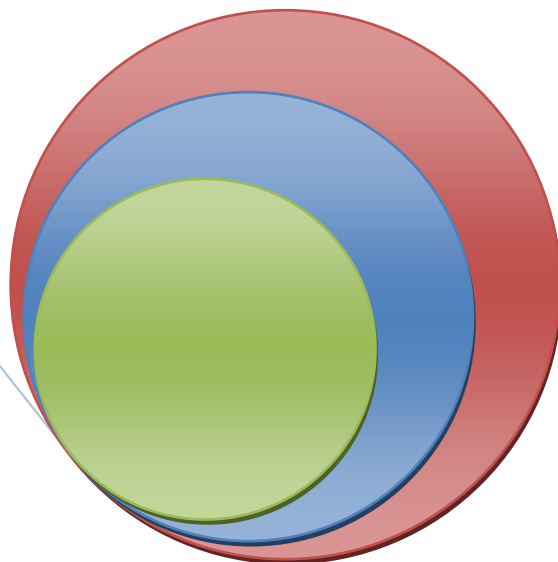
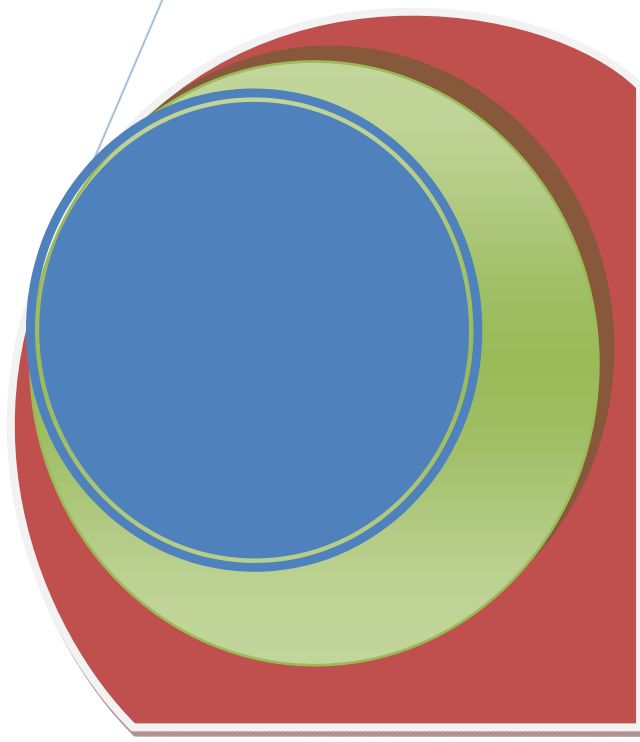




**ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΨΥΧΟΛΟΓΙΑΣ
ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ**

**Η Έννοια και ο Ορισμός του Φαινομένου του
Κυβερνοπολέμου
μέσα από μια Ανάλυση των Πληροφοριών των
Ψηφιακών Μέσων Ενημέρωσης
Οι Περιπτώσεις του BBC και του CNN**

**ΔΗΜΗΤΡΗΣ Ν. ΣΠΗΛΙΩΤΟΠΟΥΛΟΣ
ΑΜ: 608011 / 2008-2012**



ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενα.....	002
Πρόλογος.....	005
Περίληψεις.....	006
Πίνακες.....	010
Σχήματα.....	011
 <u>ΤΜΗΜΑ Ι.</u>	 012
1. <u>ΕΙΣΑΓΩΓΗ</u>	013
1.1 Επιλογή Θέματος.....	013
1.2 Σκοπός Έρευνας	017
1.3 Υποθέσεις Εργασίας.....	018
2. <u>ΜΕΘΟΔΟΛΟΓΙΑ- ΕΝΝΟΙΟΛΟΓΗΣΗ</u>	023
2.1 Σχεδιασμός.....	023
2.2 Κοινωνικές Αναπαραστάσεις.....	025
2.3 Μέθοδος.....	026
3. <u>ΤΑΥΤΟΤΗΤΑ ΕΡΕΥΝΑΣ</u>	028
3.1 Συλλογή.....	028
3.2 Επεξεργασία.....	031
3.3 Θεματικές Κατηγορίες.....	042
 <u>ΤΜΗΜΑ ΙΙ.</u>	 047
4. <u>ΑΝΑΛΥΣΗ</u>	048
4.1 Δομή Έρευνας.....	048
4.2 Υποδομές.....	050
4.2.1 Ποιοτικός Προσδιορισμός.....	050
4.2.2 Ποσοτικός Προσδιορισμός.....	055
4.2.3 Ανάλογα Κυβερνο-επεισόδια.....	057
a) <i>Estonia, 2007</i>	057
b) <i>Georgia, 2008</i>	059
4.3 <i>Διείσδυση</i> (Ghostnet, 2009 & Stuxnet, 2010).....	064
4.3.1 Ποιοτικός Προσδιορισμός.....	064
4.3.2 Ποσοτικός Προσδιορισμός.....	070

4.3.3	Ανάλογα Κυβερνο-επεισόδια.....	072
a)	<i>China, 2010</i>	073
b)	<i>Japan, 2011</i>	074
c)	<i>IMF, 2011</i>	074
d)	<i>Stuxnet, 2010</i>	075
e)	<i>Ghostnet, 2010</i>	078
f)	<i>Mafiaboy, 1993</i>	079
g)	<i>Moonlight Maze, 2001</i>	079
h)	<i>“Mother of Attacks”, 2011</i>	080
4.4	Κυβερνο-Προπαγάνδα	083
4.4.1	Ποιοτικός Προσδιορισμός.....	083
4.4.2	Ποσοτικός Προσδιορισμός.....	086
4.4.3	Ανάλογα Κυβερνο-επεισόδια.....	088
a)	<i>Serbia, 1999</i>	088
b)	<i>Zapatistas, 1994</i>	089
c)	<i>Chechnya, 1994</i>	089
d)	<i>Wikileaks, 2009</i>	090
e)	<i>USA, 2010</i>	092
f)	<i>“Arab Spring”, 2011</i>	093
4.5	Κυβερνο-Λογοκρισία	095
4.5.1	Ποιοτικός Προσδιορισμός.....	095
4.5.2	Ποσοτικός Προσδιορισμός.....	097
4.5.3	Ανάλογα Κυβερνο-επεισόδια.....	099
a)	<i>Myanmar, 2007</i>	099
b)	<i>Cuba, 2009</i>	100
c)	<i>Turkey, 2010</i>	100
d)	<i>Google, 2010</i>	101
e)	<i>Israel, 2006</i>	104
f)	<i>Iran, 2010</i>	105
e)	<i>Google Street View, 2010</i>	107
	ΤΜΗΜΑ ΙΙΙ	109
5.	ΠΡΟΣΕΓΓΙΣΗ	110

[ΤΜΗΜΑ ΙΙΙ] ΜΕΡΟΣ Α' – ΠΟΛΕΜΟΣ	112
6. <u>ΘΕΩΡΗΣΗ ΤΟΥ ΠΟΛΕΜΟΥ</u>	113
6.1 Φιλοσοφία Πολέμου	113
6.2 Στρατηγική Κουλτούρα	116
6.3 Ηθική του Πολέμου	117
6.4 Κλασσικές Ερμηνείες	118
7. <u>ΙΣΤΟΡΙΚΗ ΔΙΕΡΕΥΝΗΣΗ</u>	123
8. <u>ΟΙ ΠΡΩΤΕΣ ΕΠΙΣΤΗΜΟΝΙΚΕΣ ΘΕΣΕΙΣ</u>	131
8.1 Εισαγωγή	131
8.2 J. Arquilla & D. Ronfeldt ('93)	132
8.3 Π. Κονδύλης ('98)	134
8.4 M. Libicki ('09)	135
8.5 J. Carr ('10)	139
8.6 R. Clarke ('10)	142
9. <u>ΟΡΓΑΝΩΣΗ ΚΑΙ ΕΞΟΠΛΙΣΜΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ</u>	144
9.1 Οργάνωση	144
9.1.1 ΝΑΤΟ	144
9.1.2 ΗΠΑ	145
9.1.3 Ελλάδα	147
9.2 Εξοπλισμός	153
9.2.1 Κακόβουλο Λογισμικό (Malicious Software)	153
9.2.2 «Υποπτα» Εξαρτήματα ("Security Risk" Hardware)	153
9.2.3 Τύποι Επιθέσεων (Types of Computer Network Attacks)	154
[ΤΜΗΜΑ ΙΙΙ] ΜΕΡΟΣ Β' – ΚΥΒΕΡΝΟΧΩΡΟΣ	155
10. <u>Η ΕΝΝΟΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ</u>	156
10.1 Οι δύο πόλοι κριτικής	156
10.2 Ορισμοί και προσδιορισμός	158
10.3 Η μία όψη: Κοινωνικό-τεχνικό Σύμπλεγμα	161
10.4 Η άλλη όψη: το «Δυνητικά Φαντασιακό»	164
10.5 Συμπέρασμα: Ο αλγόριθμος	165
11. <u>ΣΥΜΠΕΡΑΣΜΑ</u>	169
Βιβλιογραφία	172
Παράρτημα	183

ΠΡΟΛΟΓΟΣ – ΕΥΧΑΡΙΣΤΙΕΣ

Από το πρώτο άκουσμα της έκφρασης «διδασκαλική διατριβή», μεγαλύτερη εντύπωση μου έκανε η λέξη που, σχεδόν πάντα, προηγείται... «εκ-πόνηση». Πλέον, μετά την ολοκλήρωση αυτής της προσπάθειας, κατανόησα το λόγο που είναι η πιο κατάλληλη. Αν κάποιος μου ζητούσε να καταθέσω την εμπειρία μου για τις προϋποθέσεις που απαιτούνται, για την πραγματοποίηση ενός τέτοιου έργου, θα έλεγα πως χωρίζονται στις τυπικές και ουσιαστικές. Οι πρώτες αφορούν θέματα, όπως η κατοχή πτυχίων (τριτοβάθμιας και μεταπτυχιακής εκπαίδευσης), η αποδοχή ενός καθηγητή να αναλάβει την εποπτεία του εγχειρήματος* και τέλος, η ύπαρξη μιας «αντικειμενικής αξίας» στο θέμα, η οποία θα πρέπει να αποδεικνύει τη χρησιμότητά του και από αυτό, να τεκμηριώνεται η καινοτομία του.

Ωστόσο, ιδιαίτερο ρόλο παίζει και ο ουσιαστικός όρος. Αυτός ξεκινάει από το ενδιαφέρον που οφείλει να έχει ο συγγραφέας για το αντικείμενο που πραγματεύεται (αυτό εξάλλου είναι και κάτι που μας διακρίνει από τις μηχανές). Το σημαντικότερο όμως είναι η **θέληση**· κυρίως για τις θυσίες που απαιτεί μια βαθιά διερεύνηση. Σε αυτήν την κατεύθυνση ήταν και η προσωπική μου πορεία. Επιχείρησα να συνδυάσω τις γνώσεις μου από το μεταπτυχιακό (με θέμα τον Κυβερνοχώρο – Τμήμα Ψυχολογίας), με το επάγγελμά μου (αναλύσεις σε ζητήματα Πολέμου – Υπ.Εθ.Α.).

Σε αυτό βεβαίως ήταν απαραίτητη -και καθοριστική- η συμβολή ορισμένων προσώπων. Αρχικά, του επιβλέποντα, Αναπληρωτή Καθηγητή κ. Κων/νου Κοσκινά, ο οποίος εκτίμησε τις δυνατότητές μου (οι οποίες πάντως δεν ήταν και πολύ έκδηλες εξ αρχής) και μου έδωσε αυτήν την ευκαιρία μετά την έγκριση της μεταπτυχιακής μου εργασίας. Τον ευχαριστώ. Στη συνέχεια τον διευθυντή κ. Χρήστο Ραζέλο, ο οποίος συναίνεσε για την παροχή εκπαιδευτικής άδειας από την εργασία μου. Ελπίζω πως γνωρίζει ότι τον ευγνωμονώ, διότι η αποδέσμευσή μου ήταν για μένα αναγκαία. Κατόπιν, αποφασιστική ήταν η συνεισφορά του καθηγητή από το ίδρυμα (ΤΕΙ Μεσολογγίου) που απόκτησα τον πρώτο ακαδημαϊκό τίτλο σπουδών μου -και πολλές άλλες εμπειρίες μαζί με αυτόν-, κ. Δημήτρη Καπογιάννη. Δεν θα ξεχάσω ποτέ τη σημαντική ανταπόκρισή του και την έκφραση: *πρόκειται για μια επιστημονική μύηση*. Εν κατακλείδι, είναι αλήθεια πως ο τίτλος του Διδάκτορα δεν θα αποτελούσε γεγονός, δίχως την αμέριστη και πολλαπλή συμπαράσταση της συζύγου μου Κατερίνας, στην οποία και επιθυμώ να τον αφιερώσω.

* Έτσι διασφαλίζεται και ο διωποκειμενικός χαρακτήρας της σύγχρονης επιστήμης. Με άλλα λόγια, ότι η «επιστημονικότητα μιας εργασίας αναγνωρίζεται από τους... αναγνωρισμένους».

ΠΕΡΙΛΗΨΗ

Ο πρωταρχικός σκοπός, ο οποίος τέθηκε στην εκπόνηση της παρούσας διδακτορικής διατριβής, είναι η συμβολή της στην κατανόηση του επικαλούμενου κυβερνοπολεμικού φαινομένου. Ειδικότερα, πρόκειται για μια προσπάθεια διαφώτισης του φαινομένου, με έναν πιο σφαιρικό από τον συνήθη μονοσήμαντο τρόπο που εφαρμόζεται διεθνώς. Ως εκ τούτου, δεν ακολουθήθηκαν αποκλειστικά στρατιωτικές ή τεχνοκρατικές αφετηρίες· τέτοια έργα εξάλλου, στη διεθνή βιβλιογραφία υπάρχουν ήδη πολλά. Αντιθέτως, οδηγό αποτέλεσε μια γενικότερη «διεπιστημονική θέαση», η οποία πάντως, συγκροτήθηκε κυρίως από μια κοινωνιοψυχολογική προσέγγιση.

Το πρώτο γνώρισμα που διακρίθηκε σε αυτό το φαινόμενο, ήταν η ανωνυμία εκείνου που διεξάγει την επίθεση. Εφόσον λοιπόν, σε κάθε πόλεμο έχουμε επιτιθέμενους και αμυνόμενους, πηγή εδώ θα μπορούσαν να συνιστούν μόνο οι δεύτεροι. Αυτοί όμως, κρίνουν τα περισσότερα σχετικά στοιχεία, ως ευαίσθητα για την εθνική ασφάλεια και άρα, δεν μπορούν να τα δημοσιεύσουν. Ελλείπει συνεπώς πρωτογενούς πηγής, διερευνήθηκαν δηλώσεις, ανακοινώσεις και επί τω πλείστον περιγραφές για τα *γεγονότα*, τα οποία επικράτησε στον λεγόμενο δυτικό κόσμο να τιτλοφορούνται «κυβερνοπόλεμος» (cyberwar).

Πιο συγκεκριμένα, πηγή αποτέλεσε η επιλογή δύο διεθνώς αναγνωρισμένων ειδησεογραφικών πρακτορείων (BBC & CNN). Από αυτά συλλέχθηκαν όλα τα διαθέσιμα, συναφή με το φαινόμενο, κείμενα (σύνολο 105 – από το 1999 ως το 2011). Στόχος ήταν να επιτευχθεί μια θεματική κατηγοριοποίηση των εννοιών, οι οποίες προσδίδονται στον κυβερνοπόλεμο. Για αυτό το λόγο, επιλέχθηκε η Μέθοδος Ανάλυσης Περιεχομένου και δη, στη σημασιολογική της εφαρμογή. Αυτό σημαίνει ότι, αφού μελετηθούν όλα τα κείμενα, διαχωρίζονται οι φράσεις και παράγραφοι που περιέχουν τις ζητούμενες αναφορές στο φαινόμενο (τελικά ανήλθαν σε 315 μονάδες). Για να ταξινομηθούν αυτές, ορίστηκε ένα ψυχοκοινωνικό -όπως το ονομάσαμε- κριτήριο. Σύμφωνα με αυτό, τα γεγονότα μπορούν να διακριθούν, από τη διάχυσή τους ή μη στην κοινωνία, τη συμμετοχή ή όχι των πολιτών, καθώς και το βαθμό τεχνολογικής τους έντασης. Έτσι, προέκυψαν οι εξής τέσσερις κατηγορίες:

- Διείσδυσης (penetration) – Κλειστή κοινωνικά και Τεχνολογικής έντασης
- Υποδομών (infrastructures) – Ανοικτή κοινωνικά και Τεχνολογικής έντασης
- Λογοκρισίας (censorship) – Κλειστή κοινωνικά και Ανθρώπινης έντασης
- Προπαγάνδας (propaganda) – Ανοικτή κοινωνικά και Ανθρώπινης έντασης

Τέλος, παρατέθηκαν τα «ιστορικά» περιστατικά που παρατηρήθηκαν ανά κατηγορία.

Στο επόμενο τμήμα της εργασίας, επιχειρήθηκε ο εντοπισμός του θεωρητικού πυρήνα προέλευσης των παραπάνω κατηγοριών. Αυτό το εγχείρημα διαχωρίστηκε σε δύο μέρη. Στο πρώτο, αναφέρθηκαν οι κλασσικές ερμηνείες του πολεμικού φαινομένου, καταλήγωντας στη σύγχρονη συζήτηση των κοινωνικών επιστημόνων. Βάσει της τελευταίας, έγινε μια ιστορική διερεύνηση της τριαδικής συσχέτισης, η οποία συνίσταται από (i) την εννοιολογική οροθέτηση του κράτους, (ii) τον τρόπο που οι ηγεσίες του αντιμετωπίζουν διαχρονικά τον πόλεμο και (iii) πώς η διεξαγωγή του τελευταίου επιδρά στην κοινωνία. Οπότε, προέκυψε μια εξήγηση της εμφάνισης καταρχάς, του πληροφοριακού πολέμου, κατόπιν του πληροφορικού και τέλος του κυβερνοπολέμου, για τον οποίο παρουσιάστηκαν οι πιο «αντιπροσωπευτικές» πρώτες επιστημονικές μελέτες. Για να καλυφτεί αυτό το θέμα σφαιρικά, από το πιο θεωρητικό του (φιλοσοφία πολέμου) ως το πιο πρακτικό του φάσμα, αντί επιλόγου, συνοψίστηκε και ο τρόπος λειτουργίας των πρωτοπόρων αρμόδιων υπηρεσιών στη Δύση (NATO και ΗΠΑ), κλείνοντας με μια έμφαση στην ελληνική περίπτωση.

Στο δεύτερο μέρος, πραγματοποιήθηκε μια εμβάθυνση στην έννοια του κυβερνοχώρου. Μέσα από τις διαδρομές της θεωρητικής και πρακτικής του κατανόησης, αποτολμήθηκε η διαμόρφωση ενός *αλγορίθμου* δυνητικής του ανάγνωσης. Με τη χρήση του, αναδείχθηκαν τρεις εκφάνσεις της έννοιας -μια κοινωνική, μια τεχνική και μια φαντασιακή-, οι οποίες ενυπάρχουν σε κάθε φάση του κυβερνοχώρου. Στη συνέχεια, εξετάστηκε η πορεία του μέχρι σήμερα, σε τέσσερις χρονικές περιόδους (φάσεις). Μετά, ερευνήθηκε η σύνδεση αυτών των φάσεων, με τις κατηγορίες των νοημάτων που προσδίδονται στον κυβερνοπόλεμο, όπως έχουν διαγνωθεί στο πρώτο τμήμα. Η απάντηση ήταν καταφατική. Αν, για παράδειγμα, στον κυβερνοχώρο αναγνωρίζεται μόνο το επιφανειακό, τεχνολογικό του περίβλημα, αγνοώντας τις κοινωνικές του προεκτάσεις, τότε ο κυβερνοπόλεμος δεν θα διαφέρει από τον πληροφορικό πόλεμο, ο οποίος εμπλέκει επιθέσεις μόνο σε δίκτυα υπολογιστικών συστημάτων (Computer Networks Attacks).

Η εργασία ολοκληρώνεται με μια πρόταση για την θεραπεία της σύγχυσης η οποία επικρατεί στην ορολογία των θεμάτων κυβερνοασφάλειας. Σύμφωνα με την προηγούμενη ανάλυση, λαμβάνονται υπόψη ως βασικά υποκείμενα οι πολίτες, το κράτος και η ηγεσία. Έτσι, στον επίλογο αποσαφηνίζονται οι όροι «έγκλημα» (μεταξύ πολιτών) και «πόλεμος» (μεταξύ κρατών) δια του κυβερνοχώρου, όπου αντίστοιχα αποτελούν αρμοδιότητα της αστυνομίας και του στρατού. Εν κατακλείδι, προτείνεται η εισαγωγή του όρου «κυβερνοέλεγχος», για τις άδηλες καταχρήσεις της εξουσίας.

SUMMARY

The primary aim of the present thesis is to contribute to the understanding of the so-called cyber-war phenomenon. More specifically, it is an effort of elucidating this phenomenon in a more global way than the usual unequivocal approach applied at an international level. Therefore, military or managerial starting-points were not exclusively followed; besides, works of this type already exist in international bibliography, in plentitude. On the contrary, a more general “interdisciplinary view” was used as a guide, which, in any case, was principally formed from a socio-psychological point of view.

The first distinguishable feature of this phenomenon was the anonymity of the party who perpetrates the attack. Since there are attackers and defenders in every war, the latter could be the only source here. However, they consider most of the relevant data as sensitive for the national security and therefore, are not allowed to publish them. Consequently, due to the lack of primary sources, statements, announcements and, for the most part, descriptions, were investigated about the *events*, predominantly called “cyber-war” in the western world.

More specifically, two internationally recognized news agencies (BBC & CNN) were selected as the primary source. All the available, relevant to the phenomenon, texts were provided by them (105 in total, from 1999 to 2011). The main aim was to perform a thematic categorization of the concepts that are attributed to cyber war. For this reason, the Content Analysis Method was selected and thus, its semantic application. This means that, after having investigated all texts, the phrases and paragraphs, which contain the requested references to the phenomenon, are separated (the final number amounted to 315 units). In order to classify them a psycho-social – as it was so-called – criterion was defined. According to this, the events can be classified, in relation to their diffusion or not, in the society, the participation or not, of the citizens and the extent of their technological intensity.

Thus, the following four categories came up:

- Penetration - Socially closed and of technological intensity
- Infrastructures - Socially open and of technological intensity
- Censorship - Socially closed and of human intensity
- Propaganda - Socially open and of human intensity

Finally, the observed “historic” events were cited, by category.

In the next section of this thesis, the detection of the theoretical core of origin of the aforementioned categories was attempted. This endeavor has been separated into two parts. In the first part, the classical interpretations of the war phenomenon were mentioned, concluding to the modern debate of social scientists. Based on the latter, a historical investigation of the triadic relation, which consists of a) the conceptual delineation of state, b) the way in which its leaderships always face the concept of war and c) the impact of the conduct of war on society was attempted. Consequently, an explanation of firstly, the emergence of *information war* (info-war), secondly of the *computer networks war* and finally, the *cyberwarfare*, for which the first most “representative” scientific studies came up. To cover the subject in a universal way, instead of an epilogue, the operation of the pioneer responsible services in the West (NATO & USA) was summarized, concluding with an emphasis on the Greek case.

In the second section, a thorough examination of the concept of cyberspace was carried out. Through the course of its theoretical and practical understanding, the formation of an algorithm for its potential reading was attempted. By its use, three expressions of the concept emerged – a social, a technical and a “potential” (or imaginary) one – which are incorporated in every phase of the cyberspace. Then, its course to the present day, in four different time phases, was examined. Furthermore, the connection between these phases and the concept categories attributed to cyber-war was investigated, as diagnosed in the first section. The answer was positive. For example, if only the technological, superficial cover is recognized in cyberspace, ignoring its social extensions, then cyber war will not differ from current CNAs (Computer Network Attacks).

The thesis concludes with a proposal for addressing the confusion of terminology in cyber security matters. According to the previous analysis, the citizens, the state and the leadership are taken into account as primary subjects. Therefore, the terms “crime” (between citizens) and “war” (between states) in cyberspace, which are a responsibility of the police and the army, respectively, are clarified in the conclusion. Finally, the introduction of the term “cyber control” for the implicit abuses of power is suggested.

ΠΙΝΑΚΕΣ

	Σελ
Π. 1 : Οι θέσεις στον Παγκόσμιο Ιστό με τη μεγαλύτερη επισκεψιμότητα	029
Π. 2^A : <i>BBC</i> -Corpus: Το Σώμα των κειμένων που συλλέχθηκαν	032
Π. 2^B : <i>CNN</i> -Corpus: Το Σώμα των κειμένων που συλλέχθηκαν	034
Π. 3 : Λεπτομέρειες Ακυρώσεων	038
Π. 4 : Συσχέτιση Θεματικών Κατηγοριών & Κριτηρίου	043
Π. 5 : Συμμετοχή Εκάστης Θεματικής Κατηγορίας	044
Π. 6 : Αποτελέσματα κατανεμημένα ανά Έτος-Θεματική Κατηγορία-Μέσο	045
Π. 7 : Ιστότοποι που επλήγησαν	059
Π. 8 : Οι συμβολισμοί των φάσεων εκδήλωσης του πολεμικού φαινομένου	129
Π. 9 : Η ιστορική ολοκλήρωση του κυβερνοχώρου	169
Π.10 : Η συμπόρευση του κυβερνοπολέμου και του κυβερνοχώρου	170
Π.11 : Η διαφύλαξη από τις μη-αποδεκτές πράξεις στον κυβερνοχώρο	171

ΣΧΗΜΑΤΑ

	Σελ
Σ.01 : Το μερίδιο των συλλεγόντων κειμένων από τα BBC & CNN	036
Σ.02^A : Το μερίδιο των ακυρωθέντων κειμένων στο BBC	037
Σ.02^B : Το μερίδιο των «ακυρωθέντων» κειμένων στο CNN	037
Σ.03 : Τελικός καταμερισμός των προς επεξεργασία κειμένων από τα BBC&CNN	038
Σ.04 : Η συνολική έκταση σε σελίδες στα δύο ειδησεογραφικά πρακτορεία	039
Σ.05 : Η συνολική έκταση σε αριθμό λέξεων στα δύο ειδησεογραφικά πρακτορεία	040
Σ.06^A : Η πυκνότητα των γεγονότων στο χρονικό φάσμα, για το BBC	041
Σ.06^B : Η πυκνότητα των γεγονότων στο χρονικό φάσμα, για το CNN	041
Σ.07 : Η απεικόνιση των συγκεντρωτικών αποτελεσμάτων	044
Σ.08 : Οι συνολικές αναφορές στα δύο ειδησεογραφικά πρακτορεία	045
Σ.09 : Διακύμανση των μονάδων αναφοράς, ανά έτος και Θεματική Κατηγορία	046
Σ.10 : Η Μεθοδολογία της Έρευνας μας	048
Σ.11 : Συγκεντρωτικό Μερίδιο «ΥΠΟΔΟΜΩΝ»	055
Σ.12 : Διαχρονική Τάση «Υποδομών» – BBC	056
Σ.13 : Διαχρονική Τάση «Υποδομών» – CNN	057
Σ.14 : “CIA TRIAD”	066
Σ.15 : Συγκεντρωτικό Μερίδιο «ΔΙΕΙΣΔΥΣΕΩΝ»	070
Σ.16 : Διαχρονική Τάση «Διεισδύσεων» – BBC	072
Σ.17 : Διαχρονική Τάση «Διεισδύσεων» – CNN	072
Σ.18 : Συγκεντρωτικό Μερίδιο «ΚΥΒΕΡΝΟΠΡΟΠΑΓΑΝΔΑΣ»	086
Σ.19 : Διαχρονική Τάση «Κυβερνοπροπαγάνδας» – CNN	087
Σ.20 : Διαχρονική Τάση «Κυβερνοπροπαγάνδας» – CNN	088
Σ.21 : Συγκεντρωτικό Μερίδιο «ΚΥΒΕΡΝΟΛΟΓΟΚΡΙΣΙΑΣ»	097
Σ.22 : Διαχρονική Τάση «Κυβερνολογοκρισίας» – BBC	098
Σ.23 : Διαχρονική Τάση «Κυβερνολογοκρισίας» – CNN	099
Σ.24 : Απεικόνιση της Πυραμοειδούς Ιεραρχικής Οργάνωσης του Κράτους	122
Σ.25 : Τα πεδία μάχης κατά τον ιστορικό ανταγωνισμό στρατιωτικής ισχύος	128
Σ.26 : Παγκόσμια Πολιτική Στρατολόγησης	130

ΤΜΗΜΑ Ι
Ο ΣΤΟΧΟΣ ΤΗΣ ΕΡΓΑΣΙΑΣ
(ΚΑΙ Ο ΤΡΟΠΟΣ ΕΠΙΤΕΥΞΗΣ ΤΟΥ)

1. ΕΙΣΑΓΩΓΗ

1.1 Η επιλογή του θέματος

Στην αφετηρία της ανθρώπινης συνύπαρξης τοποθετούνται και οι ρίζες του πολεμικού φαινομένου. Συνεπώς, η εμφάνιση του πολέμου παρατηρείται στις απαρχές της ανθρωπότητας. Επίσης, εξελίσσεται παράλληλα με αυτήν, σε μια διαδικασία αλληλεπίδρασης του τρόπου που οι άνθρωποι οργανώνουν, τόσο τη συμπόρευσή τους, όσο και την αντιπαράθεσή τους.

Η εποχή μας προσδιορίζεται από το πλαίσιο της οργανωτικής μετάβασης από την ύστερη φάση των Νέων Χρόνων στην αποκαλούμενη «μετανεωτερικότητα». Το κεντρικό αίτημα της νεωτερικότητας ήταν η *πρόοδος*, η οποία στις μέρες μας απέκτησε έναν κυρίαρχο τεχνολογικό χαρακτήρα, θέτοντας παράλληλα μείζονα προβλήματα περί του «τι εστί εκσυγχρονισμός», ή με άλλα λόγια πώς μπορεί να επιτευχθεί η τεχνοκρατική συμπόρευση με τους πρωτοπόρους (Λουδοβίκος, 2006, 14). Το ζήτημα αυτό μεγεθύνεται ακόμα περισσότερο, όταν στις διεθνείς σχέσεις, συχνά, η μη-συμμόρφωση με τους ισχυρούς, οδηγεί στο δρόμο της σύγκρουσης. Επόμενο λοιπόν είναι, ο ρόλος της τεχνογνωσίας να επικρατήσει και στον τρόπο που οι ιθύνοντες αντιλαμβάνονται, σχεδιάζουν και τελικά, διεξάγουν τον πόλεμο. Κάτω από αυτές τις συνθήκες στις αρχές της δεκαετίας του '90, άρχισαν ορισμένοι να μιλούν για ένα νέο είδος πολέμου, τον *κυβερνοπόλεμο*.

Καταρχάς, εξετάζοντας τον όρο ετυμολογικά, διακρίνουμε πως η βασική του επιρροή προέρχεται από την έννοια του «κυβερνοχώρου». Σε ένα πρώτο, επιφανειακό επίπεδο, όλοι κατανοούν ότι αυτή η έννοια περιγράφει την οικοδόμηση ενός τρόπου οργάνωσης της επικοινωνίας και πληροφόρησης, ο οποίος εξαρτάται σημαντικά από τους ηλεκτρονικούς υπολογιστές (H/Y). Σε ένα δεύτερο όμως, περισσότερο βύθιο επίπεδο, ανακαλύπτουμε ότι ο θεμέλιος λίθος αυτής της οργάνωσης βρίσκεται στην επιστήμη της κυβερνητικής.

Έτσι, γίνεται προφανές ότι στο θεωρητικό υπόβαθρο, προκαλείται μια σύγχυση για τον ορισμό της έννοιας του «κυβερνοχώρου» και κατά συνέπεια του πολέμου μέσα σε αυτόν. Αυτός είναι ο λόγος που σε αυτήν την εργασία επιχειρήθηκε μια έρευνα, η οποία ξεκινά από μια πιο «πρακτική» αφετηρία εξέτασης των νοημάτων που δίνονται στον όρο του κυβερνοπολέμου. Εν κατακλείδι, -διενεργώντας μια απαγωγική προσπάθεια- επιχειρήσαμε να συγκεντρώσουμε και να ομαδοποιήσουμε τα νοήματα που εμπεριέχει η χρήση αυτού του όρου στη δημόσια σφαίρα και δη στην

εποχή μας, στην ψηφιακή της μορφοποίηση. Οπότε, τελικός στόχος τέθηκε να φθάσουμε σε μια θεωρητική εξήγηση των διεξαχθέντων αποτελεσμάτων, βασιζόμενοι στις απαραίτητες επιστημονικές τεκμηριώσεις.

Για να κάνουμε τα παραπάνω πιο απλά, τα παρουσιάζουμε σχηματικά, διαχωρίζοντας τα περιεχόμενα της συγγραφής σε τρία τμήματα, εκ των οποίων το τελευταίο έχει δύο μέρη:

- I Ο στόχος της εργασίας και ο τρόπος επίτευξής του
- II Η πράξη (τι εννοούν «κυβερνοπόλεμο» τα μέσα)
- III Η θεωρία - Α': *ο πόλεμος*
- III Η θεωρία - Β': *ο κυβερνοχώρος*

ΤΜΗΜΑ I: Ο ΣΤΟΧΟΣ ΚΑΙ Η ΕΠΙΤΕΥΞΗ ΤΟΥ

Στο πρώτο κεφάλαιο, στο πρώτο υποκεφάλαιο, παραθέτουμε το πλαίσιο μέσα στο οποίο επιλέξαμε το συγκεκριμένο θέμα της εργασίας μας. Αφετηρία συνιστά, η ιστορική σύνδεση των ανθρωπίνων σχέσεων με το φαινόμενο του πολέμου. Θεωρούμε κομβικό σημείο την εποχή (18^{ος} αιώνας), την οποία η λέξη «πρόοδος» γίνεται το σύνθημα μιας νέας έννοιας των κοινωνικών επιδιώξεων της ανθρωπότητας και πώς αυτή η έννοια χρωματίζεται έντονα από την επιστημονική εξέλιξη, επικεντρώνεται στην τεχνολογική και τέλος, όλα αυτά, συνοδεύονται από την παράλληλη μεταλλαγή του τρόπου διεξαγωγής του πολέμου.

Στη συνέχεια, στο δεύτερο υποκεφάλαιο, αποσαφηνίζουμε ότι σκοπός της εργασίας είναι η κατηγοριοποίηση των νοημάτων, τα οποία έχουν προσδοθεί από τα ψηφιακά μέσα με παγκόσμια αναγνωσιμότητα, μέσω μιας χαρτογράφησης όλων των συναφών γεγονότων, τα οποία έχουν τιτλοφορηθεί με τον όρο του κυβερνοπολέμου. Η ουσία όλων των παραπάνω, έρχεται να διατυπωθεί στις υποθέσεις της εργασίας, στο τρίτο υποκεφάλαιο. Εκεί, λοιπόν, καταγράφουμε πως καταρχήν όλα αυτά (που περιγράφονται στο πρώτο κεφάλαιο) οδηγούν σε μια σύγχυση, την οποία οφείλουμε να ξεδιαλύνουμε. Για αυτόν το σκοπό (όπως αναφέρουμε στο δεύτερο κεφάλαιο) αποδελτιώνουμε τα «πολλά» εννοιολογικά στοιχεία των κειμένων που συλλέξαμε, σε «λίγες» θεματικές κατηγορίες. Αυτή η επεξεργασία γίνεται με ένα *ψυχοκοινωνικό* κριτήριο, όπως το καλούμε και το αναλύουμε παρακάτω.

Όσον αφορά το δεύτερο κεφάλαιο, αντικείμενό του ορίσαμε την αποτύπωση της περιγραφής του τρόπου, με τον οποίο θα απαντήσουμε στα παραπάνω ερευνητικά μας ερωτήματα. Άρα θα αναφερθούμε στο σχεδιασμό της στρατηγικής που

ακολουθήσαμε και τη μεθοδολογία που τελικά προέκυψε από αυτόν. Έτσι, στο πρώτο υποκεφάλαιο ξεκινάμε με μια πολύ σύντομη ιστορική αναδρομή για το ρόλο του μέσου στην κοινωνία. Από αυτήν αναδεικνύεται ότι το εννοιολογικό μας υπόβαθρο στηρίζεται στις Κοινωνικές Αναπαραστάσεις, των οποίων την έννοια αναπτύσσουμε στο δεύτερο υποκεφάλαιο. Από αυτή όμως την εμβάθυνση, στις έννοιες της Κοινωνικής Ψυχολογίας, «αναδύεται» και η πιο κατάλληλη -κατά την εκτίμησή μας- Μέθοδος, της οποίας η εφαρμογή δύναται να διαλευκάνει τον νοητικό μας γρίφο¹. Αυτήν και παρουσιάζουμε, μαζί με τους λόγους για τους οποίους την επιλέξαμε, στο τρίτο υποκεφάλαιο.

Στο πρώτο υποκεφάλαιο του τρίτου και τελευταίου κεφαλαίου αυτού του τμήματος, παραθέτουμε τη λεγόμενη ταυτότητα της έρευνάς μας. Εκεί, εξηγούμε τα κριτήρια επιλογής των πηγών μας, μαζί με κάποια στοιχεία σύστασής τους. Στη συνέχεια, στο δεύτερο υποκεφάλαιο, παρουσιάζουμε το «ακατέργαστο» υλικό που προέκυψε από τη συλλογή μας, καθώς επίσης και τι εξαιρέσαμε από την επεξεργασία μας. Ωστόσο, ίσως το πιο ενδιαφέρον σημείο της εργασίας εντοπίζεται στο τρίτο υποκεφάλαιο. Εκεί δείχνουμε σε ποιες θεματικές κατηγορίες κατέληξε η έρευνά μας. Επίσης, κάνουμε και έναν πρώτο προσδιορισμό των όρων που θα χρησιμοποιήσουμε στην ανάλυσή τους.

ΤΜΗΜΑ II: Η ΠΡΑΞΗ

Εξηγήσαμε τι και με ποιο τρόπο θα προσπαθήσουμε να θεραπεύσουμε. Ότι, δηλαδή, διακρίνοντας τι συμβαίνει στην καθημερινή πρακτική -για αυτό και το ονομάζουμε «η πράξη»-, θα αναζητήσουμε μια «θεωρία» (το τρίτο τμήμα), η οποία να την εξηγεί. Σε αυτήν λοιπόν, την κατεύθυνση, το πρώτο κεφάλαιο αφιερώνεται στην ποσοτική και ποιοτική ανάλυση των ευρημάτων της έρευνάς μας. Έτσι, ξεκινάμε με το εισαγωγικό υποκεφάλαιο (του τέταρτου κεφαλαίου στη σειρά περιεχομένων), στο οποίο αναφέρουμε το αντικείμενο και τη δομή της ανάλυσης.

Στα επόμενα τέσσερα υποκεφάλαια (4.2 - 4.5) πραγματοποιείται η ανάλυση των τεσσάρων αντίστοιχων θεματικών κατηγοριών. Αυτό θα γίνεται με ίδιο τρόπο για το καθένα, σε τρεις ενότητες: τον ποιοτικό προσδιορισμό, τον ποσοτικό προσδιορισμό και την παράθεση των ανάλογων περιστατικών στον κυβερνοχώρο (τα «κυβερνο-επεισόδια») που εμπεριέχονται σε κάθε κατηγορία.

¹ «Κάθε επιστημονική εργασία οικοδομείται πάνω στην εξήγηση ενός νοητικού γρίφου» (Mason, 1996/2010, 41).

ΤΜΗΜΑ ΙΙΙ: Η ΘΕΩΡΙΑ

Το τελευταίο τμήμα της εργασίας αποδείχθηκε το πιο δύσκολο, αλλά ίσως και το πιο διαφωτιστικό. Το εγχείρημα αποσκοπούσε, μέσα από την ερμηνεία του πολεμικού φαινομένου και της έννοιας του κυβερνοχώρου, να εντοπίσουμε την ενδεχόμενη συσχέτιση με τα νοήματα, τα οποία εν γένει αποδίδονται στο φαινόμενο του κυβερνοπολέμου.

Στο πέμπτο κεφάλαιο, λοιπόν, καταθέτουμε τις απαραίτητες εξηγήσεις μας για τον τρόπο που θα διεξάγουμε την εν λόγω ερμηνεία. Ωστόσο, πέρα του προαναφερόμενου εισαγωγικού κεφαλαίου, στα επόμενα θα ακολουθήσουμε μια χρονική σειρά στην ανάπτυξή μας, ξεκινώντας από το 18^ο αιώνα ως σήμερα.

ΤΜΗΜΑ ΙΙΙ: Α' ΜΕΡΟΣ - Ο ΠΟΛΕΜΟΣ

Στο κεφάλαιο 6 παραθέτουμε, επιγραμματικά, τα πιο «κλασικά» επιστημονικά έργα για το φαινόμενο του πολέμου έτσι, ώστε να συγκροτήσουμε μια θεωρητική βάση για την ερμηνεία μας. Στο κεφάλαιο 7 αποπειρόμαστε μια ιστορική διερεύνηση για την ανίχνευση των συνθηκών που οδήγησαν στο φαινόμενο του κυβερνοπολέμου. Ειδικότερα, αναζητούμε τα ίχνη της αλληλεξάρτησης των σχέσεων του κράτους με το «αίσθημα ασφάλειας» της κοινωνίας. Στο κεφάλαιο 8, εφόσον πλέον θεωρείται διεθνώς, πραγματικότητα ότι μια πτυχή του πληροφοριακού πολέμου είναι και ο αποκαλούμενος κυβερνοπόλεμος, παραθέτουμε τις πρώτες επιστημονικές προσεγγίσεις για αυτόν. Στο πρώτο υποκεφάλαιο του κεφαλαίου 9, παρουσιάζουμε τις πρώτες υπηρεσίες κυβερνοασφάλειας στον κόσμο. Μια υπερεθνική (του ΝΑΤΟ), μια εθνική (των ΗΠΑ) και τέλος, διεξοδικότερα, την κατάσταση στην Ελλάδα. Στο δεύτερο υποκεφάλαιο παραθέτουμε την βασική τεχνική ορολογία του εξοπλισμού και των τύπων των κυβερνοεπιθέσεων.

ΤΜΗΜΑ ΙΙΙ: Β' ΜΕΡΟΣ - Ο ΚΥΒΕΡΝΟΧΩΡΟΣ

Στο δέκατο κεφάλαιο, θα προβούμε στο εγχείρημα «κωδικοποίησης» της σχετικά μικρής ιστορίας του κυβερνοχώρου. Με άλλα λόγια, θα προσπαθήσουμε να φτιάξουμε έναν *αλγόριθμο* ανάγνωσης της εξέλιξής του, καθορίζοντας τα στοιχεία που συνιστούν κάθε φορά, ένα σταθμό και παράλληλα, τα χαρακτηριστικά που ενέχονται σε κάθε χρονική φάση, η οποία μεσολαβεί μεταξύ δύο σταθμών. Στο τέλος, και επιχειρώντας να ελέγξουμε την ισχύ της τρίτης υπόθεσης της εργασίας μας, θα

συνάγουμε το συμπέρασμά μας, ως προς τη σχέση της εξέλιξης του κυβερνοχώρου και του τρόπου που κατανοείται ο κυβερνοπόλεμος (κεφάλαιο 11).

Το παρόν έργο θα ολοκληρωθεί με την προσθήκη του παραρτήματος. Σε αυτό θα κατατεθούν όλα τα τεκμήρια για τη συλλογή, την επεξεργασία και την ανάλυση που βασίστηκε η έρευνά μας. Πιο συγκεκριμένα, θα περιέχονται τα κείμενα, όπως αυτούσια τα συλλέξαμε από τις αντίστοιχες ιστοσελίδες των πηγών μας. Σε αυτά, θα έχουν πραγματοποιηθεί μόνο δύο παρεμβάσεις, οι οποίες εντούτοις δεν θα είναι ικανές να αλλοιώσουν την αυθεντικότητα του κειμένου. Η πρώτη θα αφορά την προσθήκη αύξουσας αρίθμησης, με ένα επιπλέον φωτεινό φόντο στην ημερομηνία κάθε κειμένου (corpus)· δύο στοιχεία τα οποία προσδίδουν και την ταυτότητά του. Η δεύτερη θα αφορά την προσθήκη του κωδικού αριθμού του μητρώου της μονάδας αναφοράς (item), με τρόπο ωστόσο τέτοιο που να είναι δεικτικός και διακριτός από το αυτούσιου κείμενο. Η τελευταία προσθήκη θα συνοδεύεται προηγουμένως με το μαρκάρισμα της ακριβούς έκφρασης, η οποία τεκμηριώνει (σημασιολογικά) τη μονάδα αναφοράς.

1.2 Ο Σκοπός της Έρευνας

Στην κατάρτιση κάθε επιστημονικής διατριβής είναι αναγκαία η ακριβής διατύπωση του σκοπού της εκπόνησης. Επιπροσθέτως, σε αυτό και το επόμενο υποκεφάλαιο θα καλύψουμε την απαραίτητη αναφορά στα ακόλουθα ζητήματα:

- ποιο είναι το ευρύτερο πλαίσιο της επιστημονικής περιοχής που θα κινηθεί,
- ποια είναι η αξία και η χρησιμότητά της,
- ποια η συνεισφορά στην πρωτοτυπία και
- ποια είναι τα όρια και τα περιθώρια της έρευνας.

Το προαναφερόμενο πλαίσιο αυτής της εργασίας διαγράφεται από τον αντικειμενικό σκοπό της έρευνας μας, ο οποίος συνίσταται από την κατηγοριοποίηση των νοηματοδοτήσεων που προσδίδονται στον όρο «κυβερνοπόλεμος», εντοπίζοντας τα γεγονότα² στα οποία προσδόθηκε αυτή η έννοια, μέσω των ψηφιακών Μέσων Μαζικής Ενημέρωσης (ΜΜΕ) με δυνατότητα παγκόσμιας εμβέλειας. Ακολουθεί η αιτιολόγηση της επιλογής του μέσου επίτευξης αυτού του σκοπού.

² Στην εργασία αυτή «γεγονός» θα εννοούμε ένα εσκεμμένο σύνολο ενεργειών (δράσεων και δηλώσεων), το οποίο δεν εκφράζει προθέσεις, αντιθέτως έχει ήδη πραγματοποιηθεί. Επιπλέον, ενέχει πολιτική σκοπιμότητα και γνωστοποιείται διαμέσου του κυβερνοχώρου, από ένα υποκείμενο (άτομο, ομάδα, κράτος κοκ) έναντι ενός άλλου.

Ο όρος «κυβερνοπόλεμος» εμφανίστηκε περίπου πριν δύο δεκαετίες. Το βασικότερο γνώρισμα του είναι ότι ενώ οι σχετικές επιθέσεις έχουν ταυτότητα άγνωστης προέλευσης³, ούτε κανείς επιτιθέμενος μέχρι σήμερα έχει αποδεχτεί τέτοιες ενέργειες. Συνεπώς, πρωτογενής πηγή μπορούν να αποτελέσουν μόνον οι αντιδράσεις των πληγέντων. Τα θέματα όμως αυτά εκτιμώνται ως ζητήματα υψίστης ασφαλείας και παραμένουν μυστικά. Οπότε και η υλοποίηση των προαναφερόμενων αντιδράσεων συνήθως δεν αποκαλύπτεται. Συνθήκη η οποία αποτελεί και τον *περιορισμό* αυτής της διατριβής. Έτσι, στοιχεία μπορούμε να συλλέγουμε από μια (δευτερογενή) πηγή, είτε των επιστημονικών, είτε των δημοσιογραφικών δημοσιεύσεων. Επιλέξαμε την τελευταία, ώστε να μην αρκεστούμε σε μια απλή βιβλιογραφική επισκόπηση και επίσης, για αυτήν την επιλογή, λάβαμε υπόψη μας την ακόλουθη θέση.

Όπως αναφέραμε, κύριο σκοπό της εργασίας αποτελεί η χαρτογράφηση των δημοσιοποιημένων γεγονότων, τα οποία θεωρήθηκαν συνώνυμα του φαινομένου. Συμπερασματικά, σύμφωνα με όλα τα παραπάνω, εκτιμούμαι πως τεκμηριώνεται η αξία της καινοτομίας της εκπόνησής μας, της οποίας επιπλέον επισημαίνεται, πως κατόπιν αναζήτησης στο Εθνικό Κέντρο Τεκμηρίωσης (www.ekt.gr, 7/10/2011), επιβεβαιώνεται η πρωτοτυπία της.

1.3 Υποθέσεις Εργασίας

Σε συνάρτηση με το παραπάνω πλαίσιο, οι Υποθέσεις Εργασίας διατυπώθηκαν με τον ακόλουθο τρόπο:

I] Υφίσταται μια διεθνώς βεβαιωμένη σύγχυση για το ποια γεγονότα είναι ικανά να αποτελέσουν «πράξη κυβερνοπολέμου».

II] Ωστόσο, η χαρτογράφηση όλων των συναφών γεγονότων, δύναται να οδηγήσει στην ταξινόμησή τους, με τη χρήση ενός «ψυχοκοινωνικού» κριτηρίου. Αυτό θα πρέπει να εξετάζει το βαθμό που τα γεγονότα, τα οποία θεωρείται πως συνιστούν έναν κυβερνοπόλεμο: **A]** Απασχολούν «ανοικτά» την κοινωνία ή μόνον ένα συγκεκριμένο κομμάτι της. **B]** Αν η επίθεση απευθύνεται στη βλάβη κυρίως ανθρώπινων ή κυρίως τεχνολογικών πόρων.

³ Προς το παρόν είναι εφικτή η γενική γεωγραφική προσέγγιση του επιτιθέμενου συστήματος, δίχως όμως να μπορεί να αποδειχθεί ο χρήστης και κυρίως, ο κρατικός φορέας από τον οποίο εντέλλεται.

III] Η ανάλυση αυτού του «ψυχοκοινωνικού» κριτηρίου μπορεί να δείξει την άμεση σχέση που έχει ο τρόπος με τον οποίο ο καθένας κατανοεί το φαινόμενο του κυβερνοπολέμου, με τον τρόπο που αντιλαμβάνεται την έννοια του κυβερνοχώρου.

Πιο συγκεκριμένα, με τη λέξη-κλειδί «ψυχοκοινωνικό», θέλουμε να δηλώσουμε την αναζήτηση του τύπου της κυβερνοεπίθεσης ως προς μια διττή φύση της έντασης του στόχου⁴. Αφενός, από το βαθμό που η κυβερνοεπίθεση αντιμετωπίζεται ως ενδιαφέρον γεγονός από τους πολίτες, οι οποίοι, ως εκ τούτου, ασχολούνται με τις συνέπειές της. Αφετέρου, από το βαθμό που η κυβερνοεπίθεση στοχεύει είτε στην επιρροή της ανθρώπινης συμπεριφοράς, είτε στην εύρυθμη λειτουργία των τεχνολογιών πληροφορίας και επικοινωνίας (ΤΠΕ). Μπορούμε λοιπόν να πούμε ότι στην πρώτη περίπτωση, μιλάμε για *ανοικτή ή κλειστή κοινωνικά* κυβερνοεπίθεση και στη δεύτερη περίπτωση, για κυβερνοεπίθεση *ανθρώπινης ή τεχνολογικής έντασης*. Έτσι παρατηρούμε επιθέσεις, τις οποίες οι μη αρμόδιοι δεν μαθαίνουν ποτέ, έστω και αν διαπράχθηκαν στη χώρα τους (π.χ. Stuxnet-worm, 2010). Αντιθέτως, άλλες είναι αδύνατον, εξαιτίας του εύρους των επιπτώσεών τους, να μην γίνουν αντιληπτές (π.χ. Εσθονία, 2007). Επιπρόσθετα, παρατηρούνται ενέργειες, οι οποίες προκαλούν ή προκαλούνται από την ηγεσία ενός κράτους (π.χ. Ιράν, 2009) και οι ίδιες επίσης προκαλούν ή προκαλούνται από την λαϊκή βάση (π.χ. Σερβία, 1999) και για πολλούς εξειδικευμένους ερευνητές και σχολιαστές τιτλοφορούνται ως «κυβερνοπόλεμος».

Αρχικά, αν εξετάσουμε τον όρο ετυμολογικά, θα δούμε ότι συνίσταται από δύο έννοιες. Του Πολέμου και του Κυβερνοχώρου. Το παράδοξο είναι ότι, αν και οι δύο αυτές έννοιες ανήκουν κατεξοχήν στην περιοχή ενδιαφέροντος των κοινωνικών επιστημόνων, το φαινόμενο του κυβερνοπολέμου δεν έχει τύχει ιδιαίτερης μελέτης από αυτούς. Ωστόσο, δική μας επιδίωξη είναι να ολοκληρώσουμε μια επιστημονική εργασία, της οποίας το ειδικό βάρος να εστιάζεται στην κοινωνιοψυχολογική της προσέγγιση. Συνεπώς, κρίναμε ότι για αυτήν μας την εντρύφηση, η καταλληλότερη πηγή μας είναι τα ΜΜΕ.

Όπως αναφέραμε προηγουμένως, έγιναν διάφορα εγχειρήματα προσδιορισμού του όρου. Από την αρχή της χρήσης του (όπως, Arquilla και Ronfeldt, 1993) έως τις ημέρες μας, που παρατηρούμαι ότι αυτές οι προσπάθειες πληθαίνουν (ενδεικτικά ορισμένα έργα κοινής αποδοχής είναι των: Libicki, 2009 - Carr, 2010 - Clarke,

⁴ Με την έκφραση «ένταση του στόχου» εννοούμε -όπως εξηγούμε αμέσως παρακάτω- τις πιο έκδηλες πτυχές των συνεπειών του χτυπήματος.

2010)⁵. Εντούτοις, όμως, πυκνώνουν και τα επιχειρήματα αυτών που υποστηρίζουν ότι κανένα από τα δύο συνθετικά μέρη (το πρόθεμα «κυβερνο-» και ο «πόλεμος») της λέξης δεν είναι εύστοχα. Ορισμένες ανακοινώσεις που ενισχύουν αυτή την κατεύθυνση είναι:

- Ο Howard Schmidt, συντονιστής για θέματα κυβερνοασφάλειας στον Λευκό Οίκο συνέστησε ότι η χρήση μιας ορολογίας που να πυροδοτεί, μέσω των μεταφορών της, ανησυχίες για την ασφάλεια στο διαδίκτυο δεν ωφελεί (BBC, 6/10/2011).
- Σε συνέδριο που έλαβε χώρα στη Βαρκελώνη (15/3/2010) με την επωνυμία «Black Hat»⁶, τα εξειδικευμένα μέλη του κατέληξαν πως ο όρος είναι αδόκιμος.
- Σε έκθεση του ΟΟΣΑ εκτιμήθηκε ως υπερβολικός ο όρος για την περιγραφή των επιθέσεων με τη χρήση της υψηλής τεχνολογίας. Πιο συγκεκριμένα, οι συγγραφείς της έκθεσης Καθηγητής Peter Sommer (LSE) και Dr Ian Brown (Oxford Internet Institute) δήλωσαν ότι «Δεν βοηθάμε τους εαυτούς μας χρησιμοποιώντας τον όρο “κυβερνοπόλεμος”, για να περιγράψουμε την κατασκοπεία ή τις διαδικτυακές επιθέσεις με πολιτική σκοπιμότητα (hactivism)» (<http://tvxs.gr/news>, 6/8/2011).
- Ο αντιπρόεδρος του τομέα έρευνας απειλών της μεγάλης εταιρείας διαδικτυακής ασφάλειας McAfee, Dmitri Alperovitch, δηλώνει ότι δεν τον εκφράζει η αναλογία που υποδηλώνεται με τον όρο «κυβερνοπόλεμος». Ο λόγος είναι ότι είναι πολύ δύσκολο να απαντηθεί αν πρόκειται όντως για πόλεμο. Κυρίως, επειδή δεν έχουμε νεκρούς. Παρόλα αυτά, βεβαιώνει, ότι πρόκειται για μια υπαρκτή απειλή (CNN & McAfee, 15/8/11).
- Ο Διευθυντής Ασφάλειας Πληροφοριών (British Telecommunications - BT) Bruce Schneier δήλωσε πως αυτό που βλέπουμε προς το παρόν, δεν μπορεί να οριστεί ως κυβερνοπόλεμος (BBC, 7/10/2011).

Από την άλλη πλευρά, οι πολιτικό-στρατιωτικοί θεσμοί ανά τον κόσμο οργανώνουν ειδικούς στρατούς με αυτήν την ονομασία⁷. Εκτός αυτών, πρόσφατα οι ΗΠΑ (31/5/2011), ανακοίνωσε ότι θα συντάξει το Δόγμα στο οποίο θα ορίζει επακριβώς του κανόνες εμπλοκής για την Κυβερνοάμυνά της (The Wall Street Journal, 1/6/2011) και ο διεθνής οργανισμός του NATO, κατά τη σύνταξη του νέου

⁵ Θα αναφερθούμε διεξοδικότερα, στο όγδοο κεφάλαιο, το οποίο αφιρώνουμε σε αυτό το θέμα.

⁶ Το εν λόγω συνέδριο πραγματοποιείται από το 1997. Σε αυτό συμμετέχουν ερευνητές και σύμφωνα με τις φήμες, η ελίτ των χάκερ... Ιδρυτής του θεσμού θεωρείται ο Jeff Moss, ο οποίος συμπεριλαμβάνεται στη λίστα των μελών του Homeland Security Advisory Council. Πρόκειται για μια ομάδα συμβούλων σε θέματα ασφάλειας της κυβέρνησης των ΗΠΑ (athens.cafebabel.com, 6/10/2011).

⁷ Υπάρχουν επίσημες ανακοινώσεις από τις ΗΠΑ, Κίνα, Ρωσία, Γαλλία, Γερμανία, Ισραήλ, Αυστραλία, Ιράν, Ν. Κορέα, Τουρκία κ.άλ.

στρατηγικού του δόγματος στη Λισσαβόνα (Δεκέμβριος, 2010) έθεσε μεταξύ των προτεραιοτήτων του την *κυβερνοασφάλεια* (www.nato.int, 24/11/2010).

Παρόλα αυτά, την καρδιά του προβλήματος εντόπισε ο Ken Silva, υπεύθυνος τεχνολογίας σε μεγάλη εταιρεία ασφάλειας δικτύων (Semantic Co. – Verisign Inc.). Κατά τα λεγόμενα του, αυτό που ζητάει το 99% των χρηστών του διαδικτύου και πελατών των εταιρειών κατασκευής λογισμικών είναι περισσότερη ευρυζωνικότητα, δηλαδή ταχύτητα κι ευελιξία πρόσβασης στον κυβερνοχώρο. Αυτό δημιουργεί δύο προβλήματα, το ένα είναι οι εταιρείες να προσανατολίζονται στο σχεδιασμό των προϊόντων τους σε αυτές τις απαιτήσεις και το άλλο, τα νέα προϊόντα να είναι ακόμα πιο ευάλωτα στους κακοπροαίρετους. Μόλις τελευταία, λοιπόν, αρχίζει να συνειδητοποιείται η αξία της ασφάλειας στον κυβερνοχώρο, καθώς και η μεγάλη σημασία της ακρίβειας των όρων που χρησιμοποιούμε στο κάθε τμήμα της. Αυτό επιβεβαιώνεται συνεχώς και σε επίσημο επίπεδο⁸. Εξάλλου, σύμφωνα με τον Ντάιμπερτ (2009), η σπουδαιότητα ενός καθορισμού των παραμέτρων που θα συνιστούν *πράξη πολέμου* ένα σύνολο γεγονότων, που σήμερα καλούμε «κυβερνοπόλεμο», φαίνεται όταν αναλογιστούμε ότι μια αναγνωρισμένη από το Διεθνές Δίκαιο⁹ κυβερνοεπίθεση νομιμοποιεί αντίμετρα άμυνας (Ελευθεροτυπία, 18/7/2009).

Οπότε, βάσει των παραπάνω, συμπεραίνουμε ότι η απάντηση στην πρώτη υπόθεση εργασίας μας είναι καταφατική. Επισημαίνουμε ότι η επαλήθευση (ή η διάψευση) των υποθέσεων θα αποδείξει (ή όχι) την κεντρική θέση της εργασίας, η οποία ισχυρίζεται ότι το φαινόμενο του κυβερνοπολέμου είναι δυναμικό. Αυτό όμως δεν σημαίνει πως η ουσία του χθες του, δεν διεξέρχεται με μια συνάφεια από το σήμερα στο αύριο. Αυτή ακριβώς η εντύπωση, πως ο κυβερνοπόλεμος αλλάζει χωρίς να συνάδει το παρελθόν με το μέλλον του, αποτελεί και την αιτία της προαναφερόμενης σύγχυσης. Θεωρούμε ότι αν ανατρέξουμε στις ρίζες του φαινομένου (τον πόλεμο και τον κυβερνοχώρο), θα διαπιστώσουμε ότι διακατέχονται από έναν σταθερό διφυές πυρήνα (τον άνθρωπο και την τεχνολογία). Από αυτόν τον πυρήνα αναδύεται το εκάστοτε πρόσωπο του κυβερνοπολέμου, ο τύπος δηλαδή που κάθε φορά φαίνεται στην επιφάνεια ενός χτυπήματος. Έτσι, αυτή η έκφραση μπορεί

⁸ Σε συνέδριο του ΟΗΕ στο Νταβός (Δεκέμβριος 2010), ο επικεφαλής της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU), Τουρέ, δήλωσε ότι «είναι ανάγκη να συμφωνηθεί μια συνθήκη κυβερνοπολέμου ή πολέμου στο Διαδίκτυο».

⁹ Κατά τον Καταστατικό Χάρτη του ΟΗΕ «πράξη πολέμου», η οποία νομιμοποιεί την αυτοάμυνα, δεν υφίσταται αν δεν υπάρχουν ανθρώπινες απώλειες ή υλικές καταστροφές (<http://www.un.org>).

να προέρχεται πρωτεύοντος είτε από το Διαδίκτυο (μπορούμε να μιλήσουμε για διαδικτυακό τύπο κυβερνοπολέμου), είτε από τον Παγκόσμιο Ιστό (μπορούμε να μιλήσουμε για κυβερνοπόλεμο τύπου έντασης παγκόσμιου ιστού) κοκ.

Τέλος, η διττή του αυτή φύση έγκειται, αφενός στο εκάστοτε διατιθέμενο «τεχνολογικό οπλοστάσιο» και αφετέρου, στις σχέσεις εξουσίας που διαπερνούν τα εν γένει οργανωτικά μορφώματα της κοινωνίας.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΕΝΝΟΙΟΛΟΓΗΣΗ

2.1 Σχεδιασμός

Σε αυτό το κεφάλαιο παρουσιάζουμε τη στρατηγική που ακολουθήσαμε, για να διεξάγουμε την έρευνα μας με ορθολογισμό και κανονικότητα, ώστε να εκπληρώσουμε σε ικανοποιητικό βαθμό το σκοπό μας. Για να φθάσουμε σε αυτό τον σκοπό, διεξαγάγαμε μια έρευνα, η οποία είχε στόχο την αποκάλυψη της «ψυχοκοινωνικής εικόνας»¹⁰ του κυβερνοπολέμου. Τα βήματα που κάναμε, ή αλλιώς τα στάδια της μεθοδολογίας μας, είναι τα εξής (Φίλιας, 1977, 19):

- α) η συλλογή,
- β) η επεξεργασία,
- γ) η ανάλυση και
- δ) η ερμηνεία.

Έναν πολύ σημαντικό ρόλο στον τρόπο που διαμορφώνεται η γνώμη¹¹ μας για τον κόσμο, παίζει το μέσο¹², το οποίο χρησιμοποιείται από το περιβάλλον μας στη διαδικασία παραγωγής και προώθησης ιδεών. Αρχικά, στο επικοινωνιακό περιβάλλον δέσποζε η αμεσότητα. Αυτό σημαίνει, πως χωρίς διαμεσολάβηση, διαμορφώναμε άποψη μέσω των διαπροσωπικών σχέσεων. Αργότερα, έχουμε την εμφάνιση και ιδιαίτερη επίδραση των έντυπων μέσων, όπως το βιβλίο και ο τύπος. Αυτά συνέπεσαν με τη συγκυρία της μαζικοποίησης της παραγωγής και μετέπειτα, της χωρίς σύνορα διακίνησης. Σήμερα, βρισκόμαστε στη φάση της σταδιακής ψηφιοποίησης των μέσων μαζικής ενημέρωσης (MME), καθώς επίσης και της πρόσβασης σε αυτά μέσα από τον κυβερνοχώρο.

Επιπροσθέτως, εκτός από το μέσο, επίσης καθοριστική είναι και η σημασία του τρόπου που προσλαμβάνουμε τις πληροφορίες, οι οποίες αποτελούν τα συστατικά στοιχεία διαμόρφωσης της γνώμης. Με την έκφραση «τρόπος πρόσληψης», αναφερόμαστε σε ένα είδος *αφήγησης*, σύμφωνα με το οποίο μέσω ενός MME

¹⁰ Χρησιμοποιούμε την έκφραση «ψυχοκοινωνική εικόνα» για να περιγράψουμε -όπως θα εξηγήσουμε αμέσως παρακάτω- το σύνολο των κοινωνικών αναπαραστάσεων που παρέχονται για το φαινόμενο.

¹¹ Η μελέτη της γνώμης έχει σημείο αναφοράς στην επιστημονική περιοχή της κοινωνικής ψυχολογίας, όπου συσχετίζεται με τις διεργασίες πληροφόρησης και επικοινωνίας (Maisonneuve, 2001, 218).

¹² Η σπουδαιότητα του μέσου εκφράστηκε από ένα απόθεγμα, το οποίο έχει καθιερωθεί στις κοινωνικές επιστήμες «Το μέσο είναι το μήνυμα». Ο ίδιος ο εμπνευστής του από πολύ νωρίς οραματίστηκε ένα «παγκόσμιο χωριό», το οποίο θα αποκτούσε η ανθρωπότητα, με έναν τρόπο ο οποίος προσιδιάζει στον παγκόσμιο ιστό (McLuhan, 1964/1989).

ερχόμαστε σε επαφή με τη διήγηση γεγονότων. Έτσι, η αφήγηση μάς οδηγεί να διαμορφώσουμε συγκεκριμένη γνώμη για την ιστορία κοινωνικών φαινομένων των οποίων δεν έχουμε προσωπική εμπειρία¹³ (Shanahan & Morgan, 1999, 48-49). Επιπρόσθετα, σύμφωνα με την παραπάνω αναφορά, στη Θεωρία Καλλιέργειας Προτύπων, οι τύποι της αφήγησης είναι οι τρεις ακόλουθοι:

- μύθοι αναφορικού λόγου (μυθιστορίες και παραμύθια),
- περιγραφή καταστάσεων (όπως, οι ειδήσεις και τα ντοκιμαντέρ), οι οποίες διακρίνονται από έναν ερεθισμό των συναισθημάτων που επιτυγχάνεται από την άμεση ή έμμεση αξιολόγηση και
- η προτροπή, υπόδειξη ή παρακίνηση, μέσω ενός παραγγελτικού λόγου, ο οποίος υποδηλώνει έναν εξιδανικευμένο στόχο.

Κατά την επαφή μας με την προφορική ή γραπτή αφήγηση ενός γεγονότος, δεν είναι απαραίτητο να εντοπίζεται καθαρά μόνον ένας από τους τρεις τύπους. Αποτελεί συχνό φαινόμενο, η παρατήρηση όλων των πιθανών συνδυασμών. Θεωρούμε χρέος μας σε αυτή τη μελέτη να αποφύγουμε τη σύγχυση που μπορεί να επιφέρει αυτή η συνθήκη. Όπως, επίσης παρομοίως οφείλουμε να διαχωρίσουμε, ώστε να αντιμετωπίσουμε με προσοχή, τα σημεία εντυπωσιασμού, τα οποία δεν λείπουν από τα ΜΜΕ¹⁴.

Από τον τρόπο λοιπόν που «αφηγούνται» τα μέσα τα γεγονότα του φαινομένου, διαμορφώνεται και η ψυχοκοινωνική εικόνα του. Ωστόσο, η αποτύπωσή της προϋποθέτει τον εντοπισμό όλων των δομικών στοιχείων, από τα οποία συνίσταται. Αυτά, όμως, ισοδυναμούν με μια έννοια, η οποία χρησιμοποιείται στην Κοινωνική Ψυχολογία τις τελευταίες περίπου τέσσερις δεκαετίες. Αναφερόμαστε στις Κοινωνικές Αναπαραστάσεις, οι οποίες, συνοπτικά θα λέγαμε ότι, εντυπώνεται μέσα στο νου μας, ώστε να «απεικονίσουν» συμβολικά το φαινόμενο του κυβερνοπολέμου. Οι κοινωνικές αναπαραστάσεις που είναι υπεύθυνες για την καταγραφή αυτής της εικόνας, αποτελούν ένα «κοινωνικό γεγονός», στο οποίο θα προσπαθήσουμε να εμβαθύνουμε, ώστε να το κατανοήσουμε¹⁵.

¹³ Αυτή ακριβώς είναι και η έννοια του διαμεσολαβημένου μηνύματος.

¹⁴ Αναμενόμενο γνώρισμα κάθε αρθρογραφίας, η οποία -εκτός από την πνευματική της υπόσταση- αποτελεί και ένα προϊόν προς πώληση. Έτσι, αποσκοπεί πάντα και στην αποδοχή της από την αγορά για την απόκτηση κέρδους. Τότε η διαφήμιση έχει κύριο ρόλο και ο εντυπωσιασμός είναι μέρος της.

¹⁵ Ενδεικτικά, η σημαντικότητά τους φαίνεται αν αξιολογήσουμε το ότι οι κοινωνικές αναπαραστάσεις ενός πληθυσμού μπορούν να επηρεάσουν καθοριστικά την ομοιογένειά του (Καταρέλος, 1996, 70).

2.2 Κοινωνικές Αναπαραστάσεις (Social Representation)

Οι Κοινωνικές Αναπαραστάσεις εντάσσονται στην επιστημονική περιοχή της Κοινωνικής Ψυχολογίας. Η προέλευση της έννοιας βρίσκεται στον Emil Durkheim (1898), ο οποίος πρότεινε την έκφραση της συλλογικής αναπαράστασης. Η αναπαράσταση ορίζεται ως το σύνολο των πραγματικών ή δυνητικών δεδομένων, τα οποία συνθέτουν το υπόβαθρο μια έννοιας (Sorlin, 2004, 38). Τα δεδομένα αυτά μπορεί να είναι, είτε λογικοί συνειρμοί που συναθροίζονται από λέξεις και εικόνες, είτε συναισθηματικές αντιδράσεις «που ξεπηδούν από το άκουσμα» της έννοιας. Ο Durkheim, λοιπόν, θεώρησε ότι υπάρχει μία διαφορετική, από τις ατομικές, αναπαράσταση, την οποία δεν όρισε, μα περιορίστηκε να αναφέρει ότι εγκαθιδρύεται μεταξύ της κοινωνικής ζωής των ατόμων (Maisonneuve, 2001, 233). Αυτός όμως που θα θεμελιώσει επιστημονικά την έννοια είναι ο S. Moscovici (1976). Αρχικά, παρατηρεί μια ρευστότητα στην έννοια, η οποία συγγενεύει με τους όρους της γνώμης, της στάσης και του στερεότυπου. Τελικά, καταλήγει στον όρο «κοινωνικές αναπαραστάσεις», προτάσσοντας το κοινωνικό έναντι του συλλογικού χαρακτήρα τους. Ο βασικός λόγος που γίνεται αυτό είναι ότι οι κοινωνικές αναπαραστάσεις συγκροτούν μια μορφή πρακτικής γνώσης, η οποία επιτρέπει στα άτομα να συγκλίνουν και το ατομικό να γίνεται κοινωνικό.

Οι κοινωνικές αναπαραστάσεις ορίζονται ως εννοιολογικά σύνολα τα οποία παράγονται στην καθημερινή ζωή, κατά τη διαπροσωπική επικοινωνία, με σκοπό την εξήγηση της πραγματικότητας. Με άλλα λόγια, κάθε επικοινωνία πραγματοποιείται με την προϋπόθεση της ύπαρξης ενός κοινού σημείου αναφοράς· αυτό είναι οι κοινωνικές αναπαραστάσεις. Εδράζονται στο ανθρώπινο μυαλό και διακινούνται μέσα στην κοινωνία. Ένας από τους τρόπους κυκλοφορίας τους είναι τα MME και για όχημά τους μπορεί να χρησιμοποιηθεί ο διάλογος, τα κείμενα κλπ. Έτσι, όταν επιθυμούμε να προσδώσουμε νόημα σε μια σειρά ομοιογενών γεγονότων, διαμορφώνουμε συμβολισμούς, των οποίων η πρόσληψη, ενδεχομένως να έχει διαμεσολαβηθεί από τα MME. Για αυτό το λόγο τα επικοινωνιακά μέσα, πέρα από τον πληροφοριακό τους χαρακτήρα, έχουν και τη συμβολική κατασκευή αναπαραστάσεων¹⁶ (Ψύλλα, 2010).

¹⁶ Πιο συγκεκριμένα, σχετικά με την προπαγανδιστική εφαρμογή του όρου, η οποία μας ενδιαφέρει στο επόμενο κεφάλαιο της ανάλυσης, αναφέρεται πως ο ρόλος των κοινωνικών αναπαραστάσεων στη σχέση της ανθρώπινης συμπεριφοράς με την επικοινωνία γίνεται αναγκαίος και ρητός.

Ειδικότερα, μας ενδιαφέρει η εξέτασή τους από την πλευρά της δόμησης των μηνυμάτων, ως δηλαδή αποτέλεσμα της συσχέτισης του πομπού και του δέκτη. Αν και αποτελεί βασικό τους γνώρισμα ο κοινωνικός χαρακτήρας τους, η διατήρηση της υψηλής ατομικότητας στην προαναφερόμενη επικοινωνιακή σχέση είναι που επιβάλλει τη μελέτη τους, στην «αποκωδικοποίηση» των στάσεων, των στερεοτύπων και της προπαγάνδας (Moscovici, 1976/1999).

Τέλος, αναζητώντας τα συστατικά στοιχεία, τα οποία συνιστούν τις κοινωνικές αναπαραστάσεις, διακρίνουμε δύο μέρη. Έναν κεντρικό σταθερό πυρήνα συμβόλων σχετικών με την έννοια με την οποία συνδέονται και ένα μεταβαλλόμενο περιφερειακό μέρος. Αυτό το τελευταίο είναι που υπόκειται και στις επιδράσεις από το κοινωνικό περιβάλλον, ώστε να αλλάζει. Εξάλλου, κύρια αρχή στη θεώρηση των κοινωνικών αναπαραστάσεων είναι ότι δεν υφίσταται μια αντικειμενική πραγματικότητα.

Αυτές οδήγησαν την Κοινωνική Ψυχολογία από την περιοχή της λογικής στην περιοχή του συναισθήματος, δείχνοντας ότι εμείς μόνοι μας φτιάχνουμε τον κόσμο μας, όπως νομίζουμε ότι μας βολεύει, αλλοιώνοντας την «πραγματικότητα» που μας περιβάλλει, αντλώντας απ' αυτήν τα στοιχεία εκείνα που «ταιριάζουν» καλύτερα σ' αυτά που έχουμε ήδη στη διάθεσή μας από πρωτότερες «εξορμήσεις» στον περιβάλλοντα κόσμο μας (Παπαστάμου, 1995).

2.3 Η Μέθοδος

Σε κάθε έρευνα απαιτείται μια επιστημονικά αποδεκτή διαδικασία επεξεργασίας των δεδομένων της, η οποία να διασφαλίζει δύο από τα βασικά γνωρίσματά της, την ακρίβεια και την επιβεβαίωση ή επαλήθευση (Evera, 2000/2005). Το αποσπασματικό και μεμονωμένο σύνολο των τεχνικών και διαδικασιών διεξαγωγής κάθε επιστημονικής έρευνας καλούμε Μέθοδο (Ζαφειρόπουλος, 2005, 15-16). Η μέθοδο την οποία θα ακολουθήσουμε για να επιτύχουμε το σκοπό μας είναι η Ανάλυση Περιεχομένου. Σύμφωνα με τον Berelson (1948), πατέρα αυτής της μεθόδου, πρόκειται για την αντικειμενική, συστηματική και ποσοτική περιγραφή του φανερού περιεχομένου των επικοινωνιών, με σκοπό την ερμηνεία τους (Φίλιας, 1977, 196).

Ένα βασικό χαρακτηριστικό της μεθόδου μας είναι ότι οι αναλυόμενες ενότητες δεν αποτελούνται μόνο από λέξεις, αλλά κυρίως από έννοιες. Εξ άλλου, συχνά, επιλέγεται η χρήση ενοτήτων, οι οποίες συνίστανται από θέματα ή από ολόκληρες

φράσεις του κειμένου (Τζανή, 2005). Ειδικότερα, -όπως ήδη αναφέραμε- θα επιχειρήσουμε μια ταξινόμηση των νοηματοδοτήσεων που έχουν δημοσιευθεί για την έννοια της απειλής *επίθεσης στον κυβερνοχώρο* (κυβερνοεπίθεση), υποβάλλοντας το «σώμα των τεκμηρίων μας» (corpus: το σύνολο των κειμένων τα οποία θα συλλέξουμε) σε μια συντακτική επεξεργασία με γραμματική βάση. Η μονάδα ανάλυσής μας (items: το σύνολο των αναφορών – εννοιών, τα ευρήματα της έρευνας, που θα προκύψουν από την επεξεργασία του corpus) θα εμπεριέχει φράσεις και παραγράφους. Συνεπώς, θα διεξαχθεί μια σημασιολογική -και όχι γλωσσολογική¹⁷- ανάλυση. Ο κύριος λόγος αυτής της επιλογής αφορά, από τη μια πλευρά στο νεοεμφανιζόμενο χαρακτήρα του φαινομένου. Από την άλλη, είναι επακόλουθο, οι αρθρογράφοι να μην έχουν εξειδικευθεί σε μια αυστηρή ορολογία, ώστε να μπορούμε να είμαστε σίγουροι, έχοντας έναν ικανοποιητικό βαθμό βεβαιότητας, για την αυστηρή χρήση των λέξεων. Εξάλλου, το ενδιαφέρον μας εστιάζεται στις ενδεχόμενες συγκλίσεις των προσεγγίσεων για το φαινόμενο και όχι στην οριοθέτησή του, ώστε να προκύψουν οι ανάλογες θεματικές. Αναζητούμε λοιπόν με την ομαδοποίηση των φράσεων ή παραγράφων που συνδέονται με το νόημα της απειλής του κυβερνοπολέμου. Τέλος σημειώνουμε ότι σε περίπτωση διπλής αναφοράς σε μια παράγραφο, ή απολύτως ίδιας επιχειρηματολογίας δύο παραγράφων σε ένα κείμενο, αυτές θα εξαιρούνται από τη μέτρηση.

Οι εν λόγω επιλογές που θα προκύψουν από την επεξεργασία της έρευνας, θα αφορούν αυτόνομα νοηματικά τμήματα ενός κειμένου και τελικά, θα πρέπει να μπορούν να ενταχθούν σε μια και μόνο *θεματική κατηγορία* (categories: Το αποτέλεσμα της ταξινόμησης των items σε συναφείς ομάδες, βάσει του ψυχοκοινωνικού μας κριτηρίου). Κατά τον Berelson, αυτή η μέθοδος αξίζει όσο και το αποτέλεσμα των *θεματικών κατηγοριών*. Κάτι ωστόσο που για να συμβεί, θα πρέπει η κάθε μια από αυτές χωριστά, να είναι εξαντλητική, αποκλειστική, συγκεκριμένη και κατάλληλη (Κωνσταντοπούλου, 1985, 45).

¹⁷ Πρόκειται για μια ποιοτική ανάλυση περιεχομένου των κειμένων, στην οποία, εν ολίγοις, ως βάση χρησιμοποιείται επιλεγμένη λέξη ή ειδικότερα, όροι (<http://academic.csuohio.edu/kneuendorf/content>). Εκτός αυτού, σε μια ποιοτική ανάλυση, εκτός του περιεχομένου μπορεί να εστιαστούμε στη μορφή και συνολική παρουσία του κειμένου. Εξ ορισμού, αφού η φράση αποτελείται από ένα σύνολο λέξεων, η γλωσσολογική συμβάλλει στη σημασιολογική ανάλυση.

3. Η ΤΑΥΤΟΤΗΤΑ ΤΗΣ ΕΡΕΥΝΑΣ

3.1 Η Συλλογή

Αναφέραμε ήδη ότι η επιλογή της πηγής άντλησης των τεκμηρίων μας, η οποία εκπληρώνει τις παραπάνω προϋποθέσεις, είναι ο Τύπος. Ειδικότερα, η επιλογή αυτή συγκεκριμενοποιήθηκε σε δύο διεθνή Ειδησεογραφικά Πρακτορεία. Ένα από την Ευρώπη και ένα από την Αμερική. Αντίστοιχα λοιπόν, το πρώτο μέσο εδράζεται στη Μ. Βρετανία και αφορά στον δημόσιο οργανισμό ραδιοτηλεοπτικής και διαδικτυακής εκπομπής ειδήσεων British Broadcasting Corporation (BBC)¹⁸. Παρότι χρηματοδοτείται από τη βρετανική κυβέρνηση, πρόκειται για έναν αυτόνομο οργανισμό (Wikipedia, 5/10/2011). Όσον αφορά τον δεύτερο μέσο, εδράζεται στην πολιτεία της Τζόρτζιας (Γεωργία – ΗΠΑ) και αναφερόμαστε στο τηλεοπτικό δίκτυο (θυγατρική της Turner Broadcasting System και μητρική της η Time Warner) Cable News Network (CNN)¹⁹.

Το ζητούμενο, λοιπόν, ήταν μια ιστοσελίδα, η οποία να προσφέρει γενική²⁰ ειδησεογραφία (τα λεγόμενα «νέα της επικαιρότητας») με ενδεχόμενες αναφορές στο θέμα της απειλής του κυβερνοπολέμου. Στη συνέχεια θέσαμε τέσσερις κοινές προϋποθέσεις για αυτήν την επιλογή και επιπροσθέτως, η επιλογή ενισχύθηκε από μία χωριστή για την κάθε περίπτωση ιδιότητα. Οι προϋποθέσεις είναι οι εξής:

- ελεύθερα προσβάσιμη ψηφιακή έκδοση (δίχως συνδρομή ή άλλες δικλείδες),
- παροχή σε ικανοποιητική έκταση χρόνου αρχειακού υλικού,
- διάθεση στην αγγλική γλώσσα και
- προτεραιότητα στην ιεραρχική της θέση, βάσει της επισκεψιμότητας.

Η μεθοδολογία που ακολουθήσαμε για την εύρεση των δύο θέσεων στον Παγκόσμιο Ιστό ξεκίνησε αντίστροφα από τον τρόπο που παραθέτουμε τις προϋποθέσεις. Δηλαδή, αναζητήσαμε στη δημοφιλέστερη μηχανή αναζήτησης (google.com)²¹ και εντοπίσαμε έναν διεθνή ιστότοπο, ο οποίος να μας προσφέρει

¹⁸ Το BBC ιδρύθηκε στις 1 Ιανουαρίου του 1927 και η έδρα του βρίσκεται στην πόλη του Γουέστμινστερ του Λονδίνου (Ηνωμένο Βασίλειο). Ο ίδιος οργανισμός προσδιορίζει ως αποστολή του τον εμπλουτισμό των ανθρώπων με την πληροφόρηση, την εκπαίδευση και την ψυχαγωγία (<http://www.bbc.co.uk/aboutthebbc/purpose/what.shtml>, 5/10/2011).

¹⁹ Το CNN ιδρύθηκε στις 1 Ιουνίου του 1980 και η έδρα του βρίσκεται στην πόλη της Ατλάντα (Ηνωμένες Πολιτείες Αμερικής). Ο ίδιος οργανισμός συνοψίζει την αποστολή του στην έγκαιρη εκπομπή νέων (<http://edition.cnn.com/about/>, 5/10/2011).

²⁰ Εδώ εξαιρέσαμε τους ιστότοπους με ειδική θεματολογία, όπως οι αθλητικοί, ψυχαγωγικοί κλπ.

²¹ Μετά, βεβαίως, ανακαλύψαμε πως είναι και η πρώτη σε επισκεψιμότητα ιστοσελίδα παγκοσμίως.

πληροφορίες για μια παγκόσμια κατάταξη βάσει της επισκεψιμότητας. Έτσι, διακρίναμε στις 5/10/2011, ότι είχαμε τα ακόλουθα αποτελέσματα (Πίνακας 1)²².

Πίνακας 1. Οι θέσεις στον Παγκόσμιο Ιστό με τη μεγαλύτερη επισκεψιμότητα

1	Google	(google.com)
2	Facebook	(facebook.com)
3	YouTube	(youtube.com)
4	Yahoo!	(yahoo.com)
5	Baidu.com	(baidu.com)
6	Wikipedia	(wikipedia.org)
7	Blogger.com	(blogspot.com)
8	Windows Live	(live.com)
9	Twitter	(twitter.com)
10	QQ.COM	(qq.com)
11	MSN	(msn.com)
12	LinkedIn	(linkedin.com)
13	Yahoo! Japan	(yahoo.co.jp)
14	Amazon.com	(amazon.com)
15	Google India	(google.co.in)
16	淘宝网	(taobao.com)
17	新浪新闻中心	(sina.com.cn)
18	WordPress.com	(wordpress.com)
19	Google	(google.de)
20	Google谷歌	(google.com.hk)
21	eBay	(ebay.com)
22	Яндекс	(yandex.ru)
23	Google UK	(google.co.uk)
24	Google 日本	(google.co.jp)
25	Google France	(google.fr)

²² Πηγή μας αποτέλεσε ο ιστότοπος “Alexa [Web Information Service]”, ο οποίος με τη χρήση της πληροφορικής τεχνολογίας web intelligent, καταμετρά τις αιτήσεις πρόσβασης σε κάθε θέση του παγκόσμιου ιστού και κατόπιν, δημοσιοποιεί τα αποτελέσματα. Ιδρύθηκε τον Απρίλιο του 1996 και από το 2005 είναι μέλος του ομίλου Amazon.com (<http://www.alexa.com/company>).

26	Bing	(bing.com)
27	Microsoft Co.	(microsoft.com)
28	新浪微博-随时随地分享身边的新鲜事儿	(weibo.com)
29	t.co	(t.co)
30	网易	(163.com)
31	Google Brasil	(google.com.br)
32	Почта@Mail.ru	(mail.ru)
33	PayPal	(paypal.com)
34	Flickr	(flickr.com)
35	Craigslist.org	(craigslist.org)
36	Google	(google.it)
37	googleusercontent.com	(googleusercontent.com)
38	FC2	(fc2.com)
39	Apple Inc.	(apple.com)
40	Go	(go.com)
41	The Internet Movie Database	(imdb.com)
42	Google Español	(google.es)
43	V Kontakte	(vkontakte.ru)
44	soso搜搜	(soso.com)
45	BBC Online	(bbc.co.uk)
46	Ask	(ask.com)
47	Tumblr	(tumblr.com)
48	搜狐网	(sohu.com)
49	Google	(google.ru)
50	<u>xvideos.com</u>	(xvideos.com)
51	优酷	(youku.com)
52	LiveJasmin.com	(livejasmin.com)
53	CNN Interactive	(cnn.com)
54	ESPN	(espn.go.com)
55	Tudou.com 土豆网	(tudou.com)
56	Google México	(google.com.mx)
57	xhamster.com	(xhamster.com)

58	Google	(google.ca)
59	凤凰网 (凤凰新媒体)	(ifeng.com)
60	AOL	(aol.com)

Πηγή: <http://www.alexa.com/topsites>

Κατόπιν, αφαιρέσαμε όσους ιστότοπους δεν έχουν ως αντικείμενο τη γενική θεματολογία²³. Μετά, εξαιρέσαμε όσους δεν προσφέρουν κείμενα στην αγγλική γλώσσα και εν κατακλείδι, όσους δεν είχαν την επιλογή του αρχειακού υλικού²⁴.

Όπως αναφέραμε προηγουμένως, σε αυτό το κεφάλαιο, για το κάθε μέσο υπάρχει και ένα μεμονωμένο κριτήριο επιλογής. Σχετικά με το BBC, εκτιμάται ότι είναι ο μεγαλύτερος σε εμβέλεια σταθμός στον κόσμο, με προσωπικό 23000 άτομα (<http://www.medianewsline.com>, 23/9/2010). Και, όσον αφορά το CNN²⁵, παρείχε την κυρίαρχη κάλυψη στον πόλεμο του Ιράκ, γεγονός το οποίο θεωρείται εισήγαγε το πολεμικό φαινόμενο σε μια νέα πληροφοριοκεντρική εποχή²⁶ (Taylor, 2004, σ. 30).

3.2 Η Επεξεργασία

Η συλλογή τελικά οριστικοποιήθηκε στα 105 κείμενα (Πίνακας 2). Αυτά προέρχονται, τα 52 από το BBC και τα 53 από το CNN (Σχήμα 1). Από το BBC διαχωρίστηκαν ως ακατάλληλα 5 (απομένουν **47**), τα οποία και ακυρώθηκαν και αντίστοιχα από το CNN διαχωρίστηκε 1 ακατάλληλο (απομένουν **52**), το οποίο επίσης εξαιρέθηκε (Σχήμα 2). Άρα, το τελικό σώμα κειμένων (corpus) προς επεξεργασία περιλαμβάνει **99** κείμενα (Σχήμα 3).

Στον πίνακα που ακολουθεί η πρώτη στήλη (Α) δείχνει τον αύξοντα αριθμό, όταν αυτός είναι μηδέν (0), σημαίνει πως το αντίστοιχο κείμενο κρίθηκε ακατάλληλο. Η δεύτερη στήλη δείχνει την ημερομηνία ανάρτησης (προσοχή, όχι ανάκτησης από εμάς) στο διαδίκτυο, ακολουθεί ο τίτλος, τον οποίο αντιγράψαμε όπως ακριβώς τον αναγνώσαμε. Τελευταία είναι η στήλη με την έκταση του κειμένου, καταμετρημένη σε αριθμό λέξεων.

²³ Τα περισσότερα είχαν αντικείμενο την κοινωνική δικτύωση ή αποτελούσαν μια εθνική μηχανή αναζήτησης.

²⁴ Αξιοσημείωτη, εδώ, είναι η περίπτωση του “QQ international” (2^ο εκτός ΗΠΑ και 2^ο στην Κίνα). Βρίσκεται στην κατάταξη στη θέση No 10 και πληροί όλες τις προϋποθέσεις μας, εκτός από αυτήν του αρχειακού υλικού. Σημειώνουμε ότι το 1^ο κινεζικό και εκτός ΗΠΑ βρίσκεται στην κατάταξη, στη θέση No 5 και είναι το baidu.com, το οποίο όμως προσφέρει μόνο υπηρεσίες μιας μηχανής αναζήτησης.

²⁵ Του CNN, επίσης, η ευρεία δικτύωση διεθνώς είναι αξιοσημείωτη. Η συνεργασία του με άλλα δίκτυα και υπηρεσίες δίνει πρόσβαση σε περίπου 1,5 δισεκατομμύρια τηλεθεατές σε πάνω από 212 κράτη, με πλέον των τεσσάρων χιλιάδων επαγγελματιών. Τέλος, έχει και τον τίτλο του πρώτου δικτύου 24ωρης δημοσιογραφικής κάλυψης (<http://el.wikipedia.org/wiki/CNN>).

²⁶ Βλέπε, προς το τέλος της εργασίας, στο Κεφάλαιο «Ο πόλεμος» (Τμήμα ΙΙΙ – Μέρος Α’).

Πίνακας 2^Α. *BBC-Corpus*: Το Σώμα των κειμένων που συλλέχθηκαν

A	HMEP/NIA	TITΛΟΣ	ΛΕΞΕΙΣ
1	14/7/2011	Pentagon admits suffering major cyber attack in March	0
2	17/6/2011	US builds net for cyber war games	458
3	14/6/2011	Lulz attacks: US orders review as Senate site hacked	246
4	13/6/2011	IMF cyber attacks signal new spying era	462
0	2/6/2011	Cyber war's 'death and destruction'	0
5	1/6/2011	US Pentagon to treat cyber-attacks as 'acts of war'	684
6	17/3/2011	US cyber war defences 'very thin', Pentagon warns	309
7	16/2/2011	Cyber attacks 'acts of war' - Sir Richard Mottram	735
8	16/2/2011	Cyber war threat exaggerated claims security expert	897
0	4/2/2011	Calls for 'rules of engagement' for cyber conflict	0
0	3/2/2011	US cyber warfare expert on threats which exist now	0
9	17/1/2011	Risks of cyber war 'over-hyped' says OECD study	556
10	14/1/2011	Tunisia protests: Cyber war mirrors unrest on streets	1.119
11	16/12/2010	EU could turn to 'crowd sourcing' in cyber crime fight	684
12	14/12/2010	UK Government websites may be next pro-Wikileaks focus	650
0	10/12/2010	The conflict between Wikileaks supporters and the companies	0
13	9/12/2010	Why are hacktivists 'Anonymous' defending WikiLeaks	731
14	24/11/2010	Should Obama's 'internet kill switch' power be curbed?	1.181
15	4/11/2010	Europe simulates total cyber war	240
16	14/10/2010	Call to define rules of cyber war	484
17	21/6/2010	Defence review to look at all potential conflicts - Fox	428
18	17/6/2010	Cyber-war a growing threat warn experts	810
19	15/3/2010	Meet USCybercom: Why the US is fielding a cyber army	1.090
20	11/2/2010	How Iran's political battle is fought in cyberspace	783

21	17/11/2009	Age of cyber warfare is 'dawning'	500
22	24/6/2009	What rules apply in cyber-wars?	654
0	22/6/2009	West 'seeks Iran disintegration'	0
23	15/6/2009	Israel and foes in internet war	730
24	31/3/2009	The Tech Lab: Ken Silva	914
25	14/8/2008	Caucasus foes fight cyber war	740
26	14/5/2008	Estonian cyber defence hub set up	157
27	24/4/2008	Hackers warn high street chains	904
28	25/1/2008	Estonia fines man for 'cyber war'	423
29	17/5/2007	Estonia hit by 'Moscow cyber war'	616
30	17/5/2006	Web attacks end anti-spam effort	408
31	12/2/2006	'Cyber Storm' tests US defences	196
32	4/12/2005	Militants' new tack in cyber war	338
33	21/3/2003	Anti-war hackers target websites	408
34	13/3/2003	Indian hackers target Pakistan	256
35	7/2/2003	US ponders cyber war plans	698
36	17/4/2002	Indian hacker turns cyber cop	460
37	23/10/2001	Hactivists take sides in war	819
38	7/3/2001	Hamas hit by porn attack	489
39	26/10/2000	Israel under cyber attack	199
40	1/9/2000	Draskovic website hoax	311
41	7/8/2000	Taiwan plays cyber war games	200
42	23/3/2000	Liberian radio ban lifted	288
43	18/8/1999	World: Asia-Pacific Timor activists warn of cyber war	439

44	4/8/1999	Sci/Tec China accused of cyber war	306
45	1/3/1999	World: Africa Eyewitness: Reporting the war in the Horn	739
46	7/2/1999	World: Asia-Pacific: China casts a cyber net	335
47	1/2/1999	Middle East: Teenage hacker 'destroys anti-Israeli Website'	387

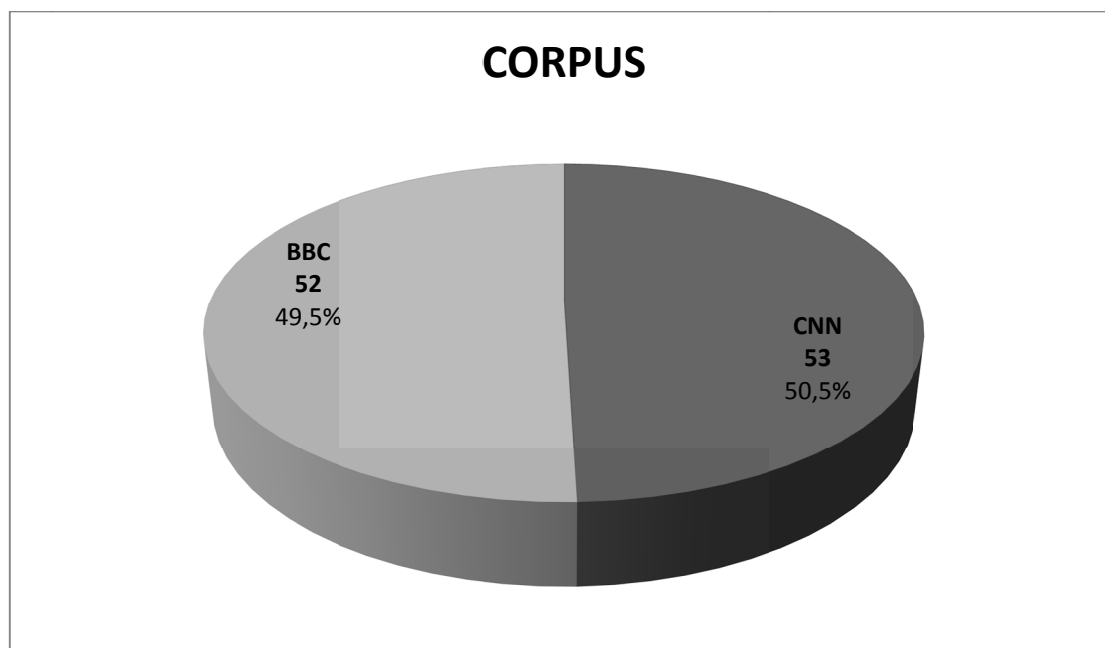
Πίνακας 2^B. *CNN-Corpus: Το Σώμα των κειμένων που συλλέχθηκαν*

A	HMEP/NIA	TITΛΟΣ	ΛΕΞΕΙΣ
1	11/10/2011	Virus infects program that controls U.S. drones	822
2	6/10/2011	Arab Spring galvanizers, WikiLeaks among Nobel contenders	966
3	3/10/2011	The Pentagon's cyberstrategy, one year later	1.709
4	15/8/2011	Cybertheft could destroy the U.S. economy	1.940
5	15/8/2011	'Mafiaboy' breaks silence, paints 'portrait of a hacker'	1.085
6	15/7/2011	Pentagon makes love, not cyber war	765
7	23/6/2011	Cyberwarfare finds a captive audience	829
8	18/1/2011	U.S. strategy on Iran is working	920
9	16/12/2010	The Sweep: WikiLeaks stirs anarchy online	1.961
10	10/12/2010	Why WikiLeaks hackers are a glitch, not a cyberwar	1.003
11	9/12/2010	Is WikiLeaks engaged in 'cyber war'?	1.158
12	3/10/2010	Iran arrests 'nuclear spies,' intelligence chief says	338
13	29/9/2010	Iran denies cyberattack hurt nuclear program -- but expert isn't sure	640
14	7/7/2010	Threat of 'cyberwar' has been hugely hyped	905
15	19/3/2010	Political hot topics (...)	80
16	28/9/2009	CNN Student News Transcript [<i>Face book</i>]	31
17	21/9/2009	Facebook gets caught in Golan Heights dispute	489
18	7/8/2009	Rus.-Geor. tensions still high one year on from conflict	354
19	8/7/2009	U.S. government sites among those hit by	818

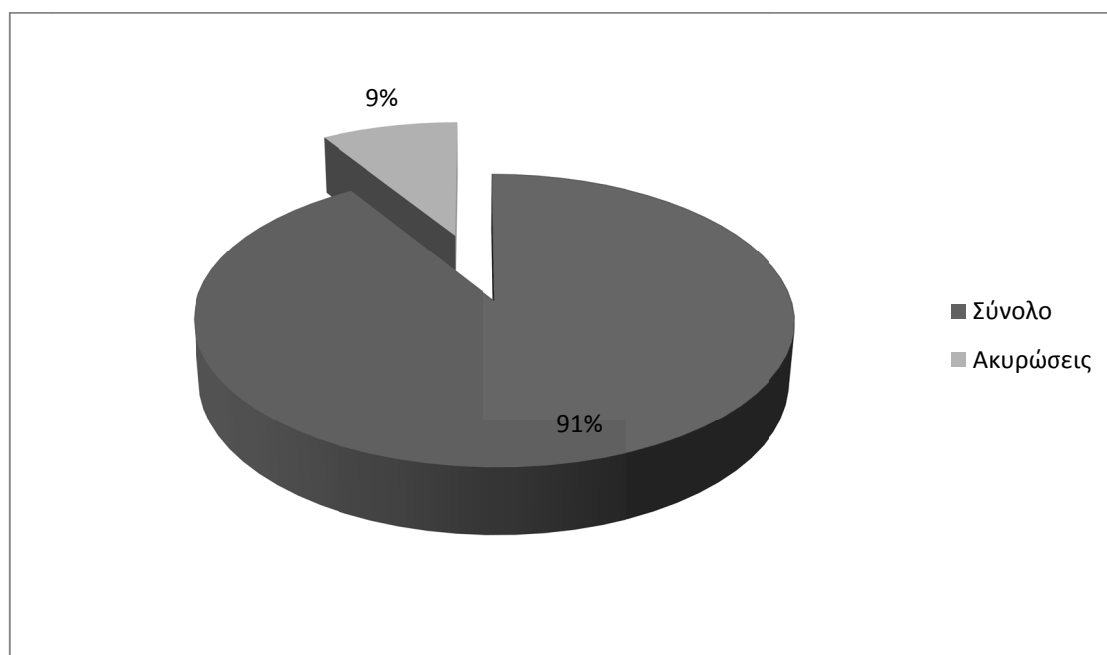
		cyberattack	
20	17/6/2009	Briton's software a surprise weapon in Iran cyberwar	420
21	21/8/2008	Experts: Internet filtering and censorship rife	902
22	18/8/2008	U.S. at risk of cyberattacks, experts say	1.070
23	4/3/2008	China denies U.S. computer hacking agenda	696
24	3/3/2008	<i>Report:</i> China trying to crack U.S. computers, buy nukes	577
25	26/9/2007	Sources: Staged cyber attack	952
26	24/8/2007	Anarchy on-line	1.414
27	29/5/2007	Cyber-spies tracking terror on Web	822
28	29/5/2007	Is it time to crack down on the blogosphere?	1.720
29	12/4/2007	Security crucial as intruders grow sophisticated	625
30	1/12/2006	Advisory on al Qaeda cyber threat issued out of caution	159
31	24/10/2006	Ronald Sugar, Chairman and CEO, Northrop Grumman	775
32	3/10/2006	Social networking fuels new Web boom	581
0	29/9/2006	Cyber-spies tracking terror on Web	-
33	13/10/2005	A convicted hacker debunks some myths	1.841
34	16/2/2005	The Internet war	952
35	19/1/2005	Uncertain state of security	1.479
36	20/7/2004	Review: A fresh 'Angle' on the spy novel	518
37	20/3/2003	Are we vulnerable to cyber-attacks?	775
38	20/11/2002	Military intelligence system draws controversy	622
39	17/11/2002	Indonesians take protests to the net	405
40	12/4/2002	Hack attack, how you might be a target	824
41	11/11/2002	Indonesian cyberprotesters target Australia	299
42	4/2/2002	Rumsfeld: Cyberwar among possible threats	456

43	8/1/2002	Report: Cybervandalism jumped in 2001	416
44	17/7/2001	Decoy PCs give hackers a security lesson	759
45	11/5/2001	Analysis: U.S.-China 'cyberwar' fires blanks	1.174
46	10/5/2001	Epic cyberattack reveals cracks in U.S. defense	675
47	2/5/2001	U.S., Chinese hackers continue Web defacements	405
48	24/1/2001	Special Report: Crime on the Internet	298
49	24/1/2001	Could a cyberwar cripple the U.S.?	1.624
50	22/11/2000	U.S. Army kick-starts cyberwar machine	603
51	2/11/2000	Mideast fighting spills onto the Internet	493
52	3/11/1999	Derailing the vision of a truly digital government	347

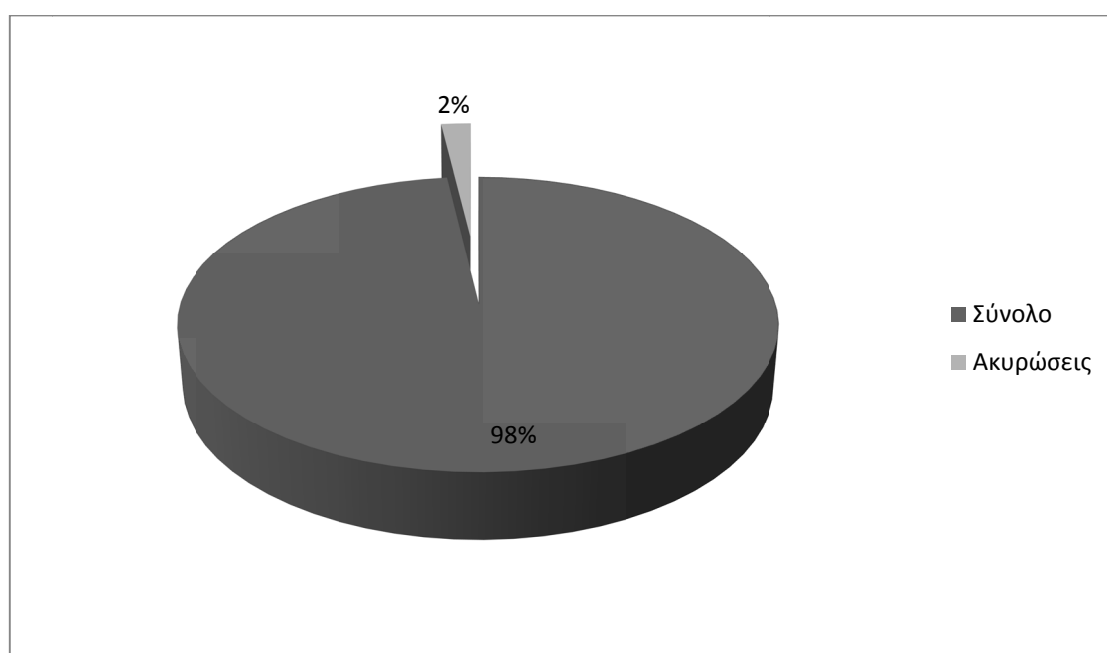
Σχήμα 1. Το μερίδιο των συλλεγόντων κειμένων από τα BBC & CNN

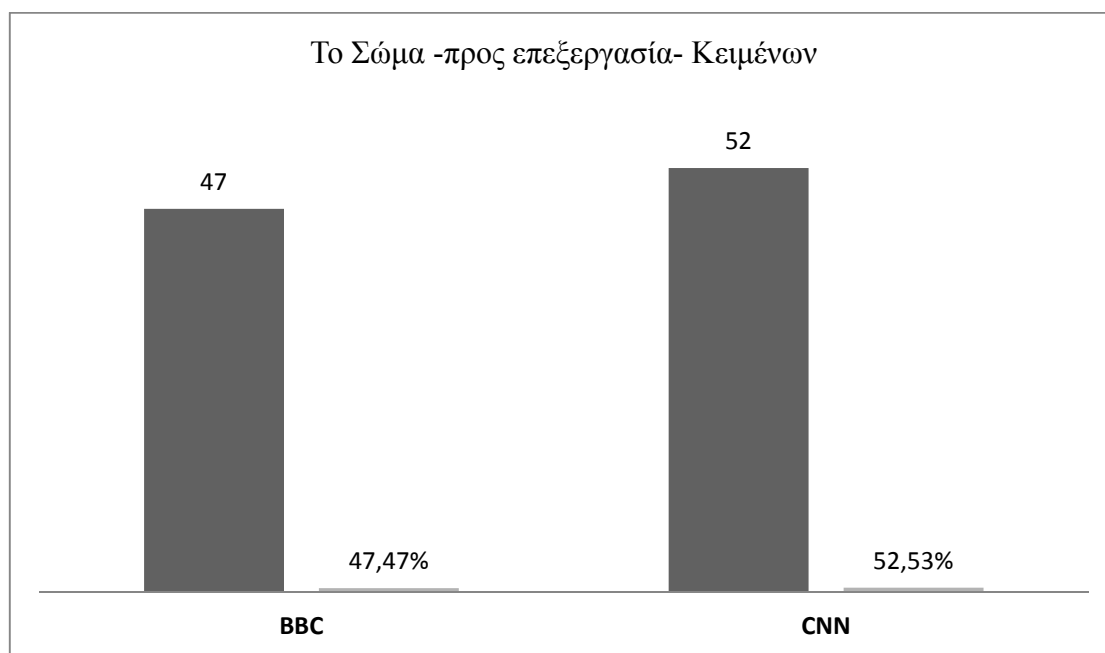


Σχήμα 2^A. Το μερίδιο των ακυρωθέντων κειμένων στο BBC



Σχήμα 2^B. Το μερίδιο των «ακυρωθέντων» κειμένων στο CNN



Σχήμα 3. Ο τελικός καταμερισμός των προς επεξεργασία κειμένων από τα BBC & CNN

Η ανάλυση των εξαιρουμένων κειμένων έχει όπως ακολούθως (Πίνακας 3). Εξαρχής θεωρήσαμε ακατάλληλα τα κείμενα με οπτικοακουστικό χαρακτήρα. Δηλαδή, είτε τηλεοπτικών εκπομπών (βίντεο κλπ), είτε ραδιοφωνικών μεταδόσεων. Στην προκείμενη περίπτωση η έρευνα θα διευρυνόταν με ανομοιογένεια. Όπως φαίνεται και στα στοιχεία τα οποία παραθέτουμε, το ποσοστό των εν λόγω ευρημάτων είναι ιδιαίτερα μικρό. Θα έπρεπε λοιπόν να αναζητήσουμε άλλα Μέσα, τα οποία να παρέχουν ικανοποιητικό δείγμα κειμένων με οπτικοακουστικό χαρακτήρα. Τα παραπάνω ισχύουν σχετικά με το BBC. Αξιοσημείωτη είναι ωστόσο, μια διαφορετική περίπτωση στο CNN. Εκεί εντοπίστηκε το ίδιο άρθρο (το ίδιο ακριβώς κείμενο), στις 29/9/2006 και 29/5/2007. Βεβαίως, καταμετρήθηκε μόνο μια φορά.

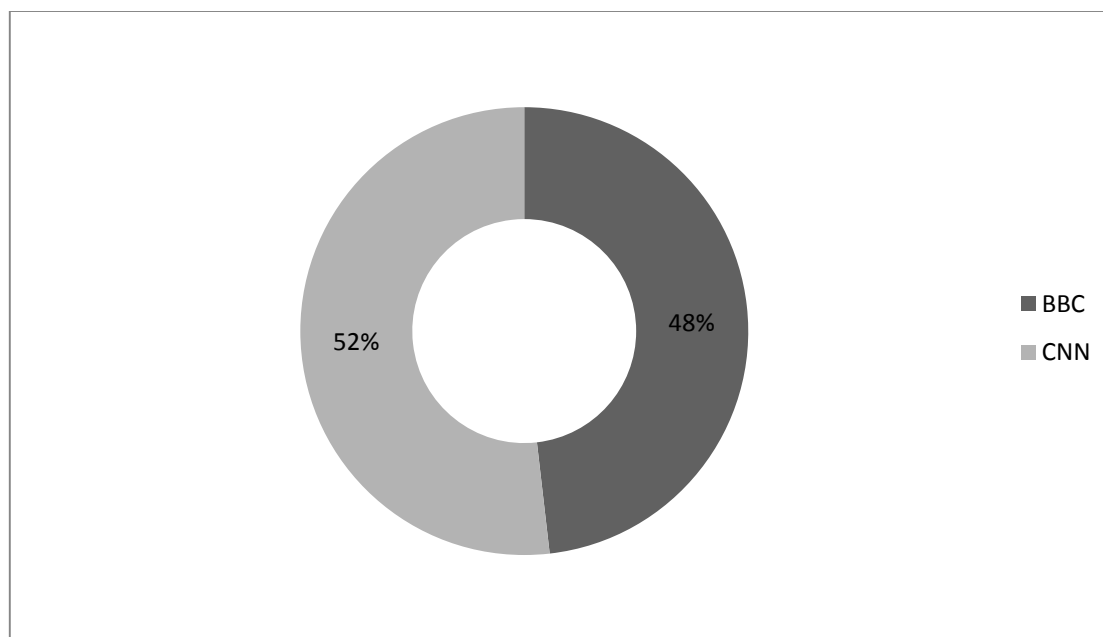
Πίνακας 3. Λεπτομέρειες Ακυρώσεων

A	ΜΕΣΟ	ΗΜΕΡ/ΝΙΑ	ΤΙΤΛΟΣ	ΑΙΤΙΑ	ΔΙΑΡΚΕΙΑ
1	BBC	2/6/2011	Cyber war's 'death and destruction'	<i>RADIO</i>	07:19
2	BBC	4/2/2011	Calls for 'rules of engagement' for cyber conflict	<i>VIDEO</i>	10:05
3	BBC	3/2/2011	US cyber warfare expert on threats	<i>VIDEO</i>	00:52

			which exist now		
4	BBC	10/12/2010	The conflict between Wikileaks supporters and the companies	VIDEO	02:41
5	BBC	22/6/2009	West 'seeks Iran disintegration'	VIDEO	02:10
6	CNN	29/9/2006	Cyber-spies tracking terror on Web	"Re-peat..."	-

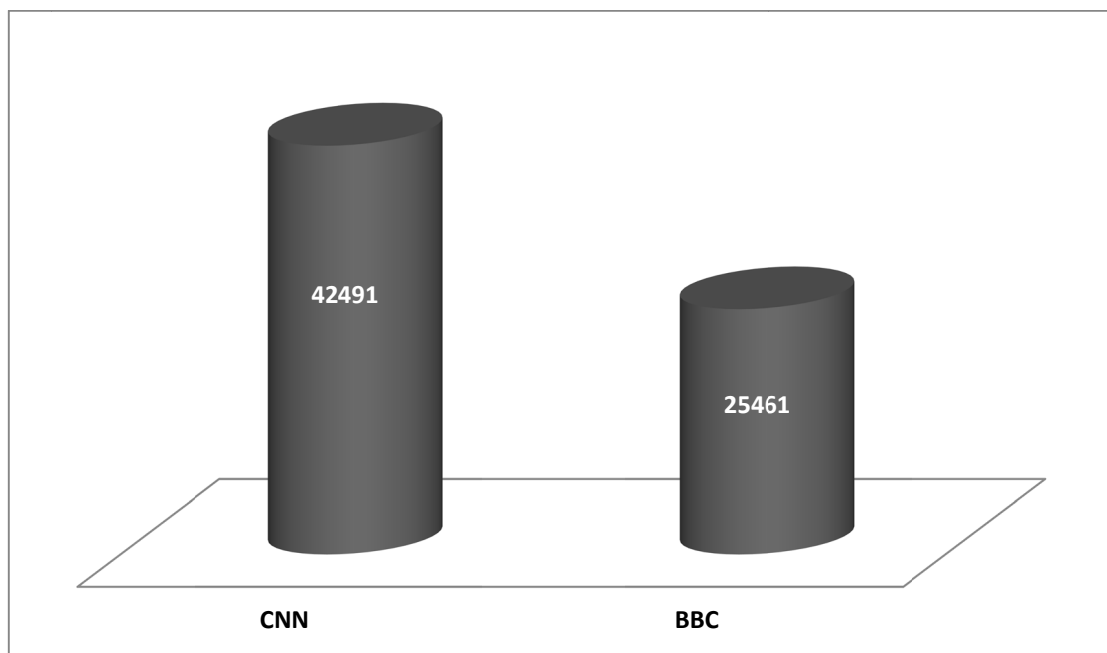
Ένα άλλο σημαντικό στοιχείο της ταυτότητας της έρευνας, αναφερόμαστε στην έκταση των ευρημάτων, όσον αφορά τις σελίδες που χρειάστηκαν για την αντιγραφή των κειμένων και το σύνολο των λέξεων που συνθέτουν αυτά τα κείμενα. Έτσι, οι σελίδες ανέρχονται σε σύνολο 193 (Σχήμα 4). Από αυτές οι 93 (48,2%) αφορούν στο BBC και οι 100 (51,8%) στο CNN. Τέλος, οι λέξεις -δίχως να συμπεριληφθεί οτιδήποτε σχετικό με τις εξαιρέσεις- φθάνουν σε σύνολο τις 67.952²⁷ (Σχήμα 5). Από αυτές οι 25.461 (63%) αφορούν στο BBC και οι 42.491 (37%) στο CNN.

Σχήμα 4. Η συνολική έκταση σε σελίδες στα δύο ειδησεογραφικά πρακτορεία



²⁷ Η τέλεια προσέγγιση είναι ασφαλώς δύσκολη, αν επιθυμούμε να αφαιρέσουμε τις διπλές αναφορές ή τις χρήσιμες, κατά το σταθμό, παραπομπές και σημειώσεις. Εφόσον, όμως, εκτιμάμε ότι η συγκεκριμένη μέτρηση αποσκοπεί σε μια ένδειξη των μεγεθών και άρα είναι δευτερεύουσας σημασίας, κρίνουμε ότι είναι χρήσιμο να το παραθέσουμε.

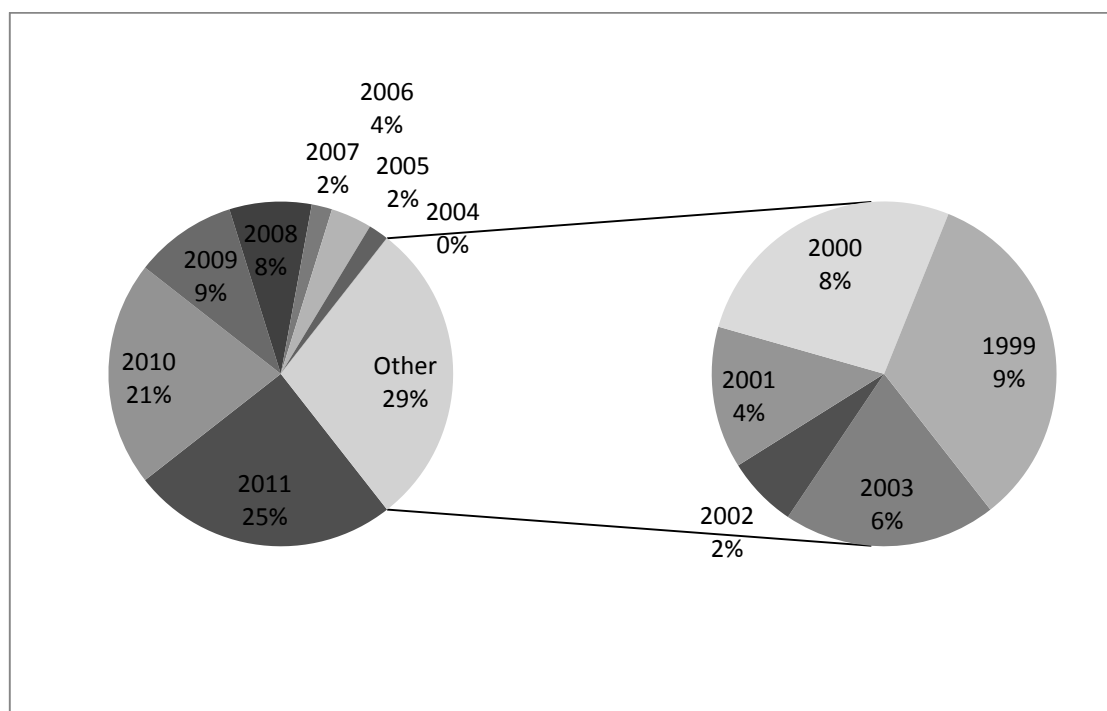
Σχήμα 5. Η συνολική έκταση σε αριθμό λέξεων στα δύο ειδησεογραφικά πρακτορεία



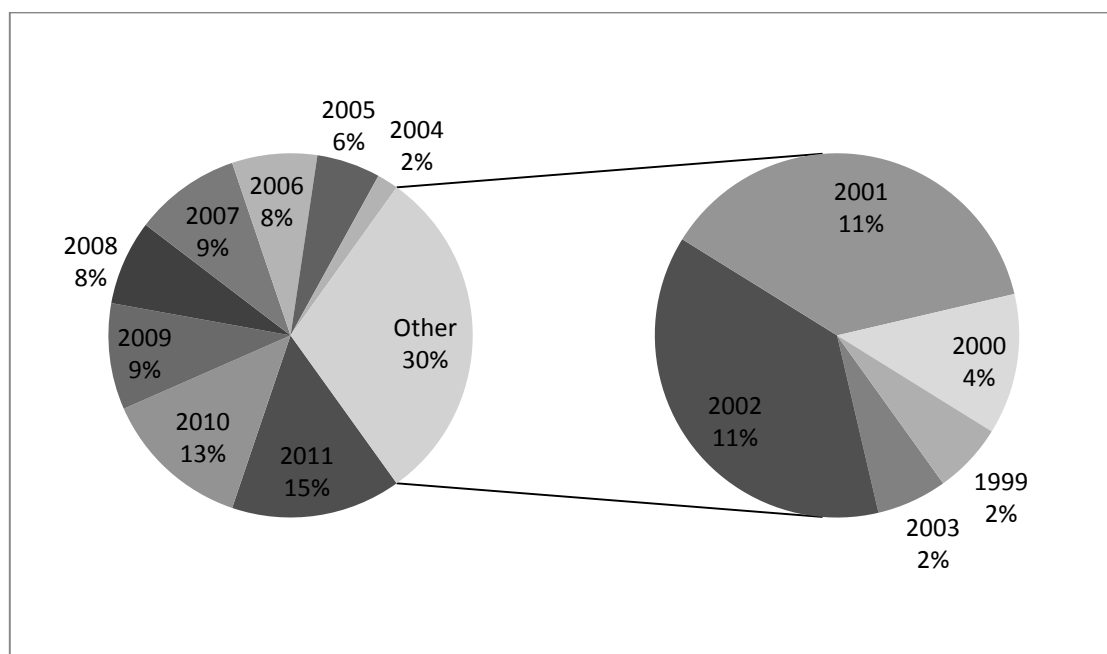
Ολοκληρώνοντας την παρουσίαση, κάτι το οποίο θα πρέπει να αναφερθεί, είναι η χρονική οριοθέτηση της έρευνας. Το σώμα λοιπόν της έρευνάς μας πρόεκυψε από κείμενα τα οποία είναι διαθέσιμα (μέχρι τουλάχιστο και την ημέρα της συγγραφής, ήτοι την 1/11/2011) στις θέσεις των δύο σταθμών στον παγκόσμιο ιστό και αναφέρονται στην περίοδο από 1/2/1999 ως και 11/10/2011.

Για την κατανόηση της κατανομής των ευρημάτων ανά έτη, θεωρήσαμε χρήσιμη την διάκριση στο χρονικό φάσμα της απεικόνισης, σε νεότερο και παλαιότερο κομμάτι. Θεωρούμε πως με αυτόν τον τρόπο φαίνεται, καθώς από το παρελθόν πλησιάζουμε το παρόν, η τάση **πυκνότερης δημοσιοποίησης των γεγονότων** που άπτονται του κυβερνοπολεμικού φαινομένου από τα ψηφιακά μέσα (Σχήμα 6). Κάτι που το πιθανότερο συμβαίνει εξαιτίας της αύξησης του ενδιαφέροντος για αυτό το θέμα.

Σχήμα 6^A. Η πυκνότητα των γεγονότων στο χρονικό φάσμα, για το BBC



Σχήμα 6^B. Το σύνολο των ετήσιων αναφορών στο CNN



3.3 Οι Θεματικές Κατηγορίες

Η συλλογή του υλικού έγινε για όλο το χρονικό διάστημα που είναι διαθέσιμο στην ιστοσελίδα και δη 12,5 περίπου έτη (1/2/1999 - 11/10/2011). Κατόπιν της επεξεργασίας των τεκμηρίων (Corpus), σύμφωνα με τη μέθοδο της Ανάλυσης Περιεχομένου, προέκυψαν 315 ευρήματα – μονάδες αναφοράς (Items). Αυτές, μετά τη χρήση του *ψυχοκοινωνικού κριτηρίου*, είναι δυνατό να ταξινομηθούν σε τέσσερις θεματικές κατηγορίες, τις οποίες τιτλοφορήσαμε ως εξής (Πίνακας 4):

- *Διείσδυση* (Penetration)
- *Υποδομές* (Infrastructures)
- *Λογοκρισία* (Censorship)
- *Προπαγάνδα* (Propaganda)

Η πρώτη θεματική κατηγορία (*Διείσδυση*), περικλείει όλα εκείνα τα γεγονότα, τα οποία έχουν κοινό παρανομαστή, (α) την μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα. Επίσης, συζευκτικά, (β) τους ενδιαφέρει η εκμετάλλευση των ξένων πληροφοριών για την εξυπηρέτηση των δικών τους συμφερόντων, τα οποία δεν συνάδουν με τη δημοσιοποίηση των δραστηριοτήτων τους. Το συμπέρασμα, λοιπόν, το οποίο συνάγουμε για τη θεματική κατηγορία της Διείσδυσης είναι:

- από το (α) ότι πρόκειται για τεχνολογικής έντασης και
- από το (β) κλειστής κοινωνικά.

Η δεύτερη θεματική κατηγορία (*Υποδομές*), περικλείει όλα εκείνα τα γεγονότα, τα οποία έχουν κοινό παρανομαστή, (α) την πρόκληση δυσλειτουργίας σε κρίσιμα πληροφοριακά συστήματα. Επίσης, συζευκτικά, (β) τους ενδιαφέρει το αποτέλεσμα του χτυπήματος να γίνει έντονα αισθητό στην κοινωνία που ανήκει και, ενδεχομένως, ευρύτερα. Το συμπέρασμα, λοιπόν, το οποίο συνάγουμε για τη θεματική κατηγορία των Υποδομών είναι:

- από το (α) ότι πρόκειται για τεχνολογικής έντασης και
- από το (β) ανοιχτής κοινωνικά.

Η τρίτη θεματική κατηγορία (*Λογοκρισία ή Κυβερνολογοκρισία*), περικλείει όλα εκείνα τα γεγονότα, τα οποία έχουν κοινό παρανομαστή, (α) την κεντρική εκμετάλλευση της πρόσβασης ή μη, στα πληροφοριακά συστήματα ενός κράτους.

Επίσης, συζευκτικά, (β) την ανάληψη της παραπάνω πρωτοβουλίας μόνο από φορείς της εξουσίας του εν λόγω κράτους και όχι από οποιονδήποτε άλλον απλό πολίτη του. Το συμπέρασμα, λοιπόν, που συνάγουμε για τη θεματική κατηγορία της Κυβερνο-λογοκρισίας είναι:

- από το (α) ότι πρόκειται για ανθρώπινης έντασης και
- από το (β) κλειστής κοινωνικά.

Η τέταρτη θεματική κατηγορία (*Προπαγάνδα ή Κυβερνοπροπαγάνδας*), περικλείει όλα εκείνα τα γεγονότα, τα οποία έχουν κοινό παρανομαστή, (α) την αποκεντρωμένη εκμετάλλευση της πρόσβασης ή μη, στα πληροφοριακά συστήματα ενός κράτους. Επίσης, συζευκτικά, (β) τη χρησιμοποίηση αυτής της μη εξουσιοδοτημένης πρόσβασης για την κοινωνικής επιρροή των πολιτών. Το συμπέρασμα, λοιπόν, που συνάγουμε για τη θεματική κατηγορία της Κυβερνο-προπαγάνδας είναι:

- από το (α) ότι πρόκειται για ανθρώπινης έντασης και
- από το (β) ανοιχτής κοινωνικά.

Πίνακας 4: Συσχέτιση Θεματικών Κατηγοριών & Κριτηρίου

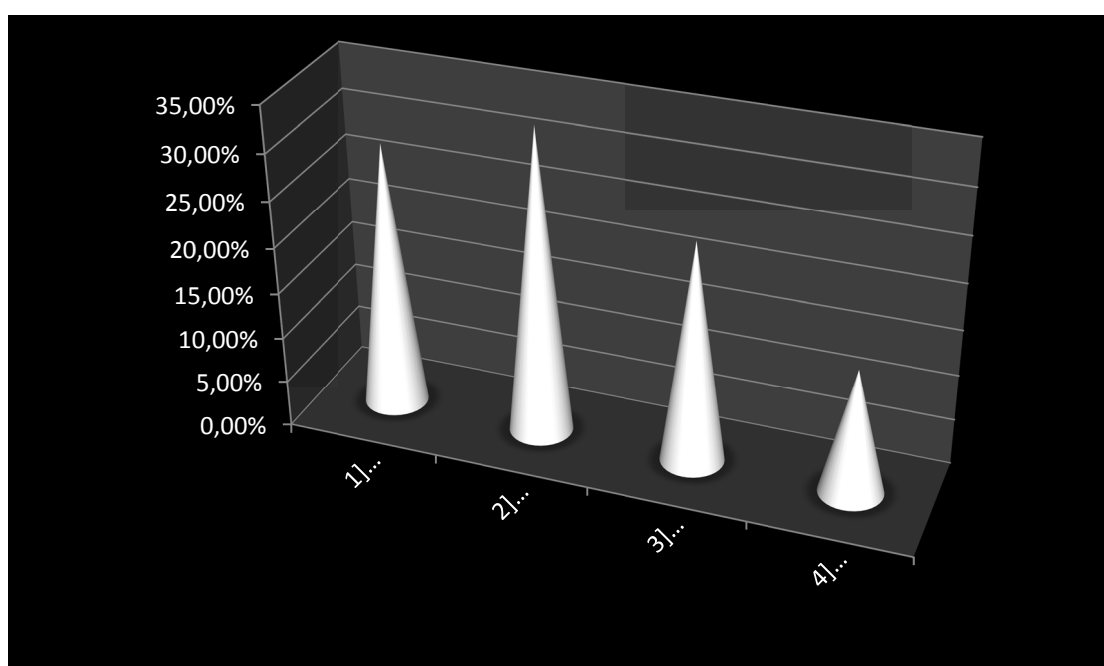
ΚΑΤΗΓΟΡΙΑ	ΕΝΤΑΣΗ	ΚΟΙΝΩΝΙΚΑ...
Διείσδυση	Τεχνολογική	Κλειστή
Υποδομές	Τεχνολογική	Ανοιχτή
Κυβερνο-λογοκρισία	Ανθρώπινη	Κλειστή
Κυβερνο-προπαγάνδα	Ανθρώπινη	Ανοιχτή

Μετά την επεξεργασία των παραπάνω κειμένων, ώστε να ταξινομηθούν οι εντοπισμένες αναφορές στις τέσσερις θεματικές κατηγορίες, με το κριτήριο που θέσαμε, προέκυψαν τα κάτωθι τελικά αποτελέσματα (Πίνακας 5 & Σχήμα 7).

Πίνακας 5: Συμμετοχή Εκάστης Θεματικής Κατηγορίας

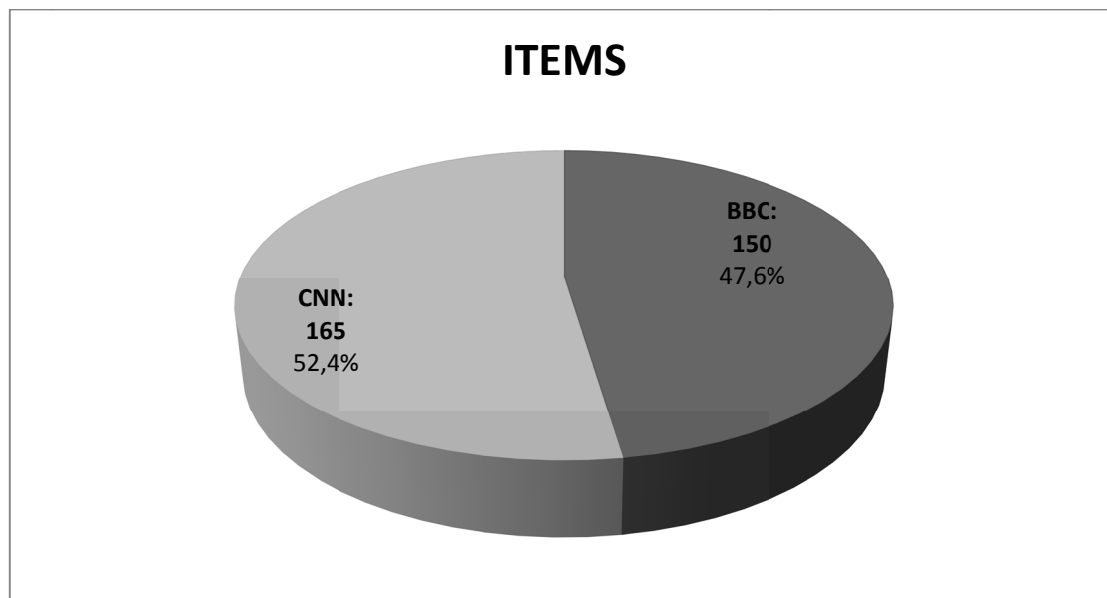
	ΚΑΤΗΓΟΡΙΑ	CATEGORY	ΜΟΝΑΔΕΣ	ΠΟΣΟΣΤΟ
1	<i>Υποδομές</i>	(Infrastructures)	105	33,3%
2	<i>Διείσδυση</i>	(Penetration)	91	28,9%
3	<i>Κυβερνο-προπαγάνδα</i>	(Cyber-propaganda)	76	24,1%
4	<i>Κυβερνο-λογοκρισία</i>	(Cyber-Censorship)	43	13,7%
	<u>ΣΥΝΟΛΟ</u>	<u>(TOTAL)</u>	<u>315</u>	<u>100%</u>

Σχήμα 7. Η απεικόνιση των συγκεντρωτικών αποτελεσμάτων



Έτσι, οι παραπάνω μονάδες αναφοράς (items) οριστικοποιούνται στις **315**. Από αυτές, οι 150 προέρχονται από το BBC και οι 165 από το CNN (Σχήμα 8).

Σχήμα 8. Οι συνολικές αναφορές στα δύο ειδησεογραφικά πρακτορεία



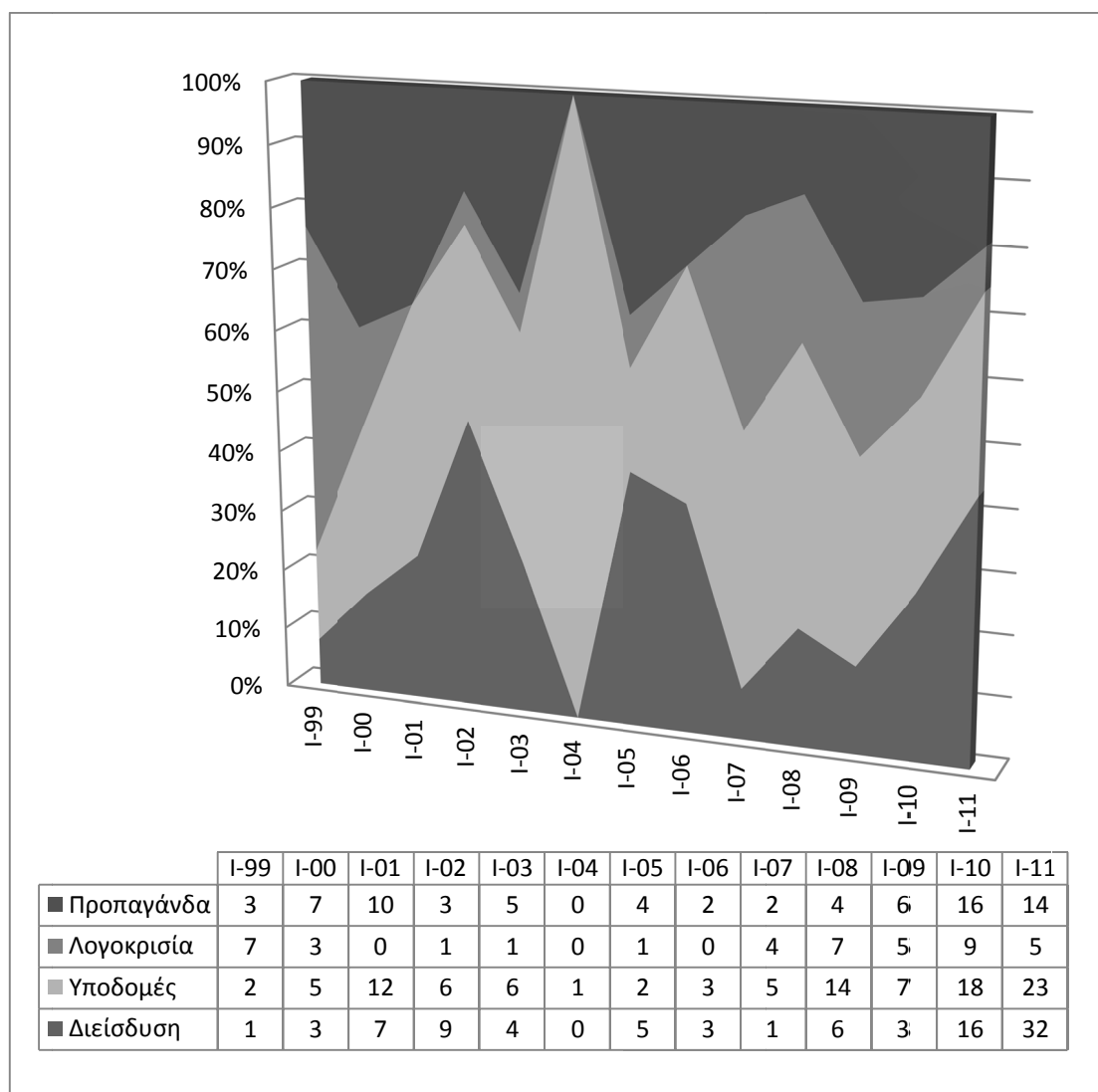
Συνεχίζοντας σε μια ακόμα πιο αναλυτική αποτύπωση των αποτελεσμάτων, μπορούμε να παρατηρήσουμε στον ακόλουθο πίνακα την πορεία των ευρεθέντων μονάδων αναφοράς, συσχετίζοντας τις παραμέτρους του έτους και των μέσων, για κάθε Θεματική Κατηγορία χωριστά. Επιπλέον, έχουμε τη δυνατότητα να συγκρίνουμε τα υποσύνολα ανά μέσο, σε κάθε Θεματική Κατηγορία. Και, επίσης, τα σύνολα διακρίνοντάς τα, ανά έτος και Θεματική Κατηγορία. Το τελευταίο σύνολο παρατίθεται και σε συνολικό ποσοστό (Πίνακας 6). Τέλος, απεικονίζεται διαγραμματικά και η διακύμανση της συμμετοχής των μονάδων αναφοράς σε κάθε έτος και για κάθε μία Θεματική Κατηγορία (Σχήμα 9).

Πίνακας 6. Αποτελέσματα κατανεμημένα ανά Έτος, κατά Θεματική Κατηγορία και Μέσο

ΕΤΟΣ	ΔΙΕΙΣΔΥΣΗ		ΥΠΟΔΟΜΕΣ		ΛΟΓΟΚΡΙΣΙΑ		ΠΡΟΠΑΓΑΝΔΑ		ΑΝΑ ΕΤΟΣ
	BBC	CNN	BBC	CNN	BBC	CNN	BBC	CNN	
2011	13	19	11	12	5	0	9	5	74
2010	6	10	14	4	5	4	6	10	59
2009	3	0	6	1	2	3	3	3	21
2008	3	3	7	7	1	6	2	2	31

2007	0	1	2	3	0	4	0	2	12
2006	2	1	2	1	0	0	1	1	08
2005	0	5	0	2	0	1	2	2	12
2004	-	0	-	1	-	0	-	0	01
2003	3	1	4	2	1	0	4	1	16
2002	0	9	2	4	0	1	0	3	19
2001	1	6	2	10	0	0	5	5	29
2000	0	3	4	1	2	1	4	3	18
1999	1	0	1	1	7	0	3	0	13
Υπο- σύνολα	32	58	55	49	23	20	39	37	313
Σύνολα	90		104		43		76		
Ποσοστό	28,75%		33,23%		13,74%		24,28%		100

Σχήμα 9. Διακύμανση των μονάδων αναφοράς, ανά έτος και Θεματική Κατηγορία



ΤΜΗΜΑ ΙΙ
Η ΠΡΑΞΗ
(ΤΙ ΕΝΝΟΟΥΝ «ΚΥΒΕΡΝΟΠΟΛΕΜΟ» ΤΑ ΜΕΣΑ)

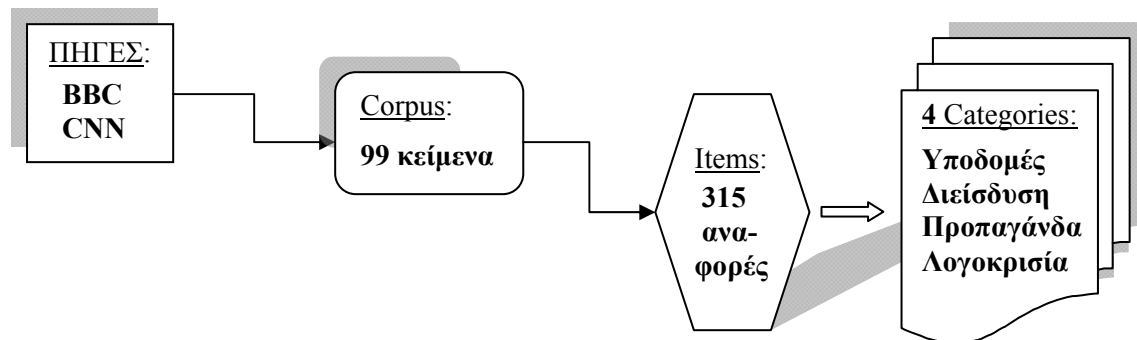
4. ΑΝΑΛΥΣΗ

4.1 Το Αντικείμενο και η Δομή της Ανάλυσης

Στα προηγούμενα κεφάλαια ακολουθήσαμε σε διαδοχικά στάδια την ακόλουθη μεθοδολογία στην έρευνά μας (Σχήμα 10):

- (α) επιλέξαμε τις δύο πηγές μας. Sources: BBC & CNN, από αυτές
- (β) συλλέξαμε τα δεδομένων μας. Corpus: 99 κείμενα, από αυτά
- (γ) επεξεργαστήκαμε τις πληροφορίες μας. Items: 315 αναφορές, από αυτές
- (δ) διεξαγάγαμε τη νέα μας γνώση. Categories: 4 θεματικές, τις οποίες τώρα και
- (ε) θα αναλύσουμε ποιοτικά, ποσοτικά και περιπτωσιολογικά.

Σχήμα 10. Η Μεθοδολογία της Έρευνας μας



Το αποτέλεσμα, λοιπόν, είναι ότι αυτές οι τέσσερις θεματικές κατηγορίες περιλαμβάνουν όλα τα νοήματα, τα οποία έχουμε εντοπίσει από το σώμα των τεκμηρίων μας (με άλλα λόγια το σύνολο των κειμένων που συλλέξαμε). Άρα, πληρείται η προϋπόθεση του *εξαντλητικού* γνωρίσματος των κατηγοριών, την οποία απαιτεί η μέθοδός μας.

Επίσης, όπως θα αποδείξουμε στο ποιοτικό μέρος της ανάλυσής μας παρακάτω, κάθε θεματική κατηγορία είναι νοηματικά μοναδική, σε σύγκριση με τις υπόλοιπες, δίχως να παρατηρούνται επικαλύψεις της μίας με την άλλη. Άρα, πληρείται η προϋπόθεση του *αποκλειστικού* γνωρίσματος των κατηγοριών, την οποία απαιτεί η μέθοδός μας.

Επιπροσθέτως, όπως θα δείξουμε στο ποσοτικό μέρος της ανάλυσής μας, κάθε θεματική κατηγορία συμμετέχει με τον δικό της τρόπο στην ολική κατανομή. Αυτή η συνθήκη ήταν το καλύτερο δυνατό επιχείρημα για την κάλυψη του όρου ύπαρξης του *συγκεκριμένου* γνωρίσματος των κατηγοριών, την οποία απαιτεί η μέθοδός μας.

Τέλος, στην περιπτωσιολογική ανάλυση των θεματικών κατηγοριών, θα φανεί η εκπλήρωση της προϋπόθεσης του γνωρίσματος του *κατάλληλου* των κατηγοριών, την οποία απαιτεί η μέθοδός μας. Αλλιώς, στην επάρκεια του «εννοιολογικού ταιριάσματος», το οποίο θα προκύπτει από τη μελέτη κάθε περίπτωσης με το περιεχόμενο κάθε θεματικής κατηγορίας.

Η τεκμηρίωση των τεσσάρων παραπάνω όρων αποτελεί το αντικείμενο της ανάλυσης. Η ικανοποίηση από την επάρκεια αυτής της τεκμηρίωσης θα αποτελεί και την απάντηση στη διάψευση ή επαλήθευση της δεύτερης υπόθεσης της εργασίας. Σε αυτήν είχαμε θέσει το ερευνητικό ερώτημα:

αν θέσουμε ένα ψυχοκοινωνικό κριτήριο -με το περιεχόμενο που ακριβώς του προσδώσαμε-, θα έχει κάποιο χρήσιμο νόημα η ταξινόμηση που θα προκύψει για τα γεγονότα, για τα οποία εκφράστηκε πως συνιστούν πράξη κυβερνοπολέμου;

Σύμφωνα, όμως, με τη Μέθοδο της Ανάλυσης Περιεχομένου, η θετική απάντηση σε αυτό το ερώτημα προϋποθέτει ότι οι θεματικές κατηγορίες, οι οποίες θα προκύψουν από την εν λόγω ταξινόμηση, θα πρέπει να είναι κατάλληλες, αποκλειστικές, συγκεκριμένες και εξαντλητικές. Οπότε, βάσει των παραπάνω, συμπεραίνουμε ότι η απάντηση στη δεύτερη υπόθεση εργασίας μας είναι καταφατική.

Όσον αφορά τη δομή της ανάλυσής μας, αυτή θα ακολουθήσει το εξής μοντέλο:

- i] *Ποιοτικός Προσδιορισμός*. Στο πρώτο υποκεφάλαιο ξεκινάμε με την αποσαφήνιση της αναγκαίας ορολογίας, ώστε να γίνεται κατανοητή η έννοια που προδίδουμε σε κάθε θεματική κατηγορία. Πέρα, όμως, αυτών των απαραίτητων οριοθετήσεων, και πάντα στα πλαίσια της ορθότερης κατανόησης εκάστης θεματικής, παραθέτουμε ορισμένες χρήσιμες πληροφορίες για την κάθε κατηγορία.
- ii] *Ποσοτικός Προσδιορισμός*. Σε αυτό το υποκεφάλαιο παρουσιάζεται το σύνολο και το αντίστοιχο ποσοστό (μερίδιο) επί του ολικού μεγέθους των ευρεθέντων αναφορών. Αυτό γίνεται, τόσο συγκεντρωτικά, όσο και αναλυτικά για τα δύο μέσα που αποτελούν τις πηγές μας. Επίσης, όλα τα παραπάνω απεικονίζονται σε σχεδιαγράμματα. Τέλος, ολοκληρώνουμε με ορισμένες συγκριτικές παρατηρήσεις.
- iii] *Ανάλογα Κυβερνο-επεισόδια*. Στο τελευταίο υποκεφάλαιο μελετάμε τις πιο «αντιπροσωπευτικές» περιπτώσεις. Εδώ προσπαθούμε να δείξουμε, μέσα από μια ιστορική αναδρομή, τον τρόπο που πραγματοποιείται κάθε θεματική κατηγορία, ώστε να δούμε αν έτσι τεκμηριώνεται η ένταξή της στη θεματική κατηγορία.

4.2 Υποδομές

4.2.1 Ποιοτικός Προσδιορισμός

Η κατάσταση των υφισταμένων, καθώς και των υπό κατασκευή υποδομών ενός κράτους καταδεικνύουν ένα τρόπο με τον οποίο μπορούμε να καταλάβουμε πώς, οι ηγεσίες του κράτους, ιεραρχούν διαχρονικά την κάλυψη των αναγκών του. Έτσι, διακρίνουμε ότι η κάθε υποδομή έχει το δικό της ρόλο στην υποστήριξη και υλοποίηση των τομέων στους οποίους στηρίζεται η οργάνωση κάθε κράτους. Κατά αυτόν τον τρόπο, ενδεικτικά, έχουμε τα οδικά μεταφορικά δίκτυα στην οικονομία, τις αναγκαίες κτηριακές εγκαταστάσεις στο στρατό, τις ενσύρματες συνδέσεις στις τηλεπικοινωνίες κοκ.

Ωστόσο, σε μια αυστηρότερη διατύπωση μπορούμε να ορίσουμε, γενικά, με τον όρο «υποδομές» (infrastructures) ένα πλέγμα αλληλοεξαρτώμενων δικτύων και συστημάτων που παρέχει αξιόπιστη ροή προϊόντων, υπηρεσιών και αγαθών, για τη λειτουργία της Δημόσιας Διοίκησης, της Οικονομίας και της Κοινωνίας. Ειδικότερα, «Κρίσιμη Υποδομή» (Critical Infrastructure) εννοούμε μια υποδομή μεγάλης κλίμακας, της οποίας τυχόν υποβάθμιση, διακοπή ή δυσλειτουργία έχει σοβαρή επίπτωση στην υγεία, ασφάλεια ή ευμάρεια των πολιτών. Επιπροσθέτως, «Πληροφοριακή και Επικοινωνιακή Υποδομή (ΠΕΥ)»: Υποδομή που αποσκοπεί στην παροχή πληροφοριών, υπηρεσιών επικοινωνίας ή άλλων ηλεκτρονικών υπηρεσιών και «Κρίσιμη ΠΕΥ» (Critical Information and Communication Infrastructure): Πληροφοριακό και επικοινωνιακό σύστημα που είναι κρίσιμη υποδομή ή αποτελεί προϋπόθεση για τη λειτουργία άλλων τέτοιων υποδομών (Γκρίτζαλης, 2008, 10).

Έτσι λοιπόν αυτή η πρώτη θεματική κατηγορία αναφέρεται σε στόχους, διαμέσου του κυβερνοχώρου, έναντι συγκεκριμένων κρίσιμων εθνικών ΠΕΥ. Εδώ πρέπει να τονίσουμε ότι, από τις περιπτώσεις που θα μελετήσουμε, συμπεραίνουμε ότι μιλάμε για ένα χτύπημα πολλαπλών στοχεύσεων, με απώτερο σκοπό την κατάρρευση ενός σημαντικού μέρους ενός πυλώνα (ισχύος) του κράτους είτε πολιτικού, είτε στρατιωτικού, είτε και συνδυασμού τους. Για παράδειγμα μπορούμε να αναφέρουμε δίκτυα τα οποία ελέγχουν σε μια χώρα την ομαλή ροή ύδατος, ενέργειας ή του στρατιωτικού συστήματος Διοίκησης, Ελέγχου, Επικοινωνιών,

Υπολογιστών, Πληροφοριών, Επιτήρησης και Αναγνώρισης (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance²⁸).

Σε κάθε υποδομή ενός κράτος, η ευρύτερη προστιθέμενη αξία της προσμετράτε από το μέγεθος της καινοτομίας που διαθέτει, η οποία αποτελεί και το βασικό ζητούμενο. Στόχος είναι η εφαρμογή της να είναι δυνατόν να ελαττώσει το κόστος λειτουργίας και να αυξήσει την απόδοση στο παρεχόμενο έργο εκάστης υποδομής. Η εφεύρεση των H/Y και κατά επέκταση η χρησιμοποίησή τους σε κάθε υποδομή χωριστά, έφερε επανάσταση στο αποτέλεσμα της σχέσης των παραμέτρων του κόστους και της απόδοσης. Ωστόσο το εν λόγω όφελος μεγιστοποιήθηκε από τη διεύρυνση των ευκαιριών που προκλήθηκαν, όταν τα επιστημονικά επιτεύγματα κατέστησαν δυνατή τη σύνδεση των H/Y σε επίπεδο εσωτερικό (intranet) και εξωτερικό (internet) των υποδομών των κρατών. Στα αρχικά χαρακτηριστικά της εμφάνισης του διαδικτύου συγκαταλέγεται και η προσφορά, για πρώτη φορά, της δυνατότητας μιας ολικής και οριζόντιας επικοινωνίας, όπως αυτή χαρακτηρίστηκε (Καϊτατζή, 2003). Αυτοί οι χαρακτηρισμοί υποδηλώνουν κυρίως την γεωγραφική ευρύτητα και τη διαπροσωπική αμεσότητα στην αλληλεπίδραση των επικοινωνούντων. Σε αυτήν την κατεύθυνση θεωρήθηκε ότι η διάθεση αυτού του μέσου επικοινωνίας υπερβαίνει το χώρο και το χρόνο (Castells, 2001/2005).

Αυτά ακριβώς τα γνωρίσματα κάνουν φανερό γιατί μια επίθεση σε συγκεκριμένο διαδικτυακό κόμβο συνιστά διαφορετικό τύπο από μία αντίστοιχη -και κατ' ανάγκη περιορισμένη- σε μεμονωμένους H/Y. Όπως δήλωσε στις Βρυξέλες (19/1/2011)²⁹, στα πλαίσια σύσκεψης του NATO, σχετικά με τις νέες μορφές κυβερνο-απειλών, ο τότε αναπληρωτής υπουργός άμυνας των ΗΠΑ William Lynn «πλέον, διακρίνεται μια “ωρίμανση” από τα εργαλεία διάρρηξης και κατασκοπείας (στα τερματικά) σε αυτά της καταστροφής των ζωτικών υποδομών». Ασφαλώς, ένας H/Y είναι δυνατόν να έχει στη μνήμη του ιδιαιτέρως σημαντικά στοιχεία. Εντούτοις, η μοναδικότητα και διαφορετικότητα αυτής της θεματικής κατηγορίας έγκειται στο ότι ένας ή πολλοί μεμονωμένοι H/Y δεν μπορούν να υποστηρίξουν τη λειτουργία μιας υποδομής. Κάτι που συμβαίνει με τη διασύνδεσή τους· και όταν αυτή ενοποιείται σε επίπεδο κράτους, αυτή η κατηγορία αποκτά τη δική της «υπόσταση».

Η επιχειρηματολογία περί της ύπαρξης ενός τέτοιου σαφούς τύπου απειλής ενισχύεται και από τα αποτελέσματα της ακόλουθης μελέτης. Μια από τις

²⁸ Πρόκειται για μια στρατολογία που περικλείει μια σειρά ενεργειών προσωπικού και τεχνολογίας.

²⁹ http://www.spacewar.com/reports/NATO_networks_vulnerable_to_cyber_threat_US_999.html

μεγαλύτερες και γνωστότερες εταιρείες ασφάλειας λογισμικού στον κόσμο, η McAfee, διεξήγαγε μια έρευνα σχετικά με την εξέλιξη των ειδών απειλής της ασφάλειας του διαδικτύου. Εκεί αναδείχθηκε ότι ένας στους τρεις ειδικούς περίπου αναφέρουν ότι έχει παρατηρηθεί αύξηση τέτοιων επιθέσεων σε μηνιαία συχνότητα. Ακόμη περισσότερο δε, δύο στους τρεις εκτιμούν ότι αυτές οι επιθέσεις επιδρούν καταλυτικά στη λειτουργία των υποδομών.

Αναφέραμε ήδη ότι σε μια χώρα δύναται να παρατηρήσουμε πολλές υποδομές και αυτές να ταξινομηθούν ως οικονομικές, στρατιωτικές κ.άλ. Στην οικονομία διακρίνουμε μεγάλη ένταση ιδιωτικής αυτονομίας. Έτσι, οι εταιρείες, είτε μεγάλες είτε μικρές, και ελλείπει επάρκειας στην κρατική προστασία, αναζητούν δικούς τους τρόπους κυβερνοάμυνας. Αντιθέτως, προς το παρόν, στο στρατό η ιδιωτική πρωτοβουλία διατηρείται σε χαμηλή ένταση, γενικότερα όμως με αυξητική τάση (Καραμπελιάς, 2009, 84). Για αυτόν το λόγο η εξέτασή μας θα εστιάσει στον τρόπο που αντιλαμβάνεται και αντιμετωπίζει ο στρατός το ζήτημα της απειλής των υποδομών από τις κυβερνοεπιθέσεις.

Αρχικά, στο στρατό άρχισαν να μιλούν για την απόκτηση ειδικού προσωπικού, το οποίο θα μπορούσε να εντοπίζει τυχών «μολυσματικά προγράμματα», τα οποία εισέβαλαν στα συστήματά τους (ιοί, λογικές βόμβες, Δούρειοι Ίπποι, κλπ.). Αυτά έχουν σκοπό την προσβολή του λογισμικού (software) των πληροφορικών συστημάτων. Αργότερα, έχουμε τα όπλα ηλεκτρομαγνητικού παλμού (EMP) και κατευθυνόμενης ενέργειας (DEW), τα οποία θέτουν στόχο την καταστροφή του υλικού μέρους (hardware) των Η/Υ (Rattray, 2001). Κατόπιν όμως, η εξειδίκευση άλλαξε κατεύθυνση και οδηγήθηκε στην εξειδικευμένη επιστημονική περιοχή της πληροφορικής που αποκαλούμε ασφάλεια δικτύων. Οι απαιτήσεις, με άλλα λόγια, προσαρμόστηκαν στις ανάγκες που ανέδειξε η επικράτηση του διαδικτύου.

Πιο συγκεκριμένα, οι ονοματοδοτήσεις της σχετικής στρατιωτικής ορολογίας, καθώς και των συναφών τμημάτων στο οργανόγραμμα των υπουργείων άρχισαν να περιέχουν τη λέξη - προσδιορισμό «δίκτυο ή δικτυακό». Στο λεξικό, επί παραδείγματι, του Υπουργείου Άμυνας των ΗΠΑ, το φάσμα επιχειρήσεων που καλύπτει ενέργειες με πληροφορικά όπλα, καλείται «Επιχειρήσεις Δικτύων Υπολογιστών (computer network operations - CNOs)». Αντίστοιχα συμβαίνει όταν πρόκειται για αμυντικές επιχειρήσεις (computer network attack - CNAs)³⁰. Το

³⁰ Joint Chiefs of Staff, Joint Publication 1-02 (2009): DoD Dictionary Of Military & Associated Terms

ευρύτερο πλαίσιο στο οποίο ανήκουν είναι ο «πληροφοριακός πόλεμος». Σε γενικές γραμμές, από την ίδια πηγή σε αυτόν εντάσσεται κάθε στρατιωτική επιχείρηση η οποία στοχεύει στο σφετερισμό της αντίπαλης διαδικασίας -ανθρώπινου ή αυτοματοποιημένου χειρισμού- είτε λήψης αποφάσεων είτε διαχείρισης πληροφοριών (προστάδιο της λήψης απόφασης). Τέλος, το σύστημα πληροφοριών προσδιορίζεται από το προσωπικό, την οργάνωση και τις υποδομές.

Οι επιτιθέμενοι στις υποδομές αναζητούν τις -πάντα υπάρχουσες- τρωτότητες των δικτύων (Watts, 2010). Ισχύει βεβαίως και εδώ ότι ο εντοπισμός των δραστών είναι αδύνατος. Το γεγονός αυτής της παραδοχής οδήγησε, αρχικά πολλούς μη κυβερνητικούς οργανισμούς, και μετέπειτα τα ίδια τα κράτη με επίσημες ανακοινώσεις να αποδεχτούν την αναγκαιότητα της συνεργασίας, ως απαραίτητη προϋπόθεση επίλυσης των διαφορών. Στην πρώτη περίπτωση μπορούμε να δούμε μια σειρά εκθέσεων της International Communication Union (ITU)³¹. Πιο συγκεκριμένα, σχετικά με την κυβερνοασφάλεια (Global Cybersecurity Agenda - GCA), τονίστηκε ιδιαίτερος η προϋπόθεση για την παγκόσμια συνεργασία, ώστε να αντιμετωπιστούν οι δυνητικές απειλές έναντι των ζωτικών υποδομών. Στη δεύτερη περίπτωση αρκεί να αναφέρουμε τα αποτελέσματα των συναντήσεων κορυφαίων στελεχών των ΗΠΑ και της ΕΕ³², οι οποίοι κατέληξαν το Νοέμβριο του 2010 σε συμφωνία συνεργατικής προάσπισης των ψηφιακών δικτύων (MEMO/10/597). Τα βασικότερα σημεία περιλαμβάνουν:

- Επέκταση της συνδιαχείρισης των επικινδύνων επεισοδίων στον κυβερνοχώρο, καθώς και τη συνδιοργάνωση ασκήσεων στο τέλος του 2011 (incident management).
- Διευρυμένη δέσμευση για συμμετοχή του ιδιωτικού τομέα στην ανταλλαγή εξειδικευμένης εμπειρίας στους διάφορους τομείς της οικονομίας (πρωτογενούς, δευτερογενούς και τριτογενούς παραγωγής). Ειδικότερα, εγκαθίδρυση συστημάτων ελέγχου της διαλειτουργικότητας³³ των υποδομών.

³¹ Η Διεθνής Τηλεπικοινωνιακή Ένωση είναι η αρμόδια υπηρεσία για τις τηλεπικοινωνίες και την πληροφορία του Οργανισμού Ηνωμένων Εθνών. Η έδρα της είναι στη Γενέβη της Ελβετίας και αποτελείται από 192 κράτη-μέλη. Έργο της είναι η συγκρότηση τακτικών εκθέσεων σε παγκόσμιο επίπεδο, μέσω της έρευνας και της διοργάνωσης συνεδρίων.

³² Η διατλαντική συνδιάσκεψη έλαβε χώρα στην Ουγγαρία με εξέχοντες παραβρισκόμενους τον αντιπρόεδρο για την Ψηφιακή Ατζέντα της Ευρωπαϊκής Επιτροπής (Neelie Kroes) και τον υπουργό για θέματα ασφάλειας των ΗΠΑ (Janet Napolitano)..

³³ Διαλειτουργικότητα καλούμε τη διασύνδεση των πληροφοριακών συστημάτων διαφορετικών κλάδων έτσι, ώστε να έχουν τη δυνατότητα να αλληλεπικοινωνούν δε διαφορετικούς βαθμούς πολυπλοκότητας (Πολυμενόπουλος, 2001, 19).

- Ένα πρόγραμμα κοινών δραστηριοτήτων, οι οποίες να αποσκοπούν στην ευαισθητοποίηση και επαγρύπνηση. Η μέθοδος θα αφορά ένα μοντέλο ανταλλαγής μηνυμάτων, με στόχο την καθιέρωση της άμεσης επικοινωνίας.

Εν κατακλείδι, μπορούμε να αναφέρουμε και ένα άλλο μέσο, στο οποίο κρατικοί και ιδιωτικοί φορείς τείνουν να συγκλίνουν σε μια κοινή δομή εξουσίας. Πρόκειται για τη ρύθμιση της κυκλοφορίας στο διαδίκτυο. Δηλαδή, την απόκτηση δικαιώματος συμμετοχής στον κυβερνοχώρο. Αυτή η υπηρεσία εξακολουθεί να παρέχεται από έναν μόνο οργανισμό (ICANN³⁴). Στη βασική αποστολή του περιλαμβάνεται η εκχώρηση ονομάτων και αριθμών και αυτή εκπληρώνεται με το δικαίωμα εποπτείας τού συστήματος κυκλοφορίας και διευθύνσεων στον κυβερνοχώρο, το οποίο του παρέχεται από το κράτος.

Έχει δημοσιοποιηθεί κατά επανάληψη το αίτημα μιας διεθνούς εποπτείας της πληροφοριακής ροής στο Διαδίκτυο. Η εν προκειμένω έκκληση υπογραμμίζει πως καμία χώρα δεν είναι δίκαιο να διαθέτει αποκλειστικά την εξουσία του ελέγχου, του μεγαλύτερου καναλιού τηλεπικοινωνιών στον κόσμο³⁵.

Στην επίσημη πτυχή αυτού του αιτήματος, μπορούμε να αναφέρουμε το εγχειρίδιο της ευρωπαϊκής επιτροπής για τη κοινωνία της πληροφορίας με τίτλο «Διακυβέρνηση του Διαδικτύου: τα επόμενα βήματα». Πάντως, φαίνεται ότι ουσία βρίσκεται στην αντιπαλότητα για το καθεστώς ιδιοκτησίας της χρήσης των κωδικών χώρας στις ηλεκτρονικές διευθύνσεις «όπως, .eu, .fr και .gr». Τέλος, όπως δήλωσε η αρμόδια Επίτροπος Βίβιαν Ρέντινγκ «φέτος βρισκόμαστε στην ιστορική καμπή αυτής της διευθέτησης».

Περιγράψαμε παραπάνω πώς τις υποδομές μπορούμε να τις διαχωρίζουμε σε τομείς. Είναι σημαντικό να καταλάβουμε ότι ένα χτύπημα σε αυτές τις δομές είναι φυσικό, εκτός των προσδιορισμών που του δίνει η ειδική κατηγορία των όπλων (π.χ. «κυβερνοόπλα» - «κυβερνοεπίθεση»), να χαρακτηρίζεται από πολλούς στρατιωτικό. Αυτό δεν πρέπει να συγχέεται με τη διάκριση των υποδομών. Αυτές τις επιθέσεις μπορούμε να τις κατατάξουμε σε διάφορες υποδομές.

Μπορούμε να παραθέσουμε πολλές δημοσιεύσεις για ανάλογα γεγονότα. Ενδεικτικά, το 2009 οι ΗΠΑ καταγγέλλουν ότι hackers από την Κίνα, τη Ρωσία και άλλες χώρες προσπαθούν να αλλοιώσουν τη λειτουργία του ηλεκτρικού της δικτύου.

³⁴ Ο ICANN ιδρύθηκε το 1998 ως φορέας μη κερδοσκοπικού χαρακτήρα εγκατεστημένος στην Καλιφόρνια. Λειτουργεί βάσει σύμβασης με την κυβέρνηση των ΗΠΑ. Αν και η σύσταση του απαρτίζεται από στελέχη από όλον τον κόσμο, λογοδοτεί στην Ουάσιγκτον.

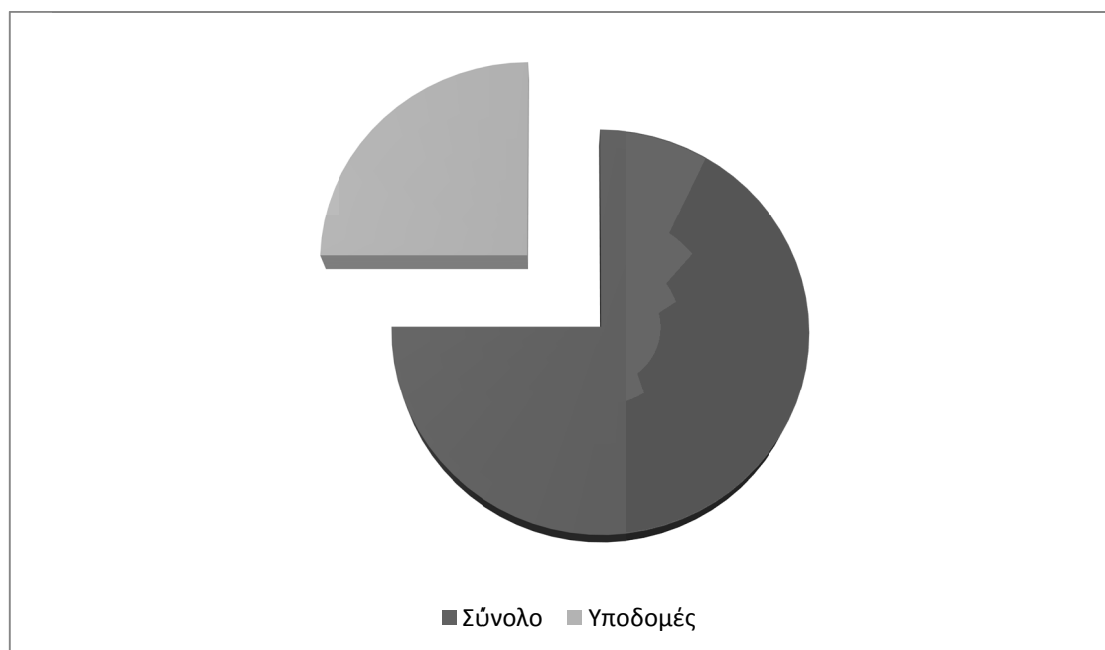
³⁵ Σημειώνουμε ότι η σύμβαση του ICANN με την κυβέρνηση των ΗΠΑ λήγει τον Σεπτέμβριο (2011).

Για αυτόν το λόγο ομοσπονδιακές υπηρεσίες ασφαλείας επιστρατεύουν ειδικούς ερευνητές με ψηφιακή τεχνογνωσία. Ακόμα σημαντικότερο γίνεται το γεγονός όταν ο ίδιος ο πρόεδρος των ΗΠΑ Barack Obama δίνει ιδιαίτερες οδηγίες για την οργάνωση της εθνικής άμυνας σε δυνητικές κυβερνοεπιθέσεις. (The Associated Press, 23/6/2011). Ωστόσο, είναι κοινώς αποδεκτό ότι χαρακτηριστικότερα περιστατικά αυτής της κατηγορίας αποτελούν τα γεγονότα, τα οποία έλαβαν χώρα στην Εσθονία (2007) και τη Γεωργία (2008), τα οποία περιγράφουμε στη συνέχεια.

4.2.2 Ποσοτικός Προσδιορισμός

Σε αυτήν την θεματική κατηγορία εντοπίστηκαν συνολικά **105** γραμματικές αναφορές. Η συμμετοχή ανήλθε σε ποσοστό 33,3%, το οποίο αντιστοιχεί στην πρώτη θέση της κατάταξής μας. Οπότε, το μερίδιο που έχουν οι *Υποδομές* στη συγκεντρωτική κατανομή ανέρχεται ακριβώς στο ένα τρίτο (1/3) του συνόλου (Σχήμα 11).

Σχήμα 11. Συγκεντρωτικό Μερίδιο «ΥΠΟΔΟΜΩΝ»



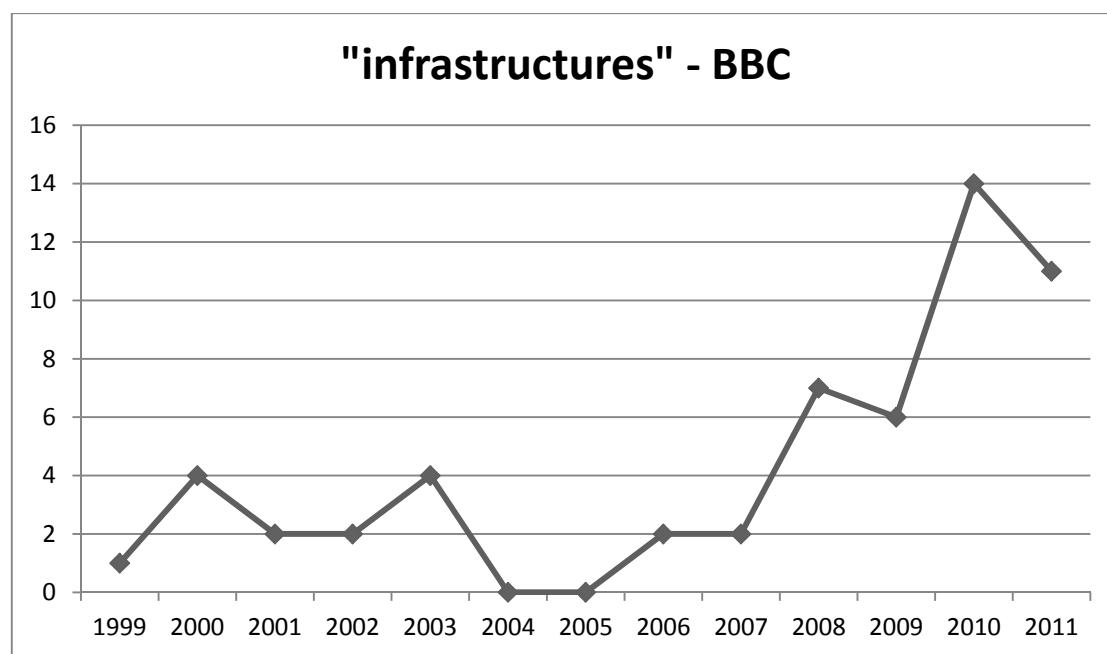
Αν αναζητήσουμε αναλυτικότερα την προέλευση της εν λόγω κατανομής, τότε μπορούμε να δούμε πως από το BBC έχουμε 55 αναφορές (σε σύνολο 150) με αναλογούν ποσοστό 36,7% και σχετικά συνεχή αυξητική διαχρονική τάση (Σχήμα 12). Όσον αφορά το CNN έχουμε 50 αναφορές (σε σύνολο 165) με αναλογούν

ποσοστό 30,3%. Η διαχρονική τάση εμφανίζεται στα άκρα (αρχή και τέλος) υψηλή, σε αντίθεση με το μέσο, όπου είναι ιδιαίτερα χαμηλή (Σχήμα 13).

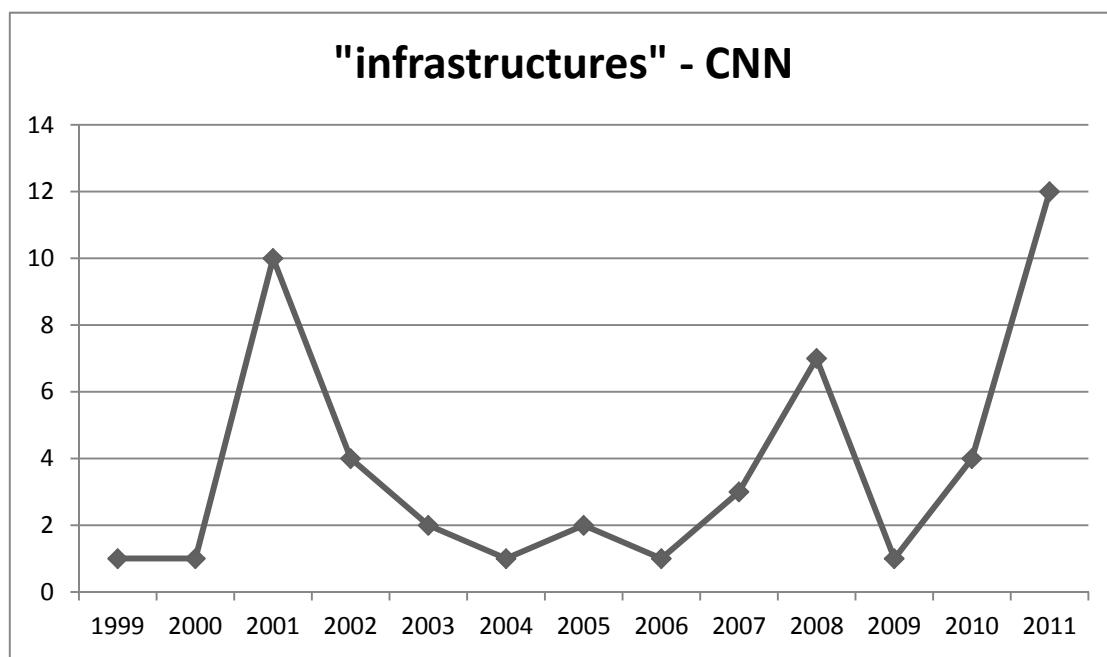
Ενδιαφέρον παρουσιάζει η διακύμανση των θέσεων που καταλαμβάνει αυτή η κατηγορία στο κάθε μέσο. Ενώ στο BBC διατηρεί την πρώτη θέση και μάλιστα με μεγαλύτερο ποσοστό από το συγκεντρωτικό (36,7% έναντι 33,3%), στο CNN φθάνει στη δεύτερη θέση χάνοντας τις τρεις ποσοστιαίες μονάδες, τις οποίες έχει κερδίσει προηγουμένως (30,3% έναντι 33,3%).

Τέλος, άξιο παρατήρησης είναι ότι στην πρώτη θέση της κατηγορίας στο BBC, διακρίνουμε συγκριτικά το μεγαλύτερο ποσοστό από όλες τις θέσεις, τόσο στο CNN, όσο και στη συγκεντρωτική κατάταξη.

Σχήμα 12. Διαχρονική Τάση «Υποδομών» – BBC



Σχήμα 13. Διαχρονική Τάση «Υποδομών» – CNN



4.2.3 Ανάλογα Κυβερνο-επεισόδια

A] Εσθονία, 2007.

Μια σειρά γεγονότων, τα οποία ξεκίνησαν στις 27 Απριλίου του 2007 και κατέληξαν το Μάιο (περίπου τρεις εβδομάδες μετά), χαρακτηρίστηκαν από πολλούς -όχι απλά ως «κυβερνοπόλεμος»³⁶-, αλλά ως «ο πρώτος κυβερνοπόλεμος». Ενδεικτικά, σημειώνουμε ότι αυτό αναφέρθηκε στο Συνέδριο για θέματα κυβερνοασφάλειας, το οποίο έλαβε χώρα το Μάρτιο του 2009 στο Σαν Φραντσίσκο των ΗΠΑ (<http://www.spacewar.com/cyberwars.html>).

Οι γεωπολιτικές εξελίξεις της δεκαετίας του '90 στην πρώην Σοβιετική Ένωση διαμόρφωσαν το πλαίσιο, μέσα στο οποίο μπορούμε να εντοπίσουμε τις ρίζες των γεγονότων που μας ενδιαφέρουν. Η απόσχιση του μικρού κράτους της Εσθονίας (με έκταση 45,227 km² και πληθυσμό 1.282,963 κατοίκους) από την πολιτειακή της σύνδεση με τη Ρωσική Ομοσπονδία, έδωσε το δικαίωμα στον εσθονικό λαό να ακολουθήσει την επόμενη δεκαετία μια πορεία με τα δικά του χαρακτηριστικά. Η κλίση των Εσθονών στη τεχνολογία (estonia.eu/about-estonia/society/estonians.html) τους έκανε να δώσουν ιδιαίτερο βάρος, για την οργάνωση του κράτους τους, στην

³⁶ Όλοι οι ειδικοί καταλήγουν σε αυτή τη διαπίστωση, κυρίως λόγω των πόρων που συγκεντρώθηκαν και διατέθηκαν (<http://www.tech-faq.com/cyber-warfare.shtml> - 28/5/09).

ηλεκτρονική διακυβέρνηση. Χαρακτηριστικό είναι πως έφτασαν στο σημείο να τους αποκαλούν «κυβέρνηση δίχως χαρτιά, στη γραφειοκρατία της» (paperless government)³⁷. Επρόκειτο, λοιπόν, για μια από τις πιο «δια-δικτυωμένες» χώρες, όχι μόνο της Ευρωπαϊκής Ένωσης, αλλά ολόκληρου του κόσμου.

Σύμφωνα με την Εσθονική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CERT), δηλαδή την αρμόδια υπηρεσία για την αντιμετώπιση των κυβερνοεπιθέσεων στις κρίσιμες εθνικές υποδομές (<http://www.ria.ee/27525> - May 10, 2008):

- το 98% των τραπεζικών συναλλαγών γίνονταν ηλεκτρονικά,
- το 66% του πληθυσμού χρησιμοποιούσε το διαδίκτυο,
- το 55% των νοικοκυριών είχαν υπολογιστή στο σπίτι και
- το 91% των υπολογιστών ήταν συνδεδεμένα με το Ιντερνέτ.

Θεωρήσαμε πολύ σημαντικό να δείξουμε την εξάρτηση της χώρα από το διαδίκτυο, ώστε να κατανοήσουμε τα γεγονότα, των οποίων η περιγραφή ακολουθεί. Η αφορμή δίνεται τον Απρίλη του 2007, όταν η εσθονική κυβέρνηση αποφασίζει να μετακινήσει ένα άγαλμα από το κέντρο της πρωτεύουσας της, το Ταλίν, σε ένα άλλο σημείο. Το εν λόγω όμως άγαλμα του «μπρούτζινου στρατιώτη», όπως λεγόταν, συμβόλιζε τους αγώνες της τέως Σοβιετικής Ένωσης έναντι των Ναζί. Για αυτό το λόγο οι ρώσοι, τόσο εντός (η μειονότητα των ρωσσόφωνων ανέρχεται σε χιλιάδες), όσο κι εκτός Εσθονίας θίχτηκαν. Στις διαμαρτυρίες που ακολούθησαν είχαμε 1300 συλλήψεις, 150 τραυματίες και 1 νεκρό (<http://news.bbc.co.uk>, 20/9/2011).

Παράλληλα με τα όσα διαδραματίστηκαν στο φυσικό χώρο, είχαμε μια καινοτόμο και πρωτοφανώς συντονισμένη επίθεση μέσω του διαδικτύου. Η επίθεση χαρακτηρίστηκε μεγάλης κλίμακας και εκδηλώθηκε σε δύο κύματα (www.riso.ee, 21/9/2011). Το πρώτο κύμα αφορούσε τον κεντρικό κυβερνητικό πυρήνα, συνδυασμένο με προσωπικά στοχευόμενα μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου σε άτομα υψηλών θέσεων, όπως ο πρωθυπουργός και το κυβερνών κόμμα (www.reform.ee, 22/9/2011). Ωστόσο, σε αντίθεση με τις ψυχολογικού εκβιασμού επιδιώξεις του πρώτου κύματος, το δεύτερο είχε χαρακτήρα περισσότερο μαζικό και ανοικτό στην κοινωνία.

³⁷ Επίσης συχνά επωνομαζόταν «E-stonia», θέλοντας να τονιστεί η ηλεκτρονικής (E-electronic) έντασης διακυβέρνηση (<http://www.ria.ee/27525>, 22/9/2011).

Με τη μέθοδο που είναι γνωστή ως Ddos³⁸ και δη σε «βαριά μορφή» τέθηκαν σε σύντομο σχετικά διάστημα, εκτός λειτουργίας σημαντικοί δημόσιοι και ιδιωτικοί φορείς (πίνακας 7). Πιο συγκεκριμένα:

- Η Εσθονική Προεδρεία
- Το Κοινοβούλιο
- Τα Υπουργεία της Κυβερνήσεως
- Τα Πολιτικά Κόμματα
- Οι δημοφιλείς οργανισμοί ειδήσεων
- Οι Τράπεζες
- Οι τηλεπικοινωνιακές υποδομές

Πίνακας 7. Ιστότοποι που επλήγησαν

Table 1. Targeted Websites

Attacks	Destination	Address or owner
35	195.80.105.107/32	pol.ee
7	195.80.106.72/32	www.rigikogu.ee
36	195.80.109.158/32	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	195.80.124.53/32	m53.envir.ee
2	213.184.49.171/32	www.sm.ee
6	213.184.49.194/32	www.agri.ee
4	213.184.50.6/32	
35	213.184.50.69/32	www.fin.ee (Ministry of Finance)
1	62.65.192.24/32	

Table 2. Number of Attacks

Attacks	Date
21	2007-05-03
17	2007-05-04
31	2007-05-08
58	2007-05-09
1	2007-05-11

Πηγή: <http://doubleshotsecurity.com/pdf/NANOG-eesti.pdf>

Ίσως, το μεγαλύτερο ενδιαφέρον έχει το συμπέρασμα μιας μελέτης που έγινε σε ένα σεμινάριο για θέματα ασφάλειας πληροφοριών, σε ένα σουηδικό πανεπιστήμιο και κατέληξε ότι «ο κυβερνοπόλεμος μάλλον δεν αφορά σε όπλα μαζικής καταστροφής. Συνιστά όμως όπλο μαζικής διάσπασης (mass disruption)» (Muhammad & Jawad, 2010). Και εμείς συμπληρώνουμε: *κράτους και κοινωνίας*.

³⁸ Βλ. Τμήμα ΙΙΙ – Κεφάλαιο 9.2.3 (8^η περίπτωση).

Μια άλλη διάσταση, της οποίας οι ελλείψεις αναδείχθηκαν με όλα αυτά τα γεγονότα, είναι η νομική. Η Εσθονική κυβέρνηση προσπαθώντας να εκμεταλλευτεί την ενεργή συμφωνία που είχε με τους Ρώσους³⁹, στην δίωξη εγκληματικών πράξεων που αφορούν και τις δύο χώρες, αιτήθηκε εξ αρχής τη συνεργασία των δύο κρατών (Tikk & Kaska, 2010). Δύο παράγοντες όμως έκαναν τη Ρωσική Κυβέρνηση να αρνηθεί τη συνεργασία. Αφενός, είναι ακόμα αδύνατον να αποδειχθεί η ταυτότητα των δραστών κι επομένως τα κίνητρά τους. Αφετέρου, η Εσθονική Κυβέρνηση υπονόησε ότι πρόκειται για ένθερμους ρώσους πατριώτες, αφήνοντας την υποψία συσχέτισής τους με την κυβέρνηση (<http://www.iar-gwu.org/node/65>, 25/7/2010). Ατελέσφορες ήταν επίσης και οι προσπάθειες προσέγγισης, από την ευρωπαϊκή πλευρά, για την ενεργοποίηση της Interpol⁴⁰.

Η τελευταία διάσταση αυτού του θέματος που θα εξετάσουμε είναι ο πετυχημένος τρόπος αξιοποίησης από την εσθονική κυβέρνηση, όλων αυτών των δυσάρεστων για την Εσθονία γεγονότων. Καταρχάς, στην οργανωτική δομή του υπουργείου άμυνας συμπεριλήφθηκε, εκτός από τους ένστολους ειδικούς (The Defence Forces) και ο σύνδεσμος για την κυβερνοάμυνα (Defence League). Το ενδιαφέρον είναι πως πρόκειται για εθελοντές πολίτες (κυρίως νεαρούς σε ηλικία), οι οποίοι θα προετοιμάζονται για την υπεράσπιση της χώρας τους σε δυνητική επανάληψη μιας κυβερνοεπίθεσης (<http://www.eesti.ee/eng>, 25/7/2010).

Κατόπιν, επιτεύχθηκε το ζήτημα να αναχθεί σε θέμα αντιπαλότητας μεταξύ της Ρωσικής Ομοσπονδίας και του NATO. Συνέπεια αυτού ήταν η ίδρυση από το NATO στο Ταλίν ενός Κέντρου Αριστείας για τη Συνεργασία στην Άμυνα στον Κυβερνοχώρο (Cooperative Cyber Defence Centre of Excellence) στις 28/10/2008 (<http://www.ccdcoe.org>). Το ενδιαφέρον για την εργασία μας είναι ο ένας από τους τομείς έρευνας του κέντρου, όπως αναφέρεται στην επίσημη ιστοσελίδα του:

- Νόμος και Πολιτική
- Έννοια και Στρατηγική
- Περιβάλλον Τακτικής
- Προστασία Κρίσιμων Πληροφοριακών Υποδομών

³⁹ Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, signed on 26 January 1993. RT (State Gazette) II 1993, 16, 27; RT II 2002, 14, 58.

⁴⁰ Η παρακάτω πηγή αφορά δημοσιογραφική ανταπόκριση μέσα από τη Μόσχα (Alastair Gee). http://www.foreignpolicy.com/articles/2008/11/11/the_dark_art_of_cyberwar.

Ολοκληρώνοντας, θα παραθέσουμε ένα τελευταίο στοιχείο, ενδεικτικό των συνεπειών της ορθολογικής αξιοποίησης των κυβερνοεπιθέσεων που δέχθηκε η Εσθονία. Πρόκειται για το συμβόλαιο της εσθονικής εταιρείας υψηλής τεχνολογίας Cybernetica, η οποία θα λάβει αρχικώς 1 εκατομμύριο δολάρια, που υπεγράφη με τη DARPA⁴¹ προκειμένου να συνεργαστούν στο ειδικό κι ευαίσθητο μέρος της κυβερνοασφάλειας, την κρυπτογράφηση (σύστημα Sharemind - λογισμικό SecreC)⁴².

B] Γεωργία, 2008

Και σε αυτήν την περίπτωση, η αιτία βρίσκεται στις γεωστρατηγικές επιλογές των χωρών οι οποίες προκύπτουν από τη διάλυση της Σοβιετικής Ένωσης. Η αντιπαλότητα σχετικά με τα εδαφικά κυριαρχικά δικαιώματα σε μια μικρή περιοχή του πρώην σοβιετικού νότου, κοντά στον Καύκασο, την Οσσετία, οδήγησε σε σύρραξη τον Αύγουστο του 2008, μεταξύ Γεωργίας και Ρωσίας.

Η διαφορά με την προηγούμενη περίπτωση είναι ακριβώς αυτή. Ότι δηλαδή το «μήνυμα» των κυβερνεπιτιθέμενων, εκτός από πολιτικό, είχε και συγκεκριμένη κατεύθυνση υποστήριξης των στρατιωτικών επιχειρήσεων. Οι στόχοι ήταν οι τηλεπικοινωνιακές υποδομές και δη τα δίκτυα των γεωργιανών ενόπλων δυνάμεων (<http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>, 24/9/2011).

Ήταν η πρώτη φορά⁴³, τέτοιου μεγέθους και έντασης στρατιωτικών κυβερνοεπιχειρήσεων. Αναμενόμενος ήταν λοιπόν ο αιφνιδιασμός από αυτή την κίνηση. Αυτό συνεπάγεται και από την προσφορά της Εσθονίας για βοήθεια και την καθυστέρηση επίσημης απάντησης της Γεωργίας (The Baltic Business News website). Εξάλλου, όπως αναφέραμε, πέρα των επιπρόσθετα στρατιωτικών, οι λοιποί στόχοι ομοιάζαν. Σε μια τελική εκτίμηση, μπορούμε να πούμε ότι το μέγεθος της βλάβης από τις κυβερνοεπιθέσεις στις ψηφιακές υποδομές της χώρας, ήταν καταστροφικό. Κάτι που επισήμανε ο Υπουργός Εθνικής Ασφάλειας της Γεωργίας, σε συνέδριο της FOSE⁴⁴.

⁴¹ Η Defence Advanced Research Projects είναι από τους συνεφευρέτες του διαδικτύου.

⁴² Το εν λόγω σύστημα και το λογισμικό του επιτρέπουν το μοίρασμα ευαίσθητων πληροφοριών μέσω δικτύου, διατηρώντας αυστηρά πρότυπα ασφαλείας και διαβάθμισης. Το σύστημα μπορεί να χρησιμοποιηθεί σε μεγάλες και μικρές βάσεις δεδομένων. Η ασφάλειά του είναι τόσο υψηλή, που δεν επιτρέπει πρόσβαση ακόμα και σε διαχειριστές του δικτύου να προβούν σε αλλαγές.
<http://www.defence-point.gr/news/?p=10364>

⁴³ Η επόμενη πραγματοποιήθηκε στη Γάζα, από το Ισραήλ έναντι των υποδομών της Χαμάς (Operation Cast Lead) στις 7 Δεκεμβρίου 2008 (Carr, 2010), σ. 19.

⁴⁴ Πραγματοποιείται σε ετήσια βάση και συμμετέχουν κυβερνητικοί υπάλληλοι, οι οποίοι εργάζονται σε τομείς πληροφορικής (<http://fose.com/events/fose-2012/home.aspx>, 25/9/2011).

Η πιο σημαντική πτυχή αυτής της υπόθεσης για την εργασία μας βρίσκεται στην αφανή μεν, αλλά ανοικτή δε, δυνατότητα συγκεκριμένης κοινωνικής συμμετοχής. Σε ένα πρώτο επίπεδο έχουμε διάφορες δηλώσεις, όπως αυτή του τότε Γεωργιανού Υπουργού Εξωτερικών, ο οποίος είπε ότι «επρόκειτο για μια εκστρατεία κυβερνοπολέμου, που είχε επιπτώσεις σε πολλές θέσεις στον παγκόσμιο ιστό». Πηγαίνοντας βαθύτερα, διαβάζουμε ειδικούς αναλυτές, οι οποίοι κατηγορούσαν ένα δίκτυο που έχει έδρα στην Αγία Πετρούπολη, το Russian Business Network (RBN), ως μια «μυστική ομάδα με μέλη εγκληματίες χάκερ, οι οποίοι έχουν σχέση με τη μαφία, αλλά και με τη ρωσική κυβέρνηση». Και σε αυτήν όμως την περίπτωση τίποτα δεν μπορούσε να αποδειχθεί (<http://www.telegraph.co.uk>, 25/9/2011). Ενισχυτικό αυτού είναι ότι τα στοιχεία που προσεγγίζουν τον τρόπο που οργανώθηκε η επίθεση, καταλήγουν στην ύπαρξη μιας «λαϊκής βάσης», είτε χρησιμοποιούν ακραίους χαρακτηρισμούς τύπου «al Qaeda» (<http://portal.acm.org>, 25/9/2011), είτε όχι.

Προσεγγίζοντας τον πυρήνα του ζητήματος, αυτό που γίνεται ακόμη πιο αξιοσημείωτο είναι ότι πίσω από τους προφανείς στόχους, όπως η προσωπική ιστοσελίδα του Προέδρου της Γεωργίας Mikheil Saakashvili και οι ιστότοποι του κοινοβουλίου (www.parliament.ge) και της Προεδρίας της Κυβερνήσεως (president.gov.ge), κρύβεται μια ευρεία ομάδα με διεθνικής κοινωνικής οργάνωσης προεκτάσεις. Αρχικά εντοπίζουμε ένα ανώνυμο ιστολόγιο (“RBNexploit” blog)⁴⁵. Εκεί είχαμε οδηγίες για τεχνικές χρησιμοποίησης διαφόρων κακόβουλων λογισμικών (π.χ. spam, identity theft και malware). Τα ίχνη των βασικών servers, οι οποίοι ήταν απαραίτητοι σε αυτή τη διαδικασία, ανιχνεύθηκαν στην Τουρκία. Στη συνέχεια, λαμβάνουμε υπόψη μας έναν Λευκορώσσο δημοσιογράφο, εξοικειωμένο με αυτήν την τεχνογνωστική περιοχή, τον Evgeny Morozov. Αυτός περιγράφει την εύρεση μιας ιστοσελίδας (StopGeorgia.ru), μέσω της οποίας ήταν εφικτή η αποστολή ταυτόχρονα πολλαπλών⁴⁶ ηλεκτρονικών μηνυμάτων σε 18 γεωργιανούς ιστότοπους (<http://www.reuters.com>, 16/8/2008).

Σε αυτή την κατεύθυνση ένας -φερόμενος ως- χάκερ, με το όνομα Leonid "R0id" Stroikov, δήλωσε σε ένα τεύχος του περιοδικού *Xakep* ("Hacker"), ότι δύναται να επιβεβαιώσει πως όλη αυτή η συναφής ιστορία που διηγείται η υπόθεση «Grey Goose» ισχύει (<http://www.wired.com/dangerroom/2008/10/government-and/>, 23/10/

⁴⁵ Πηγή μας εδώ είναι ο Ethan Zuckerman υφηγητής στο *Berkman Center for Internet and Society and a co-founder of Global Voices Online*. Οι απόψεις του αφορούν προσωπική του έρευνα, η οποία δημοσιεύθηκε στο Reuters.com.

⁴⁶ Απαραίτητες προϋποθέσεις για τη μέθοδο Ddos.

2008). Για αυτόν λοιπόν τον λόγο οφείλουμε να εξετάσουμε αυτήν την υπόθεση. Ο άνθρωπος που τη δημιούργησε -υπεύθυνος συναφούς αντικειμένου εταιρείας (GreyLogic) και ειδήμων αναλυτής (cyber intelligence analyst⁴⁷)-, περιγράφει με ενδελέχεια στο βιβλίο του⁴⁸ τα ακόλουθα αποτελέσματά της.

Μια ημέρα πριν τη σύρραξη μεταξύ ρώσων και γεωργιανών, στις 7/8/2008 ένα φόρουμ με την ηλεκτρονική διεύθυνση <http://www.stopgeorgia.ru> ήταν σε ετοιμότητα. Αρχικά τα μέλη ήταν 30 και έφθασαν πάνω από 200, ένα μήνα μετά. Σε αυτήν την ηλεκτρονική διεύθυνση προτείνονταν οι πρώτοι 37 στόχοι υψηλής αξίας. Εξαιτίας, του μπλοκαρίσματος της ροής από διαδρομές ρώσικων κόμβων, είχαν προβλεφθεί παρακάμψεις από τη Λιθουανία.

Εκτός, όμως, των τεχνικών προδιαγραφών ή της ταυτότητα του εγχειρήματος, υπάρχει ένα σημαντικό γνώρισμα, το οποίο ενισχύει την αποκλειστικότητα της *οντότητας αυτής της θεματικής κατηγορίας*. Η πρόσβαση στην εν λόγω ιστοσελίδα ήταν ανοικτή, δίχως την απαίτηση ειδικής εξουσιοδότησης. Έτσι απλοί -μη επαίοντες αυτών των θεμάτων- πολίτες μπορούσαν να εκμεταλλευθούν αυτή τη δυνατότητα και να συμμετάσχουν ενεργά σε ένα κυβερνοπόλεμο. Στην εργασία μας εξ αντικειμένου δεν μας ενδιαφέρει ποιος, πώς και γιατί ανάρτησε αυτές τις «ευκαιρίες» στον κυβερνοχώρο. Η εστίασή μας δεν επιδιώκουμε να είναι ούτε τεχνικής ούτε στρατηγικής φύσεως. Παρόλα αυτά εκείνο που αναδεικνύεται είναι ότι τα αποτελέσματα αυτού του τύπου κυβερνοπολέμου μπορεί να είναι αισθητά στην κοινωνία σε επίπεδο αυτών που επιτίθενται, αλλά και αμύνονται.

Ως προς το τελευταίο αρκεί να παραθέσουμε τα συμπεράσματα μιας πρόσφατης έκθεσης του Εθνικού Συμβουλίου Πληροφοριών – ανώτατου οργάνου ασφάλειας των ΗΠΑ (National Intelligence Council - NIC). Σε αυτήν, την οποία τιτλοφορεί “Global Trends 2025”, καταλήγει ότι η προσβολή των κρίσιμων υποδομών είναι εφικτή και μπορεί να αποβεί καταστροφική (http://www.dni.gov/nic/NIC_2025_project.html).

⁴⁷ Ο τίτλος – ειδικότητα την οποία σε ελεύθερη μετάφραση αποδίδουμε «αναλυτής πληροφοριών κυβερνοχώρου» (cyber intelligence analyst), δεν έχει σχέση με την παραδοσιακή έννοια του όρου που περιγράφει το άτομο που εργάζεται σε μια υπηρεσία πληροφοριών. Αναφέρεται σε μια εκτεχνικευμένη ιδιότητα, ενός εξειδικευμένου σε θέματα πληροφορικής ατόμου, το οποίο έχει ειδικές γνώσεις πρόσβασης, διείσδυσης και ιχνηλάτισης της πληροφοριακής ροής στο διαδίκτυο.

⁴⁸ J. Carr, *Inside Cyber Warfare – Mapping the Cyber Underworld*, O'Reilly Media Inc. (2010) σ.15

4.3 Διεισδύσεις

4.3.1 Ποιοτικός Προσδιορισμός

Στις αρχές του 2011 στο Νταβός, μια γνωστή εταιρεία με αντικείμενο την ασφάλεια στο διαδίκτυο, η Symantec Corp. (<http://www.symantec.com/about/>) ανακοίνωσε τα αποτελέσματα μιας έρευνάς της για την προστασία των κρίσιμων πληροφοριακών υποδομών για το 2010 (2010 Critical Information Infrastructure Protection). Τα αποτελέσματα αναφέρουν πως οι ίδιες οι εταιρείες παροχής κρίσιμων υποδομών (critical infrastructure providers) δήλωσαν σε ποσοστό 53% ότι τέτοιου είδους επιθέσεις αυξήθηκαν κατά μέσο όρο 10 φορές τα τελευταία πέντε χρόνια, γεγονός που προξενεί στις επιχειρήσεις τους ζημιές ύψους περίπου 850.000 δολαρίων ΗΠΑ.

Ο Justin Somaini, επικεφαλής της ασφάλειας πληροφοριών (Chief Information Security Officer) της Symantec Corp., συγκεκριμένα δήλωσε ότι «η προστασία των κρίσιμων υποδομών δεν είναι μόνο υπόθεση της πολιτείας. Σε χώρες όπου η πλειοψηφία των κρίσιμων υποδομών βασίζεται σε ιδιωτικές εταιρείες -επιπρόσθετα με τις μεγάλες επιχειρήσεις- υπάρχουν ωστόσο και οι μικρές και μεσαίες επιχειρήσεις. Η ασφάλεια από μόνη της δεν είναι αρκετή ώστε οι πάροχοι κρίσιμων υποδομών όλων των κατηγοριών να είναι σε θέση να αντέξουν τις σημερινές επιθέσεις στον κυβερνοχώρο. Το Stuxnet worm⁴⁹ που στοχεύει τις εταιρείες ενέργειας σε όλον τον κόσμο αντιπροσωπεύει το εξελιγμένο είδος απειλών που απαιτούν λύσεις για ασφάλεια, αποθήκευση και back-up μαζί με διαδικασίες πιστοποίησης και ελέγχου πρόσβασης σε ετοιμότητα για πραγματική αντοχή του δικτύου» (www.kathimerini.gr, 5-11-2010).

Παρόλα αυτά, σε γενικές γραμμές, η θεραπεία που προτείνεται είναι η οργανωτική μετάβαση στην πληροφοριοκεντρική κατεύθυνση των οργανισμών. Εν ολίγοις αυτό σημαίνει τον δομικό ανασχηματισμό υπηρεσιών, επιχειρήσεων κοκ, με επίκεντρο την προστασία της πληροφοριακής ροής και κατά συνέπεια τη θέσπιση αυστηρότερων κανόνων διαχείρισής της. Δηλαδή, μεγαλύτερος έλεγχος (όπως, οι εξουσιοδοτημένοι κωδικοί και οι μέθοδοι κρυπτογράφησης) στα πρόσωπα που θα έχουν διαβαθμισμένη πρόσβαση. Σήμερα, πλέον, έχει καθιερωθεί σε μικρούς και μεγάλους οργανισμούς, τόσο του ιδιωτικού όσο και του δημόσιου τομέα, η θέση ευθύνης του ελέγχου της ασφάλειας των πληροφοριών (info-sec). Θα εξηγήσουμε

⁴⁹ Το κακόβουλο πρόγραμμα «stux net», το οποίο θα αναλύσουμε στο τέλος του υποκεφαλαίου, αποτελεί μία από τα δύο χαρακτηριστικότερες περιπτώσεις αυτής της θεματικής κατηγορίας.

συνοπτικά την κεντρική ιδέα αυτής της αρμοδιότητας, διότι τη θεωρούμε θέση-κλειδί, η οποία γεφυρώνει την παραπάνω θεωρία με την πράξη.

Το αντικείμενο της ασφάλειας των πληροφοριών (της διακίνησής τους για την ακρίβεια), καταρχήν, εστιάζεται μόνο στην πληροφοριακή ροή μέσω των συστημάτων της πληροφορικής. Αυτό σημαίνει πως δεν ασχολείται με τη διασφάλιση της εκπομπής και αποδοχής πληροφοριών από άνθρωπο σε άνθρωπο, χωρίς τη διαμεσολάβηση των ΤΠΕ. Αντιθέτως, επικεντρώνεται στις περιπτώσεις «αυτοματοποιημένης» διακίνησης δεδομένων μεταξύ των πληροφορικών συστημάτων. Ειδικότερα, ελέγχει τις ενδεχόμενες δραστηριότητες μη εξουσιοδοτημένων χρηστών⁵⁰. Ωστόσο, στην πράξη ο υπεύθυνος της ασφάλειας των πληροφοριών ενός οργανισμού δεν ενδιαφέρεται για την αποθήκευση ή επεξεργασία των δεδομένων, αλλά ελέγχει (την γνωστή ως τριάδα της Κεντρικής Υπηρεσίας Πληροφοριών των ΗΠΑ – «CIA triad») (Σχήμα 14):

- την *εμπιστευτικότητα* (confidentiality), ή αλλιώς ο έλεγχος των παραβατών ή παραβατικών συστημάτων. Για παράδειγμα παράνομες οικονομικές συναλλαγές (όπως οι υποκλοπές των πιστωτικών καρτών),
- την *ακεραιότητα* (integrity), δηλαδή τη διατήρηση των δεδομένων στην αυθεντική τους μορφή, ώστε κανείς να μην μπορεί να τα αλλοιώσει και
- Τη *διαθεσιμότητα* (availability) των πληροφοριών. Εδώ ελέγχονται όλα τα συστήματα με τα οποία πρόκειται να επικοινωνήσει το δικό μας, με σκοπό να εντοπιστούν ύποπτες προθέσεις.

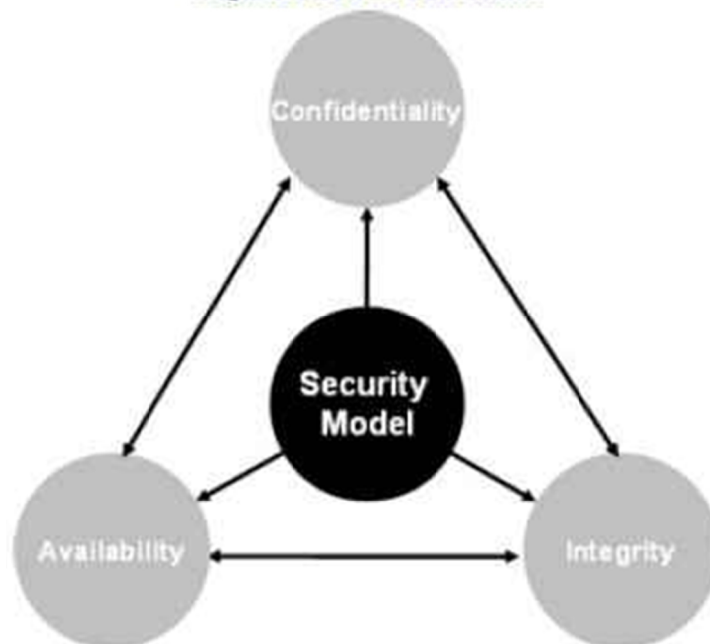
⁵⁰ Η αγγλόφωνη διατύπωση αναφέρει: Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Wikipedia, 3/11/2011).

Σχήμα 14. “CIA TRIAD”



Πηγή: <http://www.google.gr/imgres?imgurl=http>

Figure 1-2. The CIA Triad



Πηγή: <https://learningnetwork.cisco.com/thread/12148>

Το συγκεκριμένο αντικείμενο άπτεται των γνωστών υπηρεσιών Διοίκησης Ρίσκου (Risk Management). Στις μέρες μας, πλέον, οι περισσότερες από αυτές τις λειτουργίες έχουν τυποποιηθεί μέσω διαφόρων οργανισμών πιστοποίησης της αξιοπιστίας των διαδικασιών. Ένας από αυτούς είναι ο κώδικας ISO/IEC 27002:2005 σχετικά με την Διοίκηση της Ασφάλειας των Πληροφοριών, από τον οποίο προβλέπονται οι ακόλουθοι τομείς (iso.org, 4/11/2011):

- Πολιτική Ασφαλείας (security policy),
- Οργάνωση της Ασφάλειας Πληροφοριών (organization of information security),
- Διαχείρισης Κεφαλαίου (asset management),
- Ασφάλεια Ανθρωπίνων Πόρων (human resources security),
- Ασφάλεια Φυσικών – Υλικών Πόρων (physical and environmental security),
- Διοίκηση Επικοινωνιακών Λειτουργιών (communications-operations manag.),
- Έλεγχος Πρόσβασης (access control),
- Απόκτηση Πληροφοριακών Συστημάτων (information systems acquisition),
- Ανάπτυξη και Συντήρηση (development and maintenance),
- Διοίκηση Επεισοδίων Ασφάλειας (information security incident management),
- Επιχειρηματικής Ροής (business continuity management) και
- Πειθαρχίας στους Κανονισμούς (regulatory compliance).

Στο ξεκίνημα του το διαδίκτυο, ως κατεξοχήν τεχνοκρατικής φύσης εφεύρημα, ήταν επόμενο, σταδιακά με την μεγέθυνσή του, να αποκτήσει τους δικούς του ειδικούς, οι οποίοι αρχικά ήταν λίγοι (τεχνο-ελίτ). Αυτοί θα μπορούσαν να καλύψουν επί τω πλείστο τις επί μέρους του ανάγκες, όπως ο προγραμματισμός, οι επιδιορθώσεις των εξαρτημάτων και η ασφάλεια. Σε αυτά τα πρόσωπα που διατηρούσαν είτε ερασιτεχνική, είτε επαγγελματική σχέση βρίσκονται οι ρίζες του συγκεκριμένου τύπου «κυβερνοαπειλής».

Οι διάφοροι χαρακτηρισμοί που προσδόθηκαν κατά καιρούς σε αυτά τα άτομα, προκαλούσαν σύγχυση στους μη «μυημένους». Πολύ σημαντικό ρόλο βεβαίως έπαιξαν και τα MME, τα οποία προτίμησαν, τελικά, να προσδιορίζουν με τη λέξη «χάκερ» (hacker) *οποιοδήποτε διεισδύει σε έναν Η/Υ δίχως νόμιμη εξουσιοδότηση*. Εντούτοις, θα δείξουμε συνοπτικά γιατί θα πρέπει να κατανοηθεί η βασική διαφορά μεταξύ του εσφαλμένου χαρακτηρισμού «χάκερ» και του ορθού «κράκερ» (cracker). Σύμφωνα με τον Μ. Καστέλς⁵¹, οι χάκερ αποτελούν ένα συνιδρυτικό και αναπόσπαστο κομμάτι του κυβερνοχώρου. Τα βασικά χαρακτηριστικά τους είναι οι τεχνογνωστικές δεξιότητές που διαθέτουν και η ελευθεριότητα⁵², η οποία συνιστά

⁵¹ Οι τέσσερις κατηγορίες με αξιολογική σειρά είναι οι ακαδημαϊκοί, οι χάκερ, τα μέλη των εικονικών κοινοτήτων και οι επιχειρηματίες (Castells, 2001/2003, 69)

⁵² Ενώ στις ΗΠΑ αυτός ο όρος συνδέεται με ένα φιλελεύθερο οικονομικό πνεύμα, εδώ τον χρησιμοποιούμε με τις ευρωπαϊκές του προσλαμβάνουσες. Σύμφωνα με αυτές, κυριαρχεί μια ιδεολογική τάση η οποία προτάσσει πάνω από όλα την αξία της ατομικής ελευθερίας (σ. 62).

καθοριστικό συστατικό της κουλτούρας τους. Αυτό το τελευταίο γνώρισμα είναι που δημιούργησε την προαναφερθείσα παρεξήγηση.

Για να κατανοήσουμε αυτό το θέμα, θα πρέπει να αποσαφηνιστεί μια πολύ σημαντική όψη του ζητήματος της ασφάλειας των Η/Υ (και των δικτύων τους). Όσο η τεχνολογία αναπτύσσεται, τόσο διατίθενται βελτιωμένα συστήματα (π.χ. σε δυνατότητες αποθήκευσης, σε ταχύτητες επεξεργασίας κοκ). Η διάθεση όμως στην αγορά αυτών των συστημάτων δεν σημαίνει ότι καθιστά εφικτό, πριν τη χρήση τους, να εντοπιστούν οι ενδεχόμενες νέες τρωτότητες (Libisci, 2009, 19). Τους ανθρώπους λοιπόν οι οποίοι αρέσκονται στην εξεύρεση και γνωστοποίηση αυτών των τρωτοτήτων, που προκύπτουν κάθε φορά, τους καλούμε χάκερ. Σε αντίθεση με αυτούς, τα άτομα που αρέσκονται να εξερευνούν τα εν γένει κενά των νέων τηλεπικοινωνιακών προϊόντων της αγοράς, ώστε να τα εκμεταλλεύονται και συχνά να τα καταστρέφουν -εκτός από εγκληματίες- καλούνται κράκερς⁵³.

Ήταν επόμενο οι ηγεσίες των κρατών να θελήσουν να χρησιμοποιήσουν αυτούς τους δεξιότητες του είδους, για τους δικούς τους πολιτικό-στρατιωτικούς σκοπούς. Θα πρέπει ωστόσο να κατανοηθεί πως, ανεξαρτήτως αν ξεκίνησαν ως χάκερ ή κράκερ, αυτό που επιστρατεύονται να κάνουν δεν συνάδει με καμία διάταξη του Διεθνούς Δικαίου. Αυτό δε, συνάμα με τη δυνατότητα πραγματοποίησης οποιασδήποτε διείσδυσης ανώνυμα, καθιστά αναγκαίο και εφικτό το πέπλο μυστικότητας που καλύπτει τα γεγονότα αυτής της θεματικής κατηγορίας.

Αυτό, συνεπώς, που θέλουμε να τονίσουμε είναι ότι η μοναδικότητά της έγκειται στην «κλειστή» πτυχή της κοινωνικής της φύσης. Σε αντίθεση με την προηγούμενη (των Υποδομών), της οποίας εξ' ορισμού ο σκοπός είναι να πλήξει διάφορες κοινωνικές λειτουργίες, με τις όποιες δυνητικές προεκτάσεις. Εξάλλου, οι δράστες αυτών των επιθέσεων ανήκουν σε συγκεκριμένες κοινωνικές ομάδες, όπως οι δυσαρεστημένοι (από το μέρος της αγοράς που κατέχουν) ιδιωτικοί φορείς, οι αυτόνομοι (συχνά ανήλικοι) λεγόμενοι χάκερς και τα μέλη του οργανωμένου εγκλήματος (Watts, 2010). Επιπροσθέτως, αυτή η κοινή αρνητική σχέση τους με το συνολικό κοινωνικό σχηματισμό, στον οποίο ανήκουν ενισχύει την αναγκαιότητα της άδηλη δράσης τους.

Οι βασικοί λόγοι για τους οποίους αυτοί οι «απρόσκλητοι» επισκέπτες οργανώνονται από ένα κράτος, ώστε να επιτεθούν σε ένα άλλο, είναι οι εξής:

⁵³ Κράκερ είναι ένα άτομο που μπλοκάρει τον Η/Υ κάποιου άλλου, αποσκοπώντας στο «κακόβουλο κέρδος» (<http://searchsecurity.techtarget.com/definition/cracker>).

- Η παρακολούθηση της πληροφοριακής ροής του αντιπάλου (cyber-espionage).
- Η αλλοίωση ή διακοπή της πληροφοριακής ροής του αντιπάλου (cyber-sabotage ή exploitation).

Επιπρόσθετα, όπως δηλώνει και ο αντιπρόεδρος των θεμάτων έρευνας απειλών, Dmitri Alperovitch, «υπάρχει ο μύθος της αναμονής ενός Περλ Χάρμπορ, αλλά τι γίνεται με τα χιλιάδες μικρότερα χτυπήματα; Επικίνδυνες δεν είναι μόνον οι μέγα-καταστροφές του τύπου της διακοπής ηλεκτρικού ρεύματος». Οι μικρότερης έκτασης απειλές και ειδικότερα η υποκλοπή κρίσιμων εθνικών μυστικών είναι δυνατό να δημιουργήσουν μεγάλα κρατικά προβλήματα Αυτό είναι και η πρώτη φροντίδα, για την οποία πρέπει να μεριμνήσει και ο ιδιωτικός τομέας.

Ένα άλλο πεδίο εφαρμογής, από τα πρώτα που επιχειρήθηκαν στο στρατιωτικό τομέα (οι πρώτες επιχειρησιακές ενέργειες εμφανίζονται κατά τον δεύτερο παγκόσμιο πόλεμο, εξαιτίας της εισαγωγής του RADAR), είναι η εξέλιξη και η συσχέτιση του ηλεκτρονικού πολέμου (Electronic Warfare) με τις τεχνολογίες του διαδικτύου.

Καταρχάς, σύμφωνα με το σχετικό εγχειρίδιο του υπουργείου άμυνας η αποστολή του Ηλεκτρονικού Πολέμου είναι η *ηλεκτρονική κυριαρχία*. Αναλυτικότερα, ο Ηλεκτρονικός Πόλεμος συνιστά μέρος της αεράμυνας των ενόπλων δυνάμεων και προσδιορίζεται ως «η στρατιωτική ενέργεια που αφορά την χρησιμοποίηση ηλεκτρομαγνητικής ενέργειας προς καθορισμό, εκμετάλλευση, υποβιβασμό ή παρεμπόδιση της εχθρικής χρησιμοποίησης του ηλεκτρομαγνητικού φάσματος». Οι λειτουργίες του είναι οι εξής:

- *Μέτρα Υποστήριξης* (Electronic Support Measures - ESM⁵⁴): έρευνα – αποκάλυψη – εντοπισμός – ανάλυση της εκπεμπόμενης Η/Μ ενέργειας, με σκοπό την εκμετάλλευση της (άρα, Άμυνα).
- *Ηλεκτρονικά Αντίμετρα* (Electronic Counter Measures - ECM): παρεμπόδιση ή ελάττωση της αποτελεσματικής χρησιμοποίησης των ηλεκτρονικών συστημάτων του εχθρού (άρα, Επίθεση).
- *Ηλεκτρονικά Προστατευτικά Μέτρα* (Electronic Protective Measures - EPM): «απενεργοποίηση» εχθρικών αντιμέτρων με ενεργητικά ή παθητικά μέτρα.
- *Υποστήριξη Πληροφοριών*.

⁵⁴ Η συσκευή ESM είναι ένας αισθητήρας - δέκτης, του οποίου η λειτουργία ομοιάζει το ραδιόφωνο. Έτσι, αποτελούν πηγή πληροφοριών για την αποκάλυψη των εχθρικών ενεργειών.

Η τελευταία λειτουργία έγινε στην εποχή μας ο συνδυαστικός κρίκος για συσχέτιση με το διαδίκτυο. Αρχικά, τα είδη των πληροφοριών που μας ενδιαφέρουν εδώ, είναι:

- *Πληροφορίες Επικοινωνιών* (COMMunications INTelligence) με εστίαση στη γνώση των εχθρικών συστημάτων επικοινωνιών.
- *Ηλεκτρονικές Πληροφορίες* (ELEctronic INTelligence) με εστίαση στη γνώση των εχθρικών μη επικοινωνιακών ηλεκτρομαγνητικών ακτινοβολιών.
- «*Διαβιβαστικές*»⁵⁵ *Πληροφορίες* (SIGnal INTelligence) με γενικό ενδιαφέρον για τη λοιπή την επικοινωνιακή και την ηλεκτρονική εχθρογνωσία.

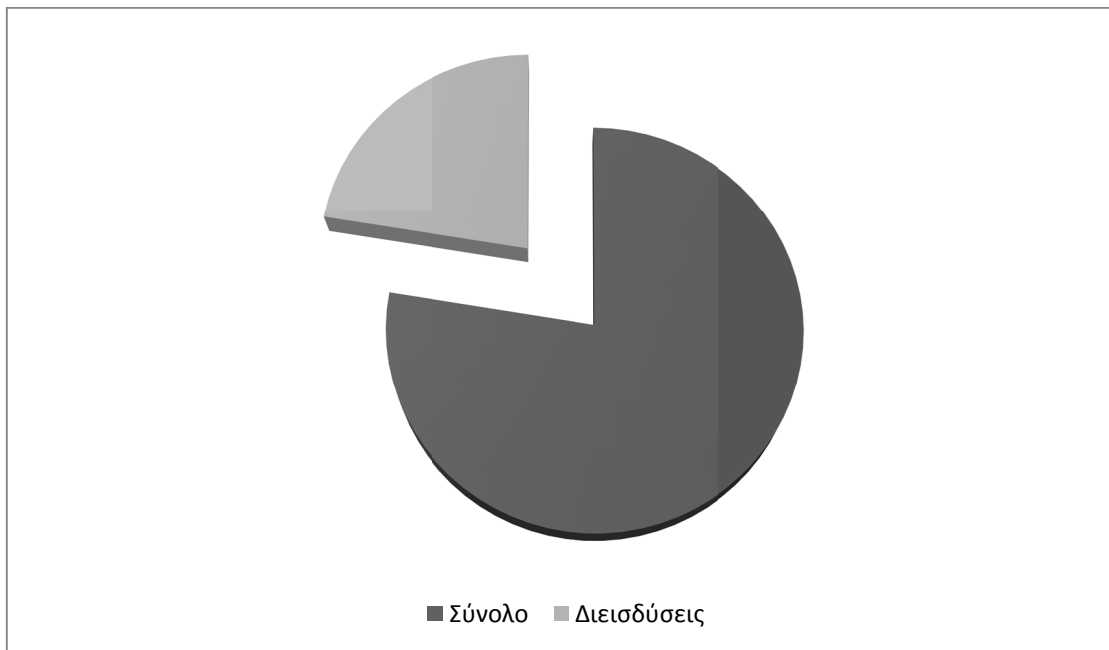
Όλες αυτές όμως οι λειτουργίες υλοποιούνται μέσα από δίκτυα των συστημάτων Διοίκησης, Ελέγχου, Επικοινωνιών και Η/Υ. Οι επιδιώξεις τους για την Ασφάλεια των Επιχειρήσεων (Operation Security) κάνουν δυνητική πιθανές τις Παραπλάνηση (Military Deception), Παρεμβολή (Jamming), ακόμα και Φυσική Καταστροφή (Physical Destruction). Τέλος, ένας τρόπος εκπλήρωσης των εν λόγω αντικειμενικών σκοπών είναι η μη εξουσιοδοτημένη διείσδυση στο διαδίκτυο.

4.3.2 Ποσοτικός Προσδιορισμός

Σε αυτήν την θεματική κατηγορία (category) εντοπίστηκαν συνολικά **91** γραμματικές αναφορές (items). Η συμμετοχή ανήλθε σε ποσοστό 28,9%, το οποίο αντιστοιχεί στη δεύτερη θέση της κατάταξης (corpus) μας. Οπότε, το μερίδιο που έχουν οι *Διεισδύσεις* στη συγκεντρωτική κατανομή ανέρχεται κατά τι παραπάνω από το ένα τέταρτο (1/4) του συνόλου (Σχήμα 15).

⁵⁵ Ο όρος «Διαβίβαση» χρησιμοποιείται για μια ευρύτερη ειδίκευση στις ένοπλες δυνάμεις και εδώ αναφέρεται -ενδεχομένως αδόκιμα- μόνο για μεταφραστικούς λόγους.

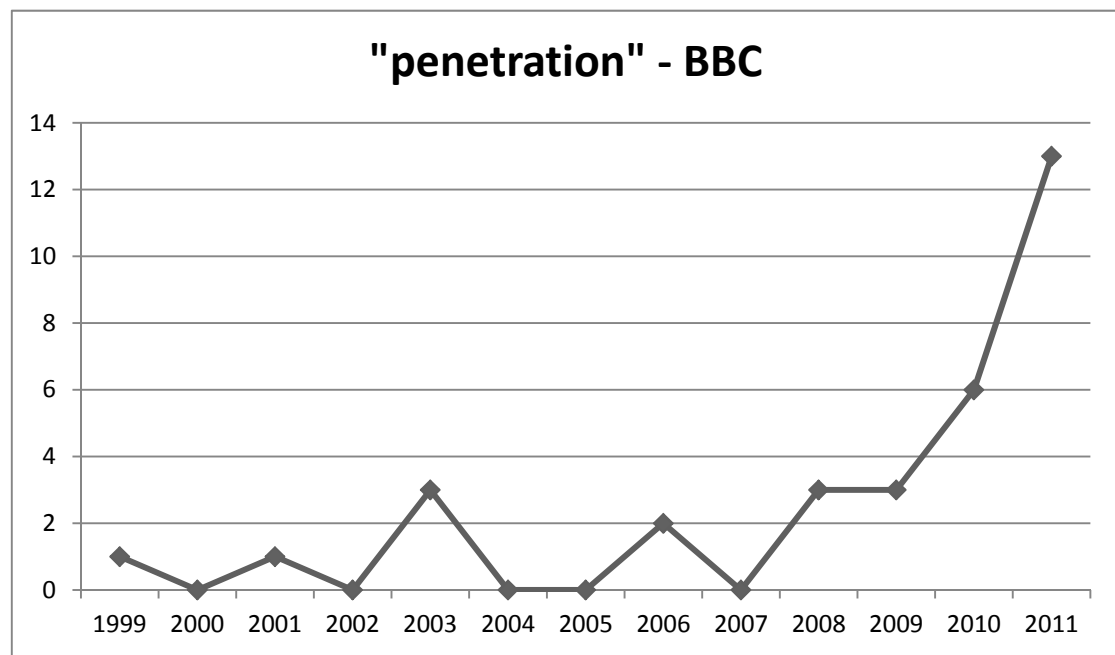
Σχήμα 15. Συγκεντρωτικό Μερίδιο «ΔΙΕΙΣΔΥΣΕΩΝ»



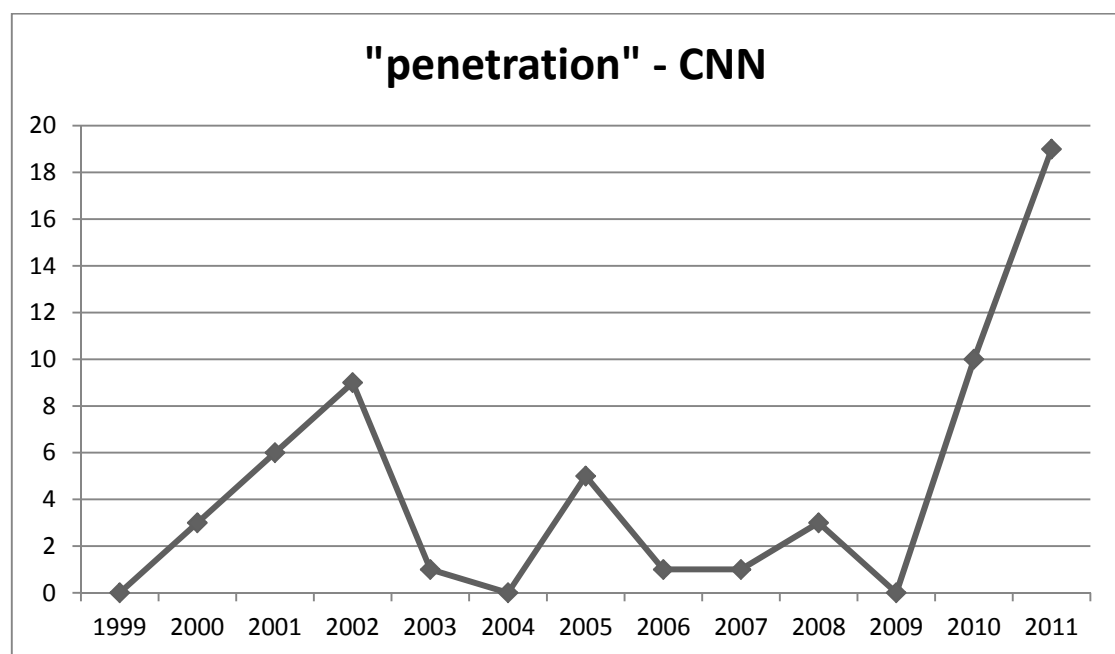
Αν αναζητήσουμε αναλυτικότερα την προέλευση της εν λόγω κατανομής, τότε μπορούμε να δούμε πως από το BBC έχουμε 33 αναφορές (σε σύνολο 150) με αναλογούν ποσοστό 22,0%. Η διαχρονική τάση εμφανίζεται χαμηλή στην αρχή και μέση και ιδιαίτερα αυξητική στο τέλος (Σχήμα 15). Όσον αφορά το CNN έχουμε 58 αναφορές (σε σύνολο 165) με αναλογούν ποσοστό 35,2%. Η διαχρονική τάση μπορεί να χαρακτηριστεί αυξητική μόνο στο τέλος, με μικρή παρόμοια ένδειξη στην αρχή, χωρίς πάντως να μπορεί να περιγραφεί ότι διαθέτει σταθερότητα (Σχήμα 16).

Επίσης, δεν μπορούμε να υποστηρίξουμε, πως υφίσταται μια σχετική σταθερότητα, ούτε και στη διακύμανση των θέσεων που καταλαμβάνει αυτή η κατηγορία στο κάθε μέσο. Ο λόγος είναι ότι ενώ στο BBC φθάνει μόλις στην τρίτη θέση, με έξι μονάδες υπολειπόμενο ποσοστό από το συγκεντρωτικό της (22,0% έναντι 28,9%), στο CNN καταλαμβάνει την πρώτη θέση με αρκετά υψηλό ποσοστό (35,2%), το οποίο αποτελεί και το δεύτερο μεγαλύτερο γενικά.

Σχήμα 16. Διαχρονική Τάση «Διεισδύσεων» – BBC



Σχήμα 17. Διαχρονική Τάση «Διεισδύσεων» – CNN



4.3.3 Ανάλογα Κυβερνο-επεισόδια

Έχουν δει το φως της δημοσιότητας πολλές περιπτώσεις αυτής της κατηγορίας. Ορισμένες εκφράζουν υποψίες για την καταβολή συνεχών προσπαθειών από κράτη, υποκλοπής κρίσιμων δεδομένων. Δίχως, πάντως, να είναι δυνατόν να αποδειχθεί οτιδήποτε άλλο, πέρα του γεγονότος της επίθεσης. Ένα από τα «κλασικά» πλέον παραδείγματα είναι οι κατηγορίες των αμερικανών για τις εχθρικές ενέργειες του

κινεζικού κυβερνοστρατού⁵⁶ (<http://blogs.sch.gr/eylignou/archives/1047>, 17/11/2010). Μια από αυτές, μέμφεται συγκεκριμένη κινεζική εταιρεία τηλεπικοινωνιών, της οποίας δρομολογητές (routers)⁵⁷ βρέθηκαν υπεύθυνοι για την εκπομπή παρεμβολών για 18 συνεχή λεπτά, στις 8 Απριλίου του 2010. Δέκτες των κακόβουλων ηλεκτρονικών μηνυμάτων υπήρξαν η Γερουσία, το Υπουργείο Άμυνας, το Υπουργείο Εμπορίου και η ΝΑΣΑ (<http://www.spacewar.com>, 17/11/2010).

Μια περίπτωση, η οποία δείχνει στην πράξη τον τρόπο που μπορεί να λειτουργήσει η συνάφεια του ηλεκτρονικού πολέμου -τον οποίο αναλύσαμε θεωρητικά στο προηγούμενο κεφάλαιο- με τον κυβερνοπόλεμο, θα περιγράψουμε τώρα. Πρόκειται για έναν ιό, ο οποίος έπληξε τα λειτουργικά συστήματα μη επανδρωμένων αεροσκαφών (Unmanned Aerial Vehicles - UAV) των ενόπλων δυνάμεων των ΗΠΑ. Τα μη επανδρωμένα αεροσκάφη, έχουν χαρακτηριστεί και ως «οι μηχανές αυτόματης παρατήρησης», αποτελούν ένα καινοτόμο είδος όπλου, του οποίου η αξία καθιερώθηκε κυρίως μετά τους πολέμους του Κόλπου, τη δεκαετία του '90. Η κύρια αποστολή του συνίσταται στην ακριβή συλλογή πληροφοριών. Τα συγκεκριμένα κατευθυνόμενα αεροσκάφη μπορούν να εξοπλιστούν με κάμερα και αισθητήρες (κυρίως εικόνας), ώστε να συλλέγουν δεδομένα σε δύσκολες καιρικές συνθήκες ημέρας και νύχτας, δίχως να διακυβευθεί ανθρώπινη απώλεια (fas.org, 17/5/2007). Επιπλέον, τα πιο εξελιγμένα μοντέλα, αν χρειαστεί, έχουν τη δυνατότητα καταστροφής στόχων, είτε με πυραύλους (Hellfire και Spike), είτε με κατευθυνόμενες με Laser βόμβες (LGB), τις οποίες φέρουν κάτω από τα πτερύγια τους. Συμπερασματικά, λοιπόν, είναι σημαντικό να αντιληφθεί κανείς, πόσο σημαντικό μέρος της στρατιωτικής ισχύος είναι γενικά αυτό το όπλο για τα κράτη. Ειδικότερα δε, για τις ΗΠΑ, για τις οποίες η χρήση του στην εμπλοκή τους στο Ιράκ και Αφγανιστάν είναι σχεδόν καθημερινή.

Σχετικά με το συγκεκριμένο επεισόδιο, σε επίσημη ανακοίνωση του υπουργείου άμυνας των ΗΠΑ, αναφέρεται ότι ιός διείσδυσε στα συστήματα διοίκησης και ελέγχου των εν λόγω αεροσκαφών, με αποτέλεσμα τη μερική απώλεια ελέγχου πλοήγησής τους. Όπως αναφέρει ιθύνων αρθρογράφος του περιοδικού Wired, Noah Schactman, είναι πραγματικά δύσκολη η ανίχνευση της προέλευσης του προβλήματος

⁵⁶ Πηγή: Financial Times (10/11/2008).

⁵⁷ Ένας δρομολογητής (router) αναλαμβάνει τη διασύνδεση μεταξύ δύο δικτύων. Ο Router είναι συσκευή στην οποία συνδέονται περισσότεροι του ενός Η/Υ ενός τοπικού δικτύου. Ο δρομολογητής αναλαμβάνει τη μεταβίβαση των δεδομένων από και προς τον κατάλληλο υπολογιστή του δικτύου, με βάση συγκεκριμένα κριτήρια που θέτει ο διαχειριστής του, όπως διεύθυνση IP, κανόνες NAT[†], κ.ά. (<http://www.hellascams.gr/grc/Router.html>, 4/11/2011).

και ένας από τους λόγους είναι ο τηλεχειρισμός των αεροσκαφών από την αρμόδια στρατιωτική εγκατάσταση της Νεβάδα των ΗΠΑ.

Οι πρώτες παρατηρήσεις έδειξαν «αυτόματες» πληκτρολογήσεις, οι οποίες ακολουθούσαν την επεξεργασία δεδομένων, με αποτέλεσμα σε πρώτη φάση να είναι άγνωστο το μέγεθος της απώλειας διαβαθμισμένων πληροφοριών όλου του δικτύου. Επίσης, την ανησυχία ενίσχυσε ότι οι πρώτες αμυντικές μέθοδοι στάθηκαν ανεπαρκείς. Έτσι, οδηγήθηκαν στις σκέψεις απενεργοποίησης των σκληρών δίσκων αποθήκευσης του συστήματος, ώστε να αποφευχθούν νέες απώλειες. Και για αυτή, όμως, τη μέθοδο διατηρήθηκαν ορισμένες αμφιβολίες, επειδή υπήρχε το προηγούμενο, του 2008, προσβολής από ιό μετακινούμενων (γνωστών ως εξωτερικών) σκληρών δίσκων του ίδιου του πενταγώνου.

Σε σχετική ομιλία του ο απερχόμενος υπουργός άμυνας των ΗΠΑ, William Lynn, και με την παρουσία του νυν, Leon Panetta, τόνισε πως τα bits and bytes⁵⁸ θα αντικαταστήσουν τις σφαίρες και τις βόμβες κατά τον 21^ο αιώνα (edition.cnn.com, 10/10/2011).

Μια ακόμη περίπτωση αποτελεί η πρόσφατη κυβερνοεπίθεση στο Διεθνές Νομισματικό Ταμείο. Υποψίες ότι με ένα κακόβουλο λογισμικό, το οποίο εγκαταστάθηκε με τη μέθοδο των «στοχευόμενων» ηλεκτρονικών μηνυμάτων που στέλνονταν σε συγκεκριμένους χρήστες (spear phishing), ύποπτες μεταφορές δεδομένων. Ο Τομ Κέλερμαν, τέως εμπειρογνώμονας στα θέματα κυβερνοασφαλείας του ΔΝΤ και νυν στέλεχος της International Cyber Security Protection Alliance, επιβεβαίωσε το γεγονός στο Reuters (<http://portal.kathimerini.gr>, 14/6/2011).

Όσον αφορά τον ιδιωτικό τομέα, τα περιστατικά είναι επίσης πολλά. Ένα από τα πιο πρόσφατα αφορά μια από τις μεγαλύτερες βαριές βιομηχανίες στον κόσμο και την πρώτη αμυντική βιομηχανία της Ιαπωνίας, τη Mitsubishi⁵⁹. Το συμβάν αφορά την υποκλοπή βιομηχανικών και κρατικών μυστικών, τα οποία το πιθανότερο είναι να αφορούσαν το σχεδιασμό σύγχρονων οπλικών συστημάτων (όπως πύραυλοι και υποβρύχια). Αυτό το γεγονός δεν αφορά ασφαλώς μόνο την εταιρεία, αλλά αναβαθμίστηκε σε ζήτημα εθνικής ασφάλειας. Έτσι, η ιαπωνική κυβέρνηση απαίτησε

⁵⁸ Πρόκειται για τις στοιχειώδεις μονάδες μέτρησης του μεγέθους προγραμματισμού των Η/Υ.

⁵⁹ Ένα από τα γνωστότερα προϊόντα που κατασκευάζει η Mitsubishi, μεταξύ άλλων, είναι οι συστοιχίες πυραύλων Patriot.

την άμεση διαλεύκανση του θέματος, με την απειλή της ενεργοποίησης ρήτρας, η οποία δύναται να διακόψει κρατικά συμβόλαια ύψους δισεκατομμυρίων δολαρίων.

Ο εντονότερος φόβος αφορά την εισβολή χάκερ στα δίκτυα της εταιρείας και την επικίνδυνη πρόσβασή του στα πυρηνικά εργοστάσια. Μέχρι στιγμής έχει ανακοινωθεί ο εντοπισμός οκτώ διαφορετικών ειδών ιών, σε 45 διακομιστές και 38 προσωπικούς υπολογιστές σε 11 τοποθεσίες. Η ιαπωνική εφημερίδα Yomiuri, έγραψε ότι οι πρώτες αναλύσεις έδειξαν ότι τα μολυσμένα συστήματα συνδέονταν σε 14 τοποθεσίες του εξωτερικού, όπως στην Κίνα, το Χονγκ Κονγκ, τις ΗΠΑ και την Ινδία (<http://news.in.gr>, 1/10/2011).

Παρόμοια είναι και η περίπτωση της Sony. Τα χτυπήματα στο γνωστότερο βιντεοπαιχνίδι της ιαπωνικής εταιρείας (PlayStation), αλλά και άλλων λιγότερο γνωστών, καθώς επίσης και οι υποκλοπές των κωδικών ονομάτων πρόσβασης των χρηστών (passwords) από την ομάδα hacker Lulz Security γίνονται κατά εξακολούθηση. Πιο συγκεκριμένα οι hackers απόκτησαν (μη εξουσιοδοτημένη) πρόσβαση σε 177.000 διευθύνσεις του ηλεκτρονικού ταχυδρομείου (e-mails) από τη γαλλική ιστοσελίδα της Sony Pictures. Ενώ, πριν μια εβδομάδα παρόμοιο γεγονός συνέβη με την υποκλοπή ενός εκατομμυρίου ηλεκτρονικών διευθύνσεων, με το μεγάλο κίνδυνο εκμετάλλευσης ευαίσθητων προσωπικών δεδομένων της αντίστοιχης αμερικανικής εταιρείας (U.S. Sony Pictures) (edition.cnn.com, 24/6/2011).

Αυτά τα γεγονότα θεωρούνται, πλέον, πολύ συνηθισμένα στο διεθνές σκηνικό στην περιοχή ασφαλείας του κυβερνοχώρου. Αν μια τέτοιου μεγέθους επιχείρηση, από τις πρώτες στον κόσμο στο αντικείμενο της υψηλής τεχνολογίας, δεν μπορεί να αποφύγει τέτοιες επιθέσεις, πόσο μάλλον οι μικρότερες. Εξάλλου, περίπου 26 εκατομμύρια προσωπικές πληροφορίες υποκλάπηκαν το 2006 από το δίκτυο των βετεράνων των ΗΠΑ (U.S. Department of Veterans Affairs). Και σε αυτήν την περίπτωση φαίνεται ότι η παγκοσμιοποίηση του φάσμα και η διακλαδικότητα της αλληλοεπίδρασης των κυβερνοεπιθέσεων. Θεωρείται αδύνατον πλέον ένα χτύπημα σε μια επιχείρηση να μην εμπλέξει τον δημόσιο τομέα, αλλά και άλλα -όχι απαραίτητως όμορα- κράτη.

Στις 16/1/2011 η The New York Times έγραψε πως οι αμερικανικές και εβραϊκές μυστικές υπηρεσίες συνεργάστηκαν στην ανάπτυξη ενός κακόβουλου λογισμικού το

οποίο θα μπορούσε να παρακωλύσει τις ιρανικές προσπάθειες κατασκευής πυρηνικής βόμβας⁶⁰ (<http://www.spacedaily.com>, 1/8/2011).

Η επιτυχής έκβαση αυτού του προγράμματος θεωρήθηκε ότι ανοίγει μια νέα εποχή στον κυβερνοπόλεμο (*Newsroom* ΔΟΛ, 24-9-2010). Το βασικότερο επιχείρημα για αυτό είναι ότι πρόκειται για τον πρώτο ιό, ο οποίος έχει επιπτώσεις άμεσες στο φυσικό περιβάλλον. Οι βεβαιότητες για την κρατική παρέμβαση προκύπτουν από το γεγονός ότι η περιπλοκότητά του προδίδει ανάγκες υψηλής χρηματοδότησης. Σύμφωνα με αυτή την επιχειρηματολογία, κατηγορήθηκε η γερμανική εταιρεία Siemens για την «φιλοξενία» του πειραματικού σταδίου στις εγκαταστάσεις της. Από την μεριά της η εταιρεία, σε επίσημη ανακοίνωσή της ισχυρίστηκε ότι δεν είχε καμία συμμετοχή (Γαλλικό Πρακτορείο Ειδήσεων – AFP, 2/8/2011)⁶¹. Ωστόσο, η εταιρεία διαβεβαίωσε ότι έχουν καλυφθεί όλα τα κενά του λογισμικού, τα οποία έχουν εντοπιστεί. Ο Ρέλ Σούουενμπερκ, στέλεχος της εταιρείας ασφαλείας δικτύων και Η/Υ «Kapersky Labs Americas», εκτίμησε πως ο συγκεκριμένος ιός είναι δυνατόν να μολύνει διάφορα συστήματα και εκτός διαδικτύου, μέσω των USB (*Newsroom* ΔΟΛ, 24/9/2010).

Όσον αφορά το τεχνικό μέρος, ο ιός ανακαλύφθηκε τον Ιούνιο του 2010. Η διαδικασία εξάπλωσής του ξεκίνησε από την ανακάλυψη κάποιων κενών στο λειτουργικό σύστημα των Windows της Microsoft (3/8/2011, <http://en.wikipedia.org/wiki/Stuxnet>). Σύμφωνα με τις Financial Times, ο ιός μένει κρυμμένος στη μνήμη των τερματικών και όταν ανιχνεύσει το στόχο του δραστηριοποιείται. Οι ενδεχόμενες βλάβες που μπορεί να προκαλέσει είναι κυρίως στη λειτουργία των βαλβίδων.

Σχετικά με το ιστορικό της συγκεκριμένης περίπτωσης, οι ετοιμασίες της κυβερνοεπίθεσης, με τη χρήση του ιού Stuxnet, διήρκησαν έναν περίπου χρόνο και πραγματοποιήθηκαν την περίοδο μεταξύ του Ιουνίου του 2009 και του Μαΐου του 2010. Όπως επιβεβαιώνουν και οι αντιδράσεις του προέδρου του Ιράν, Mahmoud Ahmadinejad, παρατηρήθηκε συγκεκριμένο πρόβλημα στον έλεγχο ενός πυρηνικού αντιδραστήρα. Η υπόθεση, όμως, δεν έχει λήξει, όπως είχε εκτιμηθεί. Η αιτία είναι ότι δίκτυα υπολογιστών σε ευρωπαϊκές βιομηχανικές εγκαταστάσεις επεξεργάζονται μια παρεμφερή τεχνολογία. Πρόκειται για ένα είδος λογισμικού, το οποίο ονομάζεται

⁶⁰ Συγκεκριμένα τα σενάρια μιλάνε για τον αντιδραστήρα στον πυρηνικό σταθμό του Μπουσέρ και τη μονάδα εμπλουτισμού ουρανίου στη Νατάνζ, στο Ιράν.

⁶¹ «Η Siemens δεν έχει πουλήσει κανένα λογισμικό εκεί και δεν έχει σχέση με το ιρανικό πυρηνικό πρόγραμμα» δήλωσε εκπρόσωπος της εταιρείας. Συνολικά έχουν εντοπισθεί 15 πελάτες που έχουν πληγεί από τον ιό, αλλά δεν έχουν υπάρξει επιπτώσεις στην παραγωγή τους, αναφέρει η Siemens.

Δούρειος Ίππος (Trojan Horse) και είναι ικανό να παραπλανήσει τον στόχο της, ώστε να προκαλέσει παρόμοιες βλάβες. Τα παραπάνω διαβεβαιώνει στο επίσημο ιστολόγιο του (blog) ο Liam Murchu, ο οποίος έχει τη θέση του υπεύθυνου ασφαλείας της εταιρίας Symantec. Πιο συγκεκριμένα γράφει ότι ευρωπαίοι ερευνητές έχουν προωθήσει σε αυτόν εφαρμογές ενός νέου κακόβουλου λογισμικού, επονομαζόμενου «Duqu». Ο σκοπός του είναι να διεισδύσει σε «αντίπαλα» πληροφορικά συστήματα, δίχως να γίνει αντιληπτός και εν συνεχεία να συγκεντρώσει χρήσιμα πληροφοριακά δεδομένα για τα πρωτόκολλα, τις διαδικασίες και γενικότερα, τον τρόπο λειτουργίας. Επιπρόσθετες ειδικότερες στοχεύσεις ενδεχομένως να αφορούν την χαρτογράφηση της αρχιτεκτονικής των συστημάτων. Επίσης, παρατηρεί ότι οι μεγάλες ομοιότητές του με τον Stuxnet, προδίδουν πως το πιθανότερο είναι να τον έχουν κατασκευάσει οι ίδιοι προγραμματιστές.

Σε ένα άλλο σχόλιο του, στο περιοδικό τεχνολογίας Wired, αναφέρει ότι το πιο εκπληκτικό είναι ότι αυτά τα πρόσωπα μπορούν ακόμα και εργάζονται στην ίδια κατεύθυνση, μετά από όλη αυτήν τη δημοσιότητα που έχει πάρει το θέμα. Αυτό τους κάνει περισσότερο επικινδύνους για μια πιο καταστροφική κυβερνοεπίθεση. Πάντως, στο ίδιο περιοδικό αναφέρεται πως ο γεωγραφικός εντοπισμός τους είναι αδύνατον. Κάτι που ενισχύεται ακόμη περισσότερο, διότι ο ιός έχει τη δυνατότητα ταχύτατων μεταλλάξεων, οι οποίες εμποδίζουν την ταυτοποίηση τους.

Οι Guilherme Venere και Peter Szor της αμερικανικής εταιρείας πληροφορικής ασφαλείας, McAfee Labs, ανακοίνωσαν την πεποίθησή τους ότι τα λογισμικά Duqu και Stuxnet δεν υπάρχει καμία αμφιβολία ότι έχουν τους ίδιους προγραμματιστές. Παραθέτοντας την επιχειρηματολογία τους για αυτήν τη θέση, εξηγούν ότι και τα δύο κακόβουλα προγράμματα χρησιμοποιούν κλεμμένα ψηφιακά πιστοποιητικά δύο εταιρείες στην πρωτεύουσα της Ταϊβάν, Τάιπεϊ, οι οποίες δραστηριοποιούνται στο ίδιο επιχειρηματικό αντικείμενο (spacedaily.com, 20/10/2011).

Μια ακόμα περίπτωση υποκλοπών διαμέσου του κυβερνοχώρου αποκαλύφθηκε από το καναδικό Κέντρο Διεθνών Σχέσεων Μουνκ του Τορόντο. Οι επιστήμονες που κατάφεραν να φέρουν στην επιφάνεια αυτήν την υπόθεση δήλωσαν πως ολόκληρο το δίκτυο, το οποίο υπέκλεπτε τα δεδομένα είναι διεσπαρμένο σε ολόκληρη την κινεζική επικράτεια⁶². Οι συγκεκριμένοι Η/Υ είχαν καταφέρει να παρεισφρήσουν σε 1.295

⁶² Υπογραμμίζοντας βέβαια ότι αυτό δεν αποτελεί απόδειξη μορφής του κινεζικού κράτους.

υπολογιστές σε 103 κράτη του κόσμου. Οι περισσότεροι από αυτούς εδράζονταν σε πρεσβείες, κρίσιμες κυβερνητικές υπηρεσίες και επιπρόσθετα σε πολιτιστικά ιδρύματα των εξόριστων Θιβετιανών στις Ινδίες, το Βέλγιο, την Βρετανία και τις ΗΠΑ (The New York Times, 22/10/2010).

Η ανακάλυψη του γεγονότος πραγματοποιήθηκε⁶³ με αφορμή το αίτημα του αυτοεξόριστου θρησκευτικού ηγέτη του Θιβέτ, Δαλάι Λάμα, προς το καναδικό ινστιτούτο. Ο ίδιος και το επιτελείο του είχαν διακρίνει από τη συμπεριφορά των Η/Υ τους κάποιες ενδείξεις ύπαρξης κακόβουλου λογισμικού. Το επιστημονικό κέντρο που ανάλαβε την εξιχνίαση της υπόθεσης κατέληξε σε μια έκθεσή, με τίτλο «Παρακολουθώντας το GhostNet: Η έρευνα ενός δικτύου κυβερνοκατασκοπείας». Ωστόσο, το σημαντικότερο στοιχείο αυτής της έκθεσης, πέρα την παράθεση της περιγραφής των γεγονότων, είναι το συμπέρασμα ότι είναι ιδιαίτερα πιθανό η γνώση της χρήση αυτού λογισμικού να βρίσκεται στην κατοχή υποψήφιων τρομοκρατών.

Μία άλλη έκθεση η οποία δημοσιεύθηκε από δύο μέλη της ακαδημαϊκής κοινότητας του Πανεπιστημίου του Κέμπριτζ της Βρετανίας, είχε τον τίτλο «Ο Αδιάκριτος Δράκος: Παρακολούθηση του θιβετιανού κινήματος μέσω malware». Αυτοί -μετά από συνεργασία τους με το Μουνκ- κατηγορούν ευθέως την κινεζική κυβέρνηση. Πρόκειται για τους καθηγητές Ρος Άντερσον και Σισίρ Ναγκαράτζα, οι οποίοι επίσης προειδοποίησαν ότι οι αρμόδιες αρχές πρέπει να επιληφθούν, διότι η συγκεκριμένη τεχνογνωσία έχει διαδοθεί επικίνδυνα.

Από τεχνικής πλευράς, το μολυσματικό πρόγραμμα είχε τη δυνατότητα να εντοπίζει τα τερματικά, τα οποία έχουν ενσωματωμένη κάμερα και μικρόφωνο και να τα ενεργοποιεί, κατά βούληση. Κατόπιν, κατέγραφε οπτικά και ηχητικά σε όλη την ακτίνα που είχαν τη δυνατότητα οι συσκευές. Το εντυπωσιακότερο ήταν η δυνατότητα να ανάψει και να σβήσει την οθόνη, καθώς επίσης και να παρακολουθήσει την πληκτρολόγηση του χρήστη.

Οι ερευνητές του Citizen Lab⁶⁴ του Πανεπιστημίου του Τορόντο σε μια έκθεσή τους με τίτλο «Σκιές στο Σύννεφο» ("Shadows in the Cloud"), ανέφεραν ότι, πέρα των κρατικής αξίας μυστικών, διέρρευσαν προσωπικά δεδομένα σχετικά με

⁶³ Η επιτυχία του εντοπισμού της κυβερνοκατασκοπείας πιστώθηκε στο μέλος του ερευνητικού κέντρου, 34χρονου μεταπτυχιακού φοιτητή, Ναρτ Βιλνέβ.

⁶⁴ Διευθυντής του Citizen Lab, είναι ο καναδός καθηγητής Πολιτικής Επιστήμης Ρον Ντάμπερτ, ο οποίος θεωρείται ένας από τους υπέρμαχους της υπεράσπισης της ελεύθερης διακίνησης στον κυβερνοχώρο. Αυτόν τον αγώνα δίνει μέσα από το Open Net Initiative, μια σύμπραξη ομοϊδεατών ερευνητών των Πανεπιστημίων του Τορόντο, της Οξφόρδης, του Κέμπριτζ και του Χάρβαρντ (Κ. Οικονομάκου, *Έντυπη Έκδοση*, Ελευθεροτυπία, 18 Ιουλίου 2009).

οικονομικά και επαγγελματικά στοιχεία πολιτών από 31 χώρες. Όσον αφορά τα κρατικά μυστικά, δήλωσαν ότι ανακάλυψαν διαβαθμισμένα έγγραφα, όπως δύο με το χαρακτηρισμό «Απόρρητο» (Secret), έξι με το χαρακτηρισμό «Περιορισμένης διακίνησης» (Restricted) και πέντε με το χαρακτηρισμό «Εμπιστευτικό» (Confidential). Τέλος, μόνο από το γραφείο του Δαλάι Λάμα διέρευσαν περί των 1500 εγγράφων (spacewar.com, 6/4/2010). «Είναι απίστευτο. Μάλλον είναι κάτι παραπάνω από βιομηχανική κατασκοπεία» δήλωσε ο Τζέιμς Λιούις, ειδικός του αμερικανικού Κέντρου Διεθνών και Στρατηγικών Σπουδών. Αυτή η επιχείρηση επονομάστηκε Δίκτυο Φάντασμα (GhostNet). Και αφορά ίσως την μεγαλύτερη υπόθεση κυβερνοκατασκοπείας (<http://news.kathimerini.gr>, 5/8/2011).

Ο πρώιμος τύπος κυβερνοεπιθέσεων -όπως αναλύσαμε νωρίτερα- είναι το γνωστό hacking. Μια από τις πιο χαρακτηριστικές περιπτώσεις αυτού του τύπου, στις οποίες έχουμε και τη σύλληψη του υπεύθυνου hacker, είναι η γνωστή ως «υπόθεση του μαφιόζικου αγοριού (Mafiaboy)». Όπως ο ίδιος γράφει, μετά την αποφυλάκισή του, οι παράνομες επιθέσεις του διαδραματίστηκαν περί το 2000. Τις χαρακτηρίζει ριψοκίνδυνες και ανόητες, ενώ δηλώνει πως ο στόχος του ήταν ή περιπέτεια και για αυτό τον θεωρεί σχετικά «αθώο». Ωστόσο, ενδιαφέρον έχει ότι εκτιμάει πως εδώ έγκεινται οι δύο διαφορές του από τους σύγχρονους hacker.

Από τη μια πλευρά, σήμερα, είναι πολύ εύκολο να γίνεις hacker δωρεάν και μέσα σε δέκα λεπτά. Αρκεί να κατεβάσεις (download) και να εγκαταστήσεις (installation) συγκεκριμένα προγράμματα, τα οποία είναι δυνατόν να βρεις ελεύθερα στον Παγκόσμιο Ιστό. Αυτή όμως η νέα συνθήκη σου στερεί το ενδιαφέρον που σου δίνει η περιπέτεια της δική σου δημιουργίας ενός τέτοιου προγράμματος. Από την άλλη πλευρά, οι στόχοι των σημερινών hacker είναι το κυβερνοέγκλημα και η κυβερνοκατασκοπεία, διότι -ελλείψει άλλου ενδιαφέροντος- αποσκοπούν μόνο στην κερδοσκοπία. Και, τέλος, αυτές οι παράνομες δραστηριότητες είναι δυνατόν να φέρουν τεράστια κέρδη⁶⁵ (<http://edition.cnn.com>, 15/8/2011).

Το Μάιο 2001 αποκαλύφθηκε ενδεχομένως η πρώτη μεγάλη κυβερνοεπίθεση στην ιστορία. Αποδέκτης της ήταν οι ΗΠΑ, η οποία κατηγόρησε, δίχως αποδείξεις για

⁶⁵ Ενδεικτικό είναι πως στην εποχή μας η πορνογραφία και δη, διαμέσου του κυβερνοχώρου και κυρίως η παιδική εκτιμάται ότι είναι το τρίτο μεγαλύτερο έσοδο του οργανωμένου εγκλήματος παγκοσμίως, μετά την πώληση όπλων και τα ναρκωτικών.

ευθύνες τη Ρωσική Ομοσπονδία. Την ύπαρξη της ομολόγησε επίσημα η Υπηρεσία Εθνικής Ασφαλείας των ΗΠΑ (National Security Agency –NSA). Η επιχείρηση επονομάστηκε «Λαβύρινθος στο Σελινόφως» ("Moonlight Maze") και αφορούσε την υποκλοπή ψηφιακών δεδομένων από το Μάιο του 1998.

Πιο συγκεκριμένα, άγνωστοι κατάφεραν να αποκτήσουν πρόσβαση σε διαβαθμισμένα αρχεία κρίσιμων κρατικών φορέων. Ενδεικτικά, σε αυτούς συμπεριλαμβάνονται το Υπουργείο Ενέργειας, το Πεντάγωνο και η ΝΑΣΑ. Το περιστατικό αποκαλύφθηκε τυχαία από ένα ατύχημα, στα τέλη του 2000 και είναι εξαιρετικά ενδιαφέρον πως οι αρμόδιες αμερικανικές υπηρεσίες ερευνούν ακόμη τι ακριβώς συνέβη (pbs.org, 25/4/2007).

Σύμφωνα με τον James Adams⁶⁶, πρόεδρο του οργανισμού παροχής συμβουλών σε θέματα ασφαλείας iDefense, πρόκειται για τη μεγαλύτερης διάρκειας κυβερνοεπίθεση που έχουν δεχτεί οι ΗΠΑ και αποδεικνύει ότι είναι ένα θέμα που πρέπει να αντιμετωπιστεί τόσο σοβαρά, όσο και η πυρηνική απειλή.

Αν και η προηγούμενη ίσως είναι η πρώτη παγκόσμια κυβερνοεπίθεση αυτής της θεματικής κατηγορίας, θα κλείσουμε αυτό το υποκεφάλαιο με την πιο πρόσφατη και ενδεχομένως, μεγαλύτερη όλων. Επονομάστηκε «μητέρα όλων των κυβερνοεπιθέσεων» και υλοποιήθηκε από το 2006 μέχρι το Μάρτιο του 2011, όταν έγιναν αντιληπτές. Οι επιπτώσεις της εκτείνονται σε 72 δίκτυα παγκοσμίως, τα οποία ανήκουν από κυβερνήσεις και επιχειρήσεις, μέχρι διεθνή οργανισμού, όπως ακόμα και τον ΟΗΕ. Στην τελευταία περίπτωση, οι χάκερ εισέβαλαν στο πληροφορικό σύστημα της γραμματείας του Οργανισμού στη Γενεύη και από το 2008 και είχαν πρόσβαση σε όλα τα δεδομένα τα οποία είχαν αποθηκευθεί. Το γεγονός ανακάλυψε και αποκάλυψε η McAfee⁶⁷. Η εταιρεία ασφαλώς δεν μπόρεσε να αποδείξει τον υπαίτιο.

Παρόλα αυτά, ο Τζιμ Λιούις, με εξειδίκευση σε θέματα κυβερνοασφάλειας, του Κέντρου Στρατηγικών και Διεθνών Μελετών, μετά από τη σχετική επικοινωνία που είχε με τη McAfee, έκανε τις ακόλουθες δηλώσεις στο Reuters. «Θα μπορούσε να είναι οι Ρώσοι, υπάρχουν όμως περισσότερα που δείχνουν στην Κίνα παρά στη

⁶⁶ Ο J. Adams διατέλεσε αρθρογράφος των λονδρέζικων Sunday Times και του περιοδικού το οποίο επικεντρώνεται στις Διεθνείς Σχέσεις Foreign Affairs. Επίσης, έχει συγγράψει και βιβλίο με θέμα τον κυβερνοπόλεμο.

⁶⁷ Σε μια έκθεση 14 σελίδων, η οποία συντάχθηκε από τον αρμόδιο της εταιρίας, Ντμίτρι Αλπέροβιτς. Η έκθεση δημοσιοποιήθηκε στο συνέδριο για θέματα ασφάλειας δικτύων, των Black Hat, στο Λας Βέγκας (2011).

Ρωσία... Για παράδειγμα, το δίκτυο της Διεθνούς Ολυμπιακής Επιτροπής και άλλων Ολυμπιακών οργανισμών παραβιάστηκαν λίγο πριν τους Ολυμπιακούς του Πεκίνου το 2008. Και επιπλέον, στη λίστα των στόχων περιλαμβάνεται η Ταϊβάν, την οποία η Κίνα δεν αναγνωρίζει ως ανεξάρτητο κράτος».

Χαρακτηριστική είναι η έκφραση ότι «πρόκειται για τη μεγαλύτερη μεταφορά πλούτου της ιστορίας σε όρους πνευματικής ιδιοκτησίας» (news.in.gr, 4/8/2011). Οι σημαντικότεροι από τους στόχους είναι οι εξής:

- Όσον αφορά στα κράτη: οι ΗΠΑ, η Ταϊβάν, η Ινδία, η Νότιος Κορέα, το Βιετνάμ και ο Καναδάς.
- Όσον αφορά στους διεθνείς οργανισμούς: τα Ηνωμένα Έθνη, η Διεθνής Ολυμπιακή Επιτροπή, η Διεθνής Υπηρεσία Αντί-Ντόπινγκ και η Ένωση Χωρών Νοτιοανατολικής Ασίας.
- Όσον αφορά στους κλάδους του επιχειρηματικού ιδιωτικού τομέα: εργολάβοι αμυντικών συστημάτων και εταιρείες υψηλής τεχνολογίας.

Στο στόχαστρο της κυβερνοεπίθεσης τέθηκε η υποκλοπή μυστικών πληροφοριών με πολλαπλή δυνητική κρίσιμη εκμετάλλευση. Η ίδια η McAfee ονόμασε τις εν λόγω κυβερνοεπιθέσεις «Επιχείρηση Σκιώδες RAT»⁶⁸ Τα αρχικά «RAT» μεταφράζονται ως «εργαλείο απομακρυσμένης πρόσβασης».

Το πιο πρόσφατο κυβερνοεπεισόδιο αυτής της κατηγορίας που έχει δημοσιευθεί είναι μια περίπτωση κυβερνοκατασκοπείας με στόχο ορισμένους εργολάβους των αμερικανικών ενόπλων δυνάμεων. Σύμφωνα με ανακοινώσεις της εταιρείας ασφάλειας πληροφορικών συστημάτων Symantec, πρόκειται για μια από τις μεγαλύτερες εταιρείες βιομηχανικής κατασκοπείας. Η κυβερνοεπίθεση αναφέρεται ότι εκδηλώθηκε από το κινεζικό έδαφος (<http://news.in.gr>, 1/11/2011).

Στο επίκεντρο του στόχου βρέθηκαν 29 εταιρείες χημικών και 19 επιχειρήσεις, οι οποίες παράγουν προϊόντα υψηλής τεχνολογίας, με τα οποία προμηθεύουν το στρατό των ΗΠΑ. Τα ονόματα των εταιρειών δεν αποκαλύφθηκαν. Ωστόσο, τα μυστικά που υποκλάπηκαν εκτιμούνται ως πολύ σημαντικά και κρίνεται πως δίνεται μεγάλο ανταγωνιστικό πλεονέκτημα στον κάτοχό τους. Η διάρκεια του κυβερνοεπεισοδίου ήταν περίπου δύο με τρεις μήνες το φετινό καλοκαίρι (2011).

⁶⁸ Ολόκληρο το περιεχόμενο της έκθεσης είναι διαθέσιμο στην ηλεκτρονική διεύθυνση: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

Με αφορμή τα παραπάνω σημειώνεται ότι τον τελευταίο μήνα του περιστατικού ο πρόεδρος της Επιτροπής Πληροφοριών της Βουλής των Αντιπροσώπων των αμερικανικών πολιτειών, εξέφρασε τη γνώμη πως οι κυβερνοεπιθέσεις από την Κίνα έχουν πλέον φτάσει σε «αφόρητα επίπεδα» (<http://news.in.gr>, 1/11/2011).

4.4 (Κυβερνο-)Προπαγάνδα

4.4.1 Ποιοτικός Προσδιορισμός

Με τον όρο «Προπαγάνδα» επικαλούμαστε μια διαδικασία πειθούς (Taylor, 1997/2004, 360-373) με σκοπό τον έλεγχο της κοινής γνώμης ή μίας συγκεκριμένης ομάδας ατόμων. Στην κατακριτέα μορφή της έχει γενικό σκοπό να «θολώσει» τις γνωστικές διεργασίες, ώστε τα άτομα, που απαρτίζουν το στόχο, να μην μπορούν να χρησιμοποιήσουν τη λογική τους, για αυτόν το λόγο χαρακτηρίστηκε και διανοητικός πόλεμος⁶⁹. 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 megάφωνο
- Μέσα Μαζικής Ενημέρωσης και
- Διαδίκτυο

Ένας άλλος, επίσης, προσδιορισμός της έννοιας της προπαγάνδας (Θεωδορακόπουλος, 2006, 27) αναφέρει ότι:

με τη λέξη αυτή επικαλούμαστε την εμφύτευση στο ασυνείδητο του δέκτη του μηνύματος μιας ιδέας, εκκόλαψή της, αποκρυστάλλωσή της και ανάδυσή της στο συνειδητό ως (νομιζόμενη) επιλογή του δέκτη. Ο προπαγανδιστής εκμεταλλεύεται δια της υποβολής τις κυρίαρχες στάσεις του προπαγανδιζόμενου (...).

Μια συνηθισμένη στρατηγική προπαγανδιστικής εφαρμογής ξεκινάει με την κολακεία του στόχου. Σε αυτό το πρώτο βήμα επιχειρείται να κερδηθεί η εμπιστοσύνη της ομάδας που θα επηρεαστεί, εγκαθιστώντας με αυτόν τον τρόπο κλίμα συμπάθειας. Στο δεύτερο βήμα έχουμε το στάδιο της «γνωστικής και συγκινησιακής σύγχυσης». Εδώ, αποσπάται η προσοχή του ατόμου ή της ομάδας, ώστε η πρόταση που θα ακολουθήσει, καταρχάς να αιφνιδιάσει και κατόπιν, να λυτρώσει, κάνοντας το στόχο να νομίσει πως -εξαιτίας του προπαγανδιστή- βγαίνει από ένα αδιέξοδο. Τέλος, αφού πλέον έχει κερδηθεί πλήρως η εμπιστοσύνη γίνεται το

⁶⁹ Τον όρο «διανοητικός πόλεμος» (Geistige Kriegführung) επινόησαν οι Γερμανοί, στο διάστημα του μεσοπολέμου, 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 (Taylor, 1997/2004, 358).

«πέραςμα» του μηνύματος, το οποίο αποτελεί το μέσο επίτευξης του σκοπού της προπαγάνδας. Στην επιτυχή έκβαση, σημαντικό ρόλο παίζει η τεχνική της παρουσίας. Πρόκειται για ένα «παιχνίδι» με τις αισθήσεις, για τις οποίες πρέπει να χρησιμοποιηθεί ο κατάλληλος συνδυασμός ήχου και εικόνας.

Ένα παράδειγμα της εφαρμογής της παραπάνω μεθόδου είναι το ακόλουθο. Έστω ότι ο σκοπός είναι η διάχυση ενός μηνύματος 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, για την επίλυση του προβλήματος προτείνεται ένας διαφορετικός κόσμος, ο οποίος θα πρέπει να είναι ομοιογενής και παρόμοιος με τον παραδοσιακό που ήταν «καθαρός» από ξένες επιδράσεις.

Από πολύ νωρίς ο Merton (1968) έχει μιλήσει για την *τεχνολογική προπαγάνδα*, η οποία αποσκοπεί στον ερεθισμό συναισθημάτων (όπως τα εθνικιστικά), τα οποία μπορούν να λειτουργήσουν ως ελατήρια κινητοποιήσεων. Εξάλλου, η επιδίωξη τόσο φυσικών καταστροφών, όσο και ψυχολογικών επιδράσεων συνιστά συχνά μια κοινή συνισταμένη για τους μελετητές των απειλών της εθνικής ασφαλείας (Lewis, 2002). Όσον αφορά την περίπτωση μας, πέρα των παραδοσιακών μέσων (έντυπα, τηλεόραση και ραδιόφωνο) μας ενδιαφέρουν οι ποροπαγανδιστικές εφαρμογές διαμέσου του κυβερνοχώρου. Και εδώ, μπορούμε να πούμε ότι, ο πυρήνας της κεντρικής ιδέας παραμένει ο ίδιος, μόνο που οι δυνατότητες άσκησης της πολλαπλασιάζονται και για αυτό περιπλέκονται.

Πιο συγκεκριμένα, όσον αφορά τη λεγόμενη Κυβερνο-προπαγάνδα, ο αμερικανός αντιπρόσωπος στο Κέντρο Αριστείας για τη Συνεργασία στην Άμυνα στον Κυβερνοχώρο (Cooperative Cyber Defence Centre of Excellence) του NATO στο Ταλίν, τη θεωρεί ρητώς ως μια από τις τακτικές του κυβερνοπολέμου. Ειδικότερα δε, της προσδίδει στην εφαρμογή της, τα πλεονεκτήματα του μικρού κόστους και της υψηλής αποδοτικότητας (Geers, 2008).

Εντούτοις, η εμπειρία έχει δείξει ότι -παραδόξως από τις παραδοσιακές μορφές πραγματοποίησής της- στον κυβερνοχώρο έχουμε περιστατικά (κι ενδεχομένως, συγκριτικά περισσότερα) άσκησης προπαγάνδας «από τα κάτω προς τα πάνω». Με άλλα λόγια, εννοούμε πως, η συνηθισμένη «διαδρομή» είναι η ηγεσία ενός κράτους (π.χ. της Γερμανίας του β' παγκοσμίου πολέμου) ή έστω μια επιχειρηματική ελίτ (πριν νομιμοποιηθεί και «μονιμοποιηθεί» η διαφήμιση), να εφαρμόζει τέτοιες

μεθόδους πειθούς. Αντιθέτως, στον κυβερνοχώρο διακρίνουμε πρωτοβουλίες από τη λαϊκή βάση⁷⁰. Αναφερόμαστε σε κοινωνικές ομάδες, οι οποίες δεν έχουν εξουσία και με διάφορες τεχνικές -τις οποίες θα αναλύσουμε- προσπαθούν να διακινήσουν στον ψηφιακό κόσμο μηνύματα, τα οποία διαδίδουν και ενισχύουν τις θέσεις τους.

Τα άτομα που έχει η δυνατότητα άσκησης κυβερνο-προπαγάνδας «από τα κάτω προς τα πάνω», ονομάστηκαν Χακτιβιστές, κυρίως εξαιτίας των ακόλουθων προϋποθέσεων που απαιτούν οι δραστηριότητές τους.

- Ειδικές γνώσεις μη εξουσιοδοτημένης διείσδυσης στο διαδίκτυο (hacking).
- Απόφαση πολιτικής δραστηριοποίησης στον κυβερνοχώρο (activism).
- Μέλος σε ομάδα των άνω γνωρισμάτων, με έστω χαλαρούς δεσμούς και αυτό-οργανωτικές δομές.

Ο όρος είναι εμπνευσμένος από τον συγγραφέα Jason Sack (1995), σε ένα άρθρο του με τίτλο «Πληροφοριακό Έθνος» (InfoNation). Αν εξετάσουμε την ετυμολογική προέλευση του όρου, επίσης καταλήγουμε στην ίδια σημασία του. Ο όρος, λοιπόν, «χακτιβισμός» προέρχεται από τους όρους «hacking»⁷¹ και «activist»⁷², υποδηλώνοντας την επιλογή της δράσης διαμέσου του κυβερνοχώρου.

Βεβαίως, ο χακτιβισμός δεν ακυρώνει τις πιθανότητες άσκησης κυβερνο-προπαγάνδας από την εκάστοτε εξουσία. Στα νέα μέσα που έχουν εμπλουτίσει το «οπλοστάσιο» της μαζικής επικοινωνίας (διαδίκτυο, δορυφόροι και ιπτάμενες πλατφόρμες μετάδοσης εκπομπών), τα οποία λειτουργούν με έναν πιο εκλεπτυσμένο και αδιαφανή τρόπο ο στόχος των ψυχολογικών επιχειρήσεων παραμένει ο ίδιος. Η καλλιέργεια κλίματος αναστάτωσης και εξέγερσης, όταν πρόκειται για έναν εχθρό, αλλά και η απόκτηση ηθικού πλεονεκτήματος («*εμείς έχουμε το δίκιο με το μέρος μας και είμαστε οι καλοί*») ώστε να δικαιολογηθούν στην εγχώρια ή διεθνή κοινή γνώμη η διάφορες πολιτικές (Γαλέρα, 27/12/2007).

Όπως υπογραμμίζει ο καθηγητής επικοινωνίας Phil Taylor⁷³, «η αμερικανική κυβέρνηση του Τζορτζ Μπους Τζουνιόρ δεν κάνει πλέον διάκριση ανάμεσα σε μία

⁷⁰ Έκφραση που χρησιμοποιεί ο Castells (2001, σ. 52).

⁷¹ Βλέπε προηγούμενο κεφάλαιο.

⁷² Ο Ακτιβισμός θεωρείται μέρος της πολιτικής φιλοσοφίας του ρεαλισμού με έμφαση στον εθελοντισμό. Με αυτό τον όρο τονίζεται το χρέος του ανθρώπου να δρα, για να κάνει πραγματικότητα αυτό που επιθυμεί. Από τους γνωστότερους ακτιβιστές είναι ο Μαχάτμα Γκάντι, ο Μάρτιν Λούθερ Κινγκ και ο Τζον Λένον (el.wikipedia.org/wiki/Ακτιβισμός, 11/10/2011).

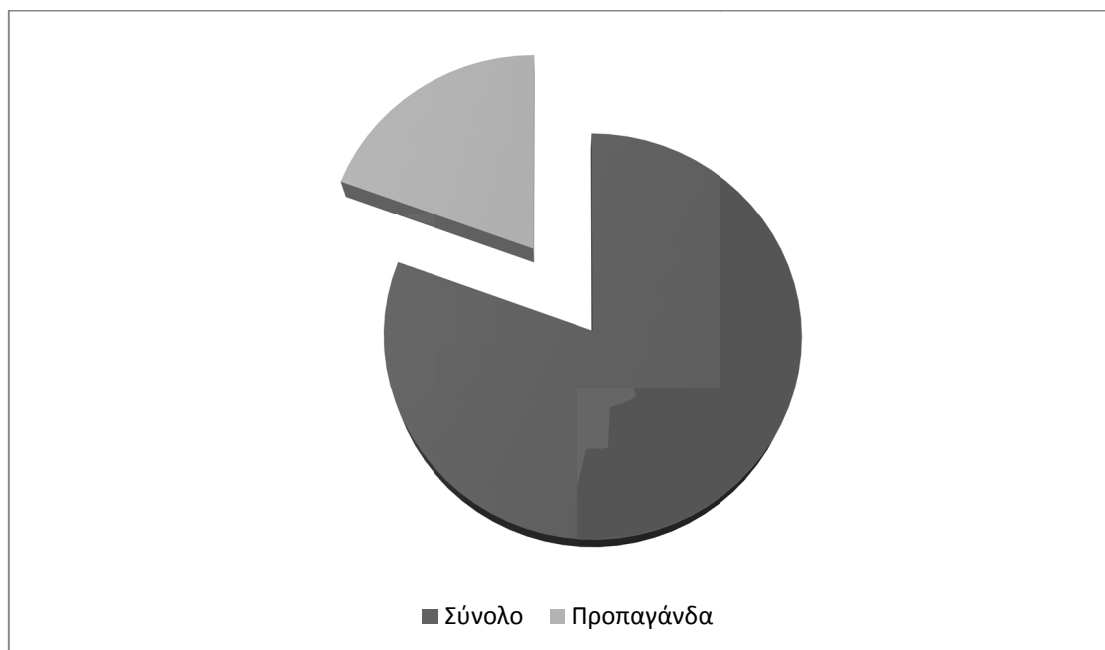
⁷³ Ο Φιλ Τάιλορ ήταν καθηγητής στον τομέα Διεθνών Επικοινωνιών στο Λιντς της Μ. Βρετανίας και ένα από τα πρόσωπα με την καλύτερη εξειδίκευση στα ζητήματα προπαγάνδας στον κόσμο. Απεβίωσε πέρυσι στις 6/12/2010 (<http://ics.leeds.ac.uk/papers/index.cfm?outfit=pmt>).

συνέντευξη Τύπου και μια στρατιωτική ψυχολογική καμπάνια»⁷⁴. Οι αλλαγές που έφεραν οι ΤΠΕ στη διακίνηση της πληροφορίας, διαμόρφωσαν νέες απαιτήσεις στο στρατηγικό σχεδιασμό ψυχολογικών επιχειρήσεων. Η συνήθης μεθοδολογία περιλαμβάνει την κατασκευή μιας κεντρικής βάσης δεδομένων (data base), σχετικά με άτομα σε «θέσεις-κλειδιά» ή σύνολα ατόμων συντονισμένα σε έναν θυμικό σκοπό (π.χ. εθντικές 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. Εκτός, ασφαλώς, της επεξεργασίας, το παραπάνω αρχείο απαιτεί συνεχή ενημέρωση (update), ώστε τα δεδομένα να βρίσκονται πάντα σε «πραγματικό χρόνο».

4.4.2 Ποσοτικός Προσδιορισμός

Σε αυτήν την θεματική κατηγορία (category) εντοπίστηκαν συνολικά **76** γραμματικές αναφορές (items). Η συμμετοχή ανήλθε σε ποσοστό 24,1%, το οποίο αντιστοιχεί στην τρίτη θέση της κατάταξης (corpus) μας. Οπότε, το μερίδιο που έχει η Κυβερνο-Προπαγάνδα στη συγκεντρωτική κατανομή ανέρχεται περίπου στο ένα τέταρτο (1/4) του συνόλου (Σχήμα 18).

Σχήμα 18. Συγκεντρωτικό Μερίδιο «ΚΥΒΕΡΝΟΠΡΟΠΑΓΑΝΔΑΣ»

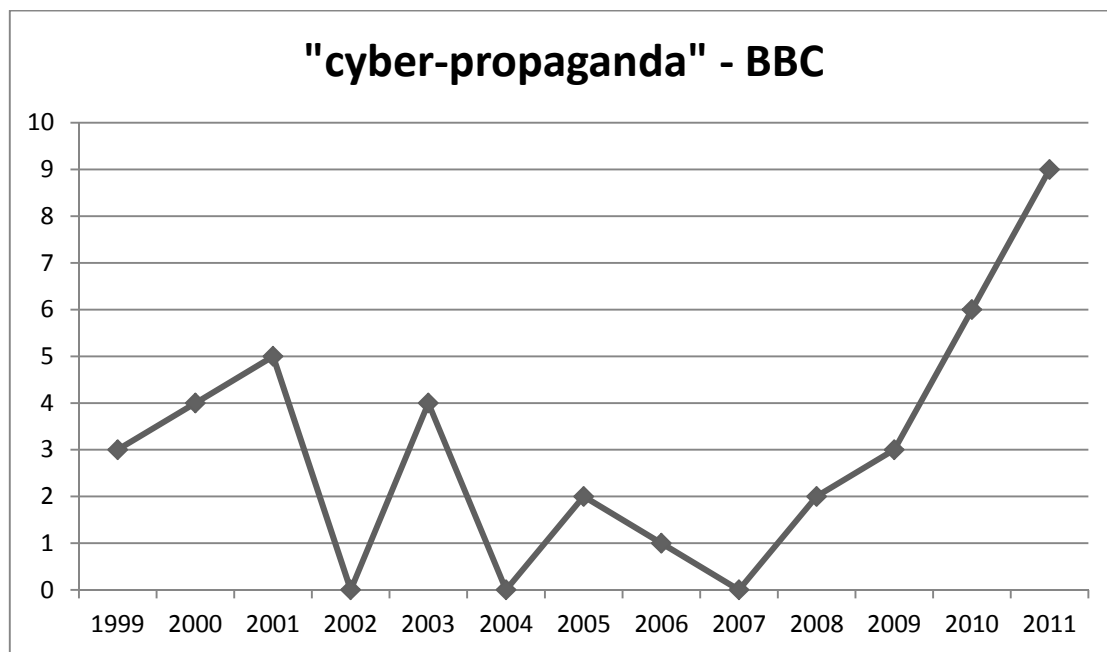


⁷⁴ Η συγκεκριμένη άποψη του καθηγητή αφορά την εξήγηση της διαδρομής που ακολούθησε η άσκηση προπαγάνδας από τις ηγεσίες, ώστε να καθιερωθεί ως πολιτική πρακτική και με τα σύγχρονα πλέον μέσα. Εδώ, πιο συγκεκριμένα αναφέρεται στις περιφημες δηλώσεις περί του «άξονα του κακού», ως ένα μέρος υλοποίησης της άσκησης Στρατηγικών Ψυχολογικών Επιχειρήσεων.

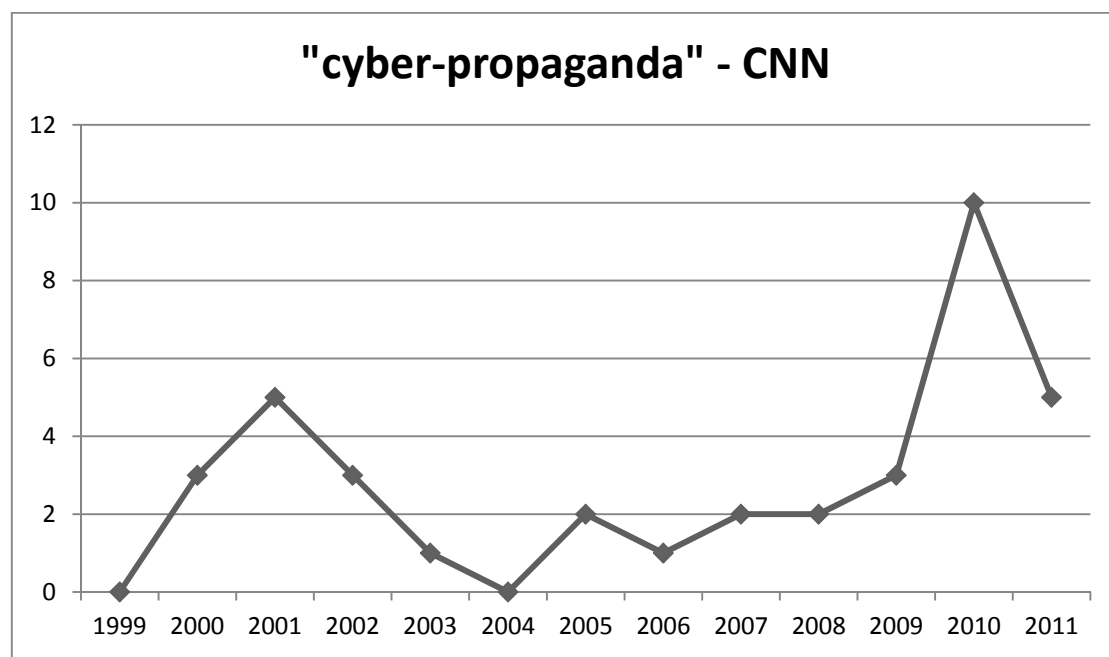
Αν αναζητήσουμε αναλυτικότερα την προέλευση της εν λόγω κατανομής, τότε μπορούμε να δούμε πως από το BBC έχουμε 39 αναφορές (σε σύνολο 150) με αναλογούν ποσοστό 26,0%. Η διαχρονική τάση, ενώ αυξομειώνεται, σε χαμηλά πάντως επίπεδα, μέχρι το 2007, εκ τότε διατηρεί συνεχή σταθερά αυξητική πορεία με καταληκτικό υψηλότερο σημείο στο τέλος, το 2011 (Σχήμα 19). Όσον αφορά το CNN έχουμε 37 αναφορές (σε σύνολο 165) με αναλογούν ποσοστό 22,4%. Η διαχρονική τάση ξεκινά αυξητικά, μόνο όμως για τα πρώτα δύο έτη. Κατόπιν, για άλλα τόσα πτοείται. Ενώ στο δεύτερο ήμισυ έχουμε συνεχή αύξηση, με υψηλότερη τιμή στο 2010, το τελευταίο έτος παρατηρείται μια σημαντική πτώση, φθάνοντας έτσι στα επίπεδα του 2001 (Σχήμα 20).

Επιπρόσθετα, παρατηρείται μια σχετική σταθερότητα στη διακύμανση των θέσεων που καταλαμβάνει αυτή η κατηγορία στο κάθε μέσο. Αυτό μπορούμε να το συμπεράνουμε από το ότι διακρίνουμε μια έλλειψη των θέσεων στις δύο «άκρες» (δηλαδή, της πρώτης και τελευταίας θέσης). Έτσι, στο BBC καταλαμβάνεται η δεύτερη θέση, με μόνο δύο μονάδες λιγότερες από το συγκεντρωτικό ποσοστό της (26,0% έναντι 24,1%) και στο CNN την τρίτη θέση με επίσης μόνο περίπου μιάμιση ποσοστιαία μονάδα διαφορά από το συγκεντρωτικό (22,4 - 24,1%).

Σχήμα 19. Διαχρονική Τάση «Κυβερνοπροπαγάνδας» – BBC



Σχήμα 20. Διαχρονική Τάση «Κυβερνοπροπαγάνδας» – CNN



4.4.3 Ανάλογα Κυβερνο-επεισόδια

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, το 1999, από το NATO. 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 αποφάσισε να μην διακόψει την πρόσβαση των Σέρβων στο διαδίκτυο. Θεώρησε ότι με αυτό τον τρόπο θα είχαν τη δυνατότητα να πληροφορηθούν για τις καταγγελίες για τα πεπραγμένα στο Κόσσοβο, από το καθεστώς του Μιλόσεβιτς. Υπό αυτή την έννοια, ο πόλεμος στο Κόσσοβο μπορεί να θεωρηθεί ως ο πρώτος «πόλεμος κυβερνοπροπαγάνδας» (Furnell, 2002/2006, 321-322).

Ο υπεύθυνος στρατηγός Wesley Clark δήλωσε στην Γερουσία των ΗΠΑ ότι εξαιτίας των σέρβων μαχητών στον κυβερνοχώρο «φθάσαμε πολύ κοντά να χάσουμε τον πόλεμο, λόγω της προπαγάνδας». Αυτή η μαρτυρία άνοιξε νέους ορίζοντες στη βαρύτητα που δίνεται στην έννοια της «κυβερνοπροπαγάνδας» (guardian.co.uk, 5/11/1999). Το NATO, προσπάθησε να αμυνθεί σε αυτές τις επιθέσεις, αλλά δεν ήταν πάντα εφικτό. Σε μια έκθεση που επακολούθησε, το Συμβούλιο των Εξωτερικών Υποθέσεων των ΗΠΑ (US Council on Foreign Relations - CFR report) συναίνεσε

στην αναγκαιότητα προσαρμογής στις συνθήκες που δημιουργούν οι νέες εξελίξεις των τεχνολογιών πληροφορίας και επικοινωνιών.

Ειδικότερα, οι στόχοι δεν αφορούσαν τόσο την καταστροφή των νατοϊκών δικτυακών κόμβων, όσο τη διάδοση μηνυμάτων «υπέρ του σερβικού αγώνα» σε ιστοσελίδες του NATO. Αντιθέτως, το NATO -όσον αφορά την επίδραση στην κοινή γνώμη- επέμεινε να στοχεύει σε τηλεπικοινωνιακούς σταθμούς στο Βελιγράδι.

Ωστόσο μια πενταετία περίπου πριν, έχουμε ίσως τις πρώτες δύο περιπτώσεις κυβερνο-προπαγάνδας στον κόσμο, οι οποίες δεν διοργανώθηκαν από κάποια ηγεσία. Η πρώτη διαδραματίστηκε στο Μεξικό το 1994 και η δεύτερη στην Τσετσενία την ίδια εποχή. Σχετικά με την πρώτη, πιο συγκεκριμένα, ξεκίνησε από την περιοχή Chiapas του νότιου Μεξικού. Μια ομάδα εξεγερμένων, οι οποίοι διεκδικούσαν σε γενικές γραμμές, καλύτερες συνθήκες διαβίωσης για τους ιθαγενείς του Μεξικού, αρχικά οργανώθηκαν, δίχως βίαιες επιδιώξεις. Ονομάστηκαν *Ζαπατίστας*⁷⁵ και «βάπτισαν» έτσι το κίνημά τους προς τιμή του αρχηγού τού απελευθερωτικού στρατού (Liberation Army of the South), κατά την περίοδο της μεξικανικής επανάστασης, Emiliano Zapata. Αρχηγός τους ήταν ο διανοούμενος, με το ψευδώνυμο Κομαντάντε Μάρκος.

Οι ειρηνικές όμως διεργασίες σύντομα τερματίστηκαν, εξαιτίας της αντίδρασης της μεξικανικής κυβέρνησης. Τότε, οι αντάρτες, πλέον, *Ζαπατίστας*, εκτός από τον παραδοσιακό τρόπο πολέμου, επέλεξαν και τη χρήση των σύγχρονων ΤΠΕ⁷⁶, ώστε να επικοινωνήσουν και να ενημερώσουν τον έξω κόσμο για τον αγώνα τους (Cleaver, 1994 και Ronfeldt & Arquilla, 2001).

Ανάλογα γεγονότα είχαμε και στην Τσετσενία, το 1994⁷⁷. Η αποστολή μηνυμάτων από χρήστες του διαδικτύου, από όλο τον κόσμο, έπαιξε ένα σημαντικό ρόλο. Από τα αρχικά ακόμα στάδια της εμφάνισης του παγκόσμιου ιστού, Τσετσένοι και Ρώσοι, ταυτόχρονα, χρησιμοποιούσαν αυτήν την τεχνολογία για την εξυπηρέτηση των δικών τους συμφερόντων ο καθένας.

⁷⁵ Επίσημη ονομασία είναι Στρατός των *Ζαπατίστας* για την Εθνική Απελευθέρωση-EZLN (Ejército Zapatista de Liberación Nacional).

⁷⁶ Αυτός ήταν και ένας από τους λόγους που ο Κομαντάντε Μάρκος, χαρακτηρίστηκε ο «Μεταμοντέρνος Τσε» (Che Guevara).

⁷⁷ Geers, K., *ό.π.*, όπου το κεφάλαιο με τη μελέτη της συγκεκριμένης περίπτωσης τιτλοφορεί: “Chechnya 1994: Propaganda” [IST-076/RSY-017].

Από την πλευρά των πρώτων τα περισσότερα μηνύματα δεν ήταν φιλο-τσετσενικά, αλλά αντι-ρωσικά. Ιδιαίτερο βάρος δόθηκε στην παρουσίαση επαχθών εικόνων με αιματοχυσίες και κακοποιημένα θύματα. Από τη δική τους πλευρά, στο Κρεμλίνο, κατηγόρησαν τις εικόνες αυτές ως παραποιημένες με τη χρήση της τεχνολογίας. Εντύπωση δημιούργησε δήλωση του ίδιου του Βλαντιμίρ Πούτιν, το 1999, για τη δυτική υποστήριξη έναντι φιλοτσετσενικού ιστότοπου, ο οποίος εντοπίστηκε στις ΗΠΑ (kavkaz.org).

Σε ένα άρθρο με τίτλο «Cyber War Israel and Hamas», ο συγγραφέας (Morrill, 2009)⁷⁸ επιχειρηματολογεί στο γιατί ο κυβερνοπόλεμος γίνεται καθοριστικός στην επικράτηση σε έναν πόλεμο. Εξηγεί ότι στους σύγχρονους πολέμους είναι καθοριστικό να επηρεάζεις τους ανθρώπους, μέσω της προπαγάνδας του κυβερνοχώρου και δη, όταν μπορείς να αυτοματοποιείς την επιλογή των ιστοσελίδων που θα παραπέμπεται ο αναγνώστης. Για παράδειγμα αναφέρεται μια ομάδα ισλαμιστών από το Μαρόκο, οι οποίοι εκμεταλλεύθηκαν με αυτό τον τρόπο την ιστοθέση «DomainTheNet's», ώστε να κατηγορήσουν τις επιχειρήσεις του Ισραήλ στη λωρίδα της Γάζας (YNetnews, 25/10/2010). Η μέθοδος διείσδυσης στο Domain Name System⁷⁹ είναι καινοτόμος και συνήθως καλείται επιγραμμικά DNS attack (it.toolbox.com, 29/10/2010).

Η υπόθεση wikileaks, αντιπροσωπεύει ίσως τον «αντιπροσωπευτικότερο» τρόπο υποκλοπής μυστικών, με σκοπό τη δημοσιοποίησή τους και άρα, κατά επέκταση την κοινωνική επιρροή. Η wikileaks ξεκίνησε τις δραστηριότητές της το 2007 και αυτοπροσδιορίζεται ως ένας μη-κερδοσκοπικός δημοσιογραφικός οργανισμός, ο οποίος έχει σκοπό να πληροφορεί το κοινό με νέα τα οποία του αποκρύπτονται (wikileaks.org, 15/9/2009). Με τη εγγύηση της ανωνυμίας και της ασφάλειας, προσκαλεί όλους τους χάκερ παγκοσμίως, να γίνουν πηγή της.

Από τον πρώτο χρόνο λειτουργίας του οργανισμού, πάνω από ένα εκατομμύριο διαβαθμισμένα έγγραφα αναρτήθηκαν στις ιστοσελίδες του. Οι περισσότεροι από τους ιδρυτές του είναι δημοσιογράφοι και επιστήμονες, κυρίως των μαθηματικών και της πληροφορικής. Οι ίδιοι θεωρούν τον εαυτό τους «πνευματικό παιδί» των

⁷⁸ Ο Dan Morrill είναι διευθυντής προγράμματος στο πανεπιστήμιο του Σιάτλ των ΗΠΑ.

⁷⁹ Το Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών (Domain Name System - DNS) είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για υπολογιστές, υπηρεσίες και οποιοδήποτε άλλο δικτυακό πόρο συνδέεται σε δίκτυο με πρωτόκολλο IP. Το σύστημα DNS μπορεί και αντιστοιχίζει ονόματα με διευθύνσεις IP ή άλλα ονόματα στο Διαδίκτυο ή ένα ιδιωτικό δίκτυο. <http://el.wikipedia.org>, 3/1/2011).

αντιφρονούντων από την Κίνα. Ως επικεφαλής παρουσιάζεται ο Αυστραλός δημοσιογράφος και ακτιβιστής του Διαδικτύου, ο Τζούλιαν Ασάντζ (Julian Assange) (The New Yorker, 7/6/2010).

Το WikiLeaks επιβραβεύθηκε αρκετές φορές για το έργο του. Καταρχάς, με το Βραβείο Νέου Μέσου (New Media Award), το έτος 2008, από το έγκριτο περιοδικό «The Economist». Κατόπιν, το έτος 2009, από την Διεθνή Αμνηστία, στην κατηγορία «Νέο Μέσο», με το UK Media Award⁸⁰. Ο λόγος που παραθέτουμε αυτές τις βραβεύσεις από τη διεθνή κοινότητα είναι επειδή έτσι φαίνεται η αντίθεση με τον τρόπο που αντιμετώπισαν οι κυβερνήσεις αυτές τις δημοσιεύσεις. Και αυτός ο τρόπος, όπως θα αναλύσουμε παρακάτω, αποδεικνύει ότι σε πρώτο επίπεδο οι κυβερνήσεις ενοχλήθηκαν από τα απόρρητα έγγραφα που διέρρευσαν. Σε δεύτερο ωστόσο επίπεδο, προβληματίζονται από την ταχύτητα και την άναρχη -με την έννοια της ανεξέλεγκτης, από αυτούς- οργάνωσης και συσπείρωσης στον κυβερνοχώρο ορισμένων χάκερ, οι οποίοι επιδρούν στην κοινή γνώμη σε εμπόλεμες ή μη συγκυρίες.

Ενδεικτικά, παρατίθενται ορισμένες από τις δημοσιοποιήσεις του WikiLeaks, κατά το ήμισυ, μόλις, ενός έτους:

- Βίντεο ενός περιστατικού του 2007, όπου Ιρακινοί άμαχοι πολίτες θανατώθηκαν από Αμερικανούς στρατιώτες (Collateral Murder, 2010).
- Τον Ιούλιο του ίδιου έτους, αναρτήθηκε το «Ημερολόγιο του Πολέμου στο Αφγανιστάν» («Afghan War Diary»), μια συλλογή περίπου 77 χιλιάδων εγγράφων για τον Πόλεμο στο Αφγανιστάν
- Τον Οκτώβριο, διατέθηκε μια συλλογή περίπου 400.000 εγγράφων με τίτλο «Ημερολόγιο του Πολέμου στο Ιράκ» («Iraq War Logs»)
- Τον Νοέμβριο, το WikiLeaks άρχισε να δίνεται μια συλλογή ενός πακέτου από συνολικά 251.287 διπλωματικά έγγραφα.

Σε αυτήν την τελευταία επίθεση, ανοιχτά κι επίσημα η Κυβέρνηση των ΗΠΑ δήλωσε ότι πρόκειται για «επίθεση κατά της διεθνούς κοινότητας» (New York Times, 2011). Ανάλογη δυσaráσκεια έδειξε και ο Τούρκος πρωθυπουργός Ρετζέπ Ταγίπ Ερντογάν, Ο λόγος ήταν η δημοσίευση τηλεγραφημάτων, τα οποία εμφανίζουν τον

⁸⁰ Αυτό το βραβείο το κέρδισε για τη δημοσίευση ενός κειμένου με τίτλο «Κένυα: Η Κραυγή του Αίματος – Εξώδικες δολοφονίες και εξαφανίσεις» (Kenya: The Cry of Blood – Extra Judicial Killings and Disappearances). Επρόκειτο για μια έρευνα της Εθνικής Επιτροπής της Κένυας για τα Ανθρώπινα Δικαιώματα (Kenya National Commission on Human Rights).

Ερντογάν ως αυταρχικό και θρησκόληπτο ηγέτη, ο οποίος πιστεύει πως η διακυβέρνηση της χώρας είναι αποστολή που του έχει δώσει ο Θεός. Κατά την αντίδρασή του ο κ. Ερντογάν εκτίμησε ότι μάλλον πρόκειται για «προπαγάνδα» με στόχο τις διεθνείς σχέσεις των Η.Π.Α. και των συμμάχων τους (τηλεοπτικό δίκτυο NTV). Μια τελευταία περίπτωση κράτους, το οποίο αντιτίθεται στο έργο του wikileaks, είναι αυτή της Γερμανίας. Ο πρώην επικεφαλής του Ανωτάτου Δικαστηρίου της χώρας, Βίνφριντ Χάσεμερ, έκανε την εκτίμηση ότι είναι πολύ πιθανό να συνίσταται παράνομη πράξη (περιοδικό Focus). «Ο νόμος περί μυστικότητας διατυπώνεται περιορισμένα στον ποινικό κώδικα της χώρας μας και σπανίως εφαρμόζεται, αλλά σε συγκεκριμένες περιπτώσεις μπορεί να υπάρξει παραβίασή του», φέρεται ότι είναι η γνώμη του Χάσεμερ (www.kathimerini.gr, 5/12/2010).

Συνέπεια όλων αυτών ήταν τελικά η σύλληψη του Τζ. Άσαντζ, ιδρυτή του ιστότοπου⁸¹, ο οποίος κρίθηκε προφυλακιστέος από το βρετανικό δικαστήριο (news.in.gr, 7/12/2010). Εντούτοις, αυτό το σημαντικό για το wikileaks γεγονός, δεν ήταν αρκετό για να σταματήσει τις δραστηριότητές του. Αντιθέτως, προς υποστήριξή του, εμφανίστηκε μια δεύτερη οργάνωση χακτιβιστών του κυβερνοχώρου, η οποία αυτοαποκαλείται «οι ανώνυμοι» (Anonymous). Τα πρώτα δείγματα των ενεργειών αυτής της «κίνησης» ήταν κυβερνοεπιθέσεις στις πολυεθνικές Mastercard, Visa, Amazon και Paypal, οι οποίες είχαν το αποτέλεσμα να διακόψουν τη λειτουργία τους. Ευρέως και εδώ χρησιμοποιήθηκε ο τίλος «κυβερνοπόλεμος», για να συμβολίσει και τα πολιτικά μηνύματα αυτών των χτυπημάτων στον κυβερνοχώρο (enet.gr, 11/12/2010).

Η εν λόγω ομάδα των χάκερ αποκάλεσε αυτά τα χτυπήματα «Επιχείρηση Ανταπόδοσης» (Operation PayBack). Η ίδια αρνείται ότι αυτό που κάνει είναι κυβερνοπόλεμος. Θεωρεί τις κινήσεις της κυβερνοδιαμαρτυρία ή κυβερνοεξέγερση, εξαιτίας το ότι οι συγκεκριμένες επιχειρήσεις – στόχοι της πάγωσαν τους λογαριασμούς ενίσχυσης του wikileaks. Για παράδειγμα η Amazon διέκοψε από τα διαθέσιμα προϊόντα της το ηλεκτρονικό βιβλίο με το περιεχόμενο του wikileaks⁸².

⁸¹ Ο 39/χρονος Άσαντζ παραδόθηκε στη Σκότλαντ Γιαρντ, σε ένα αστυνομικό τμήμα του Λονδίνου. Μέχρι την παρούσα συγγραφή περιμένει τις επόμενες ημέρες την απόφαση των βρετανικών δικαστηρίων για το αίτημα της έκδοσής του στη Σουηδία, όπου κατηγορείται για βιασμό.

⁸² Αξιοσημείωτο είναι πως ο συγγραφέας του Μανιφέστου είναι Έλληνας (<http://www.enet.gr>, 11/12/2010).

Παρόλα αυτά, αντεπίθεση πραγματοποιήθηκε στην ομάδα των anonymous. Οι φορείς της νέας κυβερνοεπίθεσης ονομάζονται «4chan»⁸³ και ακολούθησε τις ίδιες τακτικές, με τις οποίες οι «ανώνυμοι» έκαναν τις κυβερνοεπιθέσεις τους (*Newsroom* ΔΟΛ, 29/12/2010).

Εν κατακλείδι, η τελευταία εξέλιξη (24/10/2011) είναι πως ο ιστότοπος των WikiLeaks ανακοίνωσε την «προσωρινή αναστολή» της λειτουργίας του. Στην επίσημη ανακοίνωση της ιστοσελίδας του, το WikiLeaks κατηγορεί τις τράπεζες και τις υπηρεσίες συναλλαγών τους Visa, Mastercard, Western Union, PayPal. Αναφέρει ότι η αιτία είναι ότι πλέον, δεν δέχονται δωρεές υπέρ της οργάνωσης και αυτή η συνθήκη στερεί το 95% των εσόδων της (*news.in.gr*, 1/11/2011). Αυτό το γεγονός έγινε μετά τη δημοσιοποίηση 250.000 απόρρητων εγγράφων του υπουργείου των εξωτερικών των ΗΠΑ.

Αυτό το γεγονός όμως δεν σημαίνει και το πάγωμα των επιχειρήσεων από τους ανώνυμους (anonymous). Στις 7/11/2011 κυβερνητικοί εκπρόσωποι του Ισραήλ ανακοίνωσαν ότι τέθηκαν εκτός λειτουργίας τρεις κρατικοί ιστότοποι, αυτοί των ένοπλων δυνάμεων (Στρατός), της υπηρεσίας πληροφοριών (Μοσάντ) και της υπηρεσίας εσωτερικής ασφάλειας (Σιν Μπετ). Η συγκεκριμένη κυβερνοεπίθεση ακολούθησε δύο μέρες μετά τη δημοσιοποίηση βίντεο, από το YouTube, στο οποίο προειδοποιείται η ισραηλινή κυβέρνηση για τη στάση που θα κρατήσει στην αναχαίτιση των πλοίων που κατευθύνονταν στη Γάζα. Το επίμαχο οπτικοακουστικό μήνυμα, είχε τίτλο «Ανοιχτή επιστολή από τους Anonymous στην κυβέρνηση του Ισραήλ» και καταγγέλλει «πειρατεία σε διεθνή ύδατα» (*news.in.gr*, 6/11/2011).

Ένας ακόμα, από τους πιο πρόσφατους στόχους, των «Ανωνύμων» ήταν η στήριξή τους στη λεγόμενη «Αραβική Άνοιξη» (2010 - 2011). Με αυτόν τον όρο επικαλούμαστε τις διαδηλώσεις και εξεγέρσεις σε αραβόφωνες περιοχές, από τη Βόρεια Αφρική και τη Μέση Ανατολή. Πιο συγκεκριμένα εξεγέρσεις είχαμε (*Wikipedia*, 12/11/2011):

- στη Τунησία, στην Αίγυπτο, στη Λιβύη, το Μπαχρέιν, τη Συρία και την Υεμένη
 - Ενώ μεγάλες διαδηλώσεις έγιναν
 - στην Αλγερία, το Ιράν, το Ιράκ, την Ιορδανία, το Μαρόκο και το Ομάν.
- Επίσης, μικρότερες οργανωμένες διαμαρτυρίες έγιναν

⁸³ «Ο δικτυακός τόπος έχει πέσει από DDoS» έγραψε στο Twitter ο χρήστης Moot, ιδρυτής του 4chan.

- στο Τζιμπουτί, το Κουβέιτ, τον Λίβανο, τη Μαυριτανία, και το Σουδάν.

Κοινό χαρακτηριστικών όλων ήταν -εκτός από τις κινητοποιήσεις στο φυσικό χώρο, με απεργίες και πορείες- η χρησιμοποίηση των ιστοσελίδων της λεγόμενης κοινωνικής δικτύωσης (όπως τα Facebook, Twitter και YouTube), για την εξυπηρέτηση των οργανωτικών σκοπών των διαφόρων συγκεντρώσεων⁸⁴.

Ο πόθος των Αράβων για την συμμετοχή στον κυβερνοχώρο έχει καταγραφεί, από πολύ παλαιότερα, τόσο με δημοσιογραφικό, όσο και με επιστημονικό τρόπο. Ένας από τους δυσκολότερους φραγμούς όμως, έχει εκτιμηθεί ότι είναι η γλώσσα τους (Peel, 2004). Η σπουδαιότητα των γεγονότων τα οποία διαδραματίστηκαν διαμέσου του κυβερνοχώρου κατά τη διάρκεια της επονομαζόμενης «Αραβικής Άνοιξης» έγκειται στο ότι, για πρώτη φορά, οι λαοί χρησιμοποιούν τον κυβερνοχώρο με ένα τρόπο που θα μπορούσαμε να χαρακτηρίσουμε πιο *δραστικό*. Αντιλαμβανόμαστε πως από τις ιστορίες του 1994 (Τσιάπας και Τσετσενίας) που περιγράψαμε, όπου ο κυβερνοχώρος χρησιμοποιήθηκε βασικά για την ενημέρωση του κόσμου, είναι πολύ σημαντικό 16 χρόνια μετά να οργανώνονται εξαιτίας του κινητοποιήσεις (news.in.gr, 6/11/2011).

Όπως είναι επόμενο, αυτές οι κινητοποιήσεις έφεραν σοβαρές αντιδράσεις από τις κυβερνήσεις των παραπάνω κρατών. Όπως όμως δήλωσε ο γενικός γραμματέας του Οργανισμού της Διεθνούς Αμνηστίας, Σαλίλ Σχετί «Οι πολίτες αψηφούν την κρατική τρομοκρατία. Γενναίοι άνθρωποι, εμπνεόμενοι σε μεγάλο βαθμό από τη νεολαία, αντιστέκονται και αντιμετωπίζουν κατά πρόσωπο σφαίρες, ξυλοδαρμούς, χημικά και άρματα μάχης» (news.in.gr, 13/5/2011). Επίσης, στην έκθεση η οποία εμπεριέχει το παραπάνω απόσπασμα, τονίζεται η μεγάλη προσπάθεια, η οποία καταβάλλεται από τους ιθύνοντες των καθεστώτων, ώστε να μπορέσουν να ελέγξουν τη διακίνηση των πληροφοριών μέσα στον κυβερνοχώρο. Εδώ, ακριβώς, εστιάζεται το ζήτημα της κυβερνο-λογοκρισίας, η οποία αποτελεί την τελευταία θεματική κατηγορία μας και αναλύεται στο επόμενο κεφάλαιο.

⁸⁴ Το κεντρικό σύνθημα που κυριάρχησε στους διαδηλωτές του αραβικού κόσμου ήταν το «Ash-sha'ab yurid isqat an-nizam (النظام إسقاط يريد الشعب)», το οποίο μεταφράζεται πως «ο λαός θέλει να πέσει το καθεστώς».

4.5 Κυβερνο-Λογοκρισία

4.5.1 Ποιοτικός Προσδιορισμός

Σύμφωνα με το λεξικό Τεγόπουλος – Φυτράκης (σ. 428),

«λογοκρισία» καλούμε τον προληπτικό ή κατασταλτικό έλεγχο που ασκεί μια εξουσία στα μέσα ενημέρωσης, στα έργα του γραπτού λόγου, τα θεάματα, τα δημιουργήματα της τέχνης, με σκοπό να εμποδιστεί η διάδοση πληροφοριών και ιδεών αντιθέτων προς τις αρχές και τις επιδιώξεις της.

Από μία οπτική, η σχέση του προηγούμενου υποκεφαλαίου, δηλαδή της Κυβερνο-προπαγάνδας με αυτό το υποκεφάλαιο, δηλαδή της Κυβερνο-Λογοκρισίας είναι αντιθετική. Αυτός είναι ο λόγος που οι αρμόδιες κρατικές αρχές ονομάζονται Υπηρεσίες Αντί-πληροφοριών ή *Αντί-προπαγάνδας*. Οι ίδιοι πρεσβεύουν πως αποστολή τους είναι η άμυνα σε όποιες επιθετικές ενέργειες -εσωτερικού ή εξωτερικού- εχθρού παραπληροφορούν τον κόσμο ως προς τα συμφέροντα της χώρας τους. Αυτό, βεβαίως, δεν έχει αποκλείσει (μάλλον το αντίθετο) από την ιστορία τα έκτροπα φίμωσης της ελευθερίας της έκφρασης στη διεθνή κοινότητα.

Αν εστιάσουμε στον τρόπο που λειτουργεί η λογοκρισία στον κυβερνοχώρο (κυβερνο-λογοκρισία), τότε θα δούμε πως οι διαφορές ως προς την ουσία της παραδοσιακής λογοκρισίας είναι ανύπαρκτες. Αυτό, φυσικά, το οποίο αλλάζει είναι το τεχνικό κομμάτι, εφόσον αναφερόμαστε σε ένα πιο πολύπλοκο μέσο, αυτό του διαδικτύου. Έτσι, μπορούμε να παρατηρήσουμε όλο το φάσμα των απαγορεύσεων, από την ακραία διακοπής της λειτουργίας του διαδικτύου εντός της επικράτειας, ως τους συνήθεις φραγμούς στη χρήση συγκεκριμένων μηνυμάτων.

Ένα μέρος του μηνύματος του Γενικός Γραμματέας του ΟΗΕ Μπαν Κι-Μουν, για τη φετινή «Παγκόσμια Ημέρα Ελευθερίας του Τύπου» (3/5/2011), αναφέρει ότι (unric.org/el, 6/11/2011):

" Όταν οι κυβερνήσεις καταπιέζουν τους λαούς τους και προστατεύουν τους εαυτούς τους από τον έλεγχο, η ελευθερία του Τύπου είναι ένα από τα πιο ισχυρά μέσα για την αποκάλυψη των εγκλημάτων και την στήριξη της εμπιστοσύνης του κοινού.

(...)

Το θέμα του φετινού εορτασμού «Νέα Σύνορα, Νέα Εμπόδια» υπογραμμίζει αυτή τη δραματική αλλαγή στο παγκόσμιο πεδίο των μέσων μαζικής ενημέρωσης. Νέα μέσα και εργαλεία, όπως τα κινητά τηλέφωνα συνεχίζουν να ενδυναμώνουν των ανθρώπους, να

εμπλουτίζουν τη συγκέντρωση ειδήσεων και να φωτίζουν την κάποτε κρυφή λειτουργία των κυβερνήσεων, των επιχειρήσεων και της βιομηχανίας.

Ωστόσο, παράλληλα με τα οφέλη αυτά, υφίστανται ακόμα και οι παλιές προκλήσεις, όπως η χρήση των μέσων ενημέρωσης για τη διάδοση του μίσους και την υποκίνηση της βίας. Υπάρχουν επίσης νέα εμπόδια που υψώνονται από τα κράτη, συμπεριλαμβανομένης της επιτήρησης του κυβερνοχώρου, της ψηφιακής παρενόχλησης και της λογοκρισίας στο διαδίκτυο. Σύμφωνα με την Επιτροπή για την Προστασία των Δημοσιογράφων, τουλάχιστον έξι δημοσιογράφοι που εργαζόταν κυρίως στο διαδίκτυο έχασαν τη ζωή τους το 2010. Το **2008, για πρώτη φορά, είχαν φυλακιστεί περισσότεροι δημοσιογράφοι του διαδικτύου παρά δημοσιογράφοι που εργάζονταν σε παραδοσιακά μέσα ενημέρωσης.**

(...)

Το άρθρο 19 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου διακηρύσσει το δικαίωμα του κάθε ανθρώπου «να αναζητεί, να λαμβάνει και να διαδίδει πληροφορίες και ιδέες, με οποιοδήποτε μέσο, ανεξαρτήτως συνόρων». Ας επιβεβαιώσουμε την δέσμευσή μας σε αυτή τη βασική αρχή της δημοκρατίας, της ανάπτυξης και της ειρήνης."

Από το παραπάνω απόσπασμα συμπεραίνουμε ότι στο στόχαστρο των κρατικών υπηρεσιών ελέγχου της έκφρασης γνώμης, αρχίζουν να κυριαρχούν οι διαδικασίες κυβερνολογοκρισίας.

Επιπρόσθετα, μετά από εισηγητική έκθεση⁸⁵ της Επιτροπής Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων, στις 21.1.2009, το Ευρωπαϊκό Κοινοβούλιο, διαβουλεύεται Σχέδιο Έκθεσης, το οποίο όπως αναφέρει στον επεξηγηματικό του υπότιτλο θα «περιέχει πρόταση σύστασης του Ευρωπαϊκού Κοινοβουλίου προς το Συμβούλιο σχετικά με την ενίσχυση της ασφάλειας και των θεμελιωδών ελευθεριών στο Διαδίκτυο». Τα κυριότερα σημεία είναι τα εξής:

- Πλήρης και ασφαλής πρόσβαση στο Διαδίκτυο για όλους.
- Ισχυρή δέσμευση στην καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο.
- Αδιάπτωτη προσοχή στην απόλυτη προστασία και την ενισχυμένη προώθηση των θεμελιωδών δικαιωμάτων στο Διαδίκτυο.

Ένα πρόβλημα όμως που δημιουργείται, αν μελετήσουμε βαθύτερα τις παραπάνω στοχοθετήσεις, είναι ότι είναι πολύ δύσκολη η διατήρηση της ισορροπίας

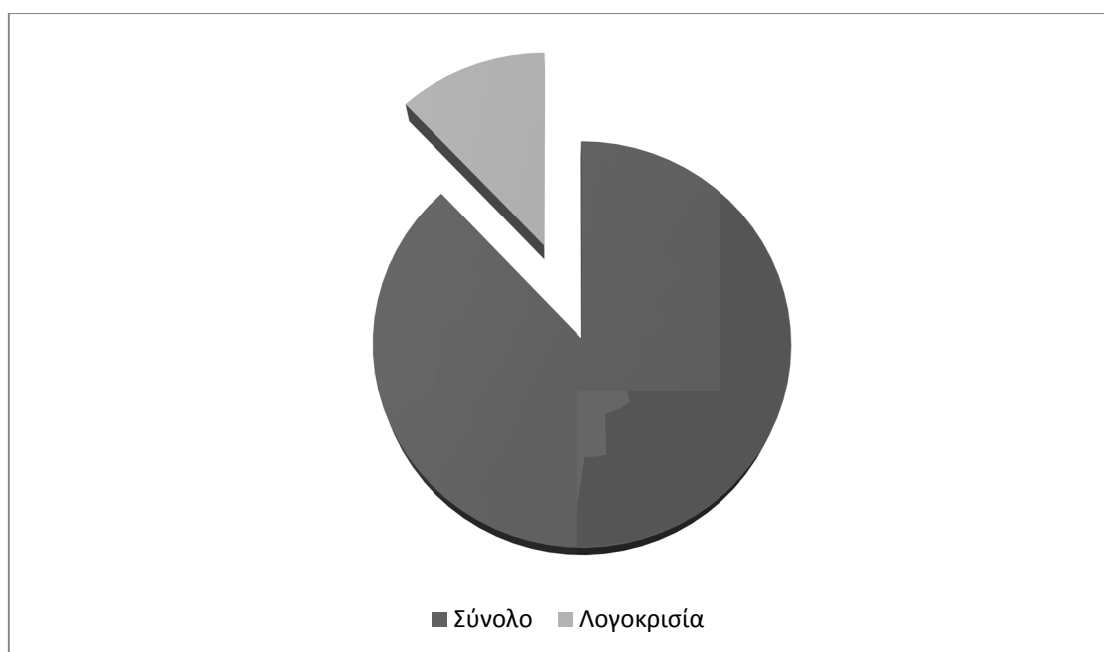
⁸⁵ Εισηγητής είναι ο τέως υπουργός των εξωτερικών της Ελλάδας, Σταύρος Λαμπρινίδης.

από έναν κρατικό φορέα μεταξύ των ακολούθων δύο πλευρών. Από τη μία να υπάρχει ελεύθερη πρόσβαση σε όλους τους πολίτες και από την άλλη, να αφαιρείται από αυτούς οι οποίοι την καταχρούνται⁸⁶. Επίσης, στη σκέψη ότι δεν πρόκειται παρά για μια άλλη αναλογία του φυσικού κόσμου, όπως δηλαδή ακριβώς συμβαίνει και με την αφαίρεση των πολιτικών δικαιωμάτων των καταδικασμένων πολιτών, οφείλουμε να αναλογιστούμε μια κρίσιμη διαφορά. Στον κυβερνοχώρο είναι συχνά πολύ δύσκολο να εξερευνηθεί ο υπαίτιος, για αυτόν το λόγο πολλοί καταφεύγουν σε μαζικές απαγορεύσεις.

4.5.2 Ποσοτικός Προσδιορισμός

Σε αυτήν την θεματική κατηγορία (category) εντοπίστηκαν συνολικά **43** γραμματικές αναφορές (items). Η συμμετοχή ανήλθε σε ποσοστό 13,7%, το οποίο αντιστοιχεί στην τέταρτη θέση της κατάταξης (corpus) μας. Οπότε, το μερίδιο που έχει η Κυβερνο-Λογοκρισία στη συγκεντρωτική κατανομή ανέρχεται περίπου στο ένα όγδοο (1/8) του συνόλου (Σχήμα 21).

Σχήμα 21. Συγκεντρωτικό Μερίδιο «ΚΥΒΕΡΝΟΛΟΓΟΚΡΙΣΙΑΣ»

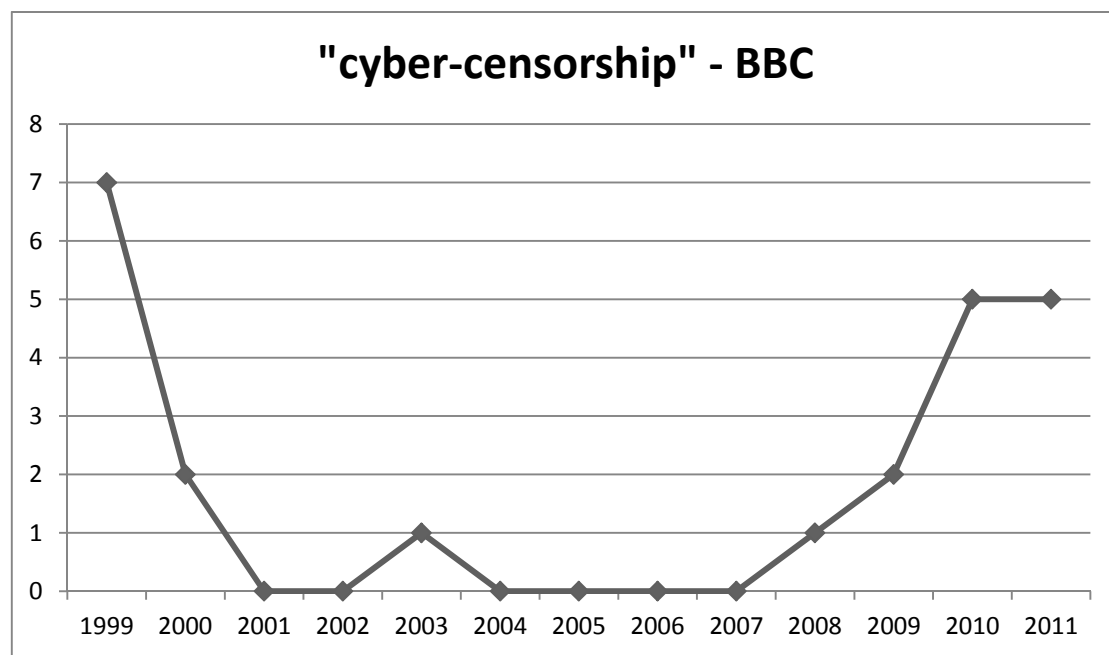


⁸⁶ Σύμφωνα με τον Ian Brown, υφηγητή στο Ινστιτούτο Διαδικτύου της Οξφόρδης (Oxford Internet Institute), οι περισσότερες χώρες στον κόσμο έχουν σε λειτουργία κατάλληλα φίλτρα κυβερνο-λογοκρισίας (<http://edition.cnn.com>, 21/8/2008).

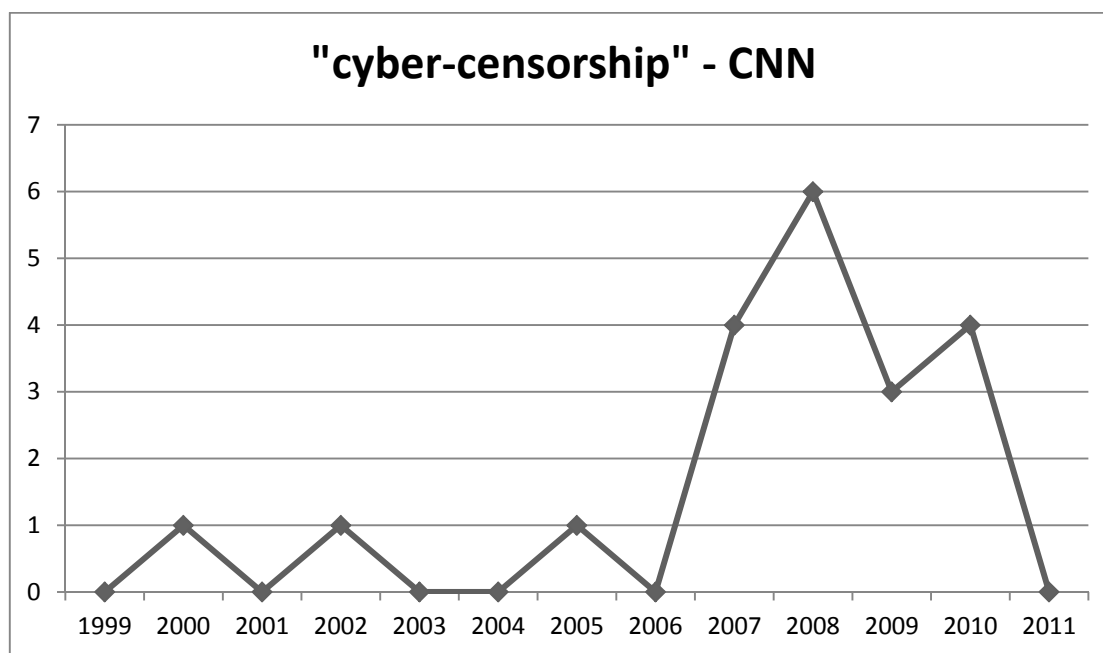
Αν αναζητήσουμε αναλυτικότερα την προέλευση της εν λόγω κατανομής, τότε μπορούμε να δούμε πως από το BBC έχουμε 23 αναφορές (σε σύνολο 150) με αναλογούν ποσοστό 15,3%. Η διαχρονική τάση, ενώ ξεκινάει σε υψηλά ποσοστά, πέφτει απότομα σε πολύ χαμηλά, διατηρείται εκεί μέχρι το 2007. Τότε αποκτά συνεχόμενη ανοδική πορεία, μέχρι το 2010, οπότε και θα σταθεροποιηθεί στην υψηλότερη τιμή της (με εξαίρεση τις 7 μονάδες αναφοράς που έχει στην «αφετηρία» του 1999) (Σχήμα 22). Όσον αφορά το CNN έχουμε 20 αναφορές (σε σύνολο 165) με αναλογούν ποσοστό 12,1%. Η διαχρονική τάση δείχνει τα πρώτα επτά έτη μια σταθερή χαμηλή πορεία. Κάτι που μεταβάλλεται το 2007, οπότε τα δύο πρώτα χρόνια αυξάνεται και τα δύο τελευταία φθάνει στο αρχικό μηδενικό επίπεδο (Σχήμα 23).

Αυτή, η τελευταία, θεματική κατηγορία είναι η μόνη με απόλυτη σταθερότητα στην τελευταία θέση που καταλαμβάνει, τόσο στο κάθε μέσο, όσο και συγκεντρωτικά. Ως άμεσο επακόλουθο παρατηρούμε και την καταγραφή του μικρότερου ποσοστού, γενικότερα. Πρόκειται για το 12,1% στο CNN.

Σχήμα 22. Διαχρονική Τάση «Κυβερνολογκρισίας» – BBC



Σχήμα 23. Διαχρονική Τάση «Κυβερνολογοκρισίας» – CNN



4.5.3 Ανάλογα Κυβερνο-επεισόδια

Μια ασιατική χώρα, μεταξύ Κίνας και Ινδίας, γνωστή ως Βιρμανία, Μιανμάρ και Μπούρμα, είχε μια πρώτη γεύση αυτού του είδους κυβερνοπολέμου, μια εβδομάδα πριν τις τελευταίες εκλογές (τις πρώτες μετά από δύο δεκαετίες). Τα στοιχεία που παρουσίασε η αμερικανική εταιρεία ασφάλειας δικτύων Arbor Networks δείχνουν ότι η χώρα, κατά αυτό το διάστημα είναι σα να μη διαθέτει διαδίκτυο.

Σχετικά με το τεχνικό μέρος, η κυβερνοεπίθεση ακολούθησε την τεχνική του DDoS. Τα χτυπήματα ανέρχονταν σε 10-15 Gigabit δεδομένων ανά δευτερόλεπτο, ενώ τα περιθώρια της χώρας περιορίζονται μόνο στα 45 Megabit ανά δευτερόλεπτο. Σύμφωνα με τη Διεθνή Ένωση Τηλεπικοινωνιών του ΟΗΕ, μόλις ο ένας στους 255 κατοίκους, είχε πρόσβαση στο Διαδίκτυο.

Το ενδιαφέρον της υπόθεσης, όμως, δεν είναι η κυβερνοεπίθεση στις υποδομές της Μιανμάρ. Ο ανταποκριτής του γαλλικού πρακτορείου σχολίασε πως οι περισσότεροι χρήστες κατηγορούν, για το τηλεπικοινωνιακό μπλακάουτ, την ίδια την κυβέρνηση. Ο λόγος είναι οι επερχόμενες εκλογές, κατά τις οποίες, έτσι κι αλλιώς, έχει απαγορευθεί η παρουσία και παρατήρηση των ξένων δημοσιογράφων. Συνεπώς είναι πολύ πιθανό να έχουμε μια ολοκληρωτική άσκηση πολιτικής λογοκρισίας. Στην ίδια λογική, αλλά με περισσότερο σκεπτικισμό, ο Κρεγκ Λάμποβιτς, στέλεχος της Arbor Networks, δήλωσε ότι «τέτοιες επιθέσεις δεν αποτελεί συχνό φαινόμενο να

έχουν γεωπολιτικά αίτια». Εντούτοις, η ίδια στρατιωτική κυβέρνηση άσκησε παρόμοια πολιτική στις διαδηλώσεις των μοναχών, το 2007 και τις εξεγέρσεις του 1998 (AFP - *Newsroom* ΔΟΛ, 4/11/10).

Παρεμφερής λόγος είχε αντίστροφα αποτελέσματα στην Κούβα το 2009. Χρήστες ιστολογίων (bloggers), με σκοπό τη διαμαρτυρία για τη λογοκρισία της κυβέρνησης στον κυβερνοχώρο, ξεκίνησαν μια σειρά κυβερνοεπιθέσεων, κάνοντας τα ψηφιακά μέσα να μιλούν για έναν «εμφύλιο κυβερνοπόλεμο» (AFP - www.kathimerini.gr, 22/5/2009).

Η σημασία των επεισοδίων αυξάνεται αν λάβουμε υπόψη μας τη σχέση του μικρού αριθμού χρηστών του διαδικτύου στη χώρα και το μέγεθος των αντικαθεστωτικών επιθέσεων. Στην Αβάνα, οι επίσημες κυβερνητικές ανακοινώσεις κατηγορούν τις ΗΠΑ, για επιστράτευση εγκάθετων (στην επίσημη ιστοσελίδα της κυβέρνησης, cubadebate.cu, όπου παραθέτει τις απόψεις του και ο Φιντέλ Κάστρο.). Παρόλα αυτά, υπάρχουν συγκεκριμένα αιτήματα των αντεπαναστατών για χορήγηση ταξιδιωτικών αδειών, βελτίωση του συστήματος υγείας και παιδείας και την αντιμετώπιση των πολιτικών κρατουμένων.

Αξιοσημείωτο δε είναι ότι πως οι πολίτες της Κούβας επιτρέπεται να έχουν πρόσβαση στο διαδίκτυο μόνο στα ιντερνέτ-καφέ. Η θέση της κυβέρνησης είναι ότι αυτή η κατάσταση οφείλεται στο εμπάργκο των ΗΠΑ, το οποίο αποκλείει την επικράτεια από τα αναγκαία υποθαλάσσια καλώδια τηλεπικοινωνιών και η εναλλακτική λύση των δορυφορικών συνδέσεων φέρνει υπερβολικές καθυστερήσεις. Για το ίδιο θέμα η Γιοάνι Σάντσεζ, που έχει τιμηθεί με τα βραβεία ψηφιακής δημοσιογραφίας (2008) Spanish Ortega και Gasset, δηλώνει πως αυτά τα γεγονότα οδηγούν πολλούς νέους να αποκτούν λογαριασμούς εκτός χώρας, εφόσον δεν μπορούν να τους αποκτήσουν από το εγχώριο domain (.cu).

Επιπρόσθετα, μια χαρακτηριστική περίπτωση λογοκρισίας στον κυβερνοχώρο έχουμε στην Τουρκία, όπου ο νέος νόμος περί διασφάλισης του διαδικτύου, υποχρεώνει τους παρόχους των παρεμφερών υπηρεσιών να φιλτράρουν (ως τις 22/8/2011) μια σειρά λέξεων, οι οποίες δεν θα πρέπει να αναφέρονται. Ειδικότερα, από το Συμβούλιο της Πληροφορικής και νέων Τεχνολογιών (που υπάγεται στον πρωθυπουργό) απαγορεύθηκε η χρήση 138 όρων-κλειδιά. Οι ως τώρα δικλείδες ασφαλείας στη χρήση του διαδικτύου ήταν προαιρετικές· στο εξής, η οποιαδήποτε αποφυγή των

προτεινόμενων φίλτρων θα αντιμετωπίζεται ως ποινικό αδίκημα. Επίσης, το ισχύον νομικό καθεστώς κατονόμαζε την απαγόρευση συγκεκριμένων ιστοτόπων, όπως το YouTube. Αρχικά, ωστόσο, κάποιοι γνώστες μπορούσαν να αποκαταστήσουν τη δυνατότητα πρόσβασης, εφόσον μπορούσαν να εκπληρώσουν ορισμένες τεχνικές προϋποθέσεις (όπως η αλλαγή του DNS). Η κυβέρνηση διαβεβαίωσε ότι ούτε αυτό πλέον θα ισχύει (nooz.gr, 5/5/2011).

Πολλές ήταν οι αντιδράσεις από διάφορους φορείς, μεταξύ των οποίων συμπεριλαμβάνονται Μη-Κυβερνητικές Οργανώσεις, δημοσιογράφοι και εκπρόσωποι των ακαδημαϊκών ιδρυμάτων⁸⁷. Σημειώνουμε πως από το 2001 έχει ήδη απαγορευθεί η ανάρτηση 5000 ιστοσελίδων.

Μια ομάδα από ακτιβιστές του διαδικτύου απείλησε πως θα προσφύγει στο Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, αν δεν καλυφθούν από τα τουρκικά ένδικα μέσα. Στην ίδια λογική το κόμμα της αξιωματικής αντιπολίτευσης (CHP) κατηγορεί την κυβέρνηση για «καταστρατήγηση των πολιτικών κριτηρίων της Κοπεγχάγης, της οποίας το σεβασμό ζητά η ΕΕ από τις υποψήφιες χώρες» (/tro-ma-ktiko.blogspot.com, 1/6//2011).

Σε ένα άλλο περιστατικό, σε μια συζήτηση την οποία είχε ο πρόεδρος της κινεζικής κυβέρνησης Χου Τζιν Τάο, δήλωσε ότι θεωρεί πως το μελλοντικό πεδίο μάχης θα είναι ο «εικονικός κόσμος» (Reuters - www.kathimerini.gr, 9/3/2011). Το ενδιαφέρον είναι ότι, κατόπιν εξήγησε πως η μέριμνα του θα εστιαστεί στους τρόπους που καθοδηγείται η κοινή γνώμη στον κυβερνοχώρο. Το σχόλιο του David Bandurski, ερευνητή στο China Media Project του πανεπιστημίου του Χονγκ-Κονγκ, ήταν πως το ζήτημα σχετίζεται με τον έλεγχο της ηλεκτρονικής διακυβέρνησης. Την κατάσταση ωστόσο δυσχέραине η ανακοίνωση του Γουάνγκ Τσέν, επικεφαλής του γραφείου πληροφοριών του κράτους, μετά από σχετική σύσκεψη, ότι μελετάται η επιβολή της υποχρέωση των συμμετεχόντων στον κυβερνοχώρο πολιτών, να καταγράφουν τα πραγματικά τους ονόματα σε οποιαδήποτε διαδικτυακή συναλλαγή (BBC - www.kathimerini.gr, 12/5/2010).

Μια από τις σημαντικότερες επιπτώσεις αυτού του ζητήματος ήταν και η εγκαθίδρυση του γνωστού ως «Μεγάλο Τείχος» (“Great Firewall”), το οποίο είχε τη

⁸⁷ «Θέλουν να κάνουν το διαδίκτυο ασφαλές ή είναι ένας τρόπος λογοκρισίας;... ελεύθερο από φίλτρα διαδίκτυο είναι ένα ανθρώπινο δικαίωμα.» διερωτάται ο νομικός Γ. Ακντενίτζ σε μια τουρκική εφημερίδα ευρείας κυκλοφορίας (Hurriyet, 9/5/2011).

δυνατότητα να αποτρέψει την είσοδο από την μεγαλύτερη διαδικτυακή αγορά στον κόσμο, σε ορισμένες από τις επίσης μεγαλύτερες επιχειρήσεις του διαδικτύου παγκοσμίως. Το συγκεκριμένο «τείχος διαδικτυακής ασφάλειας», είχε αποκλείσει στο παρελθόν, επίσης μεγάλες αμερικανικές εταιρείες από το κινεζικό κοινό, όπως τις Microsoft, Twitter και Yahoo! (<http://www.spacewar.com/cyberwars.html>, 25/3/10). Ωστόσο, το θέμα πήρε τις μεγαλύτερες διαστάσεις όταν άρχισε η αντιπαράθεση μεταξύ της Κινεζικής κυβέρνησης και της Google⁸⁸. Η κινεζική κυβέρνηση είχε υποχρεώσει την εταιρεία να φιλτράρει ορισμένες λέξεις-κλειδιά, οι οποίες είχαν για αυτήν επιπτώσεις στην κοινωνική της συνοχή. Ενδεικτικά, ορισμένοι από τους όρους, οι οποίοι χαρακτηρίστηκαν ευαίσθητοι είναι οι «"Falun Gong", "Tibet riot" και "June 4"»⁸⁹ (<http://www.spacewar.com/cyberwars.html>, 23/3/10).

Η Google αδειοδοτήθηκε τον Ιανουάριο του 2006, με την έγγραφη όμως αποδοχή εφαρμογής των όρων της κινεζικής λογοκρισίας. Στην πορεία, εν τούτοις, ορισμένοι από αυτούς τους όρους φαίνεται ότι παρακάμφθηκαν, σύμφωνα με τη δήλωση του εκπρόσωπου τύπου της κινεζικής κυβέρνησης ("violated its written promise"). Σε αντίθεση με αυτό η εταιρεία ισχυρίστηκε ότι δεν μπορεί να λογοκρίνει όλα αυτά που της ζητούνται.

Οι εκτάσεις που πήρε το θέμα μεγεθύνθηκαν εξαιτίας δύο παραγόντων. Ο πρώτος είναι οικονομικός και ο δεύτερος και σημαντικότερος πολιτικός. Ως προς τον πρώτο, αρκεί να λάβουμε υπόψη μας ότι η κινεζική αγορά είναι η μεγαλύτερη στον κυβερνοχώρο (384 εκατομμύρια χρήστες). Άρα οι συνέπειες των απωλειών θα ήταν πολύ μεγάλες. Όταν η εταιρεία συνυπέγραψε με την Κίνα, στη Wall Street, τα κέρδη ήταν σημαντικά⁹⁰. Για την επίλυση αυτού του προβλήματος η εταιρεία αποφάσισε να «εκπέμψει» από το Χονγκ Κονγκ. Αν και ο εκπρόσωπος της Google στο Πεκίνο Marsha Wang, δήλωσε ότι δεν είχε ενημερωθεί για απολύσεις, οι επιπτώσεις στο χρηματιστήριο ήταν δεικτικές.

⁸⁸ Η Google είναι η πρώτη σε επισκεψιμότητα ιστοθέση στον κόσμο, καθώς επίσης και η πρώτη σε επισκεψιμότητα μηχανή αναζήτησης στον κόσμο, αλλά η δεύτερη στην Κίνα. Δεύτερη μηχανή αναζήτησης στον κόσμο -και πρώτη στην Κίνα- είναι η κινεζική baidu.com (5^η ιστοθέση παγκοσμίως) και τρίτη, η ρωσική yandex.ru (21^η ιστοθέση παγκοσμίως) (<http://www.alexa.com/topsites>, 29/9/2011). Η έδρα της εταιρείας είναι στην Καλιφόρνια και ιδρύθηκε το 1998, από τους απόφοιτοι του Πανεπιστημίου του Στάνφορντ Larry Page και Sergey Brin, οι οποίοι είχαν ξεκινήσει δύο χρόνια πριν (<http://www.google.gr/about/corporate/company/>).

⁸⁹ Και οι τρεις περιπτώσεις αφορούν σε πολιτικές κινήσεις, οι οποίες αντιδρούσαν στον τρόπο που η κινεζική κυβέρνηση χειριζόταν κοινωνικές και πολιτισμικές ελευθερίες.

⁹⁰ Από 1.52% την προηγούμενη ημέρα, με τιμή μετοχής 549.00 δολάρια, τα κέρδη έφθασαν στο 2.62%, για να κλείσει η τιμή της μετοχής στα 594.88 δολάρια.

Σχετικά με τις πολιτικές προεκτάσεις, διακρίνουμε δύο όψεις εκδήλωσης του ζητήματος, μια επιφανειακή και μια αφανή, τόσο από την αμερικανική, όσο από την κινεζική πλευρά. Θα ξεκινήσουμε από την πρώτη, την επιφανειακή. Στη δημοσιότητα, λοιπόν, λακωνικές δηλώσεις για το θέμα έγιναν από την κορυφή της αμερικανικής πολιτειακής ιεραρχίας. Ο κοινός τόπος όλων ήταν ότι δεν δικαιολογείται άμεση κρατική εμπλοκή. Ο ίδιος ο πρόεδρος Barack Obama, δήλωσε πως είναι πολύ σπουδαίο θέμα η ελεύθερη διακίνηση της πληροφορίας στον κυβερνοχώρο (<http://www.spacewar.com/cyberwars.html>, 23/3/2010). Η υπουργός των εξωτερικών Hillary Clinton σε έναν μεγάλο λόγο, κατά τον οποίο εξύμνησε το θέμα της ελευθερίας στο διαδίκτυο, κάλεσε τις αμερικανικές επιχειρήσεις να αντιτίθενται σε οποιαδήποτε μορφή λογοκρισίας ([spacewar.com](http://www.spacewar.com), 27/3/10). Ο εκπρόσωπος του Στέιτ Ντιπάρτμεντ Philip Crowley, είπε ότι η κυβέρνηση των Ηνωμένων Πολιτειών δεν μπορεί να παρέμβει, αφού δεν υπήρξε μέρος, στην απόφαση της Google να παρέχει πλέον πληροφορίες από το -μη λογοκριμένο- Χονγκ Κονγκ στην κινεζική γλώσσα. Όσον αφορά το διπλωματικό χειρισμό της Κίνας, αυτός περιορίστηκε στο να θεωρεί το θέμα ως ένα ζήτημα «εμπορικής τακτοποίησης» και τίποτα περισσότερο. Σε αυτήν την κατεύθυνση, ο εκπρόσωπος τύπου του κινεζικού υπουργείου εξωτερικών, Qin Gang, περιέγραψε την κατάσταση ως «μια ακόμα διευθέτηση μιας περίπτωσης του εμπορίου και το εμπόριο στην Κίνα είναι εντελώς ανοικτό» (www.spacewar.com, 23/3/10).

Παρόλα αυτά, υπήρχε, όπως αναφέραμε, και μια αφανής όψη, η οποία είναι και ιδιαίτερα σημαντική στην ανάλυσή μας. Η αύξηση των στρατηγικών επενδύσεων στην Κίνα, των μεγαλύτερων αμερικανικών επιχειρήσεων, δημιούργησε ένα φόβο εξάρτησης από τις ΗΠΑ (Dmitry Kosyrev, *RIA Novosti*, Moscow, Russia - Mar 30, 2010). Έτσι, είναι πιθανό να έγιναν προσπάθειες αποτροπής αυτού του γεγονότος. Από την άλλη μεριά διαπιστώθηκε ότι την μετακόμιση της εταιρείας στο Χονγκ Κονγκ, συνόδεψαν μια σειρά συντονισμένων κυβερνοεπιθέσεων. Αυτές ξεκίνησαν από το μπλοκάρισμα της παροχής ηλεκτρονικού ταχυδρομείου και στη συνέχεια επεκτάθηκαν σε άλλες λειτουργίες της.

Σύμφωνα με τους New York Times, η Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ ανακάλυψε ότι η προέλευση αυτών των κυβερνοεπιθέσεων, έφθανε μέχρι το Πανεπιστήμιο Ζιαοτόνγκ της Σαγκάης, το οποίο έχει τη φήμη του ιδιαίτερα καινοτόμου στον τομέα της πληροφορικής. Αυτό γίνεται ακόμη πιο σημαντικό, όταν το θερινό τμήμα της σχολής ήταν υπεύθυνο για την εξειδίκευση, στα θέματα της

ασφάλειας δικτύων, του κινεζικού στρατού (Associated Press, 19/2/2010). Πιο συγκεκριμένα, οι αξιωματικοί και επιστήμονες της Ακαδημίας Στρατιωτικών Επιστημών (συνταγματάρχες Γιε Ζενγκ και Ζάο Μπαοζιάν) τόνισαν ότι ο στρατός της Λαϊκής Δημοκρατίας της Κίνας, θα δώσει μεγάλο βάρος στο αξιόμαχο του προσωπικού του, ως προς τις δυνατότητες διεξαγωγής κυβερνοπολέμου. Εξακολούθησαν, παραλληλίζοντας τον πόλεμο στο διαδίκτυο με τα πυρηνικά όπλα. Τα μεν, εξήγησαν, ανήκουν στη βιομηχανική και τα δε στην εποχή της πληροφορίας. Σε κάθε πάντως περίπτωση, κατέληξαν, οι συνέπειες μπορεί να είναι καταστροφικές (Reuters, 3/6/2011)⁹¹. Εξάλλου, η φήμη της Κίνας για τις επιδόσεις της στις νέες τεχνολογίες είναι γενικότερη⁹².

Πριν ολοκληρώσουμε το θέμα θα δείξουμε μέσα από μια μελέτη τον τρόπο που οι κινέζοι αντιλαμβάνονται την έννοια της «κυβερνοαπειλής». Η κυβερνητικά επιδοτούμενη Κινεζική Ακαδημία Κοινωνικών Επιστημών (China Academy of Social Sciences - CASS) δημοσίευσε την ετήσια έκθεση της σχετικά με την ανάπτυξη των Κοινωνικών Μέσων. Το συμπέρασμά της ήταν ότι οι ιστοθέσεις κοινωνικής δικτύωσης, όπως το Facebook και το Twitter, συνιστούν απειλή εθνικής ασφαλείας διότι επιχειρούν την ενίσχυση ανατρεπτικών κινημάτων από δυτικά κράτη, των ΗΠΑ συμπεριλαμβανομένων (AFP, 9/7/2010). Μια από τις αρκετές περιπτώσεις που παρατέθηκαν, ώστε να τεκμηριώσουν τα αποτελέσματα της έρευνας, είναι τα «προπαγανδιστικά μηνύματα» συγκεκριμένων ιστοσελίδων, οι οποίες ανήκουν σε αμερικανούς και ευρωπαίους. Αυτές, κατά τα περυσινά γεγονότα, στάθηκαν στο πλευρό, ενός μέρους των κατοίκων της Xinjiang (περιοχή της δυτικής Κίνας), οι οποίοι εξεγέρθηκαν διεκδικώντας την αυτονομία τους. Τόνισαν ότι υποστηρίζεις αυτού του είδους κρύβουν πολιτικές σκοπιμότητες.

Τέλος, η έκθεση καταλήγει με την προτροπή στην κινεζική κυβέρνηση να δώσει ιδιαίτερη προσοχή, διότι ο έλεγχος της πολύπλοκης κοινωνικής δικτύωσης είναι πολύ δύσκολο εγχείρημα.

Στη συνέχεια θα εξετάσουμε έναν άλλο τρόπο κυβερνητικής παρέμβασης, με σκοπό τη γενικότερη κοινωνική επιρροή, διαμέσου του κυβερνοχώρου. Με πρωτοβουλία του

⁹¹ http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_03/06/2011_393463

⁹² Ενδεικτικά, την πρώτη θέση στην επίσημη κατάταξη για τους ταχύτερους υπολογιστές, πρόκειται να πάρει ο *Tianhe-1A*, σύμφωνα με τον Τζακ Ντονγκάρα του Πανεπιστημίου του Τενεσί. Ο εν λόγω H/Y είναι ικανός για 2,5 τρισεκατομμύρια υπολογισμούς ανά δευτερόλεπτο. Δεν λείπουν πάντως και οι δηλώσεις πως η ρίζα της τεχνογνωσίας βρίσκεται στην Intel (ΔΟΛ, *Newsroom* -29/10/10).

υπουργείου εξωτερικών του Ισραήλ, εκπαιδεύτηκαν διπλωμάτες στη χρήση κοινωνικών δικτύων. Η αποστολή τους θα είναι η αντιμετώπιση της φιλοαραβικής προπαγάνδας στον κυβερνοχώρο. Σε αυτή την κατεύθυνση όμως κινήθηκαν και μη κυβερνητικές οργανώσεις, οι οποίες συντονίζουν τα μέλη τους σε μια καμπάνια «αντί-πληροφόρησης», όπως η παγκόσμια οργάνωση ιουδαίων μαθητών, που αριθμεί 5,000 μέλη (World Union of Jewish Students - WUJS) (timesonline.co.uk, 28/7/2006).

Ανάλογα περιστατικά έχουν παρατηρηθεί και από την κυβέρνηση του Ισραήλ. Οι υπηρεσίες ασφάλειας προειδοποιούν τους εβραίους κατοίκους της περιοχής, ότι υπάρχει μεγάλο ρίσκο όταν συμμετέχουν σε ιστοσελίδες της λεγόμενης κοινωνικής δικτύωσης. Χαρακτηρίζουν το διαδίκτυο ως «εμπόλεμη ζώνη» ("the internet is a war zone»), όπου οι εχθροί τους από τις Hamas και Hezbollah караδοκούν. Ειδικότερα, ο αναλυτής πληροφοριών του ισραηλινού κράτους, Dr Ronen Bergman, διατυπώνει δύο φόβους. Αφενός, το ενδεχόμενο του κυβερνοσμποτάζ των ισραηλινών ιστοσελίδων και αφετέρου, την εκμαίευση σημαντικών μυστικών από τους στρατιώτες – χρήστες του παγκόσμιου ιστού (bbc.co.uk, 15/6/2009).

Με αφορμή τη διεξαγωγή εκλογών στο Ιράν, η κυβέρνηση επέβαλε εκτεταμένη λογοκρισία στον παγκόσμιο ιστό. Η αιτία ήταν ότι αποδείχθηκε ο πιο προσφιλής τρόπος συνάντησης όσων ήθελαν να διαμαρτυρηθούν, σχετικά με το καθεστώς. Χαρακτηριστικοί είναι οι τίτλοι ορισμένων ψηφιακών μέσων, οι οποίοι ανέγραψαν: «αντάρτες κυβερνοπολέμου» (guerrilla cyberwar) (www.foxnews.com, 10/1/2011). Σημαντικό στοιχείο εδώ, είναι ότι στην Τεχεράνη λειτουργούν τα περισσότερα καταστήματα με υπηρεσίες πρόσβασης στο διαδίκτυο (Ιντερνέτ – καφέ) στη Μέση Ανατολή από πολλά μέρη της Ευρώπης. Επίσης, βάσει έρευνας του πανεπιστημίου το Χάρβαρντ, το 2008 καταμετρήθηκαν 60.000 ιρανικά blogs (www.kathimerini.gr, 14/2/2010).

Ένα καναδικό ερευνητικό εργαστήριο, γνωστό από την αποκάλυψη μεγάλων εγχειρημάτων υποκλοπών (Ghostnet⁹³), συνέβαλε καθοριστικά ώστε να ξεπεράσουν οι ιρανοί χακτιβιστές τους φραγμούς που έθεσε το κράτος στην πρόσβαση στο διαδίκτυο. Πρόκειται για το εργαστήριο Citizen Lab, του Πανεπιστημίου του

⁹³ Βλέπε υποκεφάλαιο 4.3.3: Διεisdύσεις.

Τορόντο, το οποίο διευθύνει ο Ρον Ντάιμπερτ. Σε συνέντευξή του εξήγησε ότι συχνά είναι πολύ εύκολο να προσπεράσεις τους φραγμούς της λογοκρισίας, όπως το να πληκτρολογήσεις την αριθμητική διεύθυνση της ιστοσελίδας⁹⁴. Η μέθοδος όμως που προτείνει, προέβλεπε ορισμένοι δυτικοί που ενστερνίζονταν τον αγώνα των ιρανών να μετατρέψουν τον Η/Υ τους σε «proxy», ώστε μέσω αυτών, να παραμένουν online οι λογοκριμένοι. Πάντως, τονίστηκε ότι, και μετά από αυτή τη μέθοδο, εξακολουθεί ο κίνδυνος παρακολούθησής τους από τις αρχές.

Η τεχνική «proxy» είναι ένας τρόπος αντίστασης στα φίλτρα του αντιπάλου (Michelle Moghtader of the National Iranian American Council, WashingtonPost.com). Όλα ξεκίνησαν από την ίδρυση της εταιρείας Psiphon Inc (http://psiphon.ca/?page_id=94), η οποία εμπορεύεται το βραβευμένο πρόγραμμα παράκαμψης της λογοκρισίας Psiphon. Με αυτόν τον τρόπο δεν χρειάζεται να αναζητούνται χρήστες για να διαθέσουν την υπολογιστική τους ισχύ. Αντί αυτού, διατίθενται proxy servers της εταιρείας, οι οποίοι αποκαθιστούν τη σύνδεση στο διαδίκτυο. Σχετικές μετρήσεις αναφέρουν 18.000 Ιρανούς συνδρομητές.

Μετά από αυτήν την εμπειρία, η ιρανική κυβέρνηση Αχμεντινετζάντ πήρε δύο μέτρα. Το πρώτο ήταν η θεσμοθέτηση ειδικής *αστυνομίας περιφρούρησης του διαδικτύου*. Αυτή η υπηρεσία θα διαθέτει εξοπλισμό υψηλής τεχνολογίας για την παρακολούθηση των πολιτών, την οποία -έχει ιδιαίτερη σημασία- ότι προμηθεύθηκε από τις δυτικές εταιρείες Nokia και Siemens (Wall Street Journal).

Το δεύτερο μέτρο πρόληψης των δυνητικών εξεγέρσεων ανταρτών του κυβερνοχώρου, είναι η ταχεία εγκατάσταση «εθνικού κλειστού διαδικτύου». Σύμφωνα με υπουργό Επικοινωνιών της χώρας, Ρεζά Τακιπούρ, θα διατίθεται στην περσική γλώσσα και θα είναι έτοιμο μέσα στο χρόνο, το 2011.

Όσον αφορά την ευρυζωνικότητα, οι τεχνικές του δυνατότητές θα αφορούν σε συνδέσεις των 8 Mbps για τους οικιακούς χρήστες, με στόχο να φθάσουν τα 20 Mbs. Τέλος, σχεδιάζεται, μέσα στον επόμενο χρόνο επίσης, να είναι έτοιμη και η «εθνική μηχανή αναζήτησης». Επικρατέστερο όνομα θεωρείται το "Ya Haq" («καλώντας τον Θεό»), κάτι όμως που, από τον τρόπο που προφέρεται θυμίζει το "Yahoo" (news.in.gr, 10/9/2011).

⁹⁴ Συνέντευξη στην Κ. Οικονομάκου, *Έντυπη Έκδοση*, Ελευθεροτυπία, Σάββατο 18 Ιουλίου 2009.

Για διαφορετικούς λόγους, η Google, είχε προβλήματα που μπορούν να τοποθετηθούν στο ζήτημα της λογοκρισίας και στη Γερμανία. Πιο συγκεκριμένα, το θέμα αφορά ένα ειδικό τομέα της εταιρείας, το οποίο καλείται Google Street View. Το αντικείμενό της εστιάζεται στη χαρτογράφηση των δρόμων, συγκροτώντας έτσι, οδοδείκτες για διάφορα μέρη της υφελίου. Για την επίτευξη αυτού του σκοπού, διατίθενται κινητές κεραίες (διακινούμενες από οχήματα της εταιρείας), οι οποίες συνδέονται με δορυφόρους και συλλέγουν, επεξεργάζονται αυτόματα και αποστέλλουν ηλεκτρονικά ψηφιακές πληροφορίες στην κεντρικής βάσης δεδομένων της εταιρείας (maps.google.com, 6/11/2011).

Στα πλαίσια αυτού του έργου, «επιστρατεύθηκαν» τα ανάλογα οχήματα με τις κεραίες και ξεκίνησαν την περιοδεία τους στην γερμανική επικράτεια. Σύντομα όμως εντοπίστηκε από τις γερμανικές αρχές ότι συλλέγονταν ταυτόχρονα και διάφορα ευαίσθητα προσωπικά δεδομένα των γερμανών πολιτών. Αυτό προφανώς ήταν παράνομο και επιπρόσθετα η κατάσταση επιδεινώθηκε, όταν διαδόθηκαν υποψίες πως αυτά τα δεδομένα ενδέχεται να αποκτήσουν και ορισμένοι ιδιωτικοί οργανισμοί, οι οποίοι θα τα χρησιμοποιήσουν για ίδιον όφελος.

Μετά από αυτό, η γερμανική κυβέρνηση απαγόρευσε τις δραστηριότητες της Google Street View. Επίσης, σε σύντομο χρονικό διάστημα κατάρτισε και ψήφισε νόμο περί της απαγόρευσης της συλλογής ορισμένου είδους πληροφοριών, οι οποίες αφορούν τους χρήστες του διαδικτύου. Ειδικότερα, ο γερμανός υπουργός των εξωτερικών, Τόμας Ντε Μεζιέρ, παρουσίασε ένα νομοσχέδιο, το οποίο κατονομάζει τους κανόνες, με τους οποίους οφείλουν να συμμορφώνονται οι εταιρείες και απαγορεύει την συλλογή συγκεκριμένων δεδομένων σχετικά με τους χρήστες του διαδικτύου.

Επίσης, οι εν λόγω ρυθμίσεις αφορούν και διαδικτυακούς τόπους, οι οποίοι συγκεντρώνουν προσωπικά δεδομένα, ώστε να διαμορφώνουν το προφίλ των πολιτών-χρηστών. Προβλέπεται αυστηρά, η συγκατάθεση της πολιτείας (tonima.gr, 2/12/2010).

Ωστόσο, η υπηρεσία Street View της Google, συνεχίζει και επεκτείνει τις δραστηριότητές της. Πλέον, προσφέρει στο καταναλωτικό κοινό εικονική ξενάγηση, με δυνατότητα περιήγησης 360 μοιρών, σε διάφορα καταστήματα, τα οποία επιθυμούν τη διαφήμισή τους. Το πρόγραμμα το οποίο στηρίζει αυτή τη λειτουργία βασίζεται στο Google Art, βάσει του οποίου είχε θεμελιωθεί και η τεχνολογία του Street View. Σήμερα, η υπηρεσία είναι διαθέσιμη σε πολυκαταστήματα στις ΗΠΑ,

την Ιαπωνία, το Παρίσι, το Λονδίνο, την Αυστραλία και τη Νέα Ζηλανδία (news.in.gr, 29/10/2011).

Στους νέους φόβους για παραβίαση της ιδιωτικότητας, η εταιρία απαντά ότι δεν υπάρχει κανένας κίνδυνος, εφόσον οι κάμερες θα τοποθετούνται στο εσωτερικό των καταστημάτων, μετά από άδεια των ιδιοκτητών τους.

Ίσως η σημαντικότερη εξουσία της σχέσης της πολιτικής με το κυβερνοχώρο, είναι η δυνατότητα της ηγεσίας μιας χώρας να διακόψει τη σύνδεση -δηλαδή ουσιαστικά τη λειτουργία- του διαδικτύου από τους πολίτες⁹⁵. Στην περίπτωση των ΗΠΑ, ο πρόεδρος έχει το δικαίωμα να το κάνει σε ειδικές συνθήκες, από το β' παγκόσμιο πόλεμο. Αυτήν την εποχή όμως, το Κογκρέσο, συζητά την αφαίρεση αυτής της εξουσιοδότησης.

Το ιστορικό αυτής της υπόθεσης ανάγεται στο 1942, μετά την ιαπωνική επίθεση στο Pearl Harbor. Τότε το Κογκρέσο των ΗΠΑ, έδωσε διευρυμένες εξουσίες Franklin Roosevelt, να διακόψει κατά την κρίση του τις τηλεφωνικές συνδέσεις, καθώς επίσης και αυτή του τηλεγραφικού δικτύου. Στις ημέρες μας όμως, αυτές οι ανάγκες καλύπτονται από τον κυβερνοχώρο, για τον οποίο η σχετική αμερικανική νομοθεσία δεν είναι σαφής⁹⁶. Επίσης, το θέμα περιπλέκεται όταν θα πρέπει να γίνουν ειδικές ρυθμίσεις για την προστασία της ελευθερίας στον κυβερνοχώρο. Τα παραπάνω υπογραμμίζει και ο Paul Rosenzweig, πρώην αξιωματικός στην υπηρεσία εγχώριας ασφάλειας του προέδρου George W Bush (bbc.co.uk., 24/11/2010).

⁹⁵ Οι Αμερικανοί χρησιμοποιούν μια εμφατική έκφραση για αυτό, «internet kill switch». Θα λέγαμε πως είναι κάτι ανάλογο με την ελληνική έκφραση «κλείσιμο της στρόφιγγας» για τα ενεργειακά θέματα.

⁹⁶ Για την ακρίβεια, αυτό το θέμα μνημονεύεται στο section 706(d) of the Communications Act.

ΤΜΗΜΑ ΙΙΙ
Η ΘΕΩΡΙΑ

5. ΠΡΟΣΕΓΓΙΣΗ

Θυμίζουμε ότι αντικειμενικό μας σκοπό αποτελεί η κατηγοριοποίηση των γεγονότων τα οποία επιλέγουν δημοσιογράφοι, ειδικοί ερευνητές και αρμόδιοι θεσμικοί παράγοντες, για να αναφέρονται μέσω του τύπου στο φαινόμενο του κυβερνοπολέμου. Για αυτό τον σκοπό, στο πρώτο τμήμα, θέσαμε ένα «ψυχοκοινωνικό» κριτήριο ταξινόμησης των παραπάνω απόψεων, σύμφωνα με το οποίο τις διακρίναμε σε τέσσερις θεματικές κατηγορίες.

Στο δεύτερο τμήμα επιχειρούμε να ερμηνεύσουμε αυτές τις θεματικές κατηγορίες. Να αναζητήσουμε δηλαδή τις θεωρητικές τους ρίζες και να εξηγήσουμε τη συνάφειά τους με αυτές. Ξεκινάμε, στο πρώτο μέρος, με τη διερεύνηση του πολεμικού φαινομένου. Ιδιαίτερης σημασίας ορόσημο -για λόγους που θα εξηγήσουμε- εκτιμούμε ότι είναι η εποχή η οποία ξεκινάει μετά το δεύτερο παγκόσμιο πόλεμο. Τότε που από τον πληροφοριακό πόλεμο περνάμε στον πληροφορικό και δυνητικά, στον κυβερνοπόλεμο. Για να κατανοήσουμε τον τελευταίο, αφού παρουσιάσουμε συνοπτικά τις κλασσικές επιστημονικές θέσεις, καταλήγουμε στην αναγκαιότητα εμβάθυνσης στην έννοια του κυβερνοχώρου. Αυτό κάνουμε στο δεύτερο μέρος. Κρίνουμε ότι αποτελεί ένα εξαιρετικά κομβικό σημείο, ώστε να μπορέσει να ελεγχθεί και η ισχύ της τρίτης υπόθεσης της παρούσας εργασίας. Για αυτόν το λόγο τολμούμε να συγκροτήσουμε μια θεώρηση, η οποία να δύναται να αιτιολογήσει τη φύση των ερευνητικών μας πορισμάτων, δηλαδή των τεσσάρων θεματικών κατηγοριών. Σε αυτό το στόχο οδηγούμαστε από τον πυρήνα μιας κοινωνιοψυχολογικής προσέγγισης, όπως εν ολίγοις την προσδιορίζουμε στη συνέχεια.

Ο πυρήνας, από τον οποίο ξεκινάει η ανάλυση στην επιστήμη της Κοινωνικής Ψυχολογίας βρίσκεται στη σχέση του ατόμου με την κοινωνία. Ειδικότερα, το ενδιαφέρον εστιάζεται στη θεραπεία των συγκρουσιακών μορφών αυτής της σχέσης⁹⁷. Οπότε, όταν επικαλούμαστε την κοινωνιοψυχολογική προσέγγιση ενός αντικειμένου – φαινομένου, εννοούμε πως ερευνούμε την αλληλεπίδραση των βιωμένων νοημάτων, αποτέλεσμα των κοινωνικών και ψυχολογικών διεργασιών στη συμπεριφορά των ανθρώπων, η οποία προκύπτει από το υπό εξέταση φαινόμενο.

Βεβαίως, σε γενικές γραμμές, το ίδιο μπορούν να ισχυριστούν οι κοινωνιολόγοι και οι ψυχολόγοι για την επιστήμη τους. Σε αυτό το σημείο, θα πρέπει να τονίσουμε

⁹⁷ «Ως προς ένα βαθμό (η Κοινωνική Ψυχολογία) είναι η μόνη που κάνει κάτι τέτοιο: προσπαθεί να καταλάβει γιατί επέρχεται σύγκρουση ανάμεσα στα άτομα και την κοινωνία.» (Παπαστάμου, 1989, 13).

ένα ιδιαίτερο γνώρισμα της Κοινωνικής Ψυχολογίας. Πέραν, των «καθαρά» κοινωνικών συνθηκών (δομή, κοινωνικοί κανόνες κοκ) και ψυχολογικών ιδιαιτεροτήτων ενός ατόμου (π.χ. έντονη παρορμητικότητα στην προστασία του βασικού ενστίκτου ζωής), υπάρχει και ένα άλλο διακριτό στάδιο, στο οποίο περικλείονται κίνητρα συμπεριφοράς. Αυτό συνίσταται από την εκπεφρασμένη τριαδική σχέση (Maisonneuve, 1973/2001, 33), στην οποία οφείλει να επικεντρώνεται το βλέμμα του παρατηρητή μιας κοινωνιοψυχολογικής έρευνας (Παπαστάμου, 1989, 17). Με αυτή την «τριαδική ματιά» ερευνούμε την αλληλεπίδραση πρώτον, ενός υποκειμένου (ατομικού-εγώ ή συλλογικού-εμείς) και δεύτερον, ενός δεύτερου υποκειμένου – του *άλλου*⁹⁸ (ατομικού-εκείνος ή συλλογικού-εκείνοι)· τρίτον, ως προς ένα ορισμένο αντικείμενο μελέτης (όπως το πολεμικό φαινόμενο). Οι διαστάσεις δε του αντικείμενου μελέτης μπορεί να είναι μικρότερες ή μεγαλύτερες. Δηλαδή, ενδεικτικά, μπορεί να μελετάμε (α) την αλληλόδραση (όπως οι σχέσεις σεβασμού) που επήλθε (β) σε μια συγκεκριμένη κοινωνική ομάδα (το υποκείμενο: π.χ. στον στρατιωτικό κλάδο της αεροπορίας), στη σχέση της με (γ) μια άλλη κοινωνική ομάδα (ο άλλος: π.χ. στην πολιτική της ηγεσία), μετά από τη νίκη ή την ήττα της σε μια κρίσιμη μάχη. Σε διαφορετική περίπτωση, τέλος, μπορούμε να διερευνήσουμε την γενική κοινωνική αποδοχή για το στράτευμα, σε μια συγκεκριμένη περιοχή και περίοδο, η οποία προηγήθηκε ενός γεγονότος.

Στη συζήτηση που ακολουθεί, θα δείξουμε γιατί για τον Κλαούσεβιτς οι σχέσεις ηγεσίας, ένοπλων μέσων και λαού είναι σημαντικές. Στη συνέχεια, θα μελετήσουμε την οντολογική θέση της παραπάνω τριαδικότητας, στο νεωτερικό κράτος. Εν κατακλείδι, θα εμβαθύνουμε στη συσχέτιση των ηγεσιών με τον πόλεμο και πώς τελικά, αυτός επιδρά στην κοινωνία διαχρονικά.

⁹⁸ «Τη σχέση υποκειμένου με υποκείμενο και τη σύνδεση της με το αντικείμενο» (Moscovici, 1984, 9) «Αυτό ακριβώς μας διδάσκει η Κοινωνική Ψυχολογία: να βλέπουμε τη συλλογικότητα και την ατομικότητα αλληλένδετες και αλληλοεξαρτημένες» (Παπαστάμου, 1989, 21).

ΜΕΡΟΣ Α΄
Ο ΠΟΛΕΜΟΣ

6. ΘΕΩΡΗΣΗ ΤΟΥ ΠΟΛΕΜΟΥ

6.1 Φιλοσοφία του Πολέμου

Πολλοί συγγραφείς έχουν ασχοληθεί με το φαινόμενο του πολέμου. Ωστόσο, τα έργα τριών στρατηγών, δηλαδή ανθρώπων με προσωπική εμπειρία στην εκδήλωση ή υλοποίηση του πολεμικού φαινομένου, θεωρούνται κλασικά στη διεθνή βιβλιογραφία. Του έλληνα Θουκυδίδη⁹⁹ (5^{ος} αι. π.Χ.), του κινέζου Σουν Τζου¹⁰⁰ (περί τον 5^ο αι. π.Χ.) και του γερμανού Καρλ Φον Κλαούσεβιτς¹⁰¹ (18^{ος} αι. μ.Χ.). Ο πρώτος ασχολήθηκε με την ρεαλιστική πλευρά και κατέγραψε πραγματικά ιστορικά γεγονότα (Πελοποννησιακός Πόλεμος). Συνοπτικά, τόνισε ότι η αναγκαιότητα για την απόκτηση ή την επέκταση της ισχύος¹⁰² ενός κράτους αποτελεί τη βασική αιτία πολέμου. Ο δεύτερος ασχολήθηκε, κυρίως, με την πλευρά της στρατηγικής και κατέγραψε κατευθύνσεις νίκης σε μια μάχη. Επιπλέον, σε ένα από τα σημαντικότερα και πιο δημοφιλή αποφθέγματα του, υπογράμμισε ότι το μεγαλύτερο συμφέρον είναι να αποφύγεις τη σύρραξη, να κερδίσεις αναίμακτα (ενδεχομένως, επηρεασμένος από τη γενικότερη κινεζική φιλοσοφία της μη-βίας) και πάντα βασικός στόχος είναι να «διασκορπίσεις» την ενότητα του εχθρού, υπονοώντας την ευαισθησία όλων των πολιτικών υποκειμένων στο ζήτημα της εσωτερικής συνοχής. Άρα, εκτίμησε ότι χαρισματικός είναι ο ηγέτης, ο οποίος θα επιβάλει τη θέλησή του, δίχως να ασκήσει βία. Ο τρίτος στρατηγός και συγγραφέας στοχάστηκε τη φιλοσοφική διάσταση της έννοιας του φαινομένου (Κονδύλης, 1999, 344) και έγραψε ένα μνημειώδες έργο για τη θεωρία και την πράξη του.

Όπως, λοιπόν, προκύπτει από την παρουσίαση της συμβολής του καθένα, χρησιμότερος για την εννοιολογική οριοθέτηση του φαινομένου είναι ο Καρλ Φον Κλαούσεβιτς. Αυτός θεώρησε ότι οδοδείκτη στην κατανόηση της φύσης του πολέμου αποτελεί η διάκριση και η συσχέτιση των δυνάμεων του ανθρώπινου ψυχισμού και δη, της ανθρώπινης διάνοιας, που εμπλέκονται σε αυτό το φαινόμενο. Ειδικότερα, κατ' αυτόν, ο πόλεμος δεν είναι παρά μια μεγεθυμένη μονομαχία (Clausewitz, 1832/2003, 83). Επειδή, λοιπόν, όταν θέλουμε να προσδιορίσουμε την έννοια ενός όρου, αναπόφευκτα περιεργαζόμαστε και τη φύση του, εδώ μπορούμε αρχικά να

⁹⁹ Θουκυδίδου *Ιστορία*, Α. Βλάχος (μτφρ), Εστία (2005)⁸.

¹⁰⁰ Σουν Τζου, *Η Τέχνη του Πολέμου*, Δ. Παυλάκης (μτφρ), Φόρμιγξ, (1997)².

¹⁰¹ C. Clausewitz, *On War*, M. Howard & P. Paret (επιμ.&μτφρ.), Everyman's Library (2003)³.

¹⁰² «Ορίζουμε δε ως ισχύ, στην διεθνή βιβλιογραφία, την ικανότητα μιας χώρας να καθιστά τις λοιπές, του διεθνούς συστήματος έτοιμες να συναινούν με τις επιλογές της» (Μάζης, 2006, 26).

υποστηρίζουμε ότι η φύση της μονομαχίας και του πολέμου, θα πρέπει να' ναι όμοια. Διευκρινίζουμε πως επικαλούμενοι τη «φύση» ενός φαινομένου, εννοούμε τον πυρήνα των ενιαίων χαρακτηριστικών του. Τα αμετάβλητα, δηλαδή, γνωρίσματά του, ανεξάρτητα από τις αλλαγές στη μορφή της εκδήλωσής του. Σύμφωνα, λοιπόν, με τον Κλαούζεβιτς, τρία είναι τα συστατικά στοιχεία της φύσης του πολέμου. Πιο συγκεκριμένα, αυτά διαφαίνονται καθαρά, από τον τρόπο με τον οποίο αρχίζει και τελειώνει το πρώτο κεφάλαιο του πρώτου του βιβλίου, το οποίο τιτλοφορεί «Τι Είναι Πόλεμος». Εξαρχής, λοιπόν, διατυπώνεται ο ορισμός του πολέμου ως η ενέργεια εκείνη, η οποία με την άσκηση (ένοπλης) βίας επιβάλλει ένα (πολιτικό) υποκείμενο τη βούλησή του σε ένα άλλο (Clausewitz, 1832/2003, 83). Κατόπιν, ολοκληρώνοντας το εν λόγω κεφάλαιο, θέτει τα τρία υπαρξιακά μεγέθη (Κονδύλης, 1999, 22), ή αλλιώς συστατικά στοιχεία της φύσης του φαινομένου του πολέμου, τα οποία συνιστούν και τη γνωστή ως «παράδοξη τριτότητα». Αυτά είναι τα ακόλουθα:

- i. Η εχθρότητα, με τη μορφή της πρωτόγονης βιαιότητας, η οποία είναι αποτέλεσμα του μίσους ενός κοινωνικού σχηματισμού για κάποιον άλλον.
- ii. Ο καθοριστικός παράγοντας της τύχης, όπως προκύπτει από ένα παίγνιο πιθανοτήτων μεταξύ της αξιοποίησης των δεξιοτήτων και ευκαιριών, οι οποίες απρόσμενα και αναπόφευκτα εμφανίζονται στη ζωή.
- iii. Ο βαθμός τελικής επικράτησης της διακυβέρνησης, υπό την έννοια της υποταγής των ανθρώπινων ορμέφυτων τάσεων, στον ορθολογισμό της πολιτικής απόφασης.

Ο ίδιος ο Κλαούζεβιτς, κατά τη συγγραφή του, εμβαθύνει την παραπάνω ανάλυσή του και καταλήγει στον εντοπισμό μιας αντιστοιχίας των τριών γνωρισμάτων της φύσης του πολεμικού φαινομένου, με τα επίπεδα της κοινωνικής οργάνωσης. Έτσι, -κατ' αριθμητική αντιστοιχία- αντιπαραβάλλει (Μαυρόπουλος, 2008):

- i. Το συναίσθημα της εχθρότητας με το Λαό.
- ii. Την πιθανολογική ρύθμιση με τα Ένοπλα Μέσα.
- iii. Την εξορθολογισμένη διοίκηση με την Ηγεσία.

Διεξοδικότερα, από τον ορισμό, καθίσταται σαφές ότι ο πόλεμος αφορά σε μια πράξη πρωτόγονης βίας (εφόσον μπορεί να στοχεύσει και στο θάνατο), η ύπαρξη της οποίας έπεται της προαπαιτούμενης αντιπαλότητας (για κάποιο αντικείμενο, το οποίο

διεκδικούν τουλάχιστο δύο), και τέλος, την αποφασιστικότητα (βούληση) από έναν ιθύνων νου για πράξη. Αυτά τα στοιχεία δύνανται να εκληφθούν και ως οι απαραίτητες προϋποθέσεις για την εκδήλωση κάθε πολεμικού συμβάντος. Θα δείξουμε ότι υφίσταται απόλυτη αντιστοιχία με τους όρους της εν λόγω τριτότητας¹⁰³. Με μια πρώτη «επιφανειακή» ανάγνωση του ορισμού θα σημειώναμε ότι στον πόλεμο αρκούν δύο υποκείμενα (π.χ. κράτη) να διεκδικούν το ίδιο αγαθό (π.χ. υδάτινους πόρους), ώστε να οδηγηθούν σε σύγκρουση. Προχωρώντας όμως βαθύτερα στον ανθρώπινο ψυχισμό, διακρίνουμε την εμφάνιση ενός αισθήματος έχθρας, του οποίου γενεσιουργός αιτία είναι ο βαθμός σημαντικότητας της απόκτησης του εν λόγω αγαθού – βαθμός τέτοιος, που να δικαιολογεί την ανάληψη του ρίσκου εμπλοκής στην άσκηση βίας. Βεβαίως, θα πρέπει να τονισθεί ότι η επικράτηση της εχθρότητας δεν είναι μόνον ανάλογη τού πόσο ζωτικής αξίας είναι ένα αγαθό για κάποιον. Σε αυτό το σημείο υπεισέρχεται και παράγοντες ιδιοσυγκρασίας, ιδεολογίας και πολιτισμού των προαναφερόμενων ομάδων. Επιπλέον, όμως, εφόσον η συμβεί η διένεξη και κατά την εξέλιξη της, εκτός από τις υποκειμενικές προϋποθέσεις, υπάρχουν και οι αντικειμενικές συνθήκες. Πρόκειται για τον παράγοντα της τύχης, ο οποίος προσδίδει τις ευκαιρίες ή τις δυσκολίες από το ευρύτερο περιβάλλον τέλεσης τέτοιας πράξης. Η ύπαρξη αυτών των «εξωγενών» ή αντικειμενικών συνθηκών είναι που επιβάλλει την αναγκαιότητα της εκτίμησης και απόφασης, της τέλεσης ή μη, της πολεμικής πράξης από έναν πολιτικά αρμόδιο φορέα.

Ολοκληρώνοντας, θα πρέπει να διευκρινίσουμε ότι ο συγγραφέας αναφέρει τις παραπάνω αντιστοιχίες ως φορείς υλοποίησης των χαρακτηριστικών της φύσης του πολέμου, κάνοντας με αυτόν τον τρόπο, μια μετάβαση από τη θεωρία στην πράξη. Έτσι, η σύμπνοια του λαού σε ένα πολεμικό γεγονός προϋποθέτει την επικράτηση του αισθήματος της εχθρότητας για τον αντίπαλο. Το ζήτημα της αξιοποίησης των ευκαιριών, για το προβάδισμα στη νίκη, σχετίζεται με τις ικανότητες του στρατεύματος. Τέλος, τα απαραίτητα καθοδηγητικά διανοητικά προσόντα εμπλοκής και απεμπλοκής ανήκουν στην κυβέρνηση. Σε αυτό το σημείο της θεωρίας υπήρξε και η σύγχρονη κατάκριση, ότι η στοχαστική αφαίρεση της τριτότητας, δεν είναι καθόλου ρεαλιστική (Κουβελιώτης, 2002, 50).

Διαπιστώνουμε, όμως, ότι ο συγγραφέας έχοντας γνώση και εμπειρία της ρευστότητας στην εκδήλωση του φαινομένου, χαρακτήρισε τον πόλεμο

¹⁰³ Επίσης, στο επόμενο κεφάλαιο θα εμβαθύνουμε περισσότερο την κοινωνική μας έρευνα σε αυτές τις αντιστοιχίες.

«χαμαιλέοντα». Με αυτή του την ιδιότητα περιέγραψε παραστατικά ότι είναι διαφορετικός σε κάθε εκδήλωσή του και εκτός από τα θεμελιώδη του χαρακτηριστικά, παίζουν σημαντικό ρόλο και άλλα, όπως ο ψυχολογικός παράγοντας, ο οργανωτικός, ο τεχνολογικός κ.ο.κ (Clausewitz, 1832/2003, 145).

Θα κλείσουμε την εξέταση της συνεισφοράς του Κλαούσεβιτς, με το σχολιασμό του δημοφιλέστερου αποσπάσματος του έργου του, το οποίο αναφέρει ότι *ο πόλεμος δεν είναι παρά η συνέχεια της πολιτικής με άλλα μέσα*. Μια κριτική παρατήρηση είναι ότι εσφαλμένα διαχωρίζονται οι έννοιες του πολέμου και της πολιτικής, ως σαν να είναι δυνατόν μια κοινωνία να ζήσει στη μία ή στην άλλη κατάσταση (Κονδύλης, 1999, 22). Με τον όρο «πολιτική» δεν εννοείται η εξευγενισμένη, ήπια και μη συγκρουσιακή διαβίωση. Θα λέγαμε ότι αυτή εγγύτερα τη χαρακτηρίζει η έκφραση «ειρηνική κατάσταση». Εδώ η πολιτική χρησιμοποιήθηκε με την έννοια της συνολικής διακυβέρνησης ενός συγκεκριμένου κοινωνικού σχηματισμού, είτε σε πολεμική είτε σε ειρηνική περίοδο. Αυτό λοιπόν στο οποίο πρέπει να σταθούμε είναι ότι αλλάζουν τα μέσα. Σε αυτό το σημείο προτείνεται μια πιο επικοινωνιακή έμφαση στον όρο. Όταν δηλαδή δεν μπορούν να επιλυθούν οι διαφορές των κρατών με τα μέσα που διατίθενται από το διεθνές δίκαιο, ή αλλιώς θα λέγαμε με τον διπλωματικό τρόπο, επέρχεται η σύρραξη.

6.2 Η Στρατηγική Κουλτούρα

Σε αυτό το υποκεφάλαιο θα επιχειρήσουμε να προσεγγίσουμε τις αφετηρίες της λαϊκής συγκατάθεσης στην τέλεση μιας πράξης πολέμου από μια διαφορετική οπτική γωνία¹⁰⁴.

Μια από τις πρώτες σκέψεις μας στο άκουσμα της λέξης «πολεμώ», άσχετα αν πρόκειται για επίθεση ή άμυνα, είναι η σύνδεση αυτής της έννοιας με αναπαραστάσεις, οι οποίες συμβολίζουν τις συνέπειες καταστροφής μιας παρουσίας, ή ακόμα χειρότερα της ζωής κάποιων ή του ίδιου μας του εαυτού. Για να οδηγηθούμε λοιπόν σε αυτήν την επιλογή με τη θέλησή μας σημαίνει πως υπάρχουν αξίες οι οποίες τίθενται υπεράνω από το θάνατο. Βεβαίως, αυτές διαφέρουν από πολιτισμό σε πολιτισμό και από εποχή σε εποχή. Ειδικότερα, ας παρατηρήσουμε την ιστορική φάση των λεγόμενων Νέων Χρόνων, οπότε η τυπική και κοινώς αποδεκτή μορφή

¹⁰⁴ Οι ρίζες αυτής της επιστημονικής θέασης βρίσκονται στην Πολιτική Ψυχολογία.

οργάνωσης υπήρξε το κράτος. Συχνά οι λόγοι για τους οποίους ένα κράτος βρίσκεται σε εμπόλεμη κατάσταση, οφείλονται στις βαθύτερες πεποιθήσεις των πολιτών του, των οποίων ο κίνδυνος κλονίζει το συλλογικό «περί ασφαλείας αίσθημα». Όπως εξηγήσαμε παραπάνω, τα μέλη του κράτους θεμελιώνουν την ταυτότητά τους με την ύπαρξη του έθνους. Όταν λόγου χάρη αυτό είναι μεγαλύτερο από την εδαφική επικράτεια, αναφέρονται στις «αλύτρωτες πατρίδες» και αναζητούν τρόπους εναγκαλισμού τους. Με άλλα λόγια, για τον τρόπο που οι πολίτες ενός κράτους βιώνουν την αναγκαιότητα της χρήσης ένοπλης βίας -καθώς και τη σχετική προετοιμασία-, με ενδεχόμενο εναλλακτικό κόστος την ίδια τους τη ζωή, χρησιμοποιείται τα τελευταία χρόνια η έκφραση *Στρατηγική Κουλτούρα* (Ντόκος, 2005, 61)¹⁰⁵. Πιο συγκεκριμένα, «Στρατηγική Κουλτούρα» θεωρούμε το σύνολο των αξιών, στάσεων, προτύπων και υποδειγμάτων συμπεριφοράς σχετικά με τη χρήση η απειλή χρήσης ένοπλης βίας¹⁰⁶. Μπορούμε να τη θεωρήσουμε μοναδική και χαρακτηριστική για κάθε έθνος-κράτος, αλλά να γνωρίζουμε ότι αποτελεί μια τάση της έκφρασης στρατηγικής συμπεριφοράς και όχι βεβαιότητα (Gray, 1995). Βασικότερες πηγές της είναι η ιστορία, η γεωγραφία και η πολιτική κουλτούρα του κάθε λαού. Ενώ, συστατικά στοιχεία συνιστούν οι εν γένει κομματικές και οικονομικές ελίτ, οι ένοπλες δυνάμεις, η κοινή γνώμη κ.λπ.

6.3 Ηθική του Πολέμου

Το βασικό ερώτημα που θα πρέπει να απαντηθεί, ώστε να βρούμε το αντικειμενικό κριτήριο της «ηθικής ή δικαιολογημένης συμμετοχής» σε έναν πόλεμο, είναι τι -από ό,τι προαναφέραμε ότι υπάρχει- στη φύση του πολέμου αποτελεί και ανθρώπινη φύση. Αν υποθέσουμε ότι η εχθρότητα είναι έμφυτη στον άνθρωπο, τότε ο πόλεμος είναι ένα φυσικό ιστορικό-κοινωνικό γεγονός (Καφφές, 2008, 15). Στην αντίθετη περίπτωση, δεν θεωρείται ως αποδεκτός ή αναπόφευκτος τρόπος συμβίωσης και επίλυσης των διαφορών μεταξύ των ανθρώπινων ομάδων.

Στην αρχαία Ελλάδα, ο Πλάτωνας δικαιολογούσε τους αμυντικούς πολέμους και κατηγορούσε τους επιθετικούς¹⁰⁷. Σε αυτό συμφώνησε, αργότερα, και ο Κ.

¹⁰⁵ Θεμελιωτής της έννοιας θεωρείται ο Jack L. Snyder (1977), *The Soviet Strategic Culture*, Rand Co.

¹⁰⁶ Ένα χαρακτηριστικό παράδειγμα, εξαίρεσης του κανόνα στην εποχή μας, είναι ορισμένες ομάδες μοναχών του Θιβέτ, οι οποίες αρνήθηκαν να χρησιμοποιήσουν βία, έναντι οποιουδήποτε τιμήματος.

¹⁰⁷ Ο Πλάτωνας, στο *Νόμοι* (803 D – E & 628 C – E), κατηγορεί τους επεκτατικούς πολέμους.

Μαρξ¹⁰⁸ χαρακτηρίζοντάς τους, με μια διαφορετική αιτιολόγηση, δίκαιους και άδικους πολέμους αντίστοιχα. Ο Τολστόι αδυνατούσε να κατανοήσει το λόγο για τον οποίο οι άνθρωποι εμπλέκονται σε *ό,τι πιο φονικό υπάρχει στη ζωή*¹⁰⁹. Βάσει των παραπάνω, φαίνεται λογικό ότι κριτήριο «δικαιολόγησης» αποτελεί, απλά, η απόδειξη για το ποιο κράτος έκανε πρώτο την επίθεση. Εντούτοις, όταν όμως έχουμε περιπτώσεις «κλασικής επίθεσης», η οποία από τους ηγέτες καλείται «ενέργεια αμυντικού πολέμου», τα πράγματα περιπλέκονται¹¹⁰. Εξάλλου, μεγάλοι πολεμολόγοι, όπως ο Αντουάν-Ανρί Ζομινί (για ορισμένους ο πατέρας της Στρατηγικής), θεώρησε πρωταρχικό παράγοντα νίκης σε έναν πόλεμο την επιθετική πρωτοβουλία (Shy, 2004, 177). Σε αυτήν την περίπτωση, δύσκολα καταλογίζουμε ευθύνες σε κάποιον, ο οποίος έχει αποφασίσει να αγωνιστεί -σε έναν ενδεχομένως, αναπόφευκτο για αυτόν πόλεμο- επειδή ακολούθησε τη «νικηφόρα συνταγή».

Συμπεραίνουμε, λοιπόν, ότι στην πραγματικότητα δεν υπάρχει ένα αντικειμενικό κριτήριο για να κρίνουμε έναν πόλεμο ως επιθετικό ή αμυντικό. Αξιοσημείωτο, εδώ, είναι να διευκρινίσουμε τη διαφορά μεταξύ των αμυντικών - επιθετικών πολέμων και των εννοιών Άμυνα - Επίθεση. Όπως γράφει χαρακτηριστικά ο Clausewitz (1832/2003, 427):

Ποια είναι η έννοια της άμυνας; Η αποφυγή του κτυπήματος (της επίθεσης). Συνεπώς, κάθε πολεμική δράση επίθεσης, επιφέρει την πολεμική αντίδραση της άμυνας. Όταν αυτή η σχέση παύει, εθεωρείτο ότι ο πόλεμος σταματά.

Εξάλλου, στην ιστορία, η πρόσμιξη της ηθικής απόχρωσης και της πολιτικής εκμετάλλευσης κατά τις επιχειρηματολογίες ενοχοποίησης είναι συνεχής. Τέλος, η έννοια του δίκαιου πολέμου εξαρτάται από τους σκοπούς του και όχι από τον τρόπο διεξαγωγής του (Κονδύλης, 1999, 295).

6.4 Οι Κλασσικές Ερμηνείες

Μετά τη λήξη του Β' Παγκοσμίου Πολέμου ξεκίνησε η διαπραγμάτευση των ηγετών των κρατών για τη ψήφιση του Καταστατικού Χάρτη του νεοϊδρυθέντος Οργανισμού Ηνωμένων Εθνών (ΟΗΕ), στον Άγιο Φραγκίσκο των ΗΠΑ, το 1945. Το πρώτο μέλημα ήταν να περάσει το μήνυμα στον ταλαιπωρημένο μεταπολεμικό κόσμο της

¹⁰⁸ Κατά τους Marx & Engels, «άδικος» είναι ο πόλεμος, ο οποίος βαθύτερα στοχεύει στην οικονομική εκμετάλλευση των ασθενέστερων (Κονδύλης, 1999, 170-206).

¹⁰⁹ Ο Λ. Τολστόι στο *Πόλεμος και Ειρήνη* τόνισε την ειρωνεία και το παράδοξο, η ανθρώπινη φύση να εμπλέκεται σε κάτι τόσο καταστροφικό για την ίδια.

¹¹⁰ Ένα πρόσφατο παράδειγμα είναι η επίθεση (Δεκέμβριος 2008) του Ισραήλ στην Παλαιστίνη, την οποία ο υπουργός άμυνας Μπάρακ αποκάλεσε «αμυντικό πόλεμο».

συμφωνίας περί «Απαγορεύσεως του Πολέμου ως Μεθόδου Εθνικής Πολιτικής»¹¹¹. Έτσι, η χρήση ένοπλων μέσων για την επίλυση των διαφορών χαρακτηρίστηκε παράνομη πράξη. Επιπρόσθετα, στην προσπάθεια απάλειψης των τραυματικών πολεμικών εμπειριών, αφαιρέθηκε από τα κείμενα η ψυχολογικά φορτισμένη λέξη «πόλεμος» και αντικαταστάθηκε με τη διατύπωση της διευρυμένης απαγόρευσης οιασδήποτε «απειλής ή χρήσεως βίας»¹¹².

Σε μια παρόμοια λογική, διάφορα λογοτεχνικά έργα, δημοφιλή και μη, ισχυρίστηκαν στην πλοκή τους εμβόλιμη τη λέξη «πόλεμος» στον ανθρώπινο εγκέφαλο¹¹³ έτσι, ώστε αν δεν υπήρχε, ο άνθρωπος δεν θα μπορούσε να διαπράξει τέτοια καταστροφή. Ωστόσο, η πραγματική αφαίρεση της χρήσης της από τις ρήτρες του ευρύτερου δυνατού βαθμού συμφωνίας σε παγκόσμιο βεληνεκές (όπως είναι ο Καταστατικός Χάρτης του ΟΗΕ), δεν στάθηκε αρκετή για την εξαφάνισή του. Σήμερα γνωρίζουμε πως αυτή η ρήτρα δεν είναι δυνατόν να ισχύσει¹¹⁴. Πέραν όμως των ρεαλιστικών (νομικών και πολιτικών) χειρισμών στη μια άκρη του φάσματος της χρήσης του όρου και των υπερρεαλιστικών (μυθιστορικών) αντιμετώπισεων του όρου στην άλλη άκρη, έχει καταγραφεί ένα μνημειώδες επιστημονικό έργο διερεύνησης του φαινομένου. Πολλοί και ιδιαίτερα αναγνωρισμένοι κοινωνικοί επιστήμονες προσπάθησαν να ερευνήσουν τα αίτια εκδήλωσης του πολεμικού φαινομένου. Παρατήρησαν τα ίχνη του από τότε που οι άνθρωποι οργανώθηκαν σε ομάδες, στις αρχές της ιστορίας. Από τη μια πλευρά, ορισμένοι το θεώρησαν μέρος της ανθρώπινης φύσης, ενώ από την άλλη, κάποιοι επιχειρηματολόγησαν ότι πρόκειται για έναν εσφαλμένο τρόπο κοινοτικής ή κοινωνικής συνύπαρξης. Γενικά, οι περισσότερες τάσεις εξήγησής του, θεμελιώθηκαν βάσει των στρουκτουραλιστικών και μετά-στρουκτουραλιστικών θέσεων¹¹⁵ (Μπάκα, 2005). Ειδικότερα, θα

¹¹¹ Κάτι που είχε μάταια επιχειρηθεί και προηγουμένως, με το Σύμφωνο των Παρισίων (1928), μετά τον Α' Παγκόσμιο Πόλεμο.

¹¹² Για την ακρίβεια το άρθρο 2(4), το οποίο συνιστά κανόνα αναγκαστικού δικαίου και ταυτόχρονα θεωρείται πως έχει εθιμικό χαρακτήρα στο διεθνές δίκαιο, αναφέρει τα εξής: *Όλα τα Μέλη, στις διεθνείς τους σχέσεις, θα απέχουν από την απειλή ή την χρήση βίας που εκδηλώνεται εναντίον της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε Κράτους είτε με οποιαδήποτε άλλη ενέργεια ασυμβίβαστη προς τους Σκοπούς των Ηνωμένων Εθνών* (Φωτίου, 2009).

¹¹³ Βλέπε: Α. Χατζηνικολάου (2002), *Ο Θαυματουργός Ψίθυρος του Ερμή*, Ελληνικά Γράμματα, σ. 199.

¹¹⁴ Τα πολεμικά επεισόδια του τελευταίου μισού του περασμένου αιώνα, είτε μικρότερα (π.χ. Νικαράγουα, 1969 και Κύπρος, 1973), είτε μεγαλύτερα (όπως στην Κορέα, το Βιετνάμ και το Ιράκ) ήταν αρκετά, ώστε να διαψευστεί η επάρκεια του «εξορκισμού» της εκφοράς της λέξης.

¹¹⁵ Αναφερόμαστε στην επιστημολογική παραδοχή ότι η κατανόηση της αντικειμενικής αλήθειας -αν αυτή υπάρχει- είναι ανέφικτη, συνεπώς επιχειρούμε να την ερμηνεύουμε με επισυνάψεις νοητικών κατασκευών του κοινωνικού κόσμου. Ο στρουκτουραλισμός ή δομολειτουργισμός είναι θεωρία της οποίας θεμελιωτής υπήρξε ο γλωσσολόγος Φερντινάντ ντε Σωσσύρ (Ferdinand de Saussure), ο οποίος και έδειξε για πρώτη φορά το «αυθαίρετο του γλωσσικού σημείου», δηλαδή ότι η γλώσσα δεν

μπορούσαμε να διαχωρίσουμε τα συμπεράσματά τους σε αυτά που θεωρούν την πολεμική πράξη φυσικό ή έμφυτο φαινόμενο και σε αυτά που τη θεωρούν αποτέλεσμα της οργάνωσης του κοινωνικού περιβάλλοντος.

Στην πρώτη περίπτωση λοιπόν εντάσσεται η Ψυχαναλυτική θεωρία, για την οποία θα αναφερθούμε σε δύο κύριους εκπροσώπους. Ο πρώτος είναι ο Freud, σύμφωνα με τον οποίο ο πόλεμος οφείλεται στον φοβικό τρόπο που ενδόμυχα αντιμετωπίζεται ο θάνατος στον πολιτισμό μας. Έτσι το ένστικτο της ζωής συγκρούεται με αυτό του θανάτου και η συνέπεια είναι να μας παρακινεί σε επιθετική εκτόνωση. Ο δεύτερος είναι ο Fromm, ο οποίος αντιμετωπίζει τον πόλεμο ως αποτέλεσμα της αλλοτρίωσης, λόγω της έντονης απομόνωσης που νιώθουμε στη σύγχρονη κοινωνία. Έτσι αναζητούμε συμμαχίες με ομοίους μας για να εκφράσουμε το μίσος μας σε άλλους. Στη συνέχεια έχουμε την Ηθοβιολογία, με επίσης δύο βασικούς εκπροσώπους. Τον Lorenz, κατά τον οποίο όπως δείχνουν τα πειράματα για την επιβίωση των ειδών του ζωικού βασιλείου, ο πόλεμος πηγάζει από την έμφυτη ανθρώπινη επιθετικότητα. Εδώ η ευφυΐα και η αγωνιστική δεξιότητα ανάγονται σε αναγκαίες πολεμικές αρετές. Ομοίως ο Wilson καταλήγει στην υπαιτιότητα του «προγραμματισμένου» διαχωρισμού των συνανθρώπων μας σε φίλους και εχθρούς. Οι τελευταίοι απειλούν δυνητικά τη ζωή μας και την περιουσία μας, για αυτό το λόγο επιθυμούμε να τους καταστρέψουμε. Από την πλευρά της Ψυχοπαθολογίας, ο Adorno επικεντρώνει την αναζήτησή του στην προβληματικά αυταρχική προσωπικότητα των ηγετών, η οποία αναζητεί βίαιες διεξόδους ικανοποίησης.

Στη δεύτερη περίπτωση προτείνονται οι «εξωτερικές του ατόμου» αιτίες και δη το κοινωνικό του περιβάλλον. Ένα διαδεδομένο ρεύμα αυτής της σχολής σκέψης αποτελεί αυτό του Συμπεριφορισμού¹¹⁶. Ο Bandura έδειξε πως ο πόλεμος επηρεάζεται από τη μάθηση και την κοινωνικοποίηση. Έτσι, όλοι οι φορείς

αντιγράφει την πραγματικότητα, καθώς δεν υπάρχει μια αιτιώδης σύνδεση ανάμεσα στο σημαίνον (τη λέξη που αποδίδεται σε ένα αντικείμενο) και το σημαινόμενο (το αντικείμενο). Έτσι, το γλωσσικό σημείο ενώνει μια ιδέα του πράγματος με μια ακουστική εικόνα. Η ιστορική γραμμή των κυριότερων εκπροσώπων περιέχει τους Κοπέρνικο και Κέπλερ (θεωρία ηλιοκεντρικού ηλιακού συστήματος, που εκτόπισε τον άνθρωπο από το κέντρο του σύμπαντος). Δαρβίνο (Η εξελικτική θεωρία του που έδειξε πως ο άνθρωπος, ως υπόσταση, δεν βρίσκεται λίγο πιο κάτω από τους αγγέλους, αλλά λίγο πιο πάνω από τους πιθήκους). Φρόιντ (Η ψυχαναλυτική θεωρία του που έδειξε πως ο ψυχισμός του ανθρώπου κυριαρχείται από ασυνείδητες ορμές). Χέγκελ (φιλοσοφικό σύστημα «Θέση - Αντίθεση - Σύνθεση»). Μαρξ (όλα τα κοινωνικοπολιτικά φαινόμενα ανάγονται στις κοινωνικές τάξεις και στην πάλη).

¹¹⁶ Αλλιώς, ο Μπιχεβιορισμός, αντιμετωπίζει το άτομο δίχως εγγενή κίνητρα συμπεριφοράς, που είναι αποτέλεσμα της δόμησης του περιβάλλοντος που αναπτύσσεται. Αξίωμα του είναι ότι η μάθηση και είναι η κοινή συνισταμένη των ερεθισμάτων που δέχεται το άτομο από το περιβάλλον του, καθώς και οι σχετικές του αντιδράσεις. Κύριοι εκπρόσωποι: A]Ed. Thorndike (1913), *συντελεστική υποκατάσταση* (συνέχισε ο Skinner). B]Iv. Pavlov (1927), *κλασική υποκατάσταση - διασύνδεση* (συνέχισε ο Watson).

κοινωνικοποίησης, από την οικογένεια και το σχολείο ως τα μέσα μαζικής ενημέρωσης, συστήνουν λόγους που δικαιολογούν τη βίαιη συμπεριφορά (αυτοθυσία, ηρωισμός κ.λπ.). Κοντά σε αυτές τις διαπιστώσεις βρίσκεται και ο Milgram, ο οποίος επικεντρώθηκε στις συνθήκες υπακοής στην εξουσία. Έντονα εμφανής είναι η εφαρμογή της θεωρίας του στο στρατό, όπου η θανάτωση μπορεί να είναι απλά αποτέλεσμα εντολής. Πιο σύγχρονες τάσεις συμπεριλαμβάνουν στις αιτίες και την εσωτερική φύση του ανθρώπου αλλά και τη συγκυρία που βιώνει. Τέλος, καταλήγουν στο διαχωρισμό των αιτιών στον ορθολογικό ή ανορθολογικό τρόπο σκέψης. Πιο συγκεκριμένα, σύμφωνα με τις κοινωνικό-γνωστικές προσεγγίσεις τα μη ορθολογικά ελατήρια διαμορφώνονται εξαιτίας της πολυπλοκότητας της σύγχρονης κοινωνίας. Σε αυτήν, εξαιτίας της ραγδαίας αύξησης στη διακίνηση των πληροφοριών οι ιθύνοντες βρίσκονται σε σύγχυση. Οπότε δεν δύνανται να λάβουν τις σωστές αποφάσεις (Geller & Singer). Επίσης, ένας άλλος λόγος μπορεί να είναι οι προσδοκίες των ομάδων, από τις οποίες εξαρτάται ο ηγέτης. Καθοριστικό ρόλο μπορεί να παίζει η επιρροή που ασκείται μέσω συναισθηματικής πίεσης των ενδεχόμενων κατακρίσεων της ομάδας που τον ελέγχει (Holsti, 1990).

Ενώ οι παραπάνω κοινωνικογνωστικές ψυχολογικές θεωρίες αναζητούν τις ρίζες του ζητήματος στο άτομο ή τις μικρές ομάδες στις οποίες αυτό συνενώνεται, οι πολιτικές επιστήμες τοποθετούνται στο συλλογικό υποκείμενο που συνήθως είναι τα έθνη-κράτη και οι μεταξύ τους σχέσεις. Μπορούμε να διακρίνουμε δύο βασικές κατευθύνσεις των Διεθνών Σχέσεων. Αφενός, αυτή του Ρεαλισμού, η οποία θεωρεί τον πόλεμο ως τη συνέπεια της άναρχης οργάνωσης των κρατών. Ο χαρακτηρισμός «άναρχη» υποδηλώνει πως δεν υπάρχει μια κεντρική και κοινώς αποδεκτή εξουσία (αρχή). Κύριοι εκπρόσωποι θεωρούνται οι Machiavelli (16^{ος} αιώνας), Hobbes (17^{ος} αιώνας), Carr (1946) και Morgenthau (1948). Αφετέρου, τον Ιδεαλισμό, κατά τον οποίο ο πόλεμος οφείλεται στην ανήθικη και μη έλλογη οργάνωση του κόσμου. Εισηγητής -στους Νέους Χρόνους, διότι έχουν εντοπιστεί και καταβολές από την Αρχαία Ελλάδα- θεωρείται ο Kant και στην εποχή μας ουσιαστικά εξέλιξή του αποτελεί ο (οικονομικός) φιλελευθερισμός. Από αυτόν πηγάζει η θέση ότι όσο παρεμβαίνουμε στην αγορά, τόσο θα αναδύονται διαφορές που θα επιλύονται συγκρουσιακά (υποστηρίχθηκε από τον Σμιθ και τον Φρίντμαν, σε αντίθεση με τον Κέυνς). Τέλος, αξιοσημείωτο εδώ είναι το παρακλάδι της γεωοικονομίας, κατά την οποία ολόκληρη η οικονομική επιστήμη βασίζεται στην εύρεση κατάλληλων τρόπων διαχείρισης των πεπερασμένων πόρων του πλανήτη. Επεκτείνοντας περισσότερο αυτή

την αρχή, η γεωπολιτική ανάλυση θεωρεί τον πόλεμο ένα αποτέλεσμα της διεκδίκησης ζωτικών αγαθών σε ένα «κλειστό» παίγνιο, με παίκτες τα κράτη (Βέργος, 2005, 142-145).

Σε συνάρτηση λοιπόν με την πρώτη περίπτωση, η εν γένει εκδήλωση του πολεμικού φαινομένου είναι αναπόφευκτη, εφόσον αποτελεί συνέπεια μη επίκτητων ανθρώπινων χαρακτηριστικών. Ενώ στη δεύτερη επισημαίνεται ότι μόνο αν η ανθρωπότητα αποφασίσει να συνεργαστεί, τότε θα είναι δυνατό να ζήσει ειρηνικά. Παρόλα αυτά, ιδιαίτερο ενδιαφέρον παρουσιάζει μια σημαντική προσέγγιση της από τη μεριά της κοινωνικής ψυχολογίας, η οποία ανάγει την ανάλυσή της στις ρίζες της οργανωτικής μετάβασης από τη φεουδαρχία στο εθνικό-κρατικό μόρφωμα. Πολύ συχνά αυτή η μετάβαση διαμορφώθηκε μέσα σε ένα πολεμικό κλίμα (όπως διαμορφώνεται από εξεγέρσεις κι απελευθερωτικούς αγώνες), οπότε στη συνείδηση των πολιτών καταγράφηκε πως η συμμετοχή στον πόλεμο είναι ένα αναγκαίο μονοπάτι στο δρόμο για την ανεξαρτησία τους. Αυτή όμως η συνθήκη, συνδέεται με την κάλυψη μιας ανάγκης, την οποία σε έναν βαθμό διαθέτουν όλοι οι άνθρωποι, αυτής του «ανήκειν». Σε κάθε άτομο, μέλος πλέον του κράτους, προσδόθηκε η ιδιότητα του πολίτη που συμμετέχει στα κοινά. Με αυτόν τον τρόπο η εθνική ταυτότητα συσχετίστηκε με ένα νόημα αυτοπροσδιορισμού, το οποίο συνίστατο από ένα σύνολο υποχρεώσεων και δικαιωμάτων. Τότε αναπτύχθηκε σε επίπεδο ιδεολογικό η πεποίθηση της «πατριωτικής υποχρέωσης» υπεράσπισης της χώρας. Συχνά όμως, με σκοπό να αποδειχθεί η δική μας ανωτερότητα (ενός εγωιστικού «εμείς οι καλοί»), αναγκαζόμασταν να συγκρουστούμε με τους άλλους («οι ξένοι οι κακοί»). Σύμφωνα λοιπόν με αυτήν την προσέγγιση, αυτός ο διαχωρισμός αποτελεί και την αιτία εμφάνισης του νεωτερικού είδους πολέμου.

Συμπεραίνουμε πως η εμφάνιση και η οργανωτική εξέλιξη του έθνους-κράτους έπαιξε καθοριστικό ρόλο στον τρόπο διεξαγωγής του πολέμου. Για αυτόν το λόγο θα επιχειρήσουμε μια περιοδολόγηση αυτής της αλληλεπίδρασης, στο επόμενο κεφάλαιο.

7. ΙΣΤΟΡΙΚΗ ΔΙΕΡΕΥΝΗΣΗ (ΠΩΣ ΦΘΑΣΑΜΕ ΣΤΟΝ ΚΥΒΕΡΝΟΠΟΛΕΜΟ)

Η τυπική μορφή κοινωνικής οργάνωσης στο λεγόμενο μοντέρνο δυτικό κόσμο, τον 18^ο αιώνα¹¹⁷ είναι το *κράτος*. Καταρχάς, θεμέλια στη σύστασή του αποτελούν ο οντολογικός προσδιορισμός του από το χρόνο, το χώρο και έναν καθορισμένο πληθυσμό¹¹⁸. Κατόπιν, βασικά συστατικά οικοδόμησής του συνιστούν ο ορθολογισμός και ο κανονιστικός έλεγχος από μια συγκεκριμένη εξουσία (Μουζέλης, 1978/1991), η οποία προκύπτει από το πολιτειακό σύστημα που επικράτησε, αυτό της αντιπροσωπευτικής δημοκρατίας. Τα άτομα τα οποία συμμετέχουν σε αυτό το σύστημα, οργανώνονται αναλόγως των δικαιωμάτων και υποχρεώσεων που αποπνέει ο ρόλος τους. Αυτή τους η οργάνωση, αφορά σε μια ιεραρχική διάρθρωση, η οποία δύναται να αναπαρασταθεί σχηματικά με μια πυραμίδα τριών επιπέδων (σχήμα 24). Στην οροφή είναι η *Ηγεσία*¹¹⁹, δηλαδή οι κυβερνήτες, οι οποίοι έχουν το ρόλο της ευθύνης της λήψης των αποφάσεων. Ενδιάμεσα υφίστανται τα (ανθρώπινα) *Μέσα*, τα οποία απαρτίζονται από τα άτομα που έχουν το καθήκον της εκτέλεσης των άνωθεν αποφάσεων. Στο τέλος, βρίσκεται ο *Λαός*¹²⁰, ο οποίος έχει τη θέση της βάσης του οικοδομήματος, που αποδέχεται ή απορρίπτει τις συνέπειες της λειτουργίας του.

Σχήμα 24. Απεικόνιση της Πυραμοειδούς Ιεραρχικής Οργάνωσης του Κράτους



¹¹⁷ Αναφερόμαστε στη γνωστή ως περίοδο της νεωτερικότητας. Βέβαια, έτος ορόσημο για τη διεθνή αναγνώριση του έθνους-κράτους θεωρείται τυπικά, η συνθήκη της Βεσφαλίας το 1648 και ουσιαστικά, η γαλλική επανάσταση το 1789. Πάντως, έχει ενδιαφέρον ότι ο όρος «Δύση» περιέχει γεωπολιτικό, παρά γεωγραφικό κριτήριο. Έτσι, περιλαμβάνεται αρχικά η κεντρική Ευρώπη, μετά η βόρεια Αμερική και αμφιλεγόμενα η Ιαπωνία και το Ισραήλ.

¹¹⁸ Ο πληθυσμός ορίζεται ως το σύνολο των κατοίκων μιας περιοχής σε ένα συγκεκριμένο χρονικό διάστημα (Τομαρά, 1998, 14).

¹¹⁹ «Με τον όρο *ηγεσία* αναφερόμαστε ως επί το πλείστον στα κορυφαία επίπεδα πάσης φύσεως διοίκησης κοινωνικής, πολιτικής, στρατιωτικής...» (Κουβελιώτης, 2002, 131).

¹²⁰ Ο *λαός* ορίζεται ως το σύνολο των πολιτών ενός κράτους. Πολίτες δε, θεωρούνται τα άτομα που διαθέτουν υπηκοότητα και πολιτικά δικαιώματα. Άρα, οι πολίτες μπορεί να είναι περισσότεροι από τον πληθυσμό, όταν συνυπολογιστούν και αυτοί του εξωτερικού ή μπορεί να είναι λιγότεροι, αν συνυπολογιστούν οι μετανάστες στο εσωτερικό (Τσαούσης, 1996/2006, σσ. 16-17).

Για τον Max Weber, το κράτος είναι ο φορέας, ο οποίος έχει την αποκλειστική διάθεση του μονοπωλίου της άσκησης βίας (Μαρκαντωνάτου, 2009, 29). Για τον Karl Marx, το κράτος αποτελεί το μέσο επίτευξης των στόχων της άρχουσας τάξης, ή αλλιώς της ηγεσίας. Στη δική μας περίπτωση, θα εξετάσουμε ειδικά την εξέλιξη αυτών των «μέσων» (άσκησης βίας, κατά Weber), τα οποία χρησιμοποιούνται από την εξουσία (κατά Marx), ώστε να επιτύχει τους σκοπούς της. Γενικά, μπορούμε να πούμε, ότι τα μέσα αφορούν στην εφαρμογή ενός συνόλου οριοθετημένων διαδικασιών και λειτουργιών των διαθέσιμων ανθρωπίνων και τεχνολογικών πόρων. Ειδικά, ένα υποσύνολο των μέσων επωμίζεται την ικανοποίηση του αισθήματος ασφάλειας των κατοίκων ενός κράτους (Μάζης, 2006, 23). Έτσι, διακρίνονται σε όσους αντιμετωπίζουν τις εσωτερικές απειλές (αστυνομία κ.λπ.) και όσους υλοποιούν την έξωθεν σχετική δραστηριότητα. Οι τελευταίοι, ευρύτερα, ονομάστηκαν *στρατός* και η αποστολή τους ξεκίνησε από τη διεξαγωγή μαχών στα σύνορα της επικράτειας για την αντιμετώπιση των έξωθεν απειλών, μετά πέρασε στην αντιμετώπιση των εκ των έσω απειλών (τρομοκρατία κ.λπ.) και κατέληξε, σήμερα, στην «προσφορά ανθρωπιστικής βοήθειας» στο εσωτερικό άλλων κρατών (Moskos, 2000, 15).

Μέσα σε αυτήν την πορεία, τα μέσα σταδιακά από ανθρώπινης έντασης μεταλλάχθηκαν σε τεχνολογικής. Εμείς θα εξετάσουμε πώς η χρήση συγκεκριμένων κατά καιρούς μέσων, οδηγούσε την ηγεσία σε διαφορετικές απαιτήσεις από το λαό¹²¹. Όπως αναφέραμε, με την έλευση του έθνους κράτους, οι κάτοικοι μιας επικράτειας αρχίζουν να αναπροσδιορίζουν την κοινωνική και εθνική τους ταυτότητα (Μπάκα, 2005). Στις κοινωνικές επιστήμες δεν υπάρχει ένας κοινά αποδεκτός ορισμός για την έννοια της ταυτότητας, είτε ατομικής, είτε συλλογικής (Θεοδωρακόπουλος, 2006, 187). Ωστόσο, όσον αφορά την περίπτωσή μας, θεωρείται πως τα άτομα στην προσπάθειά τους να καλύψουν την ανάγκη του ανήκειν (του *εμείς*), αντιλαμβάνονται τον εαυτό τους μέσα σε οργανωτικά συγκροτημένα σύνολα κοινωνικών δεσμών¹²². Παράλληλα, όμως, τα άτομα, έχουν και την ανάγκη της αυτοεκτίμησης (του *εγώ*). Έτσι, εμπλέκονται σε διαμάχες, μικρότερης ή μεγαλύτερης έκτασης, για να αποδείξουν την ανωτερότητα του δικού τους σχηματισμού. Ωστόσο, αυτή η απόδειξη απαιτεί θυσιαστική δράση, την ανάληψη δηλαδή του ρίσκου της πιθανότητας να διακινδυνεύσουν τη ζωή τους.

¹²¹ Ιδιαίτερο ενδιαφέρον στην παρακάτω ανάλυση έχει ο παραλληλισμός με την «κλαουσεβιανή τριτότητα», την οποία εξετάσαμε παραπάνω.

¹²² Εξάλλου, η κοινωνία δεν είναι παρά ένα σύνολο ανθρωπίνων σχέσεων, οι οποίες προϋποθέτουν, επιβεβαιώνουν και αναπαράγουν δεσμούς (Τσαούσης, 1996/2006, 16).

Αυτό το τελευταίο στοιχείο είναι πολύ έντονο για το λαό στις στρατιωτικές επιχειρήσεις μέχρι και τον δεύτερο παγκόσμιο πόλεμο. Το ψυχοκοινωνικό περιβάλλον στο εν λόγω πεδίο μάχης μπορεί να χαρακτηριστεί από τη λέξη «μάζα». Γενικά, οι συγκρούσεις κατακλείνονται από μια μάζα ανθρώπων και πυρός. Οι στρατιώτες οφείλουν να είναι δυνατοί σωματικά και ψυχικά, ώστε να αντέχουν την καταπόνηση και την ωμή βία που τους επιβάλλεται μέσω όλων των αισθήσεων τους. Αν προσεγγίσουμε θεωρητικά τα γεγονότα που διαδραματίζονται στο πεδίο της μάχης, θα δούμε πως η συνείδηση των στρατιωτών υπόκειται στις συνθήκες της ψυχολογίας της μάζας¹²³, σύμφωνα με την οποία υπερέχουν οι αντιδράσεις του θυμικού, δίχως ιδιαίτερα νοητικά φίλτρα. Επίσης, έντονη γίνεται η ανάγκη για καθοδήγηση, εφόσον οι τυχόν πρωτοβουλίες είναι σπασμωδικές. Εν ολίγοις, η άμεση θέαση νεκρών ή φρικτών προσώπων αφήνει στο τέλος της μάχης αποτρόπαια συναισθήματα. Αυτές οι εμπειρίες μεταφέρονται στη συνέχεια και στην κοινωνία. Βεβαίως, από τους ιθύνοντες, πέρα των ιδεών «περί του δίκαιου πολέμου», τις οποίες οι ίδιοι κατευθύνουν και διαχέουν στο λαό, επιβάλλεται αυστηρή *λογοκρισία* για οτιδήποτε συμβαίνει στο πεδίο της μάχης (Moskos, 2000, 15).

Συνεπώς, οι πληροφορίες φθάνουν μόνο από τα φιλικά και συγγενικά πρόσωπα, τα οποία επιβιώνουν και επιστρέφουν πίσω, με τον τρόπο που περιγράψαμε. Από αυτά όμως, το μήνυμα που καταλήγει στην κοινωνία για τον πόλεμο ανάγεται στην φρίκη και τελικά, στο φόβο. Οι λαοί μετά από τέτοια γεγονότα εναντιώνονται και αντιδρούν, διεκδικώντας ειρηνικές συνθήκες διαβίωσης. Συμπερασματικά, όλη αυτή η κατάσταση επιφέρει πολύ μεγάλο πολιτικό κόστος στους κατέχοντες την εξουσία και άρα δεν τους συμφέρει. Για αυτό το λόγο, σε ζητούμενο ανάγεται η απόκτηση μέσων τέτοιων, τα οποία να οδηγούν στη δυνατότητα νίκης με χτυπήματα από ασφαλή απόσταση· ώστε: όσο ελαχιστοποιούνται οι ανθρώπινες απώλειες και οι υλικές ζημιές, τόσο να μεγιστοποιείται η κοινωνική εύνοια ή τουλάχιστον ανοχή για τις επιδιώξεις της ηγεσίας.

¹²³ Θεωρούμε «μάζα», όχι ένα απλό συνονθύλευμα ατόμων, αλλά ένα σύνολο από άτομα που έχουν μια νοητική ενότητα, που συγχωνεύεται σε ένα κοινό αίσθημα και πνεύμα. Τα άτομα εξισώνονται προς τα κάτω και χάνουν την κριτική τους ικανότητα. Η συνείδηση είναι ατομική ενώ το ασυνείδητο συλλογικό... Κυριαρχούν τα ένστικτα. Ο «μαζικός άνθρωπος» υιοθετεί ιδέες, τις οποίες νομίζει ότι σκέφτεται ο ίδιος. Βλ. Ν. Χρηστάκης (2010), *Πρόλογος στην έκδοση*, στο: G. Le Bon, *Ψυχολογία των Μάζων*, Ι.Σ. Χριστοδούλου (επιμ. & μτφ), Το Βήμα (2010), σσ. 11-12. Αυτό το έργο του Gustave Le Bon (1841-1931), το οποίο δημοσίευσε το 1895, θεωρείται από πολλούς ένα από τα πρώτα της Κοινωνικής Ψυχολογίας (Παπαστάμου, 1989, 13).

Επιπρόσθετα, παρατηρούμε ότι αυτή η στοχοθέτηση είναι και σύμφωνη με μια από τις «ιδρυτικές» αρχές του κράτους που αρχικά αναφέραμε, τον ορθολογισμό¹²⁴. Συνοπτικά, *ορθολογική συμπεριφορά* θεωρούμε την επιδίωξη του μεγαλύτερου αποτελέσματος με το μικρότερο δυνατό κόστος (Αλεξιάς, 2008, 46) – κάτι, βεβαίως, που θυμίζει και τον αντικειμενικό σκοπό της στρατηγικής¹²⁵.

Το γεγονός που τάραξε συθέμελα την προαναφερθείσα κατάσταση παγκοσμίως και οδήγησε στην υλοποίηση του στρατηγικού στόχου ενός *απομακρυσμένου πεδίου μάχης* (Κονδύλης, 1999), είναι η ρίψη της ατομικής βόμβας¹²⁶. Από τα σημαντικά αποτελέσματα αυτής είναι να γίνει κοινή συνείδηση και μετά να συναφθεί μια διεθνής συμφωνία ότι η μαζική καταστροφή δεν συμφέρει κανέναν. Έτσι, με τη λήξη του παγκοσμίου πολέμου, η λέξη που χαρακτήρισε το αμυντικό δόγμα και τη στρατιωτική στάση των μεγάλων δυνάμεων είναι η *αποτροπή* (James, 1986/2004, 882). Επί του προκειμένου, αρχικά χρησιμοποιήθηκε η έκφραση «πυρηνική στρατηγική της αποτροπής». Ο λόγος είναι ότι η γνωστοποίηση της διάθεσης πυρηνικής βόμβας από τις ΗΠΑ, οδήγησε στον ανταγωνισμό για την ταχεία απόκτηση και από άλλα κράτη. Αυτό όμως οδήγησε στη συνειδητοποίηση του αδιεξόδου, ώστε να αποφευχθεί η χρησιμοποίησή της. Περιληπτικά, «αποτροπή» σημαίνει να πείθεις τον αντίπαλο για την ισχύ σου, αλλά και να γνωρίζεις την δική του πραγματική κατάσταση (ώστε να μην μπορεί να σε παραπλανήσει). Αυτό όμως απαιτεί την άριστη οργάνωση του λεγόμενου κύκλου των πληροφοριών (τη συλλογή, την επεξεργασία, την ανάλυση και την εκμετάλλευσή τους). Έτσι οι *πληροφορίες* έμελλε να αντικαταστήσουν τη *μάζα* και να κυριαρχήσουν στον επόμενο περίπου μισό αιώνα, στη σχέση κοινωνίας και πολέμου. Για να εξηγήσουμε αυτή τη συσχέτιση, μπορούμε να ισχυριστούμε ότι ο ρόλος των πληροφοριών αποκτά δύο όψεις. Αφενός, τη δυνατότητα ελέγχου των μηνυμάτων που διακινούνται στην κοινωνία. Αφετέρου, τις προϋποθέσεις διεξαγωγής του επονομαζόμενου «απομακρυσμένου πεδίου μάχης», της δυνατότητας δηλαδή πλήγματος εξ αποστάσεως με περιορισμένες καταστροφές· κάτι, το οποίο απαιτεί

¹²⁴ «Η νομικό-ορθολογική νομιμότητα του σύγχρονου κράτους στηρίζεται στο γεγονός ότι οι κυβερνήτες... μπορούν για το κοινό καλό να καταφεύγουν στη βία... με κανονισμούς...» (Καφφές, 2008, 87).

¹²⁵ Αντικείμενο της στρατηγικής είναι η βέλτιστη αξιοποίηση των πόρων για την επίτευξη ενός σκοπού

¹²⁶ Εννοούμε τη δυνατότητα νίκης του αντιπάλου με τη χρήση ελάχιστων πόρων (ανθρώπινων ή τεχνολογικών). Συμβολικά αυτό ξεκίνησε στον βομβαρδισμό της Χιροσίμα από τις ΗΠΑ (6 Αυγούστου 1945), που αποτελεί την πρώτη πυρηνική (βόμβα ουρανίου 235) επίθεση της Ιστορίας. Αν παρατηρήσουμε όμως με προσοχή την πολεμική ιστορία θα δούμε ότι προηγήθηκε μια ροή γεγονότων. Από την καθοδήγηση του στρατού με τον αρχηγό στο πεδίο της μάχης (π.χ. ναπολεόντειοι πόλεμοι), μετά στο επιτελείο (α' παγκόσμιος πόλεμος). Σήμερα πλέον υπάρχουν μη επανδρωμένα πεδία μάχης, όπως τα χτυπήματα με τηλεκατευθυνόμενα όπλα (UAV), μηδενικού κόστους ανθρωπίνων πόρων.

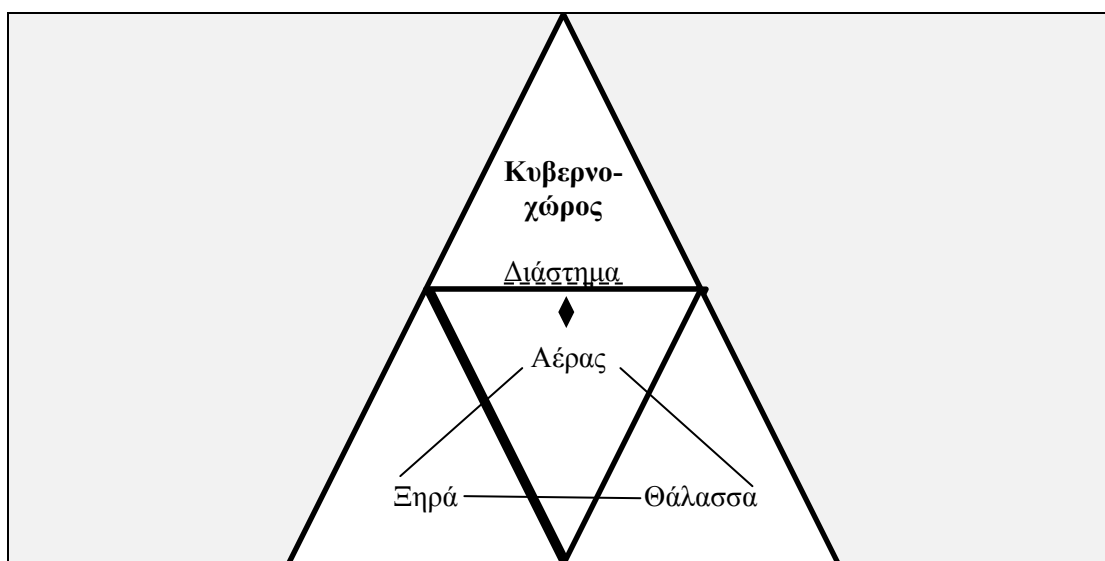
ακριβείς πληροφορίες για τη θέση του στόχου. Τότε είναι που έπρεπε να στρατευθεί και η συμβολή της τεχνογνωσίας.

Αναλυτικότερα, η εμφάνιση των μέσων μαζικής επικοινωνίας, αρχικά, δυσχεραίνει τον έλεγχο της διαμόρφωσης της κοινής γνώμης για τα εν γένει πολεμικά συμβάντα (Chomsky, 1992/1994, 12-14). Αν πριν, τη μόνη πηγή αποτελούν οι πολεμιστές που επιστρέφουν, πλέον οι ράδιο- ή τήλε- εκπομπές ενημερώνουν για τις τρέχοντες εξελίξεις. Αυτές αποκτούν τέτοια δύναμη επιρροής, ώστε να μπορούν να κινητοποιούν το λαό υπέρ ή κατά των εξελίξεων (Taylor, 1997, 149-150). Συνεπώς, σχετικά με την κοινωνία, από τη φάση της λογοκρισίας περάσαμε σε αυτήν της ελεγχόμενης ενημέρωσης (Moskos, 2000, 15). Όσον αφορά δε το πραγματικό μέρος της διεξαγωγής του πολέμου, οι ιθύνοντες προτρέπουν τους επιστήμονες για επιτεύξεις, οι οποίες να επιτρέπουν την αποδοτικότερη δυνατή διεξαγωγή εξ' αποστάσεων μαχών. Μια σειρά θεωρήσεων και εφευρέσεων έρχονται να ικανοποιήσουν αυτό το αίτημα. Η αποκορύφωση έρχεται από τον πατέρα της επιστήμης της Κυβερνητικής (Wiener, 1948). Κεντρική της ιδέα είναι η κατασκευή μηχανών, οι οποίες να διαθέτουν την «αυτόματη» ικανότητα παρακολούθησης της λειτουργίας τους και όταν αυτή παρεκκλίνει, τότε να είναι δυνατή η αυτό-ρύθμιση. Αυτή η αρχή, σε συνεργασία με την πρόοδο σε άλλες επιστήμες της εποχής, επέφερε ένα πολύ συγκεκριμένο αποτέλεσμα ως προς τις συνθήκες του πεδίου μάχης.

Σύμφωνα με μια θεώρηση για τη διαχρονική κατάκτηση της κυριαρχίας, δια της προέκτασης της ισχύος (Κυριαζής και Σπανός, 2000), αν στην προηγούμενη φάση, διαδοχικά, δέσποσαν τα πεδία μάχης στη Ξηρά, τη Θάλασσα και τον Αέρα (από το Δεύτερο Παγκόσμιο Πόλεμο), πλέον, περνάμε στην επόμενη φάση, της οποίας το πεδίο μάχης, συμβολικά, θεωρείται το Διάστημα. Βρισκόμαστε στον λεγόμενο ψυχρό πόλεμο και η επιδίωξη της πληροφόρησης μέσω των δορυφόρων κυριαρχεί (Κολοβός, 2003). Κατά συνέπεια, το βάρος πέφτει στη συνεχή αυτοματοποίηση του κύκλου των πληροφοριών, με την αναγκαία τεχνογνωσία. Ο όρος που μπορούμε να χρησιμοποιήσουμε για να αποτυπώσουμε την τελική απόλυτη αυτοματοποίηση είναι η *προσομοίωση*¹²⁷. Αυτή θα αποτελέσει και τη λέξη-κλειδί της επόμενης φάσης, η οποία θα διαδεχτεί την πληροφορία και τη μάζα των προηγούμενων. Στην τρίτη φάση, το νέο (πέμπτο) πεδίο μάχης, θα είναι ο *Κυβερνοχώρος* (economist, 2010) και αντίστοιχα, ο όρος για τον πόλεμο διαμέσου αυτού: κυβερνοπόλεμος (Σχήμα 25).

¹²⁷ Τον συγκεκριμένο όρο τον αναλύουμε στο επόμενο μέρος (του κυβερνοχώρου).

Σχήμα 25: Τα πεδία μάχης κατά τον ιστορικό ανταγωνισμό στρατιωτικής ισχύος



Στην πρώτη φάση (με κύρια πεδία, μέχρι τον Α΄ παγκόσμιο πόλεμο τα *ξηράς* και *θάλασσας*, ενώ στον Β΄ του *αέρα*) σημαντικό ρόλο παίζει το μέγεθος του ανθρώπινου δυναμικού. Έτσι, η ηγεσία χρειάζεται μεγάλους στρατούς, διότι οι πιο πολυάριθμοι διέθεταν και το συγκριτικό πλεονέκτημα. Στη δεύτερη όμως φάση (με δεσπόζων πεδίο μάχης συμβολικά το *διάστημα*), καθοριστικό ρόλο παίζει η ποιότητα του προσωπικού, η επιλεκτική δηλαδή ειδίκευσή του στο χειρισμό συγκεκριμένων μηχανών. Επίσης, στην τρίτη φάση (*κυβερνοχώρος*), η εξειδίκευση εξακολουθεί να αυξάνεται συνεχώς. Επομένως, παρατηρούμε μια μετάβαση από την έντονη επιζήτηση του ποσοτικού στοιχείου, στην ισομέρεια και μετά, στην έντονη επιζήτηση του ποιοτικού στοιχείου¹²⁸.

Αποτέλεσμα αυτής της συνθήκης, είναι και η μεταβολή των απαιτήσεων της εν γένει ηγεσίας. Ενώ στην αρχή προσπαθεί να επιστρατεύσει όσους περισσότερους μπορεί, κατόπιν αναζητάει το πιο μορφωμένο προσωπικό και όταν αυτό δεν αρκεί, αρχίζει να συνεργάζεται με κατάλληλα εξειδικευμένους πολίτες και να καταργεί την καθολική εκμετάλλευσή τους (σχήμα 26). Αυτή είναι και η μεγάλη καινοτομία αυτής της φάσης. Ενώ, αρχικά η μη εμπλεκόμενη κοινωνία λογοκρινόταν, στη συνέχεια

¹²⁸ Ενδιαφέρον έχει η αναλογία από την πλευρά της οργανωτικής δομής του στρατεύματος. Αρχικά έχουμε τα επιτελεία του Στρατού (ξηράς), Ναυτικού (θάλασσας) και της Αεροπορίας (αέρα). Μετά, όμως, ηγετικό ρόλο αποκτά το Γενικό Επιτελείο (συμβολικό πεδίο - διάστημα), το οποίο κατά κύριο λόγο έχει την αποστολή τον συντονισμό των παραπάνω. Στις ημέρες μας, οι «ανερχόμενες» Διευθύνσεις ή Διοικήσεις Κυβερνοασφάλειας, διατηρούν έναν έντονο διακλαδικό χαρακτήρα και το σημαντικότερο είναι ότι συνεργάζονται -και εξ αποστολής- με πολιτικές υπηρεσίες ασφαλείας. Για παράδειγμα, στις ΗΠΑ η Διοίκηση Κυβερνοάμυνας (USCYBERCOM) έχει τον ίδιο αρχηγό με την Υπηρεσία Εθνικής Ασφάλειας (NSA).

ενημερωνόταν μερικώς, τώρα πλέον μπορεί να συμμετέχει στα πολεμικά γεγονότα, τα οποία διαδραματίζονται και ορισμένες φορές να έχει καλύτερη αντίληψη των πεπραγμένων και από την ίδια την ηγεσία.

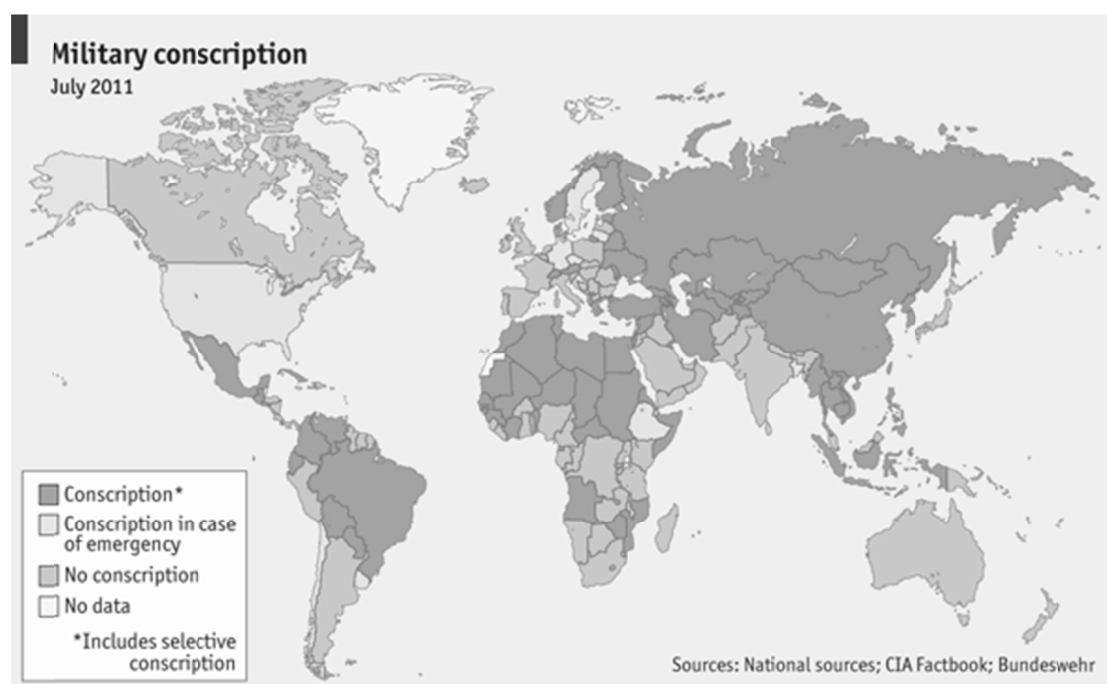
Παρεμπιπτόντως παρόμοια αλλαγή έχουμε και στην έννοια της ασφάλειας. Ενώ στην αρχή νοείται μόνο ως πρόβλημα που χρήζει στρατιωτικής επίλυσης. Στη συνέχεια «ανοίγει» (Ντόκος, 2005, 23-25) με την απαίτηση της συμβολής των επιστημόνων και τέλος, διευρύνεται επιζητώντας τη συνδρομή πολιτών, όχι μόνο με επιστημονική κατάρτιση, αλλά και με τη συγκεκριμένη τεχνολογική έφεση (πίνακας 8). Ένα χαρακτηριστικό παράδειγμα εδώ, είναι ότι στην εισηγητική παρουσίαση της Στρατηγικής Εθνικής Ασφάλειας του Ηνωμένου Βασιλείου, τον Οκτώβριο του 2010, από τον πρωθυπουργό David Cameron, με τίτλο «Μια δυνατή Βρετανία σε μια αβέβαιη εποχή» αναφέρεται (σε ελεύθερη μετάφραση)¹²⁹ ότι η Βρετανία, μπορεί να είναι ένα νησί γεωγραφικά, αλλά δυνητικά μπορεί να πληγεί από οπουδήποτε στον κόσμο, διότι είναι συνδεδεμένη στο παγκόσμιο δίκτυο».

Πίνακας 8: Οι συμβολισμοί των τριών φάσεων εκδήλωσης του πολεμικού φαινομένου

	18 ^{ος} αι. – 1945	1945-1989	1990 – 21 ^{ος} αι.
ΕΙΔΟΣ ΠΟΛΕΜΟΥ	«Κλασικός» Συμβατικός	Πληροφοριακός	Κυβερνοπόλεμος
ΠΕΔΙΟ ΜΑΧΗΣ	Ξηρά - Θάλασσα - Αέρας	Διάστημα	Κυβερνοχώρος
ΛΕΞΗ-ΚΛΕΙΔΙ ΠΕΔΙΟΥ ΜΑΧΗΣ	Μάζα	Πληροφορία	Προσομοίωση
ΑΠΕΙΛΗ	Έξωθεν (Εισβολή)	Πυρηνικός πόλεμος	Εκ των έσω (Εθνικές Συγκρούσεις)
ΑΠΟΣΤΟΛΗ	Προάσπιση συνόρων	Ενίσχυση συμμαχίας	«Ανθρωπισμός» (Ειρηνευτικές)
ΔΟΜΗ - ΕΠΙΤΕΛΕΙΑ	Στρατού Ξηράς, Ναυτικού, Αεροπορίας	Γενικό Επιτελείο Εθνικής Άμυνας	Πολιτικό/Στρατιωτικές «συνδιοικήσεις»
ΕΝΗΜΕΡΩΣΗ	Λογοκρισία	Παθητική	Εξατομικευμένη
ΣΤΡΑΤΟΛΟΓΗΣΗ	Καθολική στράτευση	Επιλεκτική	Αποδεδευσμένες
ΑΝΘΡΩΠΙΝΟΙ ΠΟΡΟΙ	«όσο περισσότεροι, τόσο καλύτερα..»	«όσο πιο ειδικοί και με εμπειρία»	«μορφωμένοι – εξειδικευμένοι»
ΑΣΦΑΛΕΙΑ	Στενά Στρατιωτική	Διεύρυνση της Έννοιας	Ο στρατιωτικός τομέας υποσύνολο

¹²⁹ Η ακριβής διατύπωση είναι: Geographically Britain is an island, but economically and politically it is a vital link in the global network.

Σχήμα 26. Παγκόσμια Πολιτική Στρατολόγησης



Πηγή: <http://www.economist.com/blogs/dailychart/2011/07/military-conscription>, 4/7/2011.

8. ΟΙ ΠΡΩΤΕΣ ΕΠΙΣΤΗΜΟΝΙΚΕΣ ΘΕΣΕΙΣ ΓΙΑ ΤΟΝ ΚΥΒΕΡΝΟΠΟΛΕΜΟ

8.1 Εισαγωγή

Ο επιστημονικός προσδιορισμός, καθώς και η θεωρητική θεμελίωση ενός φαινομένου, το οποίο έχει διάρκεια ζωής λιγότερο από δύο δεκαετίες, σίγουρα δεν αποτελεί ένα εύκολο εγχείρημα. Εντούτοις, έχουν δημοσιευθεί αρκετές πρώτες απόπειρες εννοιολογικής οριοθέτησης του φαινομένου. Σε αυτές περικλείουμε όσες διαθέτουν μια επιστημονική τεκμηρίωση και έκταση, όπως σε επίπεδο άρθρου ή βιβλίου. Δεν μπορούμε όμως να συμπεριλάβουμε και τις διάφορες προσπάθειες ορισμού του όρου, οι οποίες έχουν δημοσιοποιηθεί με την ευκαιρία δηλώσεων, συνεντεύξεων ή ακόμα και κάλυψης θεσμικών αναγκών καθορισμού αποστολών διαφόρων υπηρεσιών, συνήθως από τα υπουργεία άμυνας χωρών.

Στις τελευταίες περιπτώσεις δεν σημαίνει πως οι διατυπώσεις είναι ανακριβείς. Αντιθέτως, διακρίνουμε ιδιαίτερα εύστοχες περιγραφές, οι οποίες ωστόσο δεν συμβάλλουν σε μια πρώτη σκιαγράφηση μιας ακαδημαϊκού ύφους προσέγγισης. Ενδεικτικά, ο Amit Yoran, πρώην διευθυντής κυβερνοασφάλειας στο υπουργείο εσωτερικής ασφάλειας των ΗΠΑ και σημερινός επικεφαλής της Netwitness Corp, ορίζει, γενικά, τον κυβερνοπόλεμο ως τη χρήση της πληροφοριακής τεχνολογίας για την εξυπηρέτηση των σκοπών της διεξαγωγής ενός πολέμου (<http://news.bbc.co.uk>, 15/3/2010). Επιπρόσθετα, η ψηφιακή εγκυκλοπαίδεια του παγκόσμιου ιστού γράφει ότι ο κυβερνοπόλεμος αναφέρεται σε ένα πολιτικά υποκινούμενο hacking με σκοπό το σαμποτάζ και την κατασκοπεία. Εντοπίζει τις ρίζες του στον πληροφοριακό πόλεμο και εκτιμάει ότι μπορεί να ιδωθεί και ανάλογα του συμβατικού τρόπου διεξαγωγής πολέμου (Wikipedia, 2008).

Εξάλλου, όπως αναφέρουμε και στην εισαγωγή, πρόθεσή μας σε αυτή την εργασία δεν αποτελεί η πηγή της να ταυτιστεί με τη μέθοδο της βιβλιογραφικής επισκόπησης. Ως εκ τούτου, σκοπός αυτού του κεφαλαίου είναι η κάλυψη της απαίτησης, για την ολοκλήρωση μιας διατριβής, της παρουσίασης των ήδη διατυπωμένων απόψεων για το θέμα. Για αυτό τον λόγο, σε αυτό το κεφάλαιο έχουμε επιλέξει να παραθέσουμε τις θέσεις συγγραφέων από πέντε έργα, τα οποία κρίνουμε ότι δίνουν την πρώτη εικόνα της θεωρητικής αντιμετώπισης του φαινομένου¹³⁰.

¹³⁰ Σημειώνουμε πως η σειρά παράθεσης, η οποία ακολουθεί, δεν σχετίζεται με καμία δική μας ιεραρχική αξιολόγηση, αλλά είναι μόνο με ένα χρονικό κριτήριο.

8.2 John Arquilla & David Ronfeldt «Κυβερνοπόλεμος-Δικτυοπόλεμος»¹³¹ ('93)

Οι J. Arquilla¹³² και D. Ronfeldt¹³³ είναι ανώτεροι σύμβουλοι και μέλη του τμήματος έρευνας της διεθνούς πολιτικής, στη γνωστή «δεξαμενή σκέψης» των ΗΠΑ, RAND. Οι παραπάνω συγγραφείς, σε γενικές γραμμές, διαγιγνώσκουν ότι ο κυβερνοπόλεμος εμφανίζεται στα πλαίσια του πληροφοριακού πολέμου. Εκτιμούν ότι είναι ικανός στο μέλλον, να αντικαταστήσει τις μεγάλες, μαζικές κι αιματηρές συγκρούσεις με μικρές, μετακινούμενες συρράξεις «ακριβείας». Με το τελευταίο εννοούν την επίτευξη στόχων, δίχως πολλές παράπλευρες απώλειες. Σε αυτό θα συνεισφέρουν καθοριστικά οι λεπτομερείς πληροφορίες για τον εχθρό, οι οποίες θα είναι δυνατόν να λαμβάνονται αξιοποιώντας τις ευκαιρίες των νέων ΤΠΕ. Ειδικότερα δε, αναφέρονται στους αισθητήρες που χρησιμοποιούνται στις μάχες, καθώς και στη συμβολή των δορυφόρων.

Με σκοπό να δείξουν παραστατικότερα τι εννοούν, κάνουν μια ιστορική αντιπαραβολή με τις ορδές των Μογγόλων του 13ου αιώνα. Αυτοί, με αρχηγό τον Τζένκις Χαν (1162-1227) το μεγαλύτερο χρονικό διάστημα, κυριάρχησαν στην ευρασιατική περιοχή για παραπάνω από έναν αιώνα. Η ανάλυσή τους, λοιπόν, τους οδηγεί στο συμπέρασμα ότι η επιτυχία τους δεν οφειλόταν στις πολυάριθμες νομάδες πολεμιστών τους, οι οποίες είχαν ενωθεί. Αντιθέτως, συχνά ήταν πολύ λιγότεροι από τους αντιπάλους τους. Το κλειδί ήταν η απόλυτη υπεροχή στο πεδίο των πληροφοριών. Ο «Μεγάλος Χαν» είχε δημιουργήσει ένα τεράστιο επικοινωνιακό δίκτυο πληροφόρησης, το οποίο διατηρούσε το στρατό ενωμένο. Αυτός ακριβώς είναι και ο πυρήνας της πληροφοριακής εποχής μας, η οποία όπως υποστηρίζουν οι συγγραφείς, ακολούθησε τον μηχανοποιημένο και γεμάτο ελιγμούς στο πεδίο της μάχης δεύτερο παγκόσμιο πόλεμο, ο οποίος με τη σειρά του είχε ακολουθήσει τον βιομηχανοποιημένο και μαζικό στο πεδίο της μάχης πρώτο παγκόσμιο πόλεμο.

Στη συνέχεια διαχωρίζονται δύο είδη πολέμου, τα οποία προκύπτουν από τη χρήση των ΤΠΕ. Ο ένας είναι ο *δικτυοπόλεμος* (netwar), ο οποίος αναφέρεται σε συγκρούσεις μεταξύ εθνών και κοινωνιών. Σκοπός του είναι η διάσπαση ή

¹³¹ Η περικοπή προήλθε από το: J. Arquilla & D. Ronfeldt (1993), *Cyber War Is Coming!*, στο *Comparative Strategy*, Vol. 12, pp. 141-165.

¹³² Ο J. Arquilla είναι καθηγητής στη ναυτική σχολή μεταπτυχιακών σπουδών των ΗΠΑ. Ειδικεύεται στις ασύμβατες μορφές πολέμου, με εξειδίκευση στον πληροφοριακό πόλεμο. Κατέχει διδακτορικό δίπλωμα στις Διεθνείς Σχέσεις (Ph.D. - Stanford University).

¹³³ Ο D. Ronfeldt κατέχει πρώτο πτυχίο στις Διεθνείς Σχέσεις (B.A. - Pomona College), μεταπτυχιακό τίτλο στις λατινοαμερικανικές σπουδές (M.A. - Stanford University) και διδακτορικό στις πολιτικές επιστήμες (Ph.D. - Stanford University).

καταστροφή του τι γνωρίζει ή νομίζει πως γνωρίζει ένας πληθυσμός για τον εαυτό του. Στοχεύει στην κοινή γνώμη ή στη γνώμη μιας συγκεκριμένης ελίτ. Επίσης, είναι δυνατόν να συμπεριλαμβάνεται στη διπλωματία, την προπαγάνδα και τις ψυχολογικές εκστρατείες. Συνοπτικά, λοιπόν, σκοπός είναι η επίδραση στην κουλτούρα μιας ομάδας, μέσω του «φιλτραρίσματος» των μηνυμάτων τα οποία διακινούνται στο διαδίκτυο.

Τέλος, εμβαθύνοντας στις αιτίες εμφάνισής τους, ανακαλύπτουν ότι αυτές εντοπίζονται στον μετασχηματισμό του οργανωτικού μοντέλου της κοινωνίας, από τον ιεραρχικό τρόπο δόμησης στον δικτυακό.

Από την άλλη πλευρά θεωρούν πως ο κυβερνοπόλεμος αναφέρεται στο στρατιωτικό μέρος. Σε αυτό το μέρος επιχειρείται η διάρρηξη ή καταστροφή στρατιωτικών πληροφορικών συστημάτων του εχθρού. Μέσα από αυτές τις ενέργειες γίνεται μια προσπάθεια να ληφθεί οποιαδήποτε γνώση για τον εχθρό και παράλληλα, να εμποδιστεί η δυνατότητά του να κάνει και αυτός το ίδιο. Όπως χαρακτηριστικά εκφράζεται «να γείρει στο μέρος μας το πληροφοριακό ισοζύγιο».

Έτσι, οι στόχοι μπορεί να αφορούν είτε την αδυναμία του εχθρικού αρχηγείου να ενημερωθεί για την κατάσταση στο πεδίο της μάχης, είτε να μαθαίνουμε ταυτόχρονα τις εντολές που δίνονται για τις κινήσεις του. Οι αιτίες εδώ αποδίδονται στην ευκαιρία, η οποία δόθηκε από τις ΤΠΕ, για έναν αποκεντρωμένο τύπο διεξαγωγής πολέμου. Ο εν λόγω τύπος είναι γνωστός ως το αποτέλεσμα της οργανωτικής μετάβασης, που από τον πληροφοριοκεντικό στον δικτυοκεντρικό πόλεμο¹³⁴.

Επιπρόσθετα, για την καλύτερη κατανόηση της κρισιμότητας των παραπάνω, κατατίθενται δύο ιστορικές αναλογίες. Η πρώτη αφορά τις αστραπιαίες αεροπορικές επιθέσεις του δεύτερου παγκοσμίου πολέμου (blitzkrieg), οι οποίες εκμεταλλεύτηκαν την αντίστοιχη στρατιωτική καινοτομία της εποχής. Η δεύτερη αφορά τον μετέπειτα πόλεμο του Βιετνάμ (1959 – 1975), όπου οι Vietcong¹³⁵ εφάρμοσαν με επιτυχία μια δικτυοκεντρική οργάνωση μάχης, διεξάγοντας έναν ακανόνιστο ή άτακτο ανταρτοπόλεμο (<http://www.rand.org>, 29/5/2009).

¹³⁴ Πιο συγκεκριμένα, αυτό θεωρείται ότι προκάλεσε η λεγόμενη αμερικανική πολεμική επανάσταση, η οποία επιδίωκε αποδοτικότερο στράτευμα, με μικρότερο κόστος (Γρίβας, 2008, 155).

¹³⁵ Αλλιώς, το Εθνικό Απελευθερωτικό Μέτωπο, το οποίο ήταν το στρατιωτικό κομμάτι της κομμουνιστικής – πολιτικής οργάνωσης του Νότιου Βιετνάμ και πολέμησε την κυβέρνηση του Βόρειου Βιετνάμ που συμμαχόταν με τον στρατό των ΗΠΑ.

8.3 Π. Κονδύλης «Θεωρία πολέμου - από τον 20ο στον 21ο αιώνα»¹³⁶ ('98 – '99)

Πολλοί συγγραφείς έχουν σχολιάσει τη σημασία της έννοιας του κυβερνοχώρου και δη τη διεξαγωγή πολεμικών και συναφών φαινομένων μέσα σε αυτόν. Ορισμένοι θεωρούν ότι πρόκειται για τη νέα αποφασιστική διάσταση στο πεδίο των πολεμικών επιχειρήσεων. Άλλοι όμως, θεωρούν ότι προβάλλεται μια υπερβολή σε σχέση με την πραγματικότητα και η εμπλοκή σε αυτό το νέο άυλο χώρο δεν υποβαθμίζει διόλου τον σημαντικό ρόλο των υλικών αγαθών (π.χ. πρώτων υλών). Ένας από τους τελευταίους είναι ο Παναγιώτης Κονδύλης¹³⁷, ο οποίος είναι από τους πρώτους που συνέγραψαν τη θέση τους για τον πόλεμο στον κυβερνοχώρο.

Ο ίδιος περιγράφει τη μελέτη του φαινομένου από κάποιους μελλοντολόγους¹³⁸ του κυβερνοχώρου ως το αναγκαίο «ιδεολογικό άλλοθι» της σύγχρονης εποχής της μαζικής δημοκρατίας (Κονδύλης, 1998/2000, 9). Γενικά, η κεντρική ιδέα αυτού του ουτοπισμού -κατά το συγγραφέα- περικλείεται σε μια συστημική – κυβερνητική έποψη, η οποία θεωρεί ότι όσο πιο περίπλοκη γίνεται η κοινωνία, τόσο χρειάζεται έναν αναστοχασμό, ο οποίος όμως απαιτεί περισσότερη γνώση. Ωστόσο, για την εναντίωσή του σε αυτήν την θέση, παραθέτει το επιχείρημα πως ιστορικά, η ανθρώπινη συμπεριφορά δεν άλλαξε ποτέ εξαιτίας της μεταβολής της πυκνότητας των πληροφοριών (όπως για παράδειγμα η εποχή της τυπογραφίας) (Κονδύλης, 1998/2000, 147-148). Συνδέει δε, συμβολικά, την εποχή της νεωτερικότητας με το «πριν και το μετά» (Κονδύλης, 1998/2000, 152):

Οι κοινωνίες τότε μόνο βεβαιώνονται ότι υπάρχουν πραγματικά, όταν φαντάζονται τον εαυτό τους ως μυθικές υποστάσεις. Γιατί μέσα στις υποστάσεις αυτές, οι οποίες συμπιούνται τόσο από πραγματικά στοιχεία όσο και από τις επιθυμητές μελλοντικές επεκτάσεις τους, συμπυκνώνεται η αυτοκατανόησή τους. Αν η αυτοκατανόηση της αστικής κοινωνίας μετά το θάνατο του Θεού αναφερόταν σε μυθικές υποστάσεις όπως «Φύση», «Ιστορία» ή «Ανθρωπότητα», τώρα, μετά το θάνατο του Ανθρώπου, η μαζική δημοκρατία αυτοχαρακτηρίζεται ως «δομή» ή «λειτουργικό σύστημα», που μπορεί να

¹³⁶ Οι περικοπές προήλθαν από τα: Π. Κονδύλης (1998/2000), *Από τον 20ο στον 21ο αιώνα – Τομές στην πλανητική πολιτική περί το 2000*, Αθήνα: Θεμέλιο, σσ. 152-155 & Π. Κονδύλης (1999), *Θεωρία του Πολέμου*, Αθήνα: Θεμέλιο.

¹³⁷ Ο Π. Κονδύλης (1943 – 1998) κατάγεται από τη Αρχαία Ολυμπία. Σπούδασε κλασσική φιλολογία στο Πανεπιστήμιο Αθηνών, νεότερη ιστορία και πολιτικές επιστήμες στα Πανεπιστήμια Φραγκφούρτης και Χαϊδελβέργης, όπου και απέκτησε το διδακτορικό του στη φιλοσοφία. Έχει τιμηθεί για την εργασία του με το μετάλλιο Γκαίτε και το βραβείο Χούμπολντ.

¹³⁸ Συγκεκριμένα, με αυτόν τον τρόπο (Π. Κονδύλης (1998), *Από τον 20ο στον 21ο αιώνα*, Θεμέλιο, σ. 152) χαρακτηρίζει κυρίως τον πρώτο συγγραφέα του έργου: Α., Toffler, G., Keyworth, et.al. (1994), *Cyberspace and American Dream: A Magna Carta for the Knowledge Age*, Published by Progress and Freedom Foundation. Αξιοσημείωτο, επίσης, είναι πως ο δεύτερος συγγραφέας (Keyworth) μέσα από αυτό το κείμενο περιέγραψε και το όραμά του -εκείνης της εποχής- για ένα μέρος της μελλοντικής εξωτερικής πολιτικής του ρεπουμπλικανικού κόμματος των ΗΠΑ, ενώ διετέλεσε και επιστημονικός σύμβουλος του R. Reagan.

το συλλάβει και να το κατευθύνει κανείς μέσω της κυβερνητικής. Υπό το πρίσμα της οικουμενικής πληροφορικής τούτο το σύστημα ονομάστηκε πρόσφατα «κυβερνοχώρος».

Σε αυτή την κατεύθυνση διατυπώνει και τη θέση του για τους «νέους πολέμους», οι οποίοι επιβεβαιώνοντας τον Κλαούσεβιτς παραμένουν χαμελεωντικοί· ο διαχωρισμός τους, δηλαδή, είναι δύσκολος και είναι αδύνατο να ακυρώσουν καθοριστικούς πολιτικούς ή ψυχολογικούς συντελεστές στο βωμό μιας τεχνοκρατικής επικράτησης (Κονδύλης, 1999, 365).

8.4 M. Libicki «Κατάκτηση του κυβερνοχώρου - Κυβερνοαποτροπή» ('07 - '09)

Ένας από τους πρώτους επιστήμονες που δημοσίευσαν μελέτες για το φαινόμενο του κυβερνοπολέμου -εντάσσοντάς το στη γενικότερη κατηγορία του πληροφοριακού πολέμου- είναι ο Μάρτιν Λιμπίκι¹³⁹. Πρόκειται για ένα από τα πρώτα έργα σύνδεσης του κυβερνοχώρου με τα ζητήματα εθνικής ασφαλείας¹⁴⁰. Αποδέχεται την πολύπλοκη φύση του, αλλά εκτιμάει ότι υπάρχουν πολλές υπερβολικές αναλύσεις για την επικινδυνότητά του.

Το δεύτερο έργο εξειδικεύθηκε στον κυβερνοπόλεμο και δη στην κατανόηση των δυνατοτήτων εφαρμογής της πολιτικής και στρατηγικής της αποτροπής¹⁴¹. Από τον πρόλογό του διασαφηνίζει ότι ο κυβερνοχώρος είναι ένα ιδιαίτερο, διαφορετικό από τα άλλα (της ξηράς, της θάλασσας και του αέρα) μέσο, το οποίο διακρίνεται για τα δικά του γνωρίσματα στις πολεμικές δομές (επίθεση, άμυνα, αποτροπή κ.λπ.). Σύμφωνα με τον συγγραφέα, είναι πολύ σημαντικό, επί παραδείγματι, να κατανοήσουμε ότι ο λόγος που είναι δυνατόν να εκδηλωθούν οι κυβερνοεπιθέσεις, δεν έγκειται στον επιτιθέμενο. Αντιθέτως, όσο πιο τρωτά είναι τα πληροφοριακά και επικοινωνιακά συστήματα ενός υποκειμένου (συλλογικού ή ατομικού), τόσο πιο δεκτικός γίνεται σε αυτού του είδους τις επιθέσεις. Αυτό το χαρακτηριστικό έχει δύο άμεσες συνέπειες. Αφενός, ως προς τον επιτιθέμενο, ο οποίος θα πρέπει να αναζητά συνεχώς τα «κενά» στο αντίπαλο σύστημα και αφετέρου, ως προς τον αμυνόμενο, ο

¹³⁹ Σήμερα, κατέχει από το 1998 ανώτερη θέση στο επιστημονικό προσωπικό της «δεξαμενής σκέψης» RAND Co. Ενώ προηγουμένως εργάστηκε στο βιομηχανικό τομέα του πολεμικού ναυτικού. Επικεντρώνεται στα θέματα της ασφάλειας των πληροφοριών. Οι σπουδές του ξεκίνησαν από το Μαθηματικό (Bc), μετά στον πολεοδομικό σχεδιασμό (Ms) και τέλος, στα βιομηχανικά οικονομικά (PhD - University of California).

¹⁴⁰ M. Libicki, *Conquest in Cyberspace - National Security and Information Warfare*, The RAND Corporation - Cambridge University Press (2007).

¹⁴¹ M. Libicki, *Cyberdeterrence and Cyberwar*, The RAND Corporation - Cambridge University Press (2009).

οποίος οφείλει να διαθέτει μια διαδικασία διαρκούς κάλυψης των εν λόγω κενών του, τα οποία παραδόξως, συνήθως, ανακαλύπτει μετά από παρόμοιες επιθέσεις. Σε αυτήν την περίπτωση, λοιπόν, μπορούμε να δούμε τη διαφορά με το παρελθόν αναλογιζόμενοι τις κοινωνικές συνέπειες που θα έχει ένα πολεμικό χτύπημα σε έναν πόλεμο στο φυσικό περιβάλλον, σε σύγκριση με τον κυβερνοχώρο. Έτσι, ένας αεροπορικός βομβαρδισμός θα εξασθενούσε τους κατοίκους μιας πόλης και, αν αυτός είναι ο στόχος, επιτυγχάνεται. Ωστόσο, ένα πλήγμα στον κυβερνοχώρο αποκαλύπτει τρωτότητες των οποίων η θεραπεία, παραδόξως, δύναται να ενισχύει την κοινωνία.

Μια από τις πρώτες ασυμμετρίες που παρατηρούμε στον κυβερνοπόλεμο είναι ότι (μεγάλες) επιθέσεις μπορούν να γίνουν με πολύ μικρό κόστος, ενώ αντιθέτως, τόσο οι απαιτήσεις της αμυντικής οργάνωσης, όσο και οι συνέπειες της επίθεσης μπορεί να είναι ανυπολόγιστες (Libicki, 2009, 5). Πέρα, όμως, από την άμυνα και την επίθεση, η μελέτη εστιάζεται στους πολιτικούς στόχους της κυβερνο-αποτροπής, η οποία νοείται ως ο έλεγχος της εκδήλωσης αντικινήτρων για την κλιμάκωσης μιας επίθεσης. Αυτή είναι δυνατόν να πραγματοποιηθεί συνοπτικά, είτε μέσω της αποθάρρυνσης των πιθανών αντιπάλων, είτε μέσω της υλοποίησης αντιποίνων (Libicki, 2009, 7). Συχνά για αυτή τη στρατηγική δραστηριότητα χρησιμοποιείται η έκφραση «ενεργητική άμυνα».

Ο τρόπος που ο συγγραφέας περιγράφει τον κυβερνοχώρο είναι καθοριστικός για την αντίληψή του όσον αφορά τους στόχους των επιθέσεων μέσα σε αυτόν. Τον διαιρεί σε τρία στρώματα, με κριτήριο τη συμπύκνωση της ύλης, στη φύση της σύστασης του καθενός. Το πρώτο το επονομάζει *φυσικό*, το δεύτερο *συντακτικό* και το τρίτο *σημασιολογικό* (Libicki, 2009, 16).

Αντίστοιχα είναι και τα είδη των κυβερνοεπιθέσεων. Επιγραμματικά, μπορούμε να πούμε, πως το κοινό σημείο το οποίο εντοπίζει σε όλα τα είδη, είναι ότι ο κυβερνοπόλεμος βασίζεται στην «τέχνη» της εξαπάτησης¹⁴². Με αυτή την έκφραση εννοεί πως στο πληγέν πληροφορικό σύστημα δεν αλλάζει κάτι στη ροή της λειτουργίας του. Αντιθέτως, αυτό εξακολουθεί να υπακούει στις οδηγίες που του δίνονται· μόνο που εντολοδότης πλέον δεν είναι ο νόμιμος. Αυτή, την «κλασική» περίπτωση *hacking*, την θεωρεί ως τον εξωτερικό τρόπο μη εξουσιοδοτημένης εισβολής. Επιπρόσθετα, αναφέρονται και δύο εσωτερικοί. Αφενός, η εχθρική στρατολόγηση χειριστών (“*insiders*”, κάτι σαν μια μεταμοντέρνα εκδοχή ψηφιακής

¹⁴² Σε αυτό το σημείο παρατηρούμε μια ταυτοσημία με το ομώνυμο χαρακτηριστικό, το οποίο προσδίδει και ο Sun Tzu στο πολεμικό φαινόμενο.

προδοσίας) και αφετέρου, ενσωμάτωση κατασκοπευτικών εξαρτημάτων ήδη από την αλυσίδα της κατασκευής τους, πριν ακόμα φθάσουν σε εμάς (Libicki, 2009, 20). Επιχειρώντας να συνοψίσει την άποψή του, ότι η αποτροπή δεν είναι τίποτε άλλο παρά ένα σινιάλο στον ενδεχόμενο αντίπαλο, αναφέρει ότι θα πρέπει να πείθουμε τους άλλους -με συνηματικό έστω τρόπο- ότι έχουμε την ικανότητα και επιδιώκουμε να τους κάνουμε αυτό που θα ήθελαν αυτοί να μας κάνουν (Libicki, 2009, 27).

Επίσης, οφείλουμε να γνωρίζουμε πως η κυβερνοαποτροπή θα πρέπει να είναι επαναλαμβανόμενη (ώστε να πείθει τους αντιπάλους), συμμετρική (σε αντίθεση με την παραδοσιακή της πυρηνικής εποχής) και κυρίως, ότι έχει να κάνει με μια πολιτική προγραμματισμού, η οποία θα επιφέρει και το ανάλογο οικονομικό κόστος. Σε αντίθεση με την κοινή πεποίθηση, όσο λιγότερες είναι οι πιθανότητες να πιαστούν οι αντίπαλοι, τόσο μεγαλύτερες θα πρέπει να είναι οι ποινές που προβάλλονται για τις επικείμενες πράξεις τους, ώστε αυτός να είναι επαρκής λόγος για να τις αποφεύγουν (Libicki, 2009, 43).

Ένα ιδιαίτερο σημείο της μελέτης αποτελεί το περιεχόμενο που περιλαμβάνεται στις αιτίες που μπορούν να προκαλέσουν μία κυβερνοεπίθεση. Πιο συγκεκριμένα, πρόκειται να είναι μια από τις ακόλουθες (Libicki, 2009, 75):

- Απλά ένα λάθος. Δηλαδή εξαιτίας ενός ατυχήματος ή κακού χειρισμού, δίχως άλλο σκοπό. Ένα κριτήριο για να κατατάξουμε ένα πλήγμα σε αυτήν την κατηγορία είναι ότι αφορά συνήθως μικρές και περιφερειακές βλάβες.
- Όταν ο αντίπαλος προσπαθεί να εκβιάσει μια κατάσταση, τότε ο στόχος θα έχει μεγάλες επιπτώσεις, με επίκεντρο την αποδυνάμωση του ψυχολογικού μας σθένους.
- Όταν ο εχθρός προσπαθεί να πολλαπλασιάσει τη στρατιωτική του ισχύ, τότε ο στόχος γίνεται κεντρικός κι εντάσσεται σε ένα γενικότερο επιχειρησιακό σχεδιασμό.
- Οι διάφοροι άλλοι σκοποί ενός υποκειμένου συνήθως αποσκοπούν σε εξειδικευμένους, περιφερειακούς στόχους, οι οποίοι εκτιμούν πως θα έχουν μεγαλύτερη επισφάλεια.

Παρόλα αυτά αξιοσημείωτη είναι η παρατήρηση ότι κατά το συγγραφέα συνιστά εξαίρεση, όπως προκύπτει από τον γενικότερο ορισμό της κυβερνοεπίθεσης, η περίπτωση υπονόμευσης (αλλοίωσης ή υποκλοπής) των πληροφοριών. Ειδικότερα, αναφέρει πως, όπως και στη φυσική κατασκοπεία, δεν είναι μυστικό ότι αυτό συμβαίνει ή επιχειρείται να συμβεί παντού και πάντα. Ποτέ, σε γενικές γραμμές, αυτό δεν αποτέλεσε αιτία πολέμου, μια και το αποτέλεσμα δεν είναι μια φυσική καταστροφή. Πάντως, τονίζεται ότι οι κυβερνοεπιθέσεις είναι εξαιρετικά χρήσιμο να

δημοσιοποιούνται, με όσο το δυνατόν περισσότερα στοιχεία (ταυτότητα απειλής, δημόσιος ή ιδιωτικός χαρακτήρας, αποτελέσματα). Ο λόγος είναι ότι με αυτόν τον τρόπο αποκαλύπτεται ο δυνητικός στόχος. Επιπλέον, προσδίδει τον επιθετικό προσδιορισμό της «στρατηγικής», στις κυβερνοεπιθέσεις οι οποίες συντονίζονται εναντίον ενός κράτους και της κοινωνίας του (Libicki, 2009, 117).

Εν κατακλείδι, υπογραμμίζεται η έποψη ότι ένα κράτος το οποίο δεν διαθέτει συγκεκριμένη, δυναμική και κατάλληλα προβαλλόμενη πολιτική -μέσα από ένα συγκροτημένο δόγμα- για ένα ενδεχόμενο πλήγμα, ο κίνδυνος για αυτό το κράτος στο σύγχρονο κόσμο είναι μεγάλος. Μέσα από μια συγκριτική ιστορική μελέτη των κυρίαρχων τύπων αντιμετώπισης της απειλής, καταλήγει πως η περίοδος μέχρι τον δεύτερο παγκόσμιο πόλεμο βασίζεται στον *αφοπλισμό* (το οποίο σημαίνει την εκμηδένιση του εχθρού, μέσω της αρπαγής των όπλων του), ο λεγόμενος ψυχρός πόλεμος -που υπογραμμίζει πως δεν έγινε ποτέ «θερμός»- βασίζεται στην *αποτροπή* (η οποία εμπεριέχει την αντίδραση της απειλής, στην απειλή του αντιπάλου) και τέλος, στο μεταίχμιο του περασμένου, καθώς και αυτού του αιώνα, την *άμυνα* (την οποία περιγράφει ως την καταδίωξη των δυνητικών κακόβουλων υποκειμένων) (Libicki, 2009, 176-177).

Συμπεραίνουμε λοιπόν ότι η θέση του συγγραφέα στο έργο της *κυβερνο-αποτροπής* είναι ότι η σύγκρουση στον κυβερνοχώρο είναι ριζικά διαφορετική από αυτήν στον φυσικό και, γι' αυτόν το λόγο, οι εν λόγω (εννοιολογικές) μεταφορές θα πρέπει να λαμβάνονται σοβαρά υπόψη. Ενδεικτικά, στην κλαουσεβιτσιανή θέαση του πολέμου, ένας από τους σκοπούς -και μάλλον ο βασικότερος- είναι ο αφοπλισμός του αντιπάλου. Γίνεται εύκολα αντιληπτή η κατάρρευση αυτής της έννοιας (στη μεταφορά της) στον κυβερνοχώρο. Δηλαδή, είναι αδύνατον να εντοπιστούν όλοι οι χάκερς και μηχανήματα που μας απειλούν. Επιπροσθέτως θεμελιώδης είναι η διαφορά από έναν ενδεχόμενο πυρηνικό πόλεμο. Στην πρώτη περίπτωση, κάθε λογικός άνθρωπος θα έκανε τα πάντα για να τον αποτρέψει, ενώ στη δεύτερη περίπτωση, μυριάδες κυβερνοεπιθέσεων λαμβάνουν χώρα καθημερινά.

Ολοκληρώνουμε την προκείμενη παρουσίαση με την παράθεση ορισμένων σημαντικών στοιχείων από μία συνέντευξη του συγγραφέα¹⁴³. Σε αυτή τη συνέντευξη τονίζεται ότι βασικός στόχος είναι ο αφοπλισμός του αντιπάλου και αυτό είναι κάτι πολύ δύσκολο, ιδίως όταν εκείνος παραμένει άγνωστος. Ο κυβερνοπόλεμος, από τις

¹⁴³ Martin Libicki, *interview with Government Information Security Articles*, Eric Chabrow - Executive Editor (GovInfoSecurity.com, 9/11/2009).

άλλες μορφές πολέμου είναι πολύ αβέβαιος, εξαιτίας των άγνωστων πιθανοτήτων επίτευξης του στόχου («μερικές φορές δουλεύει κι άλλες όχι»). Για αυτό δεν προτείνεται ως προτεραιότητα στην αμερικανική στρατηγική.

Βεβαίως, υπογραμμίζει, ότι το χαμηλό κόστος μιας τέτοιας συνολικής επίθεσης. Αυτό αποτελεί και το βασικό κίνητρο της επιλογής της, σε αντίθεση με το (αντικίνητρο) του μη εγγυημένου αποτελέσματος, το οποίο δεν υφίσταται στον συμβατικό ή φυσικό πόλεμο. Θεωρεί ότι αφενός αποτελεί ένα αξιосύστατο όπλο, αφετέρου όμως, δεν πρέπει να «αναλώνεται σε κλαδικούς καταμερισμούς». Με αυτήν την έκφραση δίνεται έμφαση στην ανάγκη συνεργασίας των διαφόρων αρμόδιων φορέων, η οποία απαιτείται για την επίτευξη του βέλτιστου δυνατού αποτελέσματος. Ο όρος που έχει επικρατήσει για την έκφραση της παραπάνω προϋπόθεσης είναι η «διαλειτουργικότητα», η οποία μεγεθύνει την αποδοτικότητα της εκμετάλλευσης. Τέλος, καταλήγει ότι ο ρόλος της βιομηχανίας παραμένει και εδώ αποφασιστικός.

8.5 J. Carr «Χαρτογράφηση του υποκόσμου μέσα στον κυβερνοπόλεμο» (’10)

Μία από τις πιο πρόσφατες μελέτες που έχουν δημοσιευθεί σχετικά με την προσέγγιση του κυβερνοπολεμικού φαινομένου, είναι η συγκεκριμένη και μάλιστα ο συγγραφέας της είναι από τους πιο διάσημους εμπειρογνώμονες¹⁴⁴ των ΗΠΑ. Εξαρχής, θεωρείται πως ο όρος «κυβερνοπόλεμος» δεν είναι ο πιο κατάλληλος για να περιγράψει με ακρίβεια μια διεθνική *πράξη πολέμου* μέσω μιας σύγκρουσης στον κυβερνοχώρο. Αναφέρει πως η διερεύνηση αυτού του θέματος μπορεί να περιλαμβάνει διάφορα είδη, όπως το κυβερνοέγκλημα, την κυβερνοασφάλεια, την κυβερνοτρομοκρατία και την κυβερνοκατασκοπία. Επίσης, δύναται να εμπλέξει διάφορα πολιτικά υποκείμενα, όπως κράτη ή ενδοκρατικούς και υπερκρατικούς δρώντες. Επιπρόσθετα, στο εισαγωγικό κεφάλαιο εκφράζεται η αντίρρησή του για την τοποθέτηση του φαινομένου, σε μια «διαχρονική διαδρομή», ως το πέμπτο πεδίο κυριαρχίας (μετά την ξηρά, θάλασσα, αέρα και διάστημα). Διατυπώνεται η προτίμησή του σε έναν συμβολισμό ενός παράλληλου (με τα προηγούμενα τέσσερα) σύμπαντος· εξάλλου, πρόκειται για μια ιδέα της οποίας η προέλευση είναι κοινή με την έμπνευση του όρου και αυτή είναι η επιστημονική φαντασία.

¹⁴⁴ Ο Jeffrey Carr είναι υπεύθυνος της GreyLogic, η οποία διενεργεί έρευνες του διαδικτύου. Ειδικεύεται στις «κυβερνοπληροφορίες» (cyber intelligence), αντικείμενο στο οποίο επικεντρώνεται και η εταιρεία του. Παρεμπιπτόντως, πρόκειται για μια τεχνοκρατική ειδικότητα, ανάλυσης των ιχνών που αφήνει η συμπεριφορά κάποιου χρήστη στο διαδίκτυο. Έτσι, ερευνά τους ύποπτους κυβερνοεπιθέσεων και δεν εστιάζεται στην αξιοποίηση των πληροφοριών για την ανάλυση της εξέλιξης του φαινομένου του κυβερνοπολέμου (“Intelligence on the threat of cyber warfare”).

Στη συνέχεια παραθέτει τα χαρακτηριστικότερα συμβάντα κυβερνοπολέμου με μια σύντομη περιγραφή, ώστε να συναχθούν στο τέλος κάποια συμπεράσματα για τα κοινά τους γνωρίσματα. Έτσι, αναφέρονται:

- Κίνα (Carr, 2010, 2). Ινδονήσιοι χάκερς επιτίθενται σε κινέζους ομόλογούς τους (1998). Κινέζοι διαμαρτύρονται σε νατοϊκές ιστοσελίδες για τα γεγονότα στη Γιουγκοσλαβία (1999). Κινέζοι οργανώνονται, διαμέσου του κυβερνοχώρου, έναντι των ΗΠΑ (2001).
- Ισραήλ (Carr, 2010, 2). Κατά τον πόλεμο με τους Παλαιστίνιους διεξήχθησαν πολλές επιθέσεις σε τηλεπικοινωνιακούς κόμβους μεταξύ εβραίων και αράβων, με κύριο σκοπό την κοινωνική επιρροή (2008).
- Ρωσία (Carr, 2010, 3). Στα πλαίσια διεξαγωγής πληροφοριακών επιχειρήσεων, εθνικιστές προσπάθησαν να διαμορφώσουν την κοινή γνώμη, κατά τα πολεμικά επεισόδια με τους Τσετσένους (1997-2001). Αν και δεν υπάρχει επίσημη αποδοχή ή επαρκής απόδειξη, θεωρείται ότι Ρώσοι συντόνισαν τους υπολογιστές τους, ώστε με την αποστολή διαρκών αιτημάτων επίσκεψης σε επίσημες ιστοσελίδες της Εσθονίας να μπλοκάρουν τη λειτουργία τους (2007). Τέλος, κατά τη σύντομη πολεμική σύρραξη στα σύνορα της Γεωργίας, έχουμε την πρώτη περίπτωση παράλληλων επιχειρήσεων στον κυβερνοχώρο (2008).
- Ιράν (Carr, 2010, 3). Πολλοί αντικαθεστωτικοί χρησιμοποίησαν ιστότοπους κοινωνικής δικτύωσης για να εκφράσουν τη διαμαρτυρία τους την περίοδο πριν τις εθνικές εκλογές (2009).
- Ν. Κορέα (Carr, 2010, 4). Παρομοίως με την περίπτωση της Εσθονίας, δεν υπάρχει η απαραίτητη τεκμηρίωση, αλλά θεωρείται το πιθανότερο πως πολίτες αυτής της χώρας προσπάθησαν να διακόψουν την πληροφοριακή ροή σε κρίσιμα κέντρα των ΗΠΑ (2009).
- Ζιμπάμπουε (Carr, 2010, 38) και Μιανμάρ J. Carr, (2010, 39). Και στις δύο περιπτώσεις παρατηρήθηκε κατάχρηση εξουσίας από τις επίσημες κυβερνήσεις κατά την κρίσιμη περίοδο διεξαγωγής εκλογών. Οι μέθοδοι εκμετάλλευσης του κυβερνοχώρου που διακρίνουμε συνίστανται στην μια άκρη από απλή άσκηση λογοκρισίας, ως την άλλη άκρη, πλήρης διακοπή του Διαδικτύου.

Το πρώτο συμπέρασμα στο οποίο καταλήγει ο συγγραφέας από την επεξεργασία όλων αυτών των γεγονότων, είναι οι ποικίλες μορφές με τις οποίες μπορεί να εκδηλωθεί το φαινόμενο του κυβερνοπολέμου. Κάτι που αιτιολογεί και την πολυπλοκότητά του. Πράγματι, εντοπίζεται ένα μεγάλο φάσμα, από την υποστήριξη

στρατιωτικών επιχειρήσεων ως τη στόχευση στην επίδραση της κοινής γνώμης. Εντούτοις, ένα δεύτερο -εξίσου σημαντικό- στοιχείο είναι πως κανένα από αυτά δεν συνιστούν *πράξη πολέμου* βάσει το Διεθνές Δίκαιο (Carr, 2010, 39). Αυτό, διαμορφωμένο κατά τις συνθήκες λήξης του δεύτερου παγκοσμίου πολέμου, θέτει την απαραίτητη προϋπόθεση της ένοπλης επίθεσης, η οποία επιφέρει «ορατές» καταστροφές σε υλικούς κι ανθρώπινους πόρους. Εδώ, προκύπτει ίσως η πιο ενδιαφέρουσα πρόταση σε αυτό το έργο¹⁴⁵. Υποστηρίζεται, λοιπόν, ότι οποιαδήποτε αντίμετρα από ένα κράτος που δέχθηκε κυβερνοεπίθεση θα πρέπει να θεωρηθούν δικαιολογημένη αντίδραση, αρκεί να μπορεί ναδειχθεί το εξής: Το κράτος, στο οποίο εντοπίζεται η έδρα αυτών που καταφέρνουν το πλήγμα, δεν κάνει τις απαραίτητες ενέργειες για την αποτροπή τους. Το ζημιωμένο κράτος θα πρέπει τότε να αποκτή το δικαίωμα παρέμβασης για τη διασφάλιση των συμφερόντων του.

Ωστόσο, ιδιαίτερο ενδιαφέρον, παρουσιάζει η αφορμή για την δημιουργία του συγκεκριμένου έργου. Αυτή ήταν η ανοιχτή πρόσκληση για τη συμμετοχή σε ένα εγχείρημα αναζήτησης και εύρεσης πληροφοριών, σε ζητήματα ασφάλειας ψηφιακών δικτύων (Project Grey Goose - PGG). Ειδικότερα, η ανταπόκριση που προέκυψε για την ανίχνευση των υπαιτίων σχετικά επεισόδια στην Εσθονία και Γεωργία, έπαιξε το βασικό ρόλο. Ως εκ τούτου, ήταν επόμενη η εμβάθυνση σε ορισμένες νέες εκφάνσεις στα θέματα των πληροφοριών του κυβερνοχώρου (Carr, 2010, 77). Δύο συμπεράσματα που προέκυψαν ήταν η αύξηση του τεχνοκρατικού χαρακτήρα των προσόντων του προσωπικού καθώς, και η αναγκαιότητα συνεργασίας με ανθρώπους που υπερβαίνουν τα ως τώρα αυστηρά κλειστά όρια αυτών των υπηρεσιών. Ενδεικτικά ζητήματα είναι η εθνικότητα και ηλικία τους. Τέλος, θεωρείται ότι θα πρέπει να υπάρχουν και αυτοί που συνθέτουν τα δεδομένα δίνοντας έμφαση στον ρόλο της πρόβλεψης και πρόληψης της απειλής (Carr, 2010, 86).

Ολοκληρώνοντας, καταλήγει πως οφείλουμε να κατανοήσουμε ότι το πεδίο της απειλής διευρύνεται. Τα θέματα ασφάλειας αποκτούν μεγαλύτερης έντασης κοινωνικό χαρακτήρα. Έτσι, η συμμετοχή στην κοινωνική δικτύωση παίζει το δικό της σημαντικό ρόλο, εφόσον σε όλο τον κόσμο μεγεθύνεται (αναφερόμενοι, όχι μόνο στη λεγόμενη Δύση, αλλά και στην Κίνα, Ρωσία και Μέση Ανατολή) (Carr, 2010, 89). Βεβαίως, επαναλαμβάνει και αυτός, ότι από τους βασικότερους λόγους είναι η ευκολία πρόσβασης, το μικρό κόστος και ιδιαιτέρως η διατήρηση της ανωνυμίας

¹⁴⁵ Ειδικότερα, η επιχειρηματολογία ανήκει στον επίσης ειδικό, ο οποίος προλογίζει τη συγγραφή (Lieutenant Commander Matthew J. Sklerov), J. Carr, (2010, 46).

(Carr, 2010, 93). Μια μέθοδο εξεύρεσης των απαραίτητων πληροφοριών για εγκληματικές ενέργειες αποτελεί η έρευνα της πορείας που ακολούθησαν οι μεταβιβάσεις κάποιων μεγάλων χρηματικών ποσών (Carr, 2010, 104).

8.6 R. Clarke «Κυβερνοπόλεμος, επόμενη απειλή στην εθνική ασφάλεια» (’10)

Ο Richard Alan Clarke¹⁴⁶ ορίζει εξ αρχής τον κυβερνοπόλεμο ως «τις δραστηριότητες ενός έθνους-κράτους, οι οποίες έχουν σκοπό να διεισδύσει στους Η/Υ ή τα δίκτυα τους με στόχο την διάρρηξη ή καταστροφή τους.»¹⁴⁷. Είναι λοιπόν σαφές το κριτήριο της απαραίτητης εθνικοκρατικής παρουσίας στις εν λόγω συρράξεις, ώστε να τις αποκαλέσουμε κυβερνοπολεμικές.

Στο συγκεκριμένο βιβλίο ο συγγραφέας πραγματεύεται θέματα όπως οι ιδιότητες τις οποίες διαθέτει το προσωπικό αυτού του αντικειμένου (Clarke, 2010, 33), καθώς επίσης το ρόλο που διαδραματίζουν οι έννοιες της στρατηγικής (Clarke, 2010, 151) και της επίθεσης (Clarke, 2010, 179) στον κυβερνοχώρο. Το σημαντικότερο, όμως, για την εργασία μας είναι η αρχική αντιπαράθεση τεσσάρων περιπτώσεων, στην εισαγωγή, οι οποίες υποδηλώνουν και τις ισάριθμες μορφές που μπορεί να λάβει κατά την υλοποίησή του ένα κυβερνοπολεμικό επεισόδιο (Clarke, 2010, 1-30).

Στις προαναφερόμενες, λοιπόν, σελίδες περιγράφει τρία περιστατικά, μέσα από τα οποία δείχνει τρεις ξεχωριστούς τύπους κυβερνοπολέμου. Το πρώτο αναφέρεται στη Συρία, στις 6/9/2007. Τότε, το Ισραήλ κατηγορήθηκε ότι παραβίασε το συριακό τον εναέριο χώρο και βομβάρδισε συγκεκριμένες εγκαταστάσεις. Για ορισμένους αυτές περιείχαν πυρηνικό υλικό, ενώ άλλοι επιχειρηματολογούσαν για το αντίθετο. Αυτό που μας ενδιαφέρει όμως, δεν είναι ποιος έχει δίκιο, αλλά πως έγινε αυτή η παραβίαση, δίχως να γίνει αντιληπτή από τα ραντάρ της συριακής αεράμυνας. Σύμφωνα με το συγγραφέα, όπως φάνηκε οι ισραηλινοί κατάφεραν να διεισδύσουν στα μόνιτορ των συριακών ενόπλων δυνάμεων και για μικρό χρονικό διάστημα να «παγώσουν» την οθόνη. Αυτό, βεβαίως, έγινε με τέτοιο τρόπο, ώστε να παραπλανήσει τους χειριστές, οι οποίοι νόμιζαν ότι απλά δεν κινείται τίποτα. Αυτό,

¹⁴⁶ Ο συγγραφέας υπηρέτησε στην κυβέρνηση των ΗΠΑ επί τρεις δεκαετίες (1973–2003). Η κύρια ενασχόλησή του ήταν τα θέματα ασφάλειας, με τελευταία αρμοδιότητα, αυτήν του ειδικού συμβούλου σε θέματα κυβερνοασφάλειας του προέδρου George W. Bush.

¹⁴⁷ R. Clarke, *Cyber War – The Next Threat to National Security and What to do about it*, New York: HarperCollins Publishers (2010), σ. 6.

όμως, το μικρό χρονικό διάστημα ήταν αρκετό για να εισέλθει το ισραηλινό αεροσκάφος και να επιτελέσει την αποστολή του.

Η δεύτερη περίπτωση αναφέρεται στον πόλεμο του Ιράκ. Εκεί, ο αμερικανικός στρατός και συγκεκριμένα η Διοίκηση Ειδικών Ψυχολογικών Επιχειρήσεων, χρησιμοποίησε τον κυβερνοχώρο. Επρόκειτο για μια από τις πρώτες -αν όχι την πρώτη- απόπειρα οργανωμένης στρατιωτικής επιχείρησης, σε καιρό πολέμου, η οποία έθετε στόχο την ψυχολογική επιρροή του προσωπικού του αντιπάλου. Έτσι, οι ειδικοί των ΗΠΑ, απέστειλαν ηλεκτρονικά μηνύματα (emails) στους αμυνόμενους της Βαγδάτης, για να τους πείσουν να εγκαταλείψουν οποιαδήποτε προσπάθεια αντίστασης. Παρόλα αυτά, η επιχειρηματολογία τους δεν βασίστηκε -όπως θα ήταν αναμενόμενο- στο γεγονός ότι δεν έχουν ελπίδες νίκης. Το επίκεντρό της ήταν να πείσουν ότι στόχο της εισβολής αποτελεί αποκλειστικά ο αρχηγός τους και οι δύο του υιοί. Κλείνοντας το μήνυμα, δεσμεύονταν πως όποιος δεν εμπλακεί, μετά από αυτά τα γεγονότα θα είναι και πάλι ελεύθερος.

Το τρίτο και το τέταρτο περιστατικό αφορά δύο γεγονότα τα οποία έχουμε ήδη αναλύσει. Από τη μια πλευρά, τα γεγονότα της Εσθονίας (2007)¹⁴⁸, όπου για περίπου ένα μήνα το πιο «διαδικτυωμένο» κράτος της Ευρώπης, εκείνης της εποχής, τέθηκε εκτός διαδικτύου. Από την άλλη πλευρά, τα γεγονότα της Γεωργίας (2007)¹⁴⁹, κατά τα οποία, πριν και κατά τη διάρκεια των στρατιωτικών συγκρούσεων με τη Ρωσική Ομοσπονδία, τα γεωργιανά στρατιωτικά τηλεπικοινωνιακά συστήματα τέθηκαν εκτός διοίκησης και ελέγχου.

Το συμπέρασμα, τελικά, το οποίο εξάγεται από αυτές τις τέσσερις περιπτώσεις είναι ότι από την μέχρι σήμερα εμπειρία, μπορούμε να διακρίνουμε ότι το φαινόμενο του κυβερνοπολέμου δύναται να πάρει αντίστοιχα τις ακόλουθες μορφές:

- Επέκτασης του ηλεκτρονικού πολέμου, σε ξαφνικά θερμά επεισόδια.
- Άσκησης προπαγάνδας και γενικότερα, ψυχολογικών επιχειρήσεων.
- Αυτοτελή πολεμική πράξη -είτε αντιποίνων, είτε πολιτικού εκβιασμού-, δίχως να συνοδεύεται από άλλου είδους ενέργειες.
- Υποστήριξης στρατιωτικής εκστρατείας, σε κανονική περίοδο σύρραξης.

¹⁴⁸ Βλέπε υποκεφάλαιο 4.2.3 – Α' περίπτωση (σελίδα 55) της παρούσας εργασίας.

¹⁴⁹ Βλέπε υποκεφάλαιο 4.2.3 – Β' περίπτωση (σελίδα 59) της παρούσας εργασίας.

9. ΟΡΓΑΝΩΣΗ ΚΑΙ ΕΞΟΠΛΙΣΜΟΣ ΚΥΒΕΡΝΟΠΟΛΕΜΟΥ

Το περιεχόμενο αυτού του κεφαλαίου, εκ μιας όψεως, θα μπορούσε να τιτλοφορηθεί «αντί – παραρτήματος». Ωστόσο, έστω και αν αυτό ισχύει εν μέρει, δεν θα ήταν πλήρες. Ο λόγος είναι κυρίως η διεξοδικότερη παράθεση, την οποία διενεργούμε για την ελληνική περίπτωση οργάνωσης της κυβερνοασφάλειας στη χώρα.

Το χωρίζουμε σε δύο υποκεφάλαια, ένα για την οργάνωση και ένα για τον οπλισμό αυτού του είδους πολέμου. Στο πρώτο επιλέξαμε να μελετήσουμε τις πιο «πρωτοποριακές» περιπτώσεις (NATO & ΗΠΑ), ώστε να υπάρχει μια δυνατότητα κρίσης και σύγκρισης με την Ελλάδα. Το δεύτερο, το χωρίσαμε στο υλικό και άυλο μέρος του οπλισμού.

9.1 Η Οργανωτική Δομή των Εθνικών και Υπερεθνικών Υπηρεσιών

9.1.1 *NATO*

Ο Οργανισμός Βορειοατλαντικού Συμφώνου (North Atlantic Treaty Organization – NATO) αποτελεί την επίσημη στρατιωτική συμμαχία των χωρών της Δύσης. Η κινητοποίηση σχετικά με το ζήτημα της κυβερνοασφάλειας ουσιαστικά άρχισε μετά τα γεγονότα στην Εσθονία, το Μάιο του 2007 (Hughes, 2009).

Τυπικά, το θέμα θίχτηκε το 2008, στη σύνοδο στο Βουκουρέστι. Εκεί, αξιολογήθηκε ως ζήτημα ανερχόμενης απειλής, κατόπιν εισηγητικής έκθεσης του ρουμάνου προέδρου, Traian Băsescu, στην οποία επισυνάπτονταν και ορισμένες επιστημονικές εργασίες. Η πρώτη αντιμετώπιση, στην οποία συμφώνησαν τα μέλη ήταν η θεσμοθέτηση δύο οργάνων. Το πρώτο αφορά την κεντρική υπηρεσία χειρισμού των σχετικών περιστατικών (NATO Cyber Defence Management Authority - CDMA), με έδρα τις Βρυξέλες του Βελγίου. Το δεύτερο βήμα συνίσταται στην ίδρυση ενός ερευνητικού κέντρου αριστείας σε θέματα κυβερνοάμυνας (Cooperative Cyber Defense Centre of Excellence – CCD CoE), με έδρα το Ταλίν της Εσθονίας. Σημειώνουμε ότι, ενώ στο πρώτο συμμετέχουν όλα τα μέλη, το δεύτερο χρηματοδοτείται και διευθύνεται από έξι μέλη.

Σε ένα τρίτο, πιο στρατηγικό επίπεδο το NATO έχει θεσμοθετήσει τη διοργάνωση ετησίων κυβερνοασκήσεων, με στόχο την ενοποίηση των απαραίτητων διαδικασιών όλων των μελών του. Τέλος, συγκροτεί την ομάδα ταχείας αντίδρασης

(Computer Emergency Response Teams - CERT)¹⁵⁰, η οποία θα είναι υπεύθυνη για την άμεση αντιμετώπιση αιφνιδιαστικών περιστατικών τεχνολογικού χαρακτήρα. Ωστόσο, το ορόσημο αυτού του σταδίου πραγματοποιήθηκε με την ανακοίνωση της ομόφωνης αποδοχής του Νέου Στρατηγικού Δόγματος (“Strategic Concept For the Defense and Security of The Members of the North Atlantic Treaty Organization”)¹⁵¹, στη Λισαβόνα το 2010. Για πρώτη φορά στην ιεράρχηση των απειλών, το ζήτημα της κυβερνοάμυνας αποκτάει την πέμπτη θέση:

- [1] βαλλιστικοί πύραυλοι (proliferation of ballistic missiles),
- [2] πυρηνικά όπλα (proliferation of nuclear weapons),
- [3] τρομοκρατία και ράδιο-βιολογικό-χημικός πόλεμος (Terrorism - nuclear, chemical, biological or radiological capabilities),
- [4] οργανωμένο έγκλημα (narcotics and people) και
- [5] κυβερνοεπιθέσεις (cyber attacks).

9.1.2 ΗΠΑ

Οι ΗΠΑ πρέπει να είναι η πρώτη χώρα, η οποία συνειδητοποίησε την αξία του πληροφοριακού πολέμου και των συναφών με αυτόν στρατιωτικών επιχειρήσεων. Μετά όμως τα γεγονότα στην Εσθονία, αξιολόγησε σε υψηλή προτεραιότητα και το πληροφορικό μέρος του πληροφοριακού πολέμου. Έτσι, όπως θα δείξουμε παρακάτω, θεωρείται πρωτοπόρος¹⁵² στη διαμόρφωση θεσμικού πλαισίου, στη διοργάνωση ασκήσεων «μεγάλου βεληνεκούς» και στη συγκρότηση υπηρεσιών με αποστολές σχετικές με τον κυβερνοχώρο.

Ως προς το τελευταίο θέμα, τον Οκτώβριο του 2007, το αμερικανικό πεντάγωνο ανακοίνωσε τη λειτουργία της «Κυβερνο-Διοίκησης» (CyberCommand), αρχικά στο οργανόγραμμα της αεροπορίας (Βήμα της Κυριακής, 4/11/2007). Πρώτος της Διοικητής ανέλαβε ο πτέραρχος Γουίλιαμ Λορντ και η έδρα της ορίστηκε στην αεροπορική βάση Μπάρκοντεϊλ, στην πολιτεία της Λουιζιάνας. Ενάμιση περίπου χρόνο μετά, στις 23/6/2009, ο υπουργός εθνικής άμυνας εντελή τον Διοικητή της

¹⁵⁰ Πλέον, στις μέρες μας, σχεδόν όλες οι ανεπτυγμένες χώρες διαθέτουν παρόμοια ομάδα. Η κεντρική της ιδέα (The CERT concept) ξεκίνησε το 1988 στο Carnegie Mellon University των ΗΠΑ.

¹⁵¹ Ενδιαφέρον παρουσιάζει ο τίτλος της εισηγητικής έκθεσης: Ενεργός Συμμετοχή & Σύγχρονη Άμυνα (Active Engagement, Modern Defence).

¹⁵² Σε αυτό το σημείο θα πρέπει να διατυπώσουμε μια επιφύλαξη, λόγω της έλλειψης πληροφοριών, τόσο για την ανάλογη κατάσταση στη Ρωσία, όσο κυρίως στην Κίνα, όπου το σύστημά της είναι αρκετά κλειστό.

Στρατηγικής Διοίκησης¹⁵³ να ιδρύσει τη Διοίκηση Κυβερνοάμυνας (United States Cyber Defense Command – USCYBERCOM). Έτσι, το Μάιο του 2010, ο στρατηγός Keith Alexander αναλαμβάνει καθήκοντα. Έχει ιδιαίτερο ενδιαφέρον ότι ο ίδιος είναι και διευθυντής της Υπηρεσίας Εθνικής Ασφαλείας (NSA), η οποία επεκτείνει τις δραστηριότητές της στον κυβερνοχώρο και πέρα του στενά στρατιωτικού πλαισίου. Επιπρόσθετα, η NSA -όπως ανακοινώθηκε φέτος- εγκαθιστά το νέο κέντρο της τράπεζας δεδομένων της (με προϋπολογισμό 1,5 δισεκατομμύρια δολάρια) στην πολιτεία της Γιούτα (<http://www.ksl.com>, 18/11/2011).

Ένα άλλο σημείο που αυτό το κράτος έχει να επιδείξει αρκετή εμπειρία είναι η διοργάνωση κυβερνοασκήσεων, όπως έχει επικρατήσει να λέγονται. Πιο συγκεκριμένα, στη διοργάνωση με την ονομασία «Κυβερνο-Καταιγίδα (Cyber Storm)», έχει αναλάβει το υπουργείο Εσωτερικής Ασφάλειας και, μεταξύ άλλων, συμμετέχουν:

- το υπουργείο της Εθνικής Άμυνας,
- το υπουργείο των Εξωτερικών,
- το υπουργείο της Δικαιοσύνης,
- η Κεντρική Υπηρεσία Πληροφοριών (CIA),
- η Υπηρεσία Εθνικής Ασφάλειας (NSA) και
- η Ομοσπονδιακή Υπηρεσία Αστυνόμευσης (FBI).

Συνήθως το σενάριο αφορά ένα σύνολο μη εξουσιοδοτημένων διεισδύσεων στα πληροφορικά δίκτυα και πλασματικών καταστροφών των κρίσιμων εθνικών υποδομών. Οι ρόλοι διακρίνονται σε δύο ομάδες, τους επιτιθέμενους και τους αμυνόμενους. Η άσκηση ξεκίνησε τον Μάρτιο του 2006 και μέχρι σήμερα, υλοποιούνται κάθε δύο χρόνια (Cyber Storm II, 2008 & Cyber Storm III, 2010) και έχουν πραγματοποιηθεί τρεις. (<http://strategy-geopolitics.blogspot.com>, 5/2/2008).

Στην τελευταία, τονίζεται ότι ένας από τους βασικούς στόχους ήταν η βελτίωση της συνεργασίας των υπηρεσιών. Σε αυτήν την κατεύθυνση δημιουργήθηκε το Εθνικό Κέντρο Κυβερνοασφάλειας και Ενοποίησης Επικοινωνιών (National Cybersecurity and Communications Integration Center - NCIC), με σκοπό να συμβάλλει στη

¹⁵³ Η εν λόγω υπηρεσία (United States Strategic Command - USSTRATCOM) ιδρύθηκε, μετά τον πόλεμο του Κόλπου, το 1992. Κατόπιν, συμπεριλήφθηκε σε μια από τις ενοποιημένες διοικήσεις που προέκυψαν μετά το 2002. Συγκεκριμένα, με την Διοίκηση Διαστήματος United States Space Command (USSPACECOM) και συμπεριέλαβε, εκτός των άλλων και τις πληροφοριακές επιχειρήσεις. Έχει προσωπικό, πλέον των 2700 ατόμων και έδρα στην αεροπορική βάση της Νεμπράσκα.

διαλειτουργικότητα των διαδικασιών όλων των εμπλεκόμενων υπηρεσιών (<http://www.dhs.gov>, 18/11/2011). Χαρακτηριστική, τέλος, είναι η δήλωση ότι στόχος είναι το μοίρασμα των πληροφοριών, από τον διευθυντή Brett M. Lambo (<http://www.washingtontimes.com>, 28/9/2010).

Όσον αφορά το θεσμικό πλαίσιο, η συζήτηση για αυτό το θέμα, βρίσκεται στην αιχμή από το καλοκαίρι του 2011. Όταν ο υπουργός εθνικής άμυνας Leon E. Panetta, δήλωσε ότι σύντομα θα ανακοινωθεί το νέο Δόγμα Κυβερνοασφάλειας (<http://www.spacedaily.com>, 20/7/2011). Αργότερα, ο υφυπουργός Εθνικής Ασφάλειας, William Lynn, ενημέρωσε ότι θα ονομάζεται Cyber 3.0 και θα αφορά την πρώτη ενοποιημένη στρατηγική στον κυβερνοχώρο. Επίσης, εξήγησε ειδικότερα ότι το πλάνο που σχεδιάζεται θα έχει πέντε βασικά σημεία (<http://media.omeadiaweb.com>, 1/6/2011):

- Τη σφαίρα των στρατιωτικών επιχειρήσεων
- Τη χρήση των δικτύων στην ενεργητική άμυνα
- Στην πολιτική διάσταση, την προστασία των κρίσιμων υποδομών
- Τις συμμαχίες για την αμυντική συνεργασία
- Την καλύτερη αξιοποίηση των ανθρωπίνων πόρων.

Εν κατακλείδι, δεικτική για την υψηλή θέση, στην οποία τοποθετεί η κυβέρνηση των ΗΠΑ το ζήτημα της κυβερνοασφάλειας, είναι η ακόλουθη αποστροφή του προέδρου Barack Obama (2009). Δήλωσε, λοιπόν, ότι «όλοι οφείλουν να λαμβάνουν υπόψη τους πως οι αμερικανικές ψηφιακές υποδομές αποτελούν στρατηγικό εθνικό περιουσιακό στοιχείο και άρα, η απειλή του θα έχει την ανάλογη αντιμετώπιση».

9.1.3 ΕΛΛΑΔΑ

Η εγκαθίδρυση μιας ενοποιημένης αρχής, η οποία να είναι δυνατό να μεριμνήσει, κεντρικά, για τη συνολική ασφάλεια της χώρας στον κυβερνοχώρο, παραμένει ακόμα ζητούμενο. Έτσι, η πολιτεία έχει θεσμοθετήσει την κάλυψη επιμέρους αναγκών μέσω «αυτόνομων» οργανισμών, οι οποίοι μόλις τα τελευταία χρόνια συγκλίνουν στην αναγκαιότητα της συνεργασίας. Παρακάτω θα παρουσιάσουμε την αποστολή τους¹⁵⁴.

¹⁵⁴ Οι κύριες πηγές μας, εξεύρεσης στοιχείων για την παρακάτω έκθεση, βασίστηκε στους ιστοτόπους των αντίστοιχων υπηρεσιών και στη δουλειά της Ομάδας Εργασίας «ΣΤ-3», με θέμα *Εμπιστοσύνη και Ασφάλεια σε ένα κινητό και γρήγορο δικτυακό περιβάλλον* (2004).

➤ Υπουργείο Εθνικής Άμυνας / Γενικό Επιτελείο / Αρχή Εθνικής Ασφάλειας

Το Υπουργείο Εθνικής Άμυνας έχει την πρώτη και την τελευταία, χρονικά θεσπισμένη υποχρέωση της προστασίας, μέσω συγκεκριμένου ρόλου, της κυβερνοασφάλειας της χώρας. Καταρχήν, με το ν. 1892/1990 είναι υπεύθυνη για τη γενικότερη ασφάλεια της χώρας. Σε αυτό το πλαίσιο και με το Π.Δ. 17/74 έχει την ευθύνη της έκδοσης του Εθνικού Κανονισμού Εθνικής Ασφάλειας (ΕΚΑ), η οποία αφορά στις ρήτρες πρόσβασης και χρήσης των ευαίσθητων πληροφοριών.

Εκτός όμως των παραπάνω, έχει και την αποκλειστική ευθύνη της κυβερνοάμυνας. Ωστόσο, εδώ το θεσμικό πλαίσιο δεν είναι καθαρό. Για να αποτυπώσουμε αυτή την ασαφή κατάσταση θα παρουσιάσουμε το μικρό ιστορικό της «ανάδυσης» αυτής της υπηρεσίας. Η αρχή γίνεται με ένα τμήμα, το οποίο ανήκει στο Γενικό Επιτελείο Ναυτικού (ΓΕΝ), τον Ιούλιο του 2000. Στη συνέχεια, το Μάιο του 2003, τοποθετείται σε επίπεδο Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ) και συγκεκριμένα στη Διεύθυνση Πληροφορικής. Το 2004, πλέον, αναβαθμίζεται σε Διεύθυνση και μάλιστα, αναφερόμενη κατευθείαν στον αρχηγό του ΓΕΕΘΑ. Τα κύρια σημεία της αποστολής της είναι τα εξής:

- Η προστασία της πληροφοριακής υποδομής των ελληνικών ενόπλων δυνάμεων.
- Η γενικότερη συνδρομή στην ασφάλεια των εθνικών κρίσιμων υποδομών.
- Η πραγματοποίηση των συναφών υποχρεώσεων της χώρας από τη συμμετοχή της στους διεθνείς οργανισμούς.
- Η διοργάνωση και συμμετοχή στις εγχώριες κυβερνοασκήσεις.

➤ Υπουργείο Προστασίας του Πολίτη - Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ)

Ένα από τα σημεία ασάφειας του νομικού καθεστώτος βρίσκεται εδώ. Σύμφωνα με το ν.3649/2008, άρθρο 6, παράγραφος 1:

«Οι δημόσιες υπηρεσίες και τα νομικά πρόσωπα δημοσίου δικαίου, οι δημόσιες επιχειρήσεις, τα ελεγχόμενα ή εποπτευόμενα από το Δημόσιο νομικά Νομικό Πλαίσιο πρόσωπα ιδιωτικού δικαίου, τα νομικά πρόσωπα του ευρύτερου δημόσιου τομέα, καθώς και οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτερου βαθμού και οι επιχειρήσεις τους υποχρεούνται να παρέχουν σε ειδικά εξουσιοδοτημένους υπαλλήλους της ΕΥΠ κάθε πληροφορία, στοιχείο ή συνδρομή για την εκπλήρωση της αποστολής της.»

Η γενικότερη αποστολή της ΕΥΠ συνοψίζεται στην αναζήτηση, συλλογή, επεξεργασία και γνωστοποίηση στις αρμόδιες αρχές των πληροφοριών που αφορούν (<http://www.nis.gr/portal/page/portal/NIS/Mission>, 19/11/2011):

- [i] Στην προστασία και προώθηση των πολιτικών, οικονομικών, στρατιωτικών και εν γένει εθνικών στρατηγικών συμφερόντων της Χώρας.
- [ii] Στην πρόληψη και αντιμετώπιση δραστηριοτήτων που συνιστούν απειλή κατά του δημοκρατικού πολιτεύματος, των θεμελιωδών δικαιωμάτων του ανθρώπου, της εδαφικής ακεραιότητας και της εθνικής ασφάλειας του Ελληνικού Κράτους, καθώς και του εθνικού πλούτου της Χώρας.
- [iii] Στην πρόληψη και αντιμετώπιση δραστηριοτήτων τρομοκρατικών οργανώσεων, καθώς και άλλων ομάδων οργανωμένου εγκλήματος.

Εδώ θα πρέπει να διευκρινίσουμε πως η ΕΥΠ σε περίοδο πολέμου, επιστράτευσης ή άμεσης απειλής της εθνικής ασφάλειας υπάγεται στον Αρχηγό του Γ.Ε.ΕΘ.Α., ο οποίος, δια του Διοικητή της Ε.Υ.Π., ασκεί τον πλήρη έλεγχο. Κατά την ειρηνική όμως περίοδο και ως προς τα θέματα της κυβερνοασφάλειας, έχει μια ειδικότερη αποστολή, η οποία από τον ίδιο ν.3649/2008, άρθρο 4, παράγραφος 8 και σε συμφωνία με τις διατάξεις της παραγράφου 3 του άρθρου 2 του π.δ. 325/2003:

Ορίζεται ως η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, η οποία μεριμνά για την πρόληψη και τη στατική και ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής.

Για την εφαρμογή του προαναφερόμενου άρθρου ισχύει η αρμοδιότητα της ε' διεύθυνσης (Π.Δ. 360/92), η οποία είναι υπεύθυνη για την ασφάλεια των εθνικών επικοινωνιών (όπως, επί παραδείγματι, των κρυπτογραφικών συστημάτων). Σε αυτήν, λοιπόν, υπόκειται και η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (National CERT), της οποίας, σύμφωνα με διάλεξη σε ημερίδα της ίδιας της υπηρεσίας, με τίτλο «Ασφάλεια Πληροφοριακών Συστημάτων στο Δημόσιο τομέα» (www.cert.gov.gr, 3/2/2011), το αντικείμενο είναι το εξής:

✓ Είναι η αρμόδια εθνική αρχή αντιμετώπισης των ηλεκτρονικών απειλών, κυρίως προς τον Δημόσιο Φορέα και τις Κρίσιμες Υποδομές της χώρας. Έτσι, συλλέγει σχετικά στοιχεία – αναλύει, καταγράφει και κατηγοριοποιεί το είδος των επιθέσεων. Επίσης, παρέχει πληροφορίες και συμβουλές για την προστασία των πληροφορικών συστημάτων, κατόπιν αιτήματος των ενδιαφερομένων. Τέλος, συνεργάζεται με άλλα, εθνικά και μη, CERT καθώς και συναφείς υπηρεσίες.

➤ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Η ΑΠΔΠΧ είναι ανεξάρτητος διοικητικός φορέας και έχει την ευθύνη της εποπτείας των νόμων 2472/1997 και 2774/1999 για την προστασία των προσωπικών δεδομένων. Επομένως οι αρμοδιότητές της είναι οι εξής (<http://www.dpa.gr>):

- Τήρηση αρχείων των ευαίσθητων προσωπικών δεδομένων.
- Οδηγίες για την επεξεργασία προσωπικών δεδομένων.
- Διεκπεραίωση καταγγελιών για τις παραβιάσεις.
- Αυτεπάγγελτοι διοικητικοί έλεγχοι.
- Έκδοση κανονιστικών πράξεων.
- Σχετικές γνωμοδοτήσεις.

➤ Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ)

Η ΑΔΑΕ συστάθηκε σύμφωνα με το άρθρο 1 του νόμου 3115/2003. Σκοπό της αποτελεί, όπως καθορίζεται και από το άρθρου 19 του Συντάγματος, η προστασία του απορρήτου των επιστολών, της ελεύθερης επικοινωνίας με κάθε δυνατό τρόπο και η ασφάλεια των πληροφοριακών δικτύων. Επίσης, διαθέτει διοικητική αυτοτέλεια, εφόσον αποτελεί Ανεξάρτητη Αρχή.

Ωστόσο, οι αποφάσεις της θα πρέπει να κοινοποιούνται, με δική της ευθύνη στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους οφείλει να υποβάλλει έκθεση με τις τα πεπραγμένα της στον Πρόεδρο της Βουλής και στους αρχηγούς των κομμάτων, τα οποία εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο (<http://www.adae.gr/portal/>).

➤ Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Η ΕΕΤΤ συνιστά ανεξάρτητη αρχή από την ίδρυσή της το 1992. Αποτελεί τον Εθνικό Ρυθμιστή της τηλεπικοινωνιακής εγχώριας αγοράς, ο οποίος ελέγχει:

- (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και
- (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφορά (<http://www.eett.gr>).

Μια από τις πιο ενδιαφέρουσες δραστηριότητες που έχει αναλάβει αυτή η αρχή, είναι ο έλεγχος της παροχής και πιστοποίησης των υπηρεσιών ηλεκτρονικής υπογραφής (Π.Δ. 150/2001 – προσαρμογή Οδηγίας 99/93ΕΚ).

➤ Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος

Η εν λόγω υπηρεσία είναι ειδική αυτοτελής Κεντρική Υπηρεσία της Ελληνικής Αστυνομίας (ΕΛ.ΑΣ.). Αποτελείται από δύο υποδιευθύνσεις (τις Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος). Αναφέρεται κατευθείαν στον Αρχηγό της ΕΛ.ΑΣ. και εποπτεύεται στην προανακριτική της δράση από τον Εισαγγελέα του Οργανωμένου Εγκλήματος. Η Υποδιεύθυνση Οικονομικής Αστυνομίας συγχωνεύθηκε στην προϋπάρχουσα δεύτερη υποδιεύθυνση τον Ιούλιο του 2011. Η ίδια ασχολείται με την κυβερνοασφάλεια στο βαθμό, κατά τον οποίο ελέγχει συμβάντα υπεξαίρέσεων και φοροφυγάδων μέσω διαδικτύου.

Ωστόσο, η άλλη υποδιεύθυνση είναι παλαιότερη και ενδεχομένως να συνιστά την πιο δημοφιλή και πετυχημένη υπηρεσία κυβερνοασφάλειας στη χώρα¹⁵⁵. Ειδικότερα, η αποστολή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας (<http://www.astynomia.gr>, 19/11/2011).

Τα τμήματα τα οποία συγκροτούν την οργάνωση της υπηρεσίας είναι τα ακόλουθα τέσσερα:

- Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων.
- Τμήμα Προστασίας Ανηλίκων.
- Τμήμα Προστασίας Λογισμικού και Πνευματικών
- Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών.

Τέλος, ενδιαφέρον παρουσιάζει πως η στελέχωση της υπηρεσίας δεν απαρτίζεται μόνο από αστυνομικούς, αλλά και ειδικούς επιστήμονες, κυρίως από τους τομείς της πληροφορικής και της ψυχολογίας.

Στην τελευταία ενότητα αυτού του υποκεφαλαίου θα ασχοληθούμε με την πρώτη πανελλαδική προσπάθεια συγκέντρωσης και συντονισμού όλων των φορέων (εκτός των δημοσίων που προαναφέραμε και των ιδιωτικών), οι οποίοι εμπλέκονται στην κυβερνοασφάλεια της χώρας. Πρόκειται για την πρώτη εθνική άσκηση κυβερνοάμυνας, με την ονομασία «Πανόπτης» [Παρεμπιπτόντως, σημειώνεται ότι ο συγγραφέας αυτού του έργου είχε την ευκαιρία της «συμμετοχικής παρατήρησης»...].

¹⁵⁵ Ο αστυνόμος Α΄ Μάνος Σφακιανάκης, είναι ο πρώτος και ο μοναδικός μέχρι στιγμής προϊστάμενος της Δίωξης Ηλεκτρονικού Εγκλήματος. Από το 1995 ασχολείται με το ηλεκτρονικό έγκλημα και έχει χειριστεί περισσότερες από 500 υποθέσεις, από συκοφαντικές δυσφημήσεις και ληστείες τραπεζών μέσω Ιντερνέτ έως παιδική πορνογραφία κι υποθέσεις εθνικής ασφάλειας. (<http://www.apodimos.com>)

Η 1η Εθνική Άσκηση Κυβερνοάμυνας διενεργήθηκε στις 18 – 20 Μαΐου 2010 και οργανώθηκε με την πρωτοβουλία της Διεύθυνσης Κυβερνοάμυνας (ΔΙΚΥΒ/ΓΕΕΘΑ), του Υπουργείου Εθνικής Άμυνας. Σκοπός της άσκησης ήταν η δοκιμή της επάρκειας της υφιστάμενης εθνικής δομής στα θέματα της ασφάλειας του κυβερνοχώρου. Μπορούμε να πούμε ότι η άσκηση πέτυχε τον σκοπό της -στο μεγαλύτερο μέρος-, εξαιτίας του ότι συμμετείχαν εκπρόσωποι φορέων όπως:

- του Γραφείου του Πρωθυπουργού (Ομάδα Opengon),
- των υπουργείων Οικονομικών, Εσωτερικών και Εξωτερικών,
- της Γενικής Γραμματείας Επικοινωνιών (Υπ. Υποδομών-Μεταφορών-Δικτύων),
- του Τεχνικού Επιμελητηρίου Ελλάδας,
- πολλών τριτοβάθμιων εκπαιδευτικών ιδρυμάτων (14 Α.Ε.Ι., όπως: Καποδιστριακό, Οικονομικό Αθηνών, Πειραιώς, Θεσσαλονίκης, Πάτρας, Ιωαννίνων και Κρήτης. 4 Τ.Ε.Ι.: Αθήνας, Πειραιά κ.λπ.).
- ερευνητικών ιδρυμάτων (Δημόκριτος, EAITY, ΙΤΕ, Εθνικό Δίκτυο Έρευνας και Τεχνολογίας),
- από Ανεξάρτητες Αρχές (Αρχή Προστασίας Προσωπικών Δεδομένων, Αρχή Διασφάλισης Απορρήτου Επικοινωνιών κ.λπ.) και τέλος,
- από άλλα, εκτός των ενόπλων δυνάμεων, σώματα ασφαλείας, όπως το Λιμενικό και η ΕΥΠ.

Η προσομοίωση των επιθέσεων βασίστηκε σε ένα εκτενές φάσμα δυνητικών σεναρίων, τα οποία αποσκοπούσαν να προσδώσουν ένα ρεαλιστικό χαρακτήρα στα επεισόδια¹⁵⁶, τα οποία κυρίως ήταν:

- Κατανεμημένης Άρνηση Εξυπηρέτησης (D Dos)
- Νομικοί χειρισμοί (Legal Treatment)
- Επεισόδια χειρισμού (Incident Handling)
- Μη εξουσιοδοτημένη πρόσβαση στον Ιστό (Web Hacking)

Η παραπάνω άσκηση κυβερνοάμυνας έγινε στα πρότυπα παρόμοιας κυβερνο-άσκησης του NATO, της Cyber Coalition (NCDEX '09). Τέλος, σημαντικό είναι ότι ήδη διεξήχθη και ο ΠΑΝΟΠΤΗΣ II (31/10 – 02/11 /2011).

¹⁵⁶ Οι τεχνικοί όροι εξηγούνται στο αμέσως επόμενο κεφάλαιο. Σημειώνουμε πως ορισμένες μεταφράσεις είναι μάλλον αδόκιμες, αλλά γίνονται για επεξηγηματικούς λόγους.

9.2 Εξοπλισμός

Καθώς συμβαίνει με κάθε είδος πολέμου, έτσι και εδώ, έχουμε έναν διακριτό οπλισμό, ο οποίος εξάλλου τον χαρακτηρίζει. Όπως για παράδειγμα, στον «κλασικό» ή συμβατικό πόλεμο έχουμε τα τυφέκια, τα τεθωρακισμένα, τις φρεγάτες και τα αεροσκάφη. Από τις ανάγκες λοιπόν ονοματοδότησης των όπλων του κυβερνοπολέμου, έχει προκύψει επιγραμματικά και η παρακάτω ορολογία.

9.2.1 *Κακόβουλο Λογισμικό (Malicious Software)*

1. Ιοί (viruses). Προγραμματισμένος κώδικας αυτό-αντιγραφής. Ο ιός μολύνει μόνον όταν εκτελείται το πρόγραμμα - ξενιστής.
2. Σκουλήκια (Worms). Πρόγραμμα κατανάλωσης πόρων. Αφορά ένα ανεξάρτητο πρόγραμμα, το οποίο αυτό-αναπαράγεται και μεταφέρεται μεταξύ των χρηστών. Η διαφορά με τους ιούς, είναι ότι δεν προκαλεί βλάβη σε άλλα προγράμματα.
3. Δούρειοι Ίπποι (Trojan Horse). Το «τρωικό άλογο» συνίσταται από ένα τμήμα κώδικα, το οποίο καλύπτει την παρουσία του σε άλλο πρόγραμμα και εκτελεί διαφορετικές λειτουργίες. Δεν αφήνει ίχνη και είναι δύσκολο να εντοπιστεί.
4. Λογικές Βόμβες (Logical Bombs). Πρόκειται για μηνύματα υπερφόρτωσης δομών. Θεωρείται και ως εξειδίκευση της προηγούμενης κατηγορίας, που χρησιμοποιείται για την απελευθέρωση «ιών ή σκουληκιών».
5. Κατασκοπευτικό (Spy Ware). Εγκαθίσταται στο σύστημα για να παρακολουθεί τις κινήσεις του. Ενδεικτικά, διάφορα τέτοια προγράμματα μπορούν να καταγράφουν συστηματικά τις πληκτρολογήσεις (keylogger) ή τις διαδικτυακές κινήσεις (sniffer).

9.2.2 «Υποπτα» Εξαρτήματα (“Security Risk” Hardware)

6. Τσιπάκια (Chipping). Καταστροφή ή παραποίηση κυκλωμάτων. Τα σημερινά τσιπς περιέχουν εκατομμύρια ολοκληρωμένα κυκλώματα, τα οποία εύκολα μπορούν να διαμορφωθούν από τον κατασκευαστή τους, ώστε να περιέχουν και κάποιες «μη αναμενόμενες» λειτουργίες. Θα μπορούν να καταστρέφονται μετά από κάποιο προκαθορισμένο χρόνο, να παύουν να λειτουργούν μετά την λήψη συγκεκριμένου σήματος προκαθορισμένης συχνότητας, να εκπέμπουν σήμα συγκεκριμένης συχνότητας έτσι ώστε να προδίδουν την θέση στην οποία βρίσκονται και άλλες τέτοιου είδους λειτουργίες.
7. Νανομηχανισμοί και Μικρόβια (Nano machines & Microbes). Μικροσκοπικά ρομπότ «κομάντος». Οι νάνο-μηχανές και τα μικρόβια μπορούν να προκαλέσουν

σοβαρές ζημιές σε ένα σύστημα. Σε αντίθεση με τους ιούς επιτίθενται κατευθείαν στα ηλεκτρονικά κυκλώματα που απαρτίζουν ένα πληροφοριακό σύστημα. Ειδικότερα, οι νανομηχανές είναι μικρά ρομπότ (μεγέθους μικρότερου από ένα μυρμήγκι).

9.2.3 Τύποι Κυβερνοεπίθεσης (Types of Computer Network Attacks)

8. Κατανεμημένη άρνηση εξυπηρέτησης (Distribution denial of service – Ddos).

Πρόκειται για τον πιο διαδεδομένο και με ορατά αποτελέσματα τύπο κυβερνοεπίθεσης. Υλοποιείται με μια συντονισμένη δικτυακή ενέργεια, η οποία αποστέλλει σε ένα κόμβο συνεχή και πολλαπλές αιτήσεις πρόσβασης, ώστε να τον θέσει εκτός λειτουργίας, λόγω αδυναμίας απόκρισης. Συνήθως ο «συντονιστής» αιχμαλωτίζει ξένα συστήματα (εν αγνοία των ιδιοκτητών τους), τα οποία εντελή να κάνουν την παραπάνω ενέργεια ταυτόχρονα (αυτά τα συστήματα αποκαλούνται zombies ή bots).

9. **«Κερκόπορτες» (Backdoor - Trapdoor).** Πρόκειται για μια μέθοδο παράκαμψης του συστήματος ασφαλείας, η οποία αρχικά αχρησιμοποιήτο από τους αρμόδιους, οι οποίοι διενεργούσαν ελέγχους πληροφορικής ασφάλειας για λόγους συντήρησης. Μια τέτοια περίπτωση γίνεται στη διασύνδεση των επισκευών (craft interface). Το πιο σημαντικό σημείο εδώ είναι η προστασία των ονομάτων των χρηστών (user names), καθώς και των προσωπικών τους κωδικών πρόσβασης (pass words). Ένας τρόπος απειλής τους είναι η παραπλανητική (deception) αποστολή μηνύματος του ηλεκτρονικού ταχυδρομείου (e-mail spoofing), με απώτερο σκοπό την παραποίηση ευαίσθητων δεδομένων (digital manipulation) ή την εκμετάλλευσή τους (exploitation).

ΤΜΗΜΑ ΙΙΙ
ΜΕΡΟΣ Β΄
Ο ΚΥΒΕΡΝΟΧΩΡΟΣ

10. Η ΕΝΝΟΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

10.1 Οι δύο πόλοι κριτικής

Οι ανθρώπινες προσδοκίες για την βελτίωση των συνθηκών ζωής βασίστηκαν, κυρίως μετά τη γαλλική επανάσταση, στην επικαλούμενη επιστημονική πρόοδο. Ειδικότερα τις τελευταίες δεκαετίες, οι ελπίδες για μια καλύτερη κοινωνία επικεντρώθηκαν στα τεχνολογικά επιτεύγματα. Έτσι, κατά τα τέλη του προηγούμενου αιώνα πολλοί, κοινωνικοί και μη, επιστήμονες άρχισαν να μιλούν για την ανάδυση ενός νέου κοινωνικού περιβάλλοντος, το οποίο θα στηριζόταν στις τεχνολογίες πληροφορίας και επικοινωνίας (ΤΠΕ)· αυτό επονομάστηκε *κυβερνοχώρος*.

Από τη μία πλευρά -ο θετικός κριτικός πόλος-, οι υποστηρικτές της φιλελεύθερης και πραγματιστικής παράδοσης εξύμνησαν τον κυβερνοχώρο, στηριζόμενοι στην αρχή ότι η πληροφορία μειώνει την αβεβαιότητα και ο κυβερνοχώρος αποτελεί την πύλη σε άπειρες διαθέσιμες πληροφορίες. Διατείνονταν, επίσης, πως αυτό το γεγονός θα δώσει τη δυνατότητα να καθιερωθεί η Κοινωνία της Πληροφορίας (Negroponte, 1995), η οποία προμηνύει την έλευση της νέας εποχής της Γνώσης (Toffler, 1994). Επιπρόσθετα, εξυπηρετεί την κάλυψη των οργανωτικών αναγκών της οικονομίας, ώστε να επιτευχθεί η επιδιωκόμενη μείωση του κόστους. Εφόσον, η μεγαλύτερη δαπάνη σε μια επιχείρηση, συνήθως είναι τα έξοδα (μισθοδοσία κλπ) του προσωπικού, η αυτοματοποίηση της παραγωγικής διαδικασίας θα μειώσει το κόστος παραγωγής. Αν σε αυτό το πλεονέκτημα προσθέσουμε ότι, με την ψηφιοποίηση της εταιρικής λειτουργίας, έχουμε και καλύτερο προϊόν, τότε επιτυγχάνεται το επιθυμητό αποτέλεσμα της βελτίωσης της τελικής απόδοσης (Rifkin, 2001). Σε γενικές γραμμές, αυτές οι προσεγγίσεις βασίζονται σε μια προηγηθείσα έκφραση ενός οράματος αξιοποίησης από την ανθρωπότητα της ευκαιρίας δημιουργίας ενός «οικουμενικού» περιβάλλοντος. Σε εκείνο το περιβάλλον θα ήταν εφικτή η επικοινωνία ωσάν να είμαστε όλοι κάτοικοι ενός παγκόσμιου χωριού (McLuhan, 1965). Για πολλούς, η προοπτική αυτής της θέασης, κατέληξε σε έναν κοινό τόπο, τον οποίο εν τέλει συμβόλισε ο κυβερνοχώρος. Έτσι αρχίζει να υπογραμμίζεται πως αυτή η έννοια συνιστά κάτι παραπάνω από ένα σύνολο διασυνδεδεμένων υπολογιστών, δηλαδή το διαδίκτυο. Σε αυτήν την κατεύθυνση, έχουμε και τις πρώτες προτάσεις προσδιορισμού του περιεχομένου αυτού του περιβάλλοντος, οι οποίες υποστηρίζουν ότι συνίσταται από ανάμικτα βίο-ηλεκτρονικά συστατικά στοιχεία.

Από την άλλη πλευρά όμως, -στον αρνητικό κριτικό πόλο- αυτό το περιβάλλον κατακρίθηκε ως μια νέα ουτοπία, η οποία υποτιμά σε μη ρεαλιστικό βαθμό την αναγκαιότητα των υλικών αγαθών (Κονδύλης, 1999, 356-359)¹⁵⁷. Επίσης, πως εσφαλμένα ευαγγελίζεται ένα μέλλον δικαιοσύνης και ελευθερίας, γιατί αυτό είναι αδύνατον να το εγγυηθεί, εξαιτίας της φύσης του ανθρώπινου πολιτισμού, ο οποίος ιστορικά έχει αποδειχθεί ότι δεν αλλάζει με τέτοιες «εξωτερικές» μεταβολές, όπως δεν άλλαξε και τον προηγούμενο αιώνα με την τυπογραφία (Robins&Webster, 1999). Αποδέχονται πως η ανάπτυξη των ΤΠΕ απεγκλώβισε την ανθρωπότητα σε σύντομο διάστημα από ορισμένες δεσμεύσεις του χώρου (π.χ. τη μείωση των αποστάσεων επικοινωνίας) και του χρόνου (π.χ. τη ταχύτητα ενημέρωσης). Εντούτοις, οι επικριτές αυτού του γεγονότος, αντιθέτως, θεωρούν ότι η τεχνολογία δεν προάγει την ανάπτυξη της προσωπικότητας του ατόμου. Αυτή η θέση τονίζει τις επιπτώσεις της αποξένωσης και των απρόσωπων σχέσεων που δημιουργούν οι πληροφοριακές επικοινωνίες (Heidegger, 1953). Εν κατακλείδι, θεωρούν πως, με τη λέξη «κυβερνοχώρος», έχει εσκεμμένα προσδοθεί μια εμφατικότητα χωρίς αντίκρισμα.

Καταληκτικά, συμφωνούν και οι δύο πόλοι, ότι είναι αλήθεια ότι πρόκειται για την πρώτη φορά που ο κόσμος έχει τη δυνατότητα να επικοινωνήσει σε τέτοιο εύρος και τόσο άμεσα (όπως με ήχο και εικόνα, αντί μόνο με το γραπτό λόγο του παρελθόντος). Εντούτοις, δεν έχουμε ενδείξεις ότι αυτή η συνθήκη είναι ικανή να καταργήσει θεμελιώδη ελατήρια της αρνητικής έκφανσης της ανθρώπινης συμπεριφοράς (π.χ. τον πόλεμο ή την εγκληματικότητα). Εξάλλου, ήδη μιλάμε για το κυβερνο-έγκλημα ή τον κυβερνο-πόλεμο (Furnell, 2006). Όλα αυτά ίσως διαπνέονται, ξανά, από μια προσπάθεια στο δυτικό κόσμο για μια πολιτική και πολιτιστική χειραγώγηση (Μουζέλης, 2001), κατά την οποία η σημερινή κυρίαρχη ιδεολογία¹⁵⁸ επιχειρεί να καθιερώσει -διαμέσου του κυβερνοχώρου- τους τεχνοκρατικούς όρους στις συνθήκες ζωής (Άνδρας, 2008). Αυτό βεβαίως θα σήμανε την απαρχή διαμόρφωσης ενός νέου πλέγματος κοινωνικών σχέσεων και δεσμών εξουσίας. Συνεπώς, για να πραγματοποιηθεί ένα νέο όραμα προόδου, αυτή τη φορά λόγω του κυβερνοχώρου, οφείλουμε κατά τη διάρκεια της εφαρμογής του να διασφαλίζουμε τους απαραίτητους όρους ισοπολιτείας (Δερτούζος, 1998).

¹⁵⁷ Αυτή η θέση υποστηρίζει ότι όλα αυτά τα μικροσκοπικά επιτεύγματα της νανοτεχνολογίας απαιτούν πολλούς υλικούς πόρους, οι οποίοι, ως εκ τούτου, εξακολουθούν να έχουν σημαντική επίδραση, τουλάχιστον τόση, όση και η τεχνολογία.

¹⁵⁸ Η έννοια της «ιδεολογίας», βεβαίως, χρήζει πολύ μεγάλης ανάπτυξης (βλ. Παπαστάμου, 2011). Ωστόσο, γενικότερα, εδώ αναφερόμαστε στην υπεράσπιση των ειδικών συμφερόντων της άρχουσας (κυρίαρχης) τάξης της εποχής.

10.2 Ορισμοί και Προσδιορισμός

Μέχρι τώρα, δεν υπάρχει ομοφωνία σε ένα συγκεκριμένο ορισμό του κυβερνοχώρου (Ottis και Lorents, 2010). Με σκοπό να αναζητήσουμε ενδεχόμενα κοινά σημεία, θα παραθέσουμε ορισμένους από τους πιο «αντιπροσωπευτικούς». Το πιο παλαιό επιστημονικό κείμενο που εντοπίσαμε, σχετικά με την οριοθέτηση της έννοιας, παρουσιάστηκε σε μια εργασία, η οποία συμμετείχε στο 1^ο Διεθνές Συνέδριο για τον Κυβερνοχώρο στο Πανεπιστήμιο του Τέξας (Austin, 1991). Το ιδιαίτερο ενδιαφέρον της έγκειται στα συμπεράσματα, όπου επισημαίνεται ότι βασικό χαρακτηριστικό του κυβερνοχώρου αποτελεί το «κοινωνικό μοίρασμα» (η κοινή συμμετοχή) και πως οι μελλοντικοί αρχιτέκτονές του θα πάρουν πολλά από τις επιστήμες της πληροφορικής, των οικονομικών και της κοινωνιολογίας. Επιγραμματικά, ορισμένοι ορισμοί τονίζουν ότι:

- Ο κυβερνοχώρος είναι περισσότερο αποτέλεσμα της κοινωνικής διάδρασης, παρά των τεχνολογικών εφαρμογών (Morningstar&Farmer, 2003).
- Η Ευρωπαϊκή Ένωση ορίζει τον κυβερνοχώρο ως ένα δυνητικό¹⁵⁹ χώρο, μέσα στον οποίο κυκλοφορούν τα ηλεκτρονικά δεδομένα των Η/Υ παγκοσμίως (Ευρωπαϊκή Επιτροπή, 2011).
- Ο κυβερνοχώρος είναι ένα κοινωνικό-τεχνολογικό περιβάλλον, το οποίο το χτίζουν, το εξερευνούν και το εκμεταλλεύονται άνθρωποι (Science Enhanced Network Domains and Secure Social Spaces, 2011).
- Ο κυβερνοχώρος ορίζεται ως ένα πεδίο που χαρακτηρίζεται από τη χρήση του ηλεκτρονικού και ηλεκτρομαγνητικού φάσματος, ώστε να αποθηκευθούν, τροποποιηθούν και ανταλλαχθούν δεδομένα μέσω διασυνδεδεμένων συστημάτων και συνεργαζόμενες φυσικές υποδομές (Cyberspace Sciences and Information Intelligence Research Group, 2011).
- Κυβερνοχώρος λέγεται το ηλεκτρονικό μέσο των δικτύων των Η/Υ, μέσα στο οποίο λειτουργούν οι δυνητικές κοινότητες¹⁶⁰ (Wikipedia, 2011).
- Το αμερικανικό υπουργείο άμυνας ορίζει τον κυβερνοχώρο ως ένα παγκόσμιο πεδίο, μέσα στο οποίο το πληροφοριακό περιβάλλον συνίσταται από αλληλεξαρτώμενα δίκτυα τεχνολογικών υποδομών. Σε αυτά περιλαμβάνονται το Διαδίκτυο, τα τηλεπικοινωνιακά δίκτυα, τα συστήματα Η/Υ, καθώς και

¹⁵⁹ Η έννοια του «δυνητικού» ως μετάφραση του “virtual”, αντί για το «εικονικό» που είναι συνηθισμένο στην καθομιλουμένη, έχει καθοριστική σημασία, η οποία εξηγείται αμέσως παρακάτω.

¹⁶⁰ Επίσης αναφερόμαστε στις κοινότητες που σχηματίζονται στον κυβερνοχώρο. Τον όρο εμπνεύστηκε και διερεύνησε ο Howard Rheingold (1993), που θα αναλυθεί στη συνέχεια.

ενσωματωμένοι επεξεργαστές και ελεγκτές (DoD Dictionary of Military Terms, 17/10/2008).

- Κυβερνοχώρο ονομάζουμε έναν χρονικά εξαρτώμενο «κόσμο» αλληλεπίδρασης των διασυνδεδεμένων συστημάτων πληροφορικής και της ανθρώπινης χρήσης τους (Ottis&Lorents, 2010).

Από τους παραπάνω ορισμούς μπορούμε να διακρίνουμε ένα κοινό σημείο. Ο κυβερνοχώρος αντιμετωπίζεται σαν ένας *κόσμος* -όπως εκφράζεται στον τελευταίο ορισμό-, ο οποίος *απαρτίζεται* από τα εξής δύο μέρη: το κοινωνικό και τεχνικό. Θα επιχειρήσουμε έναν εννοιολογικό προσδιορισμό με την ακόλουθη μεθοδολογία. Καταρχάς, θα αναλύσουμε τη σχέση των όρων «κόσμος και κυβερνοχώρος» και κατόπιν, θα εμβαθύνουμε στην ιστορική συνύπαρξη των δύο μερών.

Η ανάλυσή μας θα ξεκινήσει με οδηγό μια φαινομενολογική θεώρηση¹⁶¹ (Coynne, 1995). Σύμφωνα λοιπόν με αυτήν, ο κυβερνοχώρος συνάδει εννοιολογικά με τον τρόπο που χρησιμοποιούμε τη λέξη «κόσμος» και πιο συγκεκριμένα, στο κοινό υποσυνείδητο υπόβαθρο που διαθέτουμε για αυτόν υπάρχουν τρεις συναφείς χρήσεις. Με την πρώτη, λέγοντας «κόσμος» εννοούμε ένα σύνολο *οντοτήτων και αντικειμένων*, που στη συγκεκριμένη περίπτωση του κυβερνοχώρου συνιστούν τα φυσικά εξαρτήματα των υπολογιστών και της σύνδεσής τους (hardware), καθώς και τα προγράμματα λειτουργίας τους (software). Κατά τη δεύτερη, εννοούμε ένα σύνολο εξειδικευμένων ατόμων με ειδική θεματολογία ενδιαφέροντος (επαγγελματικής ή ερασιτεχνικής ενασχόλησης, όπως οι μουσικοί και οι αθλητές), η οποία έχει τους δικούς της κώδικες (όπως η ορολογία). Η «ένταξη» των μελών διαγράφεται σε ένα ολόκληρο φάσμα, από την πυκνή (καθημερινή, ολόημερη και παραγωγική) μέχρι τη χαλαρή (σπάνια και μόνο καταναλωτική) επαφή τους. Έτσι, σε αντιστοιχία, μιλάμε για ένα σύνολο *οντοτήτων και υποκειμένων*, όπως η λειτουργία των κοινοτήτων μέσα στα ίδια τα πλαίσια της «κοινωνίας του κυβερνοχώρου»: ενδεικτικά, οι 'hackers' που γνωρίζουν τις κρυφές οδούς διακίνησης των δεδομένων στο σύστημα· οι 'moderators' (μεσολαβητές) που διοικούν (εγκρίνουν ή απορρίπτουν) και καθοδηγούν τη διασπορά των πληροφοριών· και τέλος, οι απλοί θεατές 'lurkers'¹⁶².

¹⁶¹ Η φαινομενολογία είναι φιλοσοφική σχολή σκέψης, η οποία ξεκινά τους στοχασμούς της με σημείο αναφοράς τα φαινόμενα, όπως τα αντιλαμβανόμαστε και τα συνειδητοποιούμε και όχι βάσει μιας αυθύπαρκτης υπόστασής τους. Αποτέλεσε το θεμελιώδη λίθο του υπαρξισμού.

¹⁶² Στη διαδικτυακή κουλτούρα «παρατηρητή» (lurker) ονομάζουμε το πρόσωπο που έχει παθητική σχέση με τον Ιστό, δηλαδή παρακολουθεί δίχως να καταθέτει τη γνώμη του. Δεν έχει ενεργή συμμετοχή. Έρευνες δείχνουν ότι ίσως να φθάνουν ακόμα και το 90% των χρηστών (Nonnecke &

Αυτή η δεύτερη προσέγγιση ενισχύεται και από την άποψη ότι είναι αναπόφευκτο, όποτε οι άνθρωποι έχουν την ευκαιρία (και σε αυτήν την περίπτωση από τις ΤΠΕ), να συγκροτούν κοινότητες με αιτία ή αφορμή τα ενδιαφέροντά τους (Rheingold, 1993).

Η τρίτη αντιστοιχία περικλείει ένα εναλλακτικό νόημα που δίνεται σε ένα φανταστικό κόσμο, ο οποίος εκ φύσεως δίνει έμφαση στο μέλλον και άρα, στην προσδοκία· εκεί όπου διασταυρώνονται ελπίδα και ουτοπία. Πρόκειται για την αισιόδοξη, αλλά αφηρημένη, προοπτική ενός κόσμου - κυβερνοχώρου όπως ο καθένας θα τον ήθελε. Αυτή η έκφανση βρίσκεται σε συνάφεια με τον εμπνευστή του όρου. Ο κυβερνοχώρος εμφανίζεται για πρώτη φορά σε ένα μυθιστόρημα επιστημονικής φαντασίας (Gibson, 2004)¹⁶³, εκεί παρουσιάζεται σαν ένας «α-χώρος», δίχως δηλαδή φυσικές (υλικές – μετρήσιμες) διαστάσεις. Ο ανθρώπινος νους αποτελεί τη «θύρα» σύνδεσης. Κάτι με το οποίο συμφωνεί και ένας άλλος, από τους πρώτους που εξήγησαν αυτή την έννοια, ο οποίος επίσης υπήρξε και πρωτεργάτης της άποψης ότι πρόκειται για μια μεγάλη ευκαιρία ελεύθερης διακίνησης των ιδεών (Zaleski, 2001, 38)¹⁶⁴. Μια σημαντική προέκταση της τελευταίας ερμηνείας αποτελεί η θέση πως πρόκειται για κάτι που υφίσταται μόνο στο μέλλον. Αυτός, εξηγεί, είναι ο λόγος που το αισθανόμαστε «άπιαστο» στο παρόν και για αυτό ακριβώς δεν μπορεί να γίνει κατανοητή η ύπαρξή του στο παρελθόν. Η ίδια θέση, με άλλα λόγια, κατατίθεται και σε μια εργασία τυποποίησης των ειδών πολέμου. Ο πόλεμος στον κυβερνοχώρο θεωρήθηκε ως ο πόλεμος του δυνητικού κόσμου. Αποτελεί μεν μια κατηγορία του Πληροφοριακού Πολέμου, που δεν είναι εφικτός όμως στις ημέρες μας, καθώς επίσης και στο εγγύς μέλλον. Η αιτία είναι ότι απαιτείται η ολοκλήρωση της υφιστάμενης διεθνούς πληροφοριακής υποδομής έτσι, ώστε να εξαρτάται από αυτήν σχεδόν ολοκληρωτικά κάθε πτυχή της ανθρώπινης συμπεριφοράς και κυρίως των κέντρων λήψης αποφάσεων (Libicki, 1995).

Preece 2000). Μια βασική αιτία αυτού του μεγέθους, θεωρείται η έλλειψη εμπιστοσύνης (Ridings, Gefen & Arinze, 2006). Διαθέσιμο στο: <http://en.wikipedia.org/wiki/Lurker>

Επίσης, εκτιμάται ότι η αξιοποίησή τους θα ήταν πολύ χρήσιμη... [Ridings, Catherine; Gefen, David; and Arinze, Bay (2006) "Psychological Barriers: Lurker and Poster Motivation and Behavior in Online Communities," *Communications of the Association for Information Systems*: Vol. 18, Article 16]. Available at: <http://aisel.aisnet.org/cais/vol18/iss1/16>.

¹⁶³ «Το ηλεκτροσύμπαν. Μια συμβατική παραίσθηση, την οποία μοιράζονται κάθε μέρα δισεκατομμύρια χειριστές σε όλο τον κόσμο... Μια γραφική αναπαράσταση πληροφοριών που προέρχεται από όλους τους κομπιούτερ της ανθρωπότητας. Αφάνταστη πολυπλοκότητα» (Gibson, 2004, 65-66).

¹⁶⁴ Αναφερόμαστε στον John Perry Barlow, ο οποίος εκτός από το μανιφέστο του κυβερνοχώρου, έχει διατυπώσει και έναν από τους παραστατικότερους ορισμούς περιγράφοντάς τον με το χώρο που βρισκόμαστε όταν συνδιαλεγόμαστε στο τηλέφωνο.

Μέσα από την ανάλυση της σχέσης των όρων του κόσμου και του κυβερνοχώρου αναδεικνύεται και η τομή δύο κοινών μερών τους, του *κοινωνικού και τεχνικού*. Στην πρώτη περίπτωση είδαμε πως μιλάμε για ένα σύνολο οντοτήτων και αντικειμένων, των οποίων η αντιστοιχία τους αντανακλάται στο λογισμικό και τα εξαρτήματα των μηχανημάτων. Άρα, εδώ, μπορούμε να διαπιστώσουμε την έκφανση του τεχνικού μέρους. Στη δεύτερη περίπτωση είδαμε πως μιλάμε για ένα σύνολο οντοτήτων και υποκειμένων, των οποίων η αντιστοιχία τους αντανακλάται στις ιδιότητες των ρόλων που παίζουν οι συμμετέχοντες. Άρα, εδώ διαπιστώνουμε την έκφανση του κοινωνικού μέρους. Αυτά τα μέρη θα πρέπει να νοηθούν ως τεμνόμενα και όχι σε μια γραμμική σχέση, με μια διακριτή διαχωριστική γραμμή. Αντιθέτως, το ένα μέρος αποτελεί προέκταση του άλλου σε μια λειτουργία συνεχούς ροής, κατά την οποία δεν αντιλαμβανόμαστε κάποια σύνορα. Έτσι, για παράδειγμα όταν παίζουμε ένα παιχνίδι στον υπολογιστή. Αρχικά, μπορούμε να διακρίνουμε την χονδροειδή ύλη (το πληκτρολόγιο, την οθόνη), στη συνέχεια γίνεται θολή η διάκριση από το πρόγραμμα που εκκινούμε κι εμπλεκόμαστε νοητικά και τελικά, ταυτιζόμαστε με το ρόλο του παίκτη, καθώς και με τους περιορισμούς που αυτός ενέχει, αλλά και τα περιθώρια διάνοιξης του φανταστικού που μας δίνει. Η προοπτική του φανταστικού κλιμακώνεται όσο προσπαθούμε να επιτύχουμε το σκοπό μας (τη νίκη). Αυτή είναι και η πραγμάτωση της τρίτης αντιστοιχίας, σύμφωνα με την οποία η ενασχόληση με τον κυβερνοχώρο, μας θυμίζει μια «επένδυση» στο μέλλον. Για αυτόν κυρίως το λόγο, όταν δεν πρόκειται για ένα απλό παιχνίδι, αλλά για μια πιο άμεση σύνδεση με βασικές λειτουργίες στον πραγματικό κόσμο (όπως η ενημέρωση ή ιδίως η επικοινωνία), τότε γίνεται πιθανός και ένας αναστοχασμός -συνειδητός ή όχι- περί της ταυτότητάς μας. Τότε επανακαθορίζουμε τη θέση μας μέσα τον πραγματικό κόσμο, ανάλογα με τη διαμεσολαβούμενη εμπειρία που βιώνουμε στον κυβερνοχώρο.

10.3 Η μία όψη: το Κοινωνικό-τεχνικό Σύμπλεγμα

Ωστόσο από το σημείο αυτό, κατά το οποίο προσπαθούμε να περιγράψουμε έναν χώρο που δεν γίνεται αντιληπτός όπως ο πραγματικός, τα πράγματα περιπλέκονται. Σε μια σημαντική μελέτη τεκμηριώθηκε από νωρίς, η θέση ότι πλέον διενεργείται μια υπαρξιακή μετάλλαξη του σύγχρονου δυτικού ανθρώπου σε ένα νέο τύπο κυβερνο-οργανισμού, ο οποίος ενσωματώνει στη ζωή του τις σύγχρονες τεχνολογίες ως απερίσπαστο μέρος (Haraway, 1991). Αυτή η ερευνητική θέαση έγινε αφετηρία μιας νέας διερευνητικής ματιάς. Πιο συγκεκριμένα, της τριγωνικής σχέσης μεταξύ του

ατόμου, της κοινωνίας και της τεχνολογίας, η οποία αποκαλέστηκε κυβερνο-ψυχολογία (Gordo-Lopez και Parker, 1999/2008)¹⁶⁵. Με έντονη την πολιτική έμφαση, συνοπτικά, θεωρείτε ότι στην προηγούμενη φάση της καπιταλιστικής εποχής μας, το άτομο αυτό-προσδιορίζεται μέσα σε ένα κλίμα μαζικής παραγωγής και κατανάλωσης. Εκεί τα υφιστάμενα MME λειτουργούν με ένα γενικό μοντέλο, το οποίο περικλείει έναν πομπό που εκπέμπει σε πολλούς αποδέκτες (παραδείγματα ραδιοφώνου και τηλεόρασης). Πλέον, οδηγούμαστε στη σύγχρονη φάση όπου η απαρχή της έγινε με την προβολή της κεντρικής ιδέας της κυβερνητικής (Wiener, 1948)¹⁶⁶.

Παρεμπιπτόντως, σε αυτήν οφείλεται ο πυρήνας του νοήματος, που αρχικά προσδόθηκε, και αργότερα εξαπλώθηκε, στη διευρυμένη χρήση του προθέματος «κυβερνό-» (από την κυβερνητική, στον κυβερνοχώρο, ως και τον κυβερνοπόλεμο). Αξιοσημείωτη δε, και για τη νοηματόδοσή του, είναι ότι η προέλευσή του εντοπίζεται -όπως αναφέρει και ο ίδιος ο συγγραφέας- στο ελληνικό «κυβερνώ / κυβερνήτης». Η ιδέα λοιπόν, αφορά την κατασκευή μηχανών, οι οποίες έχουν τη δυνατότητα *ελέγχου* του εαυτού τους (Ευκλείδη, 2005, 248-249). Εδώ πρέπει να υπογραμμίσουμε τη μεγάλη σημασία που έχει η κατανόηση της έννοιας του ελέγχου. Έλεγχος ονομάζουμε τη διττή δυνατότητα αφενός παρακολούθησης μιας λειτουργίας/διαδικασίας και αφετέρου, αν αυτή παρεκκλίνει από το στόχο, της παρέμβασης προς (αυτό)ρύθμιση της πορείας της. Με άλλα λόγια, περιγράφουμε την παραδοχή μιας ερμηνείας της έννοιας του ελέγχου, η οποία εκφράζεται μέσω μιας μεθοδολογίας των εξής βημάτων:

- i. Θέτουμε σε ένα αντικείμενο ή υποκείμενο έναν στόχο (π.χ. τη διαδρομή από το σημείο 0 στο σημείο 1, με βήματα ανά 0,2),
- ii. αυτό μπορεί να παρακολουθήσει την εξέλιξή του (π.χ. 0,2 – 0,4 – 0,6 κοκ) και
- iii. αν κάποια στιγμή λανθάνει (π.χ. 0,2 – 0,4 – 0,3...), τότε έχει ρυθμιστεί έτσι, ώστε να διορθώνει τον εαυτό του (0,2 – 0,4 – 0,3 = 0,6 – 0,8 – 1).

Τα πράγματα είναι απλά, όταν το σύστημα λειτουργεί με έναν κεντρικό καθοδηγητή, ο οποίος θέτει τις εντολές και αυτές εκτελούνται. Στη σύγχρονη συγκυρία όμως, η πολυπλοκότητα αυξάνεται. Ο λόγος που συμβαίνει αυτό είναι ότι

¹⁶⁵ Επιστημολογική άποψη, εκ της κριτικής σχολής, η οποία δεν αντιλαμβάνεται τη θέση της ως ένα άλλον τομέα της ψυχολογίας, αλλά ένα είδος μετα-ψυχολογίας· όπως αυτή διαδέχτηκε την ψυχιατρική.

¹⁶⁶ Το θεωρητικό υπόβαθρο συναποτελούν -όπως συμβαίνει με κάθε επιστημονικό έργο σταθμό- πολλά προηγούμενα πορίσματα. Από τα σημαντικότερα είναι η θεωρία των Πληροφοριών (Claude E. Shannon) και η θεωρία των Παιγνίων (εισήχθηκε από τους John von Neumann και Oskar Morgenstern, στο βιβλίο «Θεωρία Παιγνίων και Οικονομική Συμπεριφορά» και θεμελιώθηκε με τη δημοσίευση της *Ισορροπίας* του John Forbes Nash - *Nash Equilibrium*).

το προαναφερόμενο γενικό μοντέλο αλλάζει, και οι πομποί γίνονται πολλοί (δηλαδή αυτοί που «δρουν» στον κυβερνοχώρο, είτε χρησιμοποιώντας το ηλεκτρονικό ταχυδρομείο, είτε με οποιονδήποτε άλλο τρόπο)¹⁶⁷. Προσπαθώντας να εκφράσουμε το ίδιο πιο αφαιρετικά, διακρίνουμε ότι λόγω της διαμεσολάβησης του προαναφερόμενου τεχνικού μέρους (ή αλλιώς των νέων ευκαιριών που δίνονται από την τεχνολογία), διακινούνται ποικίλα μηνύματα, τα οποία διασταυρώνονται. Ωστόσο, όπως εξηγήσαμε, εφόσον στην εποχή μας ο αυτοπροσδιορισμός μας γίνεται συναρτήσεως της τεχνολογίας, αναδύεται μια σύγχυση που επιδρά και στην ταυτότητά μας. Οι «ψηφιακές εμπειρίες» δύσκολα βιώνονται, για αυτό εντείνουμε μια προσπάθεια μεταφοράς τους (Σκαρπέλος, 1999) ή και πλήρους απώθησής τους. Στην ανθρώπινη συνείδηση η τεχνολογία αντιμετωπίζεται σαν την προέκταση της ύπαρξης. Οπότε μπορούμε να πούμε ότι ο κυβερνοχώρος έρχεται να υποκαταστήσει μεγάλο μέρος των φυσικών εμπειριών μας από την κοινωνία, προσφέροντας βιώματα που την προσομοιάζουν.

Ο όρος *προσομοίωση* (simulation) αποτελεί μια λέξη-κλειδί για τον κυβερνοχώρο. Μεταφορικά, ορισμένοι συγγραφείς πλέον ομιλούν για την «αντικειμενική κουλτούρα» της προσομοίωσης (Γιαννακόπουλος, 2005, 285). Θα εξηγήσουμε αυτή τη λέξη, λαμβάνουμε υπόψη μας ότι σχεδόν όλοι οι όροι με ιδιαίτερα σημαντική αξία για τον κυβερνοχώρο έχουν οριστεί σε ένα φάσμα, το οποίο επίσης, ξεκινά από τον απόλυτα τεχνολογικό ορισμό και φθάνει στο κοινωνικό. Για παράδειγμα, η έννοια της ασφάλειας της πρόσβασης σε μια θέση του Παγκόσμιου Ιστού. Ξεκινάει από τη διάσταση των κρυπτολογικά ορθών κωδικών λέξεων του χρήστη (password & username) και φθάνει ως την πλήρωση των προϋποθέσεων του προσώπου-χρήστη, την οποία οφείλει να εξετάσει ο υπεύθυνος ασφάλειας των πληροφοριών (info-sec). Έτσι λοιπόν, η προσομοίωση, όσον αφορά σε γενικές γραμμές την τεχνοκρατική της προσέγγιση (η υπολογιστική προσομοίωση), ορίζεται ως η διαδικασία σχεδιασμού ενός μαθηματικολογικού και πληροφορικού μοντέλου για την αναπαράσταση μιας διεργασίας (Ο.Π.Α., 2011). Οι διεργασίες αυτές μπορεί να αφορούν τομείς χρηματοοικονομικούς, επικοινωνιακούς, ψυχαγωγικούς, υγείας, ασφάλειας, ενέργειας κ.ο.κ (Σφακιανάκης, 2001, 14-22). Μια από τις πιο γνωστές της

¹⁶⁷ Ένα χαρακτηριστικό παράδειγμα είναι ο Παγκόσμιος Ιστός. Οι ευκαιρίες για «δράση» στον κυβερνοχώρο είναι μηδαμινές στο web 1.0 και άπειρες στο web 2.0. Έτσι, στην πρώτη περίπτωση, σχηματικά, μια ειδησεογραφική εταιρεία παρουσιάζει τα νέα και οι υπόλοιποι τα παρακολουθούν. Στη δεύτερη, τα νέα μπορούν να περάσουν από τον ένα στον άλλον διαδοχικά. Εξάιρεση εδώ αποτελεί η υπηρεσία του ηλεκτρονικού ταχυδρομείου, η οποία ισχύει και στις δύο περιπτώσεις.

εφαρμογές είναι η λεγόμενη εικονική πραγματικότητα (virtual reality)¹⁶⁸. Ορίζεται ως εκείνη η τεχνολογία που επιτρέπει στον χρήστη να αλληλεπιδρά με ένα περιβάλλον προσομοίωσης ενός υπολογιστή, είτε το περιβάλλον αυτό είναι μια προσομοίωση του πραγματικού κόσμου είτε αποτελεί έναν άλλο, ξεχωριστό, φανταστικό κόσμο (Ε.Κ.Π.Α., 2011). Η έκφραση αυτή λοιπόν υποδηλώνει τη διαμόρφωση μιας κατάστασης που κινείται μεταξύ αισθήσεων και ψευδαισθήσεων, ώστε να βιώνονται διαμέσου του κυβερνοχώρου εμπειρίες ενός μη πραγματικού κόσμου. Σε αυτό το σημείο ανακύπτει η χρησιμότητα μιας ψυχό-κοινωνιολογικής οριοθέτησης. Και για να διαχωριστεί με σαφήνεια αυτή η πλευρά προτιμάται (στις συναφείς ελληνόγλωσσες δημοσιεύσεις) ο όρος «δυνητική»¹⁶⁹. Πάντως, για την ορθότερη κατανόηση της έκφρασης «Δυνητική Πραγματικότητα» είναι σημαντικό να δοθεί ιδιαίτερη προσοχή στον από-συμβολισμό της συσχέτισης αυτών των δύο λέξεων (Sherman και Craig, 2003).

10.4 Η άλλη όψη: το «Δυνητικά Φαντασιακό»

Ένας από τους διανοητές που εντάρφισε φιλοσοφικά στη συσχέτιση αυτών των δύο λέξεων είναι ο P. Lèvy (1995)¹⁷⁰. Αυτός έδειξε ότι η διεπαφή¹⁷¹ που έχουμε από όσα επισυμβαίνουν στον κυβερνοχώρο, αποτελεί τη ρίζα εμφάνισης των εννοιών «δυνητικό – δυνητικοποίηση». Με αυτόν τον όρο δηλώνεται το πλέγμα των προβλημάτων που ενέχεται στη φύση κάθε πραγματικής υπόστασης, η οποία συνιστά τη λύση σε ένα πρόβλημα. Έτσι, για παράδειγμα, η εφεύρεση των μηχανών της κυβερνητικής μπορεί να αποτέλεσαν την επίλυση σε μια σειρά ζητημάτων στη γραμμή παραγωγής των επιχειρήσεων, αλλά με την παρουσία των μηχανών διαμορφώθηκαν οι όροι ώστε να προκύψουν *δυνητικά* νέα οργανωτικά πρόβλημα. Το εννοιολογικά καινοτόμο στοιχείο του «δυνητικού» δεν έχει σημείο αναφοράς την υλοποίηση (εφεύρεση μηχανών), όπως το «πραγματικό», αλλά την έμπνευση

¹⁶⁸ Πρώτη φορά ο όρος χρησιμοποιήθηκε στο βιβλίο *The Theatre and Its Double* ενός Γάλλου καλλιτέχνη (Artaud, 1938). Η πρώτη όμως περιγραφή του έγινε από τον Dr. Ivan Sutherland (1965), ο οποίος υπήρξε πρωτοπόρος στα γραφικά των υπολογιστών. «Ένας (εικονικός) κόσμος που φαίνεται αληθινός, ακούγεται αληθινός, μοιάζει αληθινός, και αντιδρά ρεαλιστικά στις πράξεις του χρήστη». Στα τέλη, όμως, της δεκαετίας του '50 το όραμα έκφρασε ένας νεαρός ηλεκτρολόγος μηχανικός και πρώην ναυτικός τεχνικός ραντάρ, ο Douglas Engelbart.

¹⁶⁹ Στην καθομιλούμενη, καθώς επίσης και σε κάποιες, κυρίως θετικής κατεύθυνσης, επιστημονικούς τομείς χρησιμοποιείται ο επιθετικός προσδιορισμός «εικονικό». Θα φανεί παρακάτω ο λόγος που προτιμάμε εδώ -όπως επί τω πλείστον κάνουν οι κοινωνικοί επιστήμονες στη χώρα μας- το «δυνητικό»

¹⁷⁰ Γενικά, στο έργο του ανέλυσε τους τρόπους του *είναι*: πραγματικός – δυνατός – δυνητικός – ενεργά υπαρκτός, καθώς και τις αντίστοιχες δυναμικές που συνδέουν σαν αγωγοί ροών τον κάθε τρόπο αντίστοιχα: πραγματοποίηση – δυνατοποίηση – δυνητικοποίηση – ενεργοποίηση.

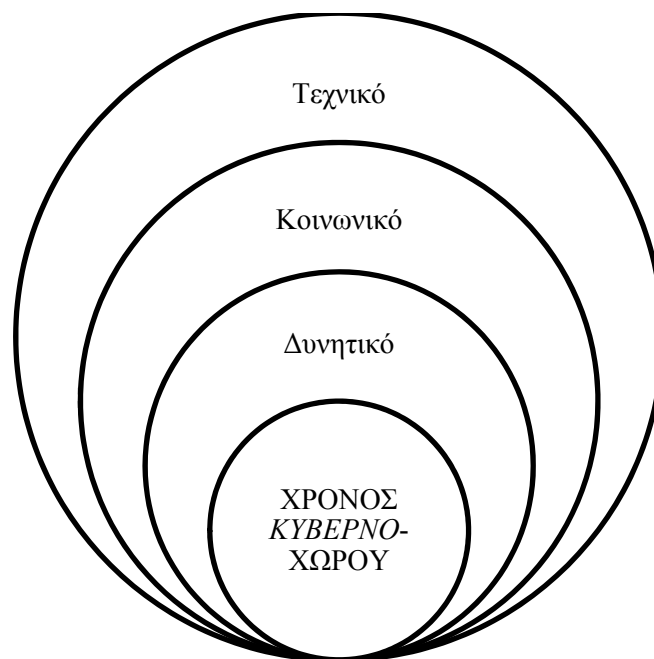
¹⁷¹ Αυτός ο όρος τονίζει τη δυναμική αλληλεπίδραση των χρηστών στον κυβερνοχώρο.

(προετοιμάζει το χώρο και το χρόνο της νέας πραγματικότητας). Δεν είναι όμως το αντίθετο του πραγματικού, όπως δεν είναι και το παραπλανητικό ή ψευδές (εικονικό). Το δυνητικό προσφέρει χώρο για δημιουργία, διανοίγει προοπτικές και δίνει νέες δυνατότητες. Υπάρχει, αλλά δεν γίνεται αντιληπτό από τις αισθήσεις. Η σχέση τους με το πραγματικό αφορά σε μια παράλληλη συνύπαρξη. Εν κατακλείδι, μέσω του δυνητικού επινοούνται τα νέα προβλήματα δια μιας πυροδότησης του γίγνεσθαι. Άρα, μπορούμε να πούμε πως σε κάθε πραγματικότητα η δυνητική της έκφραση περικλείει τις καινούριες και μελλοντικές ανάγκες προς κάλυψη και ανακάλυψη!

Συμπερασματικά, μέσα από την παραπάνω ανάλυση, μπορούμε να διαμορφώσουμε μια μεθοδολογία -έναν «αλγόριθμο»- ανάγνωσης της σύντομης ιστορίας του κυβερνοχώρου, της οποίας κάθε σταθμός θα πρέπει σχηματικά να διαθέτει (σχήμα 27).

- I. Το τεχνικό μέρος (το σύνολο των αντικειμένων).
- II. Το κοινωνικό μέρος (το σύνολο των υποκειμένων).
- III. Το δυνητικό μέρος (ανάγκες που καλύφθηκαν κι αναδύθηκαν)

Σχήμα 27. Τα ενυπάρχοντα μέρη του κυβερνοχώρου



10.5 Συμπέρασμα: ο Αλγόριθμος

Όπως δείξαμε σε προηγούμενο κεφάλαιο, η τυπική οργανωτική δόμηση του κόσμου και κυρίως μετά το δεύτερο παγκόσμιο πόλεμο είναι πλέον το έθνος-κράτος. Η εποχή των αποικιών έχει σχεδόν ολοκληρωθεί και κάθε κράτος ουσιαστικά «κυριαρχεί

επίσημα» μόνο στο εσωτερικό του. Βεβαίως, ο κόσμος έχει χωριστεί στα δύο, περίπου σε όλα τα επίπεδα (ιδεολογικό, οικονομικό κοκ). Ειδικότερα, στο στρατηγικό ανταγωνισμό ισχύος μεταξύ των πρωταγωνιστών (ΗΠΑ και Σοβιετική Ένωση) η προστιθέμενη αξία -ο πολλαπλασιαστής ισχύος κατά τη στρατιωτική ορολογία- των πληροφοριών αρχίζει να γίνεται κοινή συνείδηση των ηγεσιών (Stonier, 1984). Πιο συγκεκριμένα, μετά την επιτυχία των σοβιετικών με την εκτόξευση του (πρώτου τεχνητού δορυφόρου της γης) Σπούτνικ, το 1957, οι αμερικανοί ιθύνοντες θέτουν στόχο τη διαμόρφωση ενός ασφαλούς περιβάλλοντος επικοινωνίας και ανταλλαγής πληροφοριών υψίστης σημασίας¹⁷². Για αυτό το σκοπό εκμεταλλεύονται την ήδη διαθέσιμη τεχνολογία των H/Y, οι οποίοι έχουν αποδείξει τη χρησιμότητά τους στην εξοικονόμηση χρόνου (με τη μεγάλη ταχύτητα επεξεργασίας που διαθέτουν) και χώρου (με την έννοια της αποθήκευσης στοιχείων, η επικαλούμενη οργανωσιακή μνήμη). Αξιοσημείωτο είναι ότι οι πρώτοι H/Y δεν διακρίνονταν ιδιαίτερα από τις άλλες μηχανές, οπότε και το προσωπικό που απασχολούσαν ανήκε στην γενική κατηγορία των χειριστών¹⁷³.

Για την κάλυψη λοιπόν της παραπάνω ανάγκης, εμπνεύστηκαν την ιδέα της διασύνδεσης των H/Y έτσι, ώστε να είναι εφικτή η μεταφορά δεδομένων καθώς και η επικοινωνία στελεχών, όταν χρειαστεί αυτή να γίνεται σε απομονωμένο περιβάλλον. Αυτή περιληπτικά είναι η αφετηρία της εποχής του Διαδικτύου. Από τη στόχευση της κάλυψης μιας συγκεκριμένης ανάγκης (ασφαλείς και μυστικές συνδιαλλαγές), στην εκμετάλλευση της υπάρχουσας τεχνολογίας (computer) και με αποτέλεσμα τη νέα εφεύρεση (internet).

Το ερώτημα, το οποίο προκύπτει από τον «αλγόριθμό» μας, έχει να κάνει με τις κοινωνικές συνέπειες του τεχνολογικού επιτεύγματος. Το «κλειστό κύκλωμα δικτύωσης» υπό τον αυστηρό έλεγχο του υπουργείου Άμυνας των ΗΠΑ άρχισε κατ' ανάγκη να «ανοίγει» εξαιτίας των φανερών αναγκών και περιθωρίων βελτίωσής του. Στην αρχή εμπλέκονται αναγκαστικά τα πανεπιστημιακά ιδρύματα, στη συνέχεια παίρνουν πρωτοβουλίες οι φοιτητές και τέλος, πριν ακόμα απεγκλωβιστεί και νομότυπα από την κυβέρνηση (1990), είχε προωθηθεί προς εμπορική αξιοποίηση στις αγορές τη δεκαετία του '80. Σε αυτό το σημείο, όταν η οικονομική δραστηριότητα

¹⁷² Αρμόδια για την επίτευξη αυτού του στόχου χρίστηκε η Υπηρεσία Προηγμένων Ερευνητικών Έργων (ARPA) τον Σεπτέμβριο του 1969. Την ευθύνη ανέλαβε το Γραφείο Τεχνικών Επεξεργασίας Πληροφοριών (IPTO), με διευθυντή έναν ψυχολόγο, που μετεκπαιδεύτηκε στο MIT στους H/Y, τον Τζότζεφ Λίκλιντερ. Πρώτη κίνηση ήταν η συνεργασία με τους ερευνητές της RAND (Castells, 2003).

¹⁷³ Η 1^η γενιά H/Y λειτουργούσε με λυχνίες ('40), η 2^η με τρανζίστορ ('50) και η 3^η με ολοκληρωμένα κυκλώματα ('60) (Παπαδάκης και Χατζηπέρης, 2002, 5).

αναλαμβάνει τα ηνία, συνειδητοποιείται η ωφελιμότητα από την ηλεκτρονική δικτύωση των επιχειρήσεων και μετέπειτα της δημόσιας διοίκησης. Τότε διατυπώνεται και το όραμα της ηλεκτρονικής διακυβέρνησης και επιπρόσθετα η σημασία να δοθεί πρόσβαση σε όσο το δυνατόν περισσότερους πολίτες, ώστε να αυξάνονται συνεχώς οι υπηρεσίες που μπορούν να διεκπεραιωθούν μέσω του διαδικτύου. Σε αυτές τις κοινωνικές συνθήκες όλο και περισσότεροι αρχίζουν να μιλούν για τον δυνητικό αναλφαριθμητισμό ή το *ψηφιακό χάσμα* (digital divide). Συμπεραίνουμε, λοιπόν πως η πρώτη διάκριση των πολιτών είναι μεταξύ αυτών που έχουν πρόσβαση στο δίκτυο και γνωρίζουν να το χρησιμοποιούν (χρήστες) και των υπόλοιπων οι οποίοι υφίστανται την απειλή της περιθωριοποίησης για τον ένα (αδεξιότητα προσβασιμότητας – ανεπάρκεια γνώσης χρήσης) ή τον άλλο λόγο (ελλείψει πρόσβασης – ανεπάρκεια υποδομών).

Το ζήτημα στην κατανόηση της μετάβασης από τη μία φάση της ανάπτυξης του κυβερνοχώρου στην άλλη, είναι η εύρεση του δυνητικού στοιχείου. Των οριζόντων, με άλλα λόγια, που ξεπροβάλλουν ως συμπεριλαμβανόμενο συστατικό στη φύση της επίλυσης του προβλήματος της προηγούμενης φάσης. Έτσι, η εφεύρεση του διαδικτύου κάλυψε μεν τη μία ανάγκη, ανέδειξε δε, τα πλεονεκτήματα της κοινωνικής του διάδοσης. Η νέα φάση άρχισε να δρομολογείται από την επιχείρηση εγκατάστασης μιας συνεχώς επεκτεινόμενης ευρυζωνικής¹⁷⁴ επάρκειας καθ' όλη την επικράτεια. Όλο και περισσότεροι ήθελαν να έχουν πρόσβαση σε αυτήν την επαναστατική τεχνολογία. Ήταν πια φανερό η προοπτική της δυνατότητας ταχείας και καθολικής επικοινωνίας και ενημέρωσης. Την βέλτιστη αξιοποίηση της υφιστάμενης αποκεντρωμένης υπολογιστικής ισχύος, έδωσε ένας άλλος επιστήμονας με ενδιαφέρον στην καινοτομία (Berners Lee, 1990). Το νέο τεχνολογικό επίτευγμα ονομάστηκε Παγκόσμιος Ιστός (World Wide Web)¹⁷⁵ και έδινε, με ένα σχετικά εύχρηστο τρόπο, τη δυνατότητα επικοινωνίας ελεύθερα πλέον στην κοινωνία.

Σε αυτή τη φάση, αν εξαιρέσουμε την εκμετάλλευση του ηλεκτρονικού ταχυδρομείου, με την ανταλλαγή προσωπικών και ομαδικών μηνυμάτων, σε

¹⁷⁴ Η ευρυζωνικότητα ορίζεται ως το προηγμένο, εφικτό και καινοτόμο περιβάλλον από πολιτική, κοινωνική, οικονομική και τεχνολογική άποψη (Πολέμη, 2004)

¹⁷⁵ Συνολικά το Web αποτελεί ένα ενιαίο σύστημα επικοινωνίας και αναπαράστασης της πληροφορίας. Είναι ανοιχτό (ελεύθερου κώδικα), ανεξάρτητο από λογισμικό και τεχνολογική υποδομή, επεκτάσιμο και ουδέτερο απέναντι στη γλώσσα, την πολιτιστική ταυτότητα, το φύλο και τη φυλή. Προσφέρει πρόσβαση στην ανάγνωση και τη δημοσίευση κειμένων σε όλους με ασήμαντο κόστος. Μπορεί να λειτουργεί ως λογισμικό και με «τυχαίες» συνάψεις όπως ο εγκέφαλος. Αξιοποίησε και διεύρυνε σε οικουμενική κλίμακα τη μετάβαση από το ASCII (American Standard Code for Information Interchange) στο υπερ-κείμενο.

πρωτογενές στάδιο¹⁷⁶ τους χρήστες ενημέρωναν λίγα ειδησεογραφικά πρακτορεία. Έτσι, τους μετέτρεπαν σε «παθητικούς θεατές».

Αυτό ακριβώς το πρόβλημα θεραπεύθηκε στην επόμενη φάση. Η προηγούμενη τεχνολογία (web 1.0), αναβαθμίστηκε σε καινούρια (web 2.0). Η τελευταία δίνει τη δυνατότητα έκφρασης στους απλούς πολίτες, δίχως να απαιτείται να ανήκουν κάπου (πίνακας 9). Τέλος, στις ημέρες μας είναι πολύ εύκολο για τους περισσότερους να αποκτήσουν τη δική τους ιστοσελίδα και να αναρτήσουν τις θέσεις τους για οποιοδήποτε θέμα, καθώς επίσης και τις κριτικές όσων αυτοί επιθυμούν.

Πίνακας 9. Η ιστορική ολοκλήρωση του κυβερνοχώρου

	ΕΠΙΚΡΑΤΗΣΗ	ΤΕΧΝΙΚΟ	ΚΟΙΝΩΝΙΚΟ	«ΔΥΝΗΤΙΚΗ ΑΝΑΓΚΗ»
1	1970 - '80	Computer	Χειριστές	Χρόνου (ταχεία επεξεργασία) Χώρου (αποθηκευτική μνήμη)
2	1980 - '90	Internet	Χρήστες	Ασφαλούς επικοινωνίας και ανταλλαγής στοιχείων
3	1990 - '00	Web 1.0	Παθητικοί θεατές	Ενημέρωσης
4	2000 - '10	Web 2.0	Ενεργητικοί δράστες...	Έκφρασης

¹⁷⁶ Η δυνατότητα κάλυψης των ειδήσεων και δη παγκοσμίως, ήταν αδύνατη μέσω μηνυμάτων (emails).

11. ΣΥΜΠΕΡΑΣΜΑ

11.1 Συσχέτιση Κυβερνοχώρου και Κυβερνοπολέμου

Από το συμπέρασμα του προηγούμενου κεφαλαίου (Πίνακας 9) συνάγουμε ότι, μέχρι σήμερα, διακρίνουμε τέσσερις φάσεις στην εξέλιξη του κυβερνοχώρου. Με σκοπό λοιπόν να ελέγξουμε την ισχύ της τρίτης υπόθεσης εργασίας, θα εξετάσουμε αν κάθε φάση συμπίπτει με μια και μόνο, από τις τέσσερις θεματικές κατηγορίες, στις οποίες κατέληξε η έρευνά μας στο πρώτο τμήμα της εργασίας.

Η πρώτη θεματική κατηγορία αφορά τη Διείσδυση και τα κύρια χαρακτηριστικά της είναι αφενός, ότι απασχολεί μια μικρή ομάδα ατόμων, αφού τα γεγονότα που ταξινομήθηκαν σε αυτήν δεν έλαβαν ευρείες κοινωνικές διαστάσεις. Αφετέρου, αυτή η μικρή ομάδα έχει κοινό της γνώρισμα την υψηλή τεχνολογική εξειδίκευση. Αν παρατηρήσουμε την πρώτη χρονικά φάση του κυβερνοχώρου (την οποία ονομάσαμε «computer») και τη συγκρίνουμε με τη Διείσδυση θα αναγνωρίσουμε πως έχουν έναν κοινό παρανομαστή: Τους λίγους επαίοντες και το στενά τεχνοκρατικό αντικείμενο ενασχόλησής τους (γλώσσα μηχανής, σύνδεση δικτύων κ.ά.).

Η δεύτερη θεματική κατηγορία αφορά τις Υποδομές και το κύριο χαρακτηριστικό της είναι η εστίαση σε στόχους, οι οποίοι έχουν ευρείες κοινωνικές επιπτώσεις. Αν παρατηρήσουμε τη δεύτερη χρονικά φάση του κυβερνοχώρου (την οποία ονομάσαμε «internet») και τη συγκρίνουμε με τις Υποδομές, τότε θα αναγνωρίσουμε πως έχουν έναν κοινό παρανομαστή: Τη στήριξή τους στα δίκτυα οργάνωσης ενός κράτους, είτε στον δημόσιο, είτε στον ιδιωτικό τομέα.

Η τρίτη θεματική κατηγορία αφορά τη Κυβερνολογοκρισία και το κύριο χαρακτηριστικό της είναι η συγκέντρωση εξουσίας και η διαχείριση των γεγονότων από οργανισμούς που έχουν θέση ισχύος. Αν παρατηρήσουμε την τρίτη χρονικά φάση του κυβερνοχώρου (την οποία ονομάσαμε «web 1.0») και τη συγκρίνουμε με τη Λογοκρισία, μπορούμε να εντοπίσουμε έναν κοινό παρανομαστή: Την εξάρτηση της δημόσιας ενημέρωσης από λίγες (ιδιωτικές ή δημόσιες) υπηρεσίες, συνθήκη η οποία καθιστά τους πολίτες παθητικούς παρατηρητές.

Η τέταρτη θεματική κατηγορία αφορά την Κυβερνοπροπαγάνδα και το κύριο χαρακτηριστικό της είναι η δραστηριοποίηση του μεγάλου κοινωνικού στρώματος ειδικών και μη στους Η/Υ. Αν παρατηρήσουμε την τέταρτη χρονικά φάση του κυβερνοχώρου (την οποία ονομάσαμε «web 2.0») και τη συγκρίνουμε με την

Προπαγάνδα, διακρίνουμε έναν κοινό παρανομαστή: Την απλοποίηση και κατά συνέπεια την διάδοση της συμμετοχής στον κυβερνοχώρο στους ενεργούς πολίτες.

Όλα τα παραπάνω συμπεράσματα, μας επιτρέπουν να οδηγηθούμε στο πόρισμα της σύμπτωσης των τεσσάρων χρονικών φάσεων του κυβερνοχώρου, με τις ισάριθμες θεματικές μας κατηγορίες (Πίνακας 10). Άρα ισχύει και η τρίτη υπόθεση εργασίας μας.

Πίνακας 10. Η ταυτοσημία Θεματικών Κατηγοριών και Φάσεων του Κυβερνοχώρου

ΦΑΣΗ	ΘΕΜΑΤΙΚΗ	ΚΟΙΝΩΝΙΚΑ	ΕΝΤΑΣΗ
Computer	Διείσδυση	Κλειστό	Τεχνολογικής
Internet	Υποδομές	Ανοικτό	Τεχνολογικής
Web 1.0	Λογοκρισία	Κλειστό	Ανθρώπινης
Web 2.0	Προπαγάνδα	Ανοικτό	Ανθρώπινης

11.2 Επίλογος: Αποσαφήνιση Ορολογίας

Πρόσφατα, η επιχείρηση Cisco Systems¹⁷⁷, ανακοίνωσε τα αποτελέσματα μιας έρευνας, με τίτλο «Visual Networking Index (VNI) Forecast and Methodology, 2008-2013» (<http://enet.s3.amazonaws.com/20090718/EL180709.pdf>). Η Έκθεση της έρευνας κατέληξε ότι η «ψηφιακή» ημέρα του μέσου ατόμου, όπως την ονόμασε, που συμμετέχει στον κυβερνοχώρο, διαρκεί σήμερα 36 ώρες και σε δύο χρόνια (2013), θα φθάσει τη διπλάσια διάρκεια των 24 ωρών της «φυσικής» ημέρας. Με άλλα λόγια, πρόκειται για μια διαστολή του ανθρώπινου χρόνου.

Τα πορίσματα της παραπάνω έρευνας αποτελούν ένα ακόμα ενισχυτικό στοιχείο των συμπερασμάτων μας. Δείχνουν ότι τα βιώματά μας από την «σχέση προσομοίωσης» με τον κυβερνοχώρο, μεταλλάσσουν την αντίληψή μας, τόσο για τον εαυτό μας όσο και για το κοινωνικό μας περιβάλλον. Ένα από αυτά τα είδη των σχέσεων που μεταβάλλονται είναι και οι σχέσεις εξουσίας, οι οποίες εξακολουθούν να υπάρχουν, με διαφορετικούς όμως όρους. Έτσι, το κράτος πλέον χρησιμοποιεί τεχνοκρατικά μέσα ελέγχου των πολιτών και κατ' επέκταση αξιοποιεί ανθρώπινους πόρους που εξειδικεύονται σε αυτά. Αν, όμως δεχθούμε τους καθορισμούς των

¹⁷⁷ Η Cisco Systems, Inc. είναι μια πολυεθνική εταιρεία, της οποίας η έδρα της βρίσκεται στο Σαν Χοσέ της Καλιφόρνια. Αντικείμενό της αποτελεί ο σχεδιασμός και η πώληση προϊόντων των ΤΠΕ. Απασχολεί πάνω από 70 χιλιάδες υπαλλήλους σε όλο τον κόσμο, και τα περσινά της κέρδη ήταν 40 δισεκατομμύρια δολάρια (<http://www.cisco.com>).

εννοιολογικών ορίων όπως αυτοί προκύπτουν, τόσο από την ανάλυση μας, όσο και από τα πρώτα επιστημονικά έργα περί κυβερνοπολέμου, τότε αυτό το είδος «υπέρβασης εξουσίας» και άρα παρανομίας των κρατικών ιθυνόντων στους πολίτες, δεν συνιστά πράξη κυβερνοπολέμου. Όπως ακριβώς συμβαίνει και με την εκμετάλλευση πολιτών από πολίτες διαμέσου του κυβερνοχώρου. Η τελευταία, ωστόσο, έχει επικρατήσει να καλείται κυβερνοέγκλημα. Αντιθέτως, για την πρώτη περίπτωση, εκμετάλλευσης πολιτών από την κρατική (συχνά ιδιωτικής και δημόσιας σύμπραξης) εξουσία διαμέσου του κυβερνοχώρου, δεν υπάρχει ονομασία. Αποτέλεσμα είναι να μην υφίσταται και συγκεκριμένο ακαδημαϊκό αντικείμενο έρευνας μέχρι σήμερα (Δεκέμβριος, 2011).

Όσον αφορά τη συμφωνία στην ελάχιστο προϋπόθεση της πράξης κυβερνοπολέμου, κοινός τόπος είναι η εμπλοκή δύο κρατών. Το ένα δέχεται την επίθεση, η οποία θα πρέπει να εκτιμάται ότι είναι σε τέτοιο βαθμό οργανωμένη, που δηλώνει ότι συντονίζεται ή τουλάχιστον υποθάλπεται από το άλλο κράτος.

Οπότε, οι υπόλοιπες μη-αποδεκτές πρακτικές στον κυβερνοχώρο δύναται να συνιστούν (πίνακας 11):

- ❖ είτε εγκληματική εκμετάλλευση των πολιτών από πολίτες (Κυβερνο-έγκλημα),
- ❖ είτε εγκληματική εκμετάλλευση του κράτους από πολίτες (Κυβερνο-έγκλημα),
- ❖ είτε εγκληματική εκμετάλλευση των πολιτών από το κράτος (Κυβερνο-έλεγχος).

Πίνακας 11. Μη αποδεκτές πράξεις στον κυβερνοχώρο

ΔΡΑΣΤΗΣ	ΑΠΟΔΕΚΤΗΣ	ΠΡΑΞΗ	TERM
Κράτος	Κράτος	Κυβερνο-πόλεμος	Cyber-War
Πολίτες	Πολίτες - Κράτος	Κυβερνο-έγκλημα	Cyber-Crime
Κράτος	Πολίτες	Κυβερνο-έλεγχος	Cyber-Control

ΒΙΒΛΙΟΓΡΑΦΙΑ

[Α] Βιβλία & Άρθρα

- Άνδρας, Χ. (2008). *Διαδίκτυο - Μια Κοινωνιολογική Προσέγγιση*. [Διδακτορική Διατριβή] Πανεπιστήμιο Μακεδονίας, Τμήμα Πληροφορικής επιστήμης. Θεσσαλονίκη.
- American Psychological Association (1994). *Publication Manual* (4th ed.). Washington DC: APA.
- Arquilla, J., & Ronfeldt D. (1993). Cyberwar is coming!, *Comparative Strategy*, 12(2), 141-165.
- Βέργος, Κ. (2004). *Γεωπολιτική των Εθνών και της Παγκοσμιοποίησης* (Ι. Μάζης, Επιμέλ.). Αθήνα: Παπαζήσης.
- Baker, S., Waterman, S., & Ivanov, G. (2011). *In the Crossfire - Critical Infrastructure in the Age of Cyber War*, Minneapolis: McAfee.
- Berners-Lee, T. (2007). *Το πλαίσιο της Επιστήμης του Web* (Μ. Βαφόπουλος Μετάφρ.). Αθήνα: Ελευθερουδάκης (Το πρωτότυπο έργο δημοσιεύτηκε το 2006).
- Bon (Le), G. (2004). *Ψυχολογία των Μαζών* (Ι. Χριστοδούλου, Μετάφρ.). Θεσσαλονίκη: Ζήτρος (Το πρωτότυπο έργο δημοσιεύτηκε το 1895).
- Brzezinski, Z. (2008). *Η Δεύτερη Ευκαιρία* (Δ. Βούβαλη, Μετάφρ.). Αθήνα: Λιβάνης (Το πρωτότυπο έργο δημοσιεύτηκε το 2007).
- Γιαννακόπουλος, Κ. (2005). *Εικονικές Κοινότητες*. Αθήνα: Παπαζήσης.
- Γκρίτζαλης, Δ. (2008). *Προστασία Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης: Στρατηγικός Σχεδιασμός*, e-Government Forum, Αθήνα: Κοινωνία της Πληροφορίας Α.Ε.
- Γρίβας, Κ. (2008). *Το Τέλος του Πετρελαίου και η Αρχή της Νέας Αμερικανικής Γεωστρατηγικής*. Αθήνα: Λιβάνης.
- Carr, J. (2010). *Inside Cyber Warfare*. Sebastopol CA: O'Reilly Media Inc.
- Castells, M. (2005). *Ο Γαλαξίας του Διαδικτύου* (Ε. Αστερίου, Μετάφρ.). Αθήνα: Καστανιώτης (Το πρωτότυπο έργο δημοσιεύτηκε το 2001).
- Castells, M. & Ibanez, T. (2008). *Ο Νεοαναρχισμός και η Σύγχρονη Κοινωνία* (Π. Καλαμαράς, Επιμέλ.-Μετάφρ.). Αθήνα: Ελευθεριακή Κουλτούρα.
- Chomsky, N. (1994). *Ο Έλεγχος των Μ.Μ.Ε. και η Κατασκευή της Συναίνεσης* (Π. Καλαμαράς, Μετάφρ.). Αθήνα: Ελευθεριακή Κουλτούρα (Το πρωτότυπο έργο δημοσιεύτηκε το 1992).

Chomsky, N. (2000). *Κυριαρχία και Παγκόσμια Τάξη* (Ν. Αλεξίου, Μετάφρ.). Αθήνα: Ελεύθερος Τύπος (Το πρωτότυπο έργο δημοσιεύτηκε το 1999)

Clarke, R., Knake, R. (2010). *Cyberwar – The Next Threat to National Security and What to do about it* New York: HarperCollins Publishers.

Clausewitz, C. (2003). *On War* (M. Howard & P. Paret, edit. – transl.), N. York: Everyman's Library (Το πρωτότυπο έργο δημοσιεύτηκε το 1832).

Coyne, R. (1995). *Που στον κόσμο είναι ο κυβερνοχώρος; Η φαινομενολογία των επικοινωνιών μέσω υπολογιστών* (Β. Βαλάσκα & Ε. Κατσίμπα, Μετάφρ.). Αθήνα: Κάκτος (Το πρωτότυπο έργο δημοσιεύτηκε το 1995).

Δερτούζος, Μ. (1998). *Τι μέλλει γενέσθαι: πώς ο νέος κόσμος της πληροφορίας θ' αλλάξει τη ζωή μας* (Κ. Κουνινιώτη, Μετάφρ.). Αθήνα: Νέα Σύνορα.

Durkheim, E. (χ.ε.). *Κοινωνικές αιτίες της αυτοκτονίας* (Μ. Μαρκάκης, Μετάφρ.). Αθήνα: Γερ. Αναγνωστήδη (Το πρωτότυπο έργο δημοσιεύτηκε το 1898).

Evera Van, S. (2005). *Εισαγωγή στη Μεθοδολογία της Πολιτικής Εεπιστήμης*, (Ε. Συλογίδου, Μετάφρ.). Αθήνα: Ποιότητα (Το πρωτότυπο έργο δημοσιεύτηκε το 1997).

Fitsanakis, J. (2009). *Cells Wars: The Changing Landscape of Communications Intelligence*. RIEAS Research Paper 131, Internet: Ανάκτηση στις 2/2/2010 από: <https://www.rieas.gr>

Freedman, L. (2004). Οι δύο πρώτες γενιές των στρατηγιστών της πυρηνικής εποχής (Ε. Κατσάνης, Μεταφρ.). στο P. Paret (επιμ.), *Οι Δημιουργοί της Σύγχρονης Στρατηγικής*, Θ. Ντόκος (ελ. επισ. επιμ.) (σελ. 869-875). Αθήνα: Κ. Τουρίκη. (Το πρωτότυπο έργο δημοσιεύτηκε το 1986).

Fukuyama, F. (1992). *Το τέλος της ιστορίας και ο τελευταίος άνθρωπο* (Α. Φακατσέλης, Μετάφρ.). Αθήνα: Λιβάνης (Το πρωτότυπο έργο δημοσιεύτηκε το 1993).

Furnell, S. (2006). *Cybercrime-Κυβερνοέγκλημα* (Χ. Τσουραμάνης Επιμέλ. – Φ. Μηλιώνη, Μετάφρ.). Αθήνα: Παπαζήσης (Το πρωτότυπο έργο δημοσιεύτηκε το 2002).

Ζαφειρόπουλος, Κ. (2005). *Πώς Γίνεται Μια Επιστημονική Εργασία; Επιστημονική Έρευνα και Συγγραφή Εργασιών*. Αθήνα: Κριτική.

Zaleski, J. (1997). *Η Ψυχή του Κυβερνοχώρου* (Β. Αδραχτάς, Μετάφρ.). Αθήνα: Αρχέτυπο. (Το πρωτότυπο έργο δημοσιεύτηκε το 2001).

Geers, K. (2008). *Cyberspace and the Changing Nature of Warfare. "Hakin9" E-Book* SC Magazine, 6.

- Gibson, W. (1984). *Νευρομάντης* (Γ. Δεληολάνης, Μετάφρ.). Αθήνα: Αίολος (Το πρωτότυπο έργο δημοσιεύτηκε το 1998).
- Gray, C. (1995). Strategic Culture as Context. *Review of International Studies*, 25-1.
- Gordo-Lopez, A., Parker, I. (2008). *Κυβερνοψυχολογία* (Μ. Ντάβου, Επιμέλ. – Β. Γαλάνη, Μετάφρ.). Αθήνα: Παπαζήσης (Το πρωτότυπο έργο δημοσιεύτηκε το 1999).
- Huges, R. (2009). Towards a Global Regime for Cyber Warfare. *CCDCOE Conference Proceedings*. Internet: Ανάκτηση στις 1/12/2010, από: <https://www.ccdcoe.org/230.html>.
- Haraway, D. (1985). *A Manifesto for Cyborgs: Science, Technology and Socialist Feminism in the 1980s*. Oxford: Blackwell.
- Heidegger, M. (1953). *The Question Concerning Technology* in *Basic Writings*, D. Kell Ed (2^η έκδοση). London: Routledge (Ανατύπωση της πρώτης έκδοσης του 1953).
- Hildreth, S. (2001). Cyberwarfare, *CRS Congressional Research* [Report for U.S. Congress]. Washington D.C.: The Library of Congress.
- Huntington, S. (2002). *The Clash of Civilizations*. Sydney: The Free Press
- Θουκυδίδης (2005). *Ιστορία του Πελοποννησιακού Πολέμου* (Α. Βλάχος, Μετάφρ.). Αθήνα: Εστία (Το πρωτότυπο έργο συγγράφηκε περί το 411 π.Χ).
- Θεοδωρακόπουλος, Π. (2006). *Προπαγάνδα η Ένδοξη*. Αθήνα: Ι. Σιδέρης.
- Joint Staff, Joint Doctrine Division, J-7 (2009). *Department of Defense - Dictionary of Military Terms*. Washington, D.C.: Joint Publication 1-02. Internet: Ανάκτηση στις 4/7/2010, από: http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf
- Καϊτατζή-Γουίτλοκ, Σ. (2003). *Η Επικράτεια των Πληροφοριών*. Αθήνα: Κριτική.
- Καραμπελιάς, Γ. (2009). *Κοινωνιολογία και Ένοπλες Δυνάμεις*. Αθήνα: Νομική Βιβλιοθήκη.
- Καφφές, Γ. (2001). *Τι είναι ο πόλεμος*. Αθήνα: Παπαζήσης.
- Κολοβός, Α. (2004). *Διάστημα και εθνικής ασφάλεια*. Αθήνα: Ποιότητα.
- Κονδύλης, Π. (1998). *Από τον 20ο στον 21ο αιώνα*. Αθήνα: Θεμέλιο.
- Κονδύλης, Π. (1999). *Θεωρία του Πολέμου*. Αθήνα: Θεμέλιο.
- Κοσκινάς, Κ. & Αρσένης, Σ. (Επιμέλ.), (2008). *Δυνητικές κοινότητες και διαδίκτυο*, Αθήνα: Κλειδάριθμος.
- Κουβελιώτης, Κ. (2002). *Φιλοσοφία του Πολέμου και Ηγεσία*. Αθήνα: Επικοινωνίες.

- Κυριαζής, Ν., & Σπανός, Σ. (2000). *Το Πρόσωπο του Πολέμου στον 21ο αιώνα*. Αθήνα: Εστία,
- Κωσταρίδου-Ευκλείδη, Α. (2005). *Μεταγνωστικές Διεργασίες και Αυτό-ρύθμιση*, Αθήνα: Ελληνικά Γράμματα.
- Karatzogianni A. & Robinson, A. (2009). *Power, Resistance and Conflict in the Contemporary World, Social movements, networks and hierarchies*. London: Routledge.
- Kissinger, H. (1994). *Διπλωματία* (Γ. Κοβαλένκο, Μετάφρ.). Αθήνα: Λιβάνη (Το πρωτότυπο έργο δημοσιεύτηκε το 1995).
- Λουδοβίκος, Ν. (2006). *Ορθοδοξία και Εκσυγχρονισμός*. Αθήνα: Αρμός.
- Lèvy, P, (1995). *Δυνητική Πραγματικότητα (Realité Virtuelle) – Η Φιλοσοφία του Πολιτισμού του Κυβερνοχώρου*, (Μ. Καραχάλιος, Μετάφρ.) Αθήνα: Κριτική (Το πρωτότυπο έργο δημοσιεύτηκε το 1999).
- Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington: Center for Strategic and International Studies
- Libicki, M. (1995). *What is Information Warfare*, Center for Advanced Concepts and Technology, Washington: Library of Congress.
- Libicki, M. (2007). *Conquest in Cyberspace - National Security and Information Warfare*. Internet: Ανάκτηση στις 2/3/2009 από: <http://www.rand.com>
- Libicki, M. (2009). *Conquest in Cyberspace - National Security and Information Warfare*. - Santa Monica, Ca: Cambridge University Press The RAND Corporation.
- Lilesiles, S. (2010). *Cyber Warfare: As a Form of Low-Intensity Conflict & Insurgency*,” *CCDCOE Conference Proceedings*. Internet: Ανάκτηση στις 1/12/2010, από: <https://www.ccdcoe.org/229.html>
- Μάζης, Ι. (2006). *Γεωπολιτική προσέγγιση για ένα νέο Ελληνικό Δόγμα*, Αθήνα: Παπαζήσης,
- Μαρκαντωνάτου, Μ., (2009), *Το κράτος και το μονοπώλιο της βίας*. Αθήνα: Παπαζήσης.
- Μαυρόπουλος, Π. (2008). Η παράδοση τριάδα του Κλαούσεβιτς, *Στρατιωτική Επιθεώρηση*, τεύχος Ιουλίου-Αυγούστου, 122-131.
- Μπάκα, Α. (2005). Κοινωνικο-ψυχολογικές θεωρίες για το σύγχρονο πόλεμο: Κριτική Ανασκόπηση. Στο, Δ. Μαρκουλής και Μ. Δικαίου (Επιμ.), *Πολιτική Ψυχολογία, Προβλήματα και Προοπτικές*, (σελ. 77-102). Αθήνα: Τυπωθήτω.

- Μουζέλης, Ν. (1991). *Οργάνωση και Γραφειοκρατία* (3^η έκδοση). (Ε. Σοφούλη, Μετάφρ.) Αθήνα: Α. Μαθιουδάκη & Π. Ανδρονόπουλου (Το πρωτότυπο έργο εκδόθηκε το 1967).
- Μουζέλης, Ν. (2001). *Για έναν εναλλακτικό τρίτο δρόμο*. Αθήνα: Θεμέλιο.
- Mason, J. (2010), *Η Διεξαγωγή της Ποιοτικής Έρευνας* (Ν. Κυριαζή, Επιμέλ. – Ε. Δημητριάδου, Μετάφρ.). Αθήνα: Ελληνικά Γράμματα (Το πρωτότυπο έργο δημοσιεύτηκε το 1996).
- Moskos, C. (1996). *Η Στρατιωτική Κοινωνιολογία στην Αμερική* (Δ. Σμοκοβίτης, Μεταφρ.). Αθήνα: Παπαζήσης (Το πρωτότυπο έργο δημοσιεύτηκε το 1966).
- Moskos, C., Williams, J., & Segal, D. (2000). *The Postmodern Military: Armed Forces after the Cold War*. New York: Oxford University Press.
- Maisonneuve, J. (2001). *Εισαγωγή στην Ψυχοκοινωνιολογία* (Ν. Χρηστάκης, Μετάφρ.). Αθήνα: Τυπωθήτω (Το πρωτότυπο έργο δημοσιεύτηκε το 1973).
- McLuhan, M. (1964). *Understanding Media: the Extensions of Man*. New York: McGraw-Hill.
- Morningstar, C., & Randall Farmer, F. (2003). The Lessons of Lucasfilm's Habitat. *The New Media Reader*. W. Fruin & N. Montfort (Επιμ.). London: The MIT Press. Internet: Ανάκτηση στις 11/9/2011, από: <http://www.fudco.com/chip/lessons.html>
- Moscovici, S., (1999) *Η ψυχανάλυση, η εικόνα της και το κοινό της* (Α. Μαντόγλου, Επιμέλ. – Χ. Κολώνιας, Μετάφρ.). Αθήνα: Οδυσσέας (Το πρωτότυπο έργο δημοσιεύτηκε το 1976).
- Muhammad, S., & Jawad, H. (2010). "Cyber warfare" the truth in a real case, Στο Project Report for Information Security Course, Viiveke Fåk (Επιμ.). Sweden: Linköping Universitetet
- Νεγροπόντης, Ν. (1995). *Ψηφιακός Κόσμος* (Α. Κατσικάς, Μετάφρ.). Αθήνα: Καστανιώτη (Το πρωτότυπο έργο εκδόθηκε το 1995).
- Ντόκος, Θ., & Τσάκωνας, Π. (2005). *Στρατηγική εθνικής ασφαλείας*. Αθήνα: Παπαζήσης.
- Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. *In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April*. Reading: Academic Publishing Limited, (σελ. 267-270). Internet: Ανάκτηση στις 1/12/2010, από: <http://www.ccdcoe.org/205.html>
- Παπαστάμου, Σ. (1989). *Εγχειρίδιο Κοινωνικής Ψυχολογίας*. Αθήνα: Οδυσσέας.
- Παπαστάμου, Σ. (1995). *Κοινωνικές αναπαραστάσεις*. Αθήνα: Οδυσσέας.

- Πλάτωνας (χ.έ.). *Πολιτεία* (Ι. Γρύπαρη, Μετάφρ.). Αθήνα: Βιβλιοθήκη Αρχαίων Ελλήνων Συγγραφέων (Το πρωτότυπο έργο συγγράφηκε περί το 380 π.Χ).
- Πολυμενόπουλος, Α. (2001). *Ο ψηφιακός κόσμος στην εθνική άμυνα*. Αθήνα: Υπουργείο Εθνικής Άμυνας - Ελληνικά Γράμματα.
- Peel, R. (2004), The Internet and Language Use: A Case Study in the United Arab Emirates, Higher Colleges of Technology, *U.A.E - International Journal on Multicultural Societies* (IJMS), 6(1), 79-91, Internet: Ανάκτηση στις 19/10/2010, από: <http://www.unesco.org/shs/ijms>
- Rattray, G. (2001). *Strategic Warfare in Cyberspace*. Cambridge MA: MIT Press
- Rheingold, H. (2000). *The Virtual Community: Homesteading oh the Electronic Frodier*. Internet: Ανάκτηση στις 12/1/2006, από: <http://www.rheingold.com/vc/book/>
- Rifkin, J. (1996). *Το τέλος της εργασίας και το μέλλον της* (Γ. Κοβαλένκο, Μετάφρ.). Αθήνα: Λιβάνης (Το πρωτότυπο έργο εκδόθηκε το 1995).
- Robins, K., & Webster, F. (2002). *Η εποχή του τεχνοπολιτισμού: Από την κοινωνία της πληροφορίας στην εικονική ζωή*. (Κ. Μεταξιά, Μεταφρ.). Αθήνα: Καστανιώτη. (Το πρωτότυπο έργο δημοσιεύτηκε το 1999).
- Σκαρπέλος, Γ. (1999). *Terra Virtualis. Η κατασκευή του κυβερνοχώρου*. Αθήνα: Θεμέλιο.
- Σφακιανάκης, Μ. (2001). *Προσομοίωση και Εφαρμογές*. Αθήνα: Πατάκης
- Schnapper, D. (2008). *Η κοινωνική ενσωμάτωση*, (Ξ. Γιαταγάνας, Μετάφρ.). Αθήνα: Κριτική (Το πρωτότυπο έργο δημοσιεύτηκε το 2004).
- Sherman, W., & Craig, A. (2003). *Understanding Virtual Reality*. San Francisco: Morgan Kaufmann.
- Spykman, N. (2004). *Η Γεωγραφία της Ειρήνης* (Π. Κελάνδριας, Μετάφρ.). Αθήνα: Παπαζήσης (Το πρωτότυπο έργο δημοσιεύτηκε το 1944).
- Stavridis, J. (2010). *Cyberspace Innovation in a Networked World* [παρουσίαση]. San Diego: Saceur Address to Armed Forces Communications and Electronics Association.
- Stonier, T. (1984). *Ο πλούτος των πληροφοριών. Το προφίλ της μεταβιομηχανικής οικονομίας* (Τ. Νικηφόρου, Μετάφρ.). (2^η έκδοση). Θεσσαλονίκη: Αγροτικές Συνεταιριστικές Εκδόσεις Α.Ε.
- Τσαούσης, Δ. (2006). *Κοινωνική Δημογραφία* (2^η έκδοση). Αθήνα: Gutenberg.
- Τεγόπουλου-Φυτράκη, *Ελληνικό λεξικό* (4^η έκδ.). (1991). Αθήνα: Αρμονία.

Τζανή, Μ. (2005), *Μεθοδολογία Έρευνας Κοινωνικών Επιστημών* [Πανεπιστημιακές Σημειώσεις]. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, Παιδαγωγικό Τμήμα Δημοτικής Εκπαίδευσης, Εργαστήριο «Βιοφυσικό Περιβάλλον: Νευροεπιστήμες και Μάθηση». Internet: Ανακτήθηκε στις 07/11/2010, από: <http://benl.primedu.uoa.gr/database1/method.pdf>

Τζου Σουν, *Η τέχνη του πολέμου* (Δ. Παυλάκης Μετάφρ.). Αθήνα: Φόρμιγξ (1997) (Το πρωτότυπο έργο συγγράφηκε περίπου τον 5^ο αιώνα π.Χ).

Taylor, P. (2004). *Πόλεμος και Διεθνείς Σχέσεις στην εποχή της Πληροφορίας* (Κ. Περεζούς, Μετάφρ.). Αθήνα: Παπαζήση (Το πρωτότυπο έργο δημοσιεύτηκε το 1997).

Tikk, E. (2010). "Global Cyber Security - Thinking About The Niche for NATO." *SAIS Review*. 30(2), (σελ. 105-119). Internet: Ανακτήθηκε στις 22/03/2011, από: www.ccdcoe.org/205.html

Toffler, A., Dyson, E., Gilder, G., & Keyworth, G. (1994). *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age*. Washington, DC: Progress and Freedom Foundation.

Virilio, P., & Lotringer, S. (1997). *Καθαρός Πόλεμος* (Α. Δρατζίδης, Μετάφρ.). Θεσσαλονίκη: Νησίδες. (Το πρωτότυπο έργο δημοσιεύτηκε το 1983).

Watts, S. (2010). Combatant Status and Computer Network Attack, *Virginia Journal of International Law*, 50(2), 400.

Weber, M. (1984). *Η Προτεσταντική Ηθική και το Πνεύμα του Καπιταλισμού*, (Μ. Κυπραίου, Μεταφ.). Αθήνα: Gutenberg. (Το πρωτότυπο συγγράφηκε το 1905 και εκδόθηκε μεταφρασμένο στην αγγλική, από το Talcott Parsons, το 1930).

Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*. John Wiley: New York.

Φίλιας, Β. (1977). *Εισαγωγή στη Μεθοδολογία και τις τεχνικές των Κοινωνικών Ερευνών*. Αθήνα: Gutenberg

Φωτίου, Π. (2008). Δίκαιο Ένοπλων Συγκρούσεων. *Στρατιωτική Επιθεώρηση*, τεύχος Ιουλίου-Αυγούστου, 62-85.

Χουλιάρας, Α. (2004). *Γεωγραφικοί μύθοι της Διεθνούς Πολιτικής*, Αθήνα: Ροές

Χρυσόχου, Ξ. (2008). *Κοινωνικές αναπαραστάσεις*. [Πανεπιστημιακές σημειώσεις]. Πάντειο Πανεπιστήμιο, Τμήμα Ψυχολογίας, χειμερινό εξάμηνο 2007-2008, Αθήνα. Internet: Ανακτήθηκε στις 01/09/2010, από: <http://library.panteion.gr:8080/dspace/bitstream/123456789/422/1/xrysoxoou.pdf>

[B] Ιστοσελίδες

Απόδημος, “Η καλλίτερη υπηρεσία του κόσμου και μορφές ηλεκτρονικού εγκλήματος”,
http://www.apodimos.com/arthra/08/Mar/TO_HLEKTRONIKO_EGGLHMA_TOY_INTERNET_KAI_MORFES_TOY/index.htm

Agence France-Presse & United Press International – Space daily – Space war – Cyberwars, “More 'Stuxnet' cyberattacks feared”,
http://www.spacedaily.com/reports/More_Stuxnet_cyberattacks_feared_999.html

Agence France-Presse & United Press International – Space daily – Space war – Cyberwars, “Iran says Duqu malware under 'control'”,
<http://www.spacewar.com/cyberwars.html>.

Βήμα (To), “Γερμανία: Αυστηροί κανόνες προστασίας των προσωπικών δεδομένων στο Διαδίκτυο”, <http://www.tovima.gr/default.asp?pid=2&ct=85&artid=370782>

B.B.C., “Israel and foes in internet war”,
http://news.bbc.co.uk/2/hi/middle_east/8079774.stm

B.B.C., “Should Obama's 'internet kill switch' power be curbed?”,
<http://www.bbc.co.uk/news/world-us-canada-11736545>

C.N.N., “Cyberwarfare finds a captive audience”,
<http://edition.cnn.com/2011/TECH/web/06/23/hacks/index.html?iref=allsearch>

C.N.N., “Cyberwarfare finds a captive audience”,
<http://edition.cnn.com/2011/TECH/web/06/23/hacks/index.html?iref=allsearch>

C.N.N., “Virus infects program that controls U.S. drones”,
<http://edition.cnn.com/2011/10/10/us/drone-program-virus/index.html?iref=allsearch>

C.N.N., “Mafiaboy' breaks silence, paints 'portrait of a hacker'”,
<http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html?iref=allsearch>

C.N.N., “Experts: Internet filtering and censorship rife”,
<http://edition.cnn.com/2008/TECH/08/21/internet.filtering/index.html?iref=allsearch>

Cyberspace Science and information Intelligence Research Group, “Definitions”,
<http://www.ioc.ornl.gov/>

Δ.Ο.Λ.-Newsroom, “Κυβερνήσεις και οργανισμοί θύματα της «μητέρας όλων των κυβερνοεπιθέσεων»”, <http://news.in.gr/science-technology/article/?aid=1231122702>

Δ.Ο.Λ.-Newsroom, “Προφυλακιστέος ο Άσαντζ με απόφαση βρετανικού δικαστηρίου” <http://news.in.gr/world/article/?aid=1231070319>

Δ.Ο.Λ.-Newsroom, “Το WikiLeaks αναστέλλει τη δημοσιοποίηση διαβαθμισμένων εγγράφων”, <http://news.in.gr/world/article/?aid=1231134444>

Δ.Ο.Λ.-Newsroom, “Τον Αύγουστο τα εγκαίνια του ιρανικού «εθνικού Διαδικτύου»”, <http://news.in.gr/science-technology/article/?aid=1231116331>

Δ.Ο.Λ.-Newsroom, “Το Street View της Google μπαίνει τώρα και σε κτίρια”, <http://news.in.gr/science-technology/article/?aid=1231135188>

Δ.Ο.Λ.-Newsroom, “Νέα υπόθεση κυβερνοκατασκοπείας σε βάρος εργολάβων του αμερικανικού στρατού”, <http://news.in.gr/science-echnology/article/?aid=1231135588>

Δ.Ο.Λ.-Newsroom, “Εκτός λειτουργίας δικτυακοί τόποι του Ισραήλ έπειτα από απειλές των Anonymous”, <http://news.in.gr/science-technology/article/?aid=1231136344>

Department of Homeland Security (US), “About the National Cybersecurity and Communications Integration Center (NCCIC)”, http://www.dhs.gov/xabout/structure/gc_1306334251555.shtm

Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, “Ιστορία Εικονικής Πραγματικότητας”, http://cgi.di.uoa.gr/~std02199/Virtual_Reality_History.html

ΕΛ.ΑΣ., “Υποδιεύθυνση Δίωξης Ηλεκτρονικούς Εγκλήματος”, http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=

Ε.Υ.Π., “Εθνικό CERT”, <http://www.nis.gr/portal/page/portal/NIS/NCERT>

Ευρωπαϊκή Ένωση, “Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats”, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246&format=HTML&aged=0&language=EN&guiLanguage=en>

Economist, “Cyberwar - War in the fifth domain”, www.economist.com/node/16478792.

Federation of American Scientists, “Unmanned Aerial Vehicles (UAVs)”, <http://www.fas.org/irp/program/collect/uav.htm>

Foxnews, “Crisis in Iran Sparks Global Guerrilla Cyberwar”, <http://www.foxnews.com/story/0,2933,526627,00.html>

Free Dictionary, “Cyberspace Defined” Free Dictionary, <http://www.thefreedictionary.com/Cyberspace+Defined>

Global Public Square, “Cybertheft could destroy the U.S. economy”, <http://globalpublicsquare.blogs.cnn.com/2011/08/15/cybertheft-could-destroy-the-u-s-economy/?iref=allsearch>

Google, “Street View: Explore the world at street level”,
http://maps.google.com/intl/en/help/maps/streetview/#utm_campaign=en&utm_medium=van&utm_source=en-van-na-us-gns-svn

GovInfoSecurity, “Aggressive Cyber Offense Questioned”,
http://www.govinfosecurity.com/articles.php?art_id=1853&search_keyword=Martin+Libicki&search_method=exact

Guardian, “Cyberwar could spare bombs”,
<http://www.guardian.co.uk/world/1999/nov/05/balkans>

I.S.O., “Information technology -- Security techniques -- Code of practice for information security management”,
http://www.iso.org/iso/catalogue_detail?csnumber=50297

ITU, “International Telecommunication Union - Measuring the Information Society”,
<http://www.itu.int/ITU->

Καθημερινή, “Ο κυβερνοχώρος ως νέο πεδίο μάχης κρατών και κινημάτων”,
http://news.kathimerini.gr/4dcgi/_w_articles_ell_2_23/12/2010_426620

K.S.L., “Utah's NSA spy center will house data, not analysts”,
<http://www.ksl.com/?nid=148&sid=13908592>

McAfee, “Revealed: Operation Shady RAT”,
<http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>

Media News Line, “BBC: World's largest broadcaster & Most trusted media brand”,
<http://www.medianewsline.com/news/151/ARTICLE/4930/2009-08-13.html>.

NATO Cooperative Cyber Defence Centre of Excellence, “Cyber Defence”,
<http://www.ccdcoe.org>

Nooz, “Το τέλος της εποχής του Ίντερνετ στην Τουρκία”,
<http://www.nooz.gr/tech/to-telos-tis-epoxis-tou-internet-stin-tourkia>

Οικονομικό Πανεπιστήμιο Αθηνών, “Simulation”,
<http://dmst.aueb.gr/dds/intro.pascal/appl/simul.htm>

Omedia Web, “William Lynn, U. S. Deputy Secretary of Defense”,
<http://media.omediaweb.com/rsa2011/keynotes/webcast.htm?id=1-6>

Πληροφοριακό Κέντρο Πληροφόρησης των Ηνωμένων Εθνών, “Παγκόσμια ημέρα ελευθερίας του τύπου – 3/5/11”,
http://www.unric.org/el/index.php?option=com_content&view=article&id=26606:-3-2011&catid=4:latest-news&Itemid=18

Public Broadcasting Service, “Cyberwar! The Warnings?”,
<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html>

RAND CO., “Research Staff Profiles” <http://www.rand.org/about/people.html>

Reuters, “Misunderstanding Cyberwar in Georgia”,
<http://www.reuters.com/article/reutersEdge/idUSGOR66065320080816?pageNumber=3&virtualBrandChannel=0>

ΣΥ.ΡΙ.ΖΑ., “Ένας καλός πόλεμος είναι θέμα ψυχολογίας ή αλλιώς μαύρης προπαγάνδας”, <http://syryza-vyrona.pblogs.gr/2007/12/paihnia-toy-myaloy.html>

Science Enhanced Network Domains, “Cyberspace Science and Cyberspace Security Science: Why Both?”, <http://sendsonline.org/>

Spacewar - Cyberwar, “Internet traffic hijacked to China”,
http://www.spacewar.com/reports/Internet_traffic_hijacked_to_China_servers_says_US_report_999.html,

Strategy-Geopolitics, “Κυβερνοάσκησις στις ΗΠΑ”
<http://strategy-geopolitics.blogspot.com/2008/02/cyber-storm.html>

Τρομακτικό, “Νόμος-παρωδία για το διαδίκτυο στην Τουρκία”,
http://tro-ma-ktiko.blogspot.com/2011/05/blog-post_2730.html#more

Telegraph co., “Πόλεμος Ρωσίας – Γεωργίας”,
<http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> - <http://www.stopgeorgia.ru>

Toolbox, “Cyber War Israel and Hamas”,
<http://it.toolbox.com/blogs/managing-infosec/cyber-war-israel-and-hamas-29096>

United Nations, “UN - Charter”, <http://www.unric.org/el/about-un-greek/14>

Washington Times, “Cyber Storm III aims to protect against real thing”,
<http://www.washingtontimes.com/news/2010/sep/28/cyber-storm-iii-aims-protect-against-real-thing/>

Wikileaks, “What is Wikileaks?”, <http://wikileaks.org/About.html>

Wikipedia, “Cyberspace”, <http://en.wikipedia.org/wiki/Cyberspace>

Wikipedia, “Αραβική Άνοιξη”,
http://el.wikipedia.org/wiki/%CE%91%CF%81%CE%B1%CE%B2%CE%B9%CE%BA%CE%AE_%CE%86%CE%BD%CE%BF%CE%B9%CE%BE%CE%B7

ΠΑΡΑΡΤΗΜΑ*

i] Αντικείμενο. Το περιεχόμενο του παρόντος παραρτήματος αποτελείται από το σύνολο των κειμένων - τεκμηρίων (corpus), τα οποία συλλέξαμε από τις δύο πηγές μας, επεξεργασμένο έτσι, ώστε να δείχνουμε ευκρινώς τα ευρήματά μας. Τα τελευταία συνιστούν το σύνολο των μονάδων αναφοράς (items), τα οποία με τη σειρά τους μας οδήγησαν στη σύνθεση των θεματικών μας κατηγοριών.

ii] Οδηγός Ανάγνωσης. Όσον αφορά στα κείμενα, ο στόχος που θέσαμε ήταν η σαφής εικόνα του αυθεντικού κειμένου που συλλέξαμε και των δικών μας παρεμβάσεων (επεξεργασίας) σε αυτό. Έτσι, όλα τα κείμενα έχουν κοινή μορφοποίηση, ως εξής:

- Ξεκινούν με τον *Αύξοντα αριθμό* «μητρώου» (TimesNewRoman-12-Red in Blue and Bold).
- Δίπλα ακριβώς βρίσκεται η *Ημερομηνία* (TimesNewRoman-12-Black in Blue).
- Στη συνέχεια, αμέσως από κάτω, ο *Τίτλος* (Verdana 24,5-Black).
- Παρακάτω, το *Κείμενο* αυτούσιο, με την ακόλουθη επεξεργασία:
 - Η σημασιολογική αναφορά μαρκαρισμένη σε κίτρινο φόντο.
 - Όπου ακριβώς τελειώνει η σημασιολογική (ή εννοιολογική) ενότητα: η ένδειξη [**1cm**]. Δηλαδή ο αύξων αριθμός -ενιαίος για όλες τις αναφορές, ανεξαρτήτου θεματικής κατηγορίας και μοναδικός για κάθε μέσο (αρχίζει από την αρχή για το BBC & CNN)- και δίπλα ο συμβολισμός (δύο γράμματα) της θεματικής κατηγορίας, ως εξής:

ΔΙΕΙΣΔΥΣΗ: **cm**, ΥΠΟΔΟΜΕΣ: **in**, ΛΟΓΟΚΡΙΣΙΑ: **wa**, ΠΡΟΠΑΓΑΝΔΑ: **wb**.

- Τέλος, κάθε κείμενο ολοκληρώνεται με την *Ηλεκτρονική Διεύθυνσή* του, προς επιβεβαίωση της ύπαρξής του (TimesNewRoman-9-Blue in Blue & Underline).

ΠΑΡΑΤΗΡΗΣΕΙΣ. Στο BBC μετά τον α/α και την ημερομηνία αναγράφεται και η ώρα τελικής ενημέρωσης, κάτι που στο CNN δεν ήταν διαθέσιμο. Η μορφοποίηση των τίτλων, την οποία αναφέρουμε, ισχύει μόνο για το BBC και αυτό όχι επειδή την επιλέξαμε, αλλά διότι αυτή χρησιμοποιεί το ίδιο. Ωστόσο, το CNN δεν διατηρούσε μια ενιαία. Τέλος, όταν τα κίτρινα φόντα, κατά την επεξεργασία, τελειώνουν χωρίς ένδειξη αναφοράς, αυτό σημαίνει ότι η σημασιολογική ενότητα τελειώνει παρακάτω.

iii] Περιεχόμενα: Πίνακας κειμένων BBC - Πίνακας ευρημάτων BBC - Κείμενα BBC – Πίνακας κειμένων CNN - Πίνακας ευρημάτων CNN - Κείμενα CNN.

* Ακολουθεί στον επόμενο (δεύτερο) τόμο...

ΠΑΡΑΡΤΗΜΑ

i] Αντικείμενο. Το περιεχόμενο του παρόντος παραρτήματος αποτελείται από το σύνολο των κειμένων - τεκμηρίων (corpus), τα οποία συλλέξαμε από τις δύο πηγές μας, επεξεργασμένο έτσι, ώστε να δείχνουμε ευκρινώς τα ευρήματά μας. Τα τελευταία συνιστούν το σύνολο των μονάδων αναφοράς (items), τα οποία με τη σειρά τους μας οδήγησαν στη σύνθεση των θεματικών μας κατηγοριών.

ii] Οδηγός Ανάγνωσης. Όσον αφορά στα κείμενα, ο στόχος που θέσαμε ήταν η σαφής εικόνα του αυθεντικού κειμένου που συλλέξαμε και των δικών μας παρεμβάσεων (επεξεργασίας) σε αυτό. Έτσι, όλα τα κείμενα έχουν κοινή μορφοποίηση, ως εξής:

- Ξεκινούν με τον **Αύξοντα αριθμό** «μητρώου» (TimesNewRoman-12-Red in Blue and Bold).
- Δίπλα ακριβώς βρίσκεται η **Ημερομηνία** (TimesNewRoman-12-Black in Blue).
- Στη συνέχεια, αμέσως από κάτω, ο **Τίτλος** (Verdana 24,5-Black).
- Παρακάτω, το **Κείμενο** αυτούσιο, με την ακόλουθη επεξεργασία:
 - ο Η σημασιολογική αναφορά μαρκαρισμένη σε κίτρινο φόντο.
 - ο Όπου ακριβώς τελειώνει η σημασιολογική (ή εννοιολογική) ενότητα: η ένδειξη [**1cm**]. Δηλαδή ο αύξων αριθμός -ενιαίος για όλες τις αναφορές, ανεξαρτήτου θεματικής κατηγορίας και μοναδικός για κάθε μέσο (αρχίζει από την αρχή για το BBC & CNN)- και δίπλα ο συμβολισμός (δύο γράμματα) της θεματικής κατηγορίας, ως εξής:

ΔΙΕΙΣΔΥΣΗ: **cm**, ΥΠΟΔΟΜΕΣ: **in**, ΛΟΓΟΚΡΙΣΙΑ: **wa**, ΠΡΟΠΑΓΑΝΔΑ: **wb**.

- Τέλος, κάθε κείμενο ολοκληρώνεται με την **Ηλεκτρονική Διεύθυνσή** του, προς επιβεβαίωση της ύπαρξής του (TimesNewRoman-9-Blue in Blue & Underline).

ΠΑΡΑΤΗΡΗΣΕΙΣ. Στο BBC μετά τον α/α και την ημερομηνία αναγράφεται και η ώρα τελικής ενημέρωσης, κάτι που στο CNN δεν ήταν διαθέσιμο. Η μορφοποίηση των τίτλων, την οποία αναφέρουμε, ισχύει μόνο για το BBC και αυτό όχι επειδή την επιλέξαμε, αλλά διότι αυτή χρησιμοποιεί το ίδιο. Ωστόσο, το CNN δεν διατηρούσε μια ενιαία. Τέλος, όταν τα κίτρινα φόντα, κατά την επεξεργασία, τελειώνουν χωρίς ένδειξη αναφοράς, αυτό σημαίνει ότι η σημασιολογική ενότητα τελειώνει παρακάτω.

iii] Περιεχόμενα. Η παρούσα εισαγωγή – Πίνακας κειμένων BBC – Πίνακας ευρημάτων BBC – Κείμενα BBC / Πίνακας κειμένων CNN – Πίνακας ευρημάτων CNN – Κείμενα CNN.

Πίνακας κειμένων BBC

A	ΣΕΛ.	ΗΜΕΡ/ΝΙΑ	ΤΙΤΛΟΣ	ΛΕΞΕΙΣ
1	156	14/7/2011	Pentagon admits suffering major cyber attack in March	0
2	157	17/6/2011	US builds net for cyber war games	458
3	159	14/6/2011	Lulz attacks: US orders review as Senate site hacked	246
4	160	13/6/2011	IMF cyber attacks signal new spying era	462
0	162	2/6/2011	Cyber war's 'death and destruction'	0
5	162	1/6/2011	US Pentagon to treat cyber-attacks as 'acts of war'	684
6	164	17/3/2011	US cyber war defences 'very thin', Pentagon warns	309
7	166	16/2/2011	Cyber attacks 'acts of war' - Sir Richard Mottram	735
8	168	16/2/2011	Cyber war threat exaggerated claims security expert	897
0	172	4/2/2011	Calls for 'rules of engagement' for cyber conflict	0
0	172	3/2/2011	US cyber warfare expert on threats which exist now	0
9	172	17/1/2011	Risks of cyber war 'over-hyped' says OECD study	556
10	174	14/1/2011	Tunisia protests: Cyber war mirrors unrest on streets	1.119
11	178	16/12/2010	EU could turn to 'crowd sourcing' in cyber crime fight	684
12	180	14/12/2010	UK Government websites may be next pro-Wikileaks focus	650
0	183	10/12/2010	The conflict between Wikileaks supporters and the companies	0
13	183	9/12/2010	Why are hacktivists 'Anonymous' defending WikiLeaks?	731
14	186	24/11/2010	Should Obama's 'internet kill switch' power be curbed?	1.181
15	191	4/11/2010	Europe simulates total cyber war	240
16	192	14/10/2010	Call to define rules of cyber war	484
17	193	21/6/2010	Defence review to look at all potential conflicts - Fox	428
18	195	17/6/2010	Cyber-war a growing threat warn experts	810
19	198	15/3/2010	Meet US Cybercom: Why the US is fielding a cyber army	1.090
20	201	11/2/2010	How Iran's political battle is fought in cyberspace	783
21	203	17/11/2009	Age of cyber warfare is 'dawning'	500

22	205	24/6/2009	What rules apply in cyber-wars?	654
0	207	22/6/2009	West 'seeks Iran disintegration'	0
23	208	15/6/2009	Israel and foes in internet war	730
24	210	31/3/2009	The Tech Lab: Ken Silva	914
25	213	14/8/2008	Caucasus foes fight cyber war	740
26	216	14/5/2008	Estonian cyber defence hub set up	157
27	217	24/4/2008	Hackers warn high street chains	904
28	219	25/1/2008	Estonia fines man for 'cyber war'	423
29	221	17/5/2007	Estonia hit by 'Moscow cyber war'	616
30	223	17/5/2006	Web attacks end anti-spam effort	408
31	224	12/2/2006	'Cyber Storm' tests US defences	196
32	225	4/12/2005	Militants' new tack in cyber war	338
33	226	21/3/2003	Anti-war hackers target websites	408
34	228	13/3/2003	Indian hackers target Pakistan	256
35	229	7/2/2003	US ponders cyber war plans	698
36	231	17/4/2002	Indian hacker turns cyber cop	460
37	233	23/10/2001	Hacktivists take sides in war	819
38	236	7/3/2001	Hamas hit by porn attack	489
39	237	26/10/2000	Israel under cyber attack	199
40	238	1/9/2000	Draskovic website hoax	311
41	239	7/8/2000	Taiwan plays cyber war games	200
42	240	23/3/2000	Liberian radio ban lifted	288
43	241	18/8/1999	World: Asia-Pacific Timor activists warn of cyber war	439
44	243	4/8/1999	Sci/Tech China accused of cyber war	306
45	244	1/3/1999	World: Africa Eyewitness: Reporting the war in the Horn	739
46	246	7/2/1999	World: Asia-Pacific: China casts a cyber net	335
47	247	1/2/1999	Middle East: Teenage hacker 'destroys anti-Israeli Website'	387

Πίνακας ευρημάτων BBC

A	Σελ.	Διείσδυση	Υποδομές	Λογοκρισία	Προπαγάνδα	Σύνολο
1	156	2	2	0	0	4
2	157	1	0	0	0	1
3	159	0	0	0	1	1
4	160	2	2	0	0	4
0	162	RADIO 07:19				0
5	162	2	2	0	0	4
6	164	2	0	0	0	2
7	166	2	0	0	0	2
8	168	0	3	1	2	6
0	172	VIDEO 10:05				0
0	172	VIDEO 00:52				0
9	172	2	1	0	2	5
10	174	0	1	4	4	9
11	178	0	0	0	0	0
12	180	0	1	0	2	3
0	183	VIDEO 02:41				0
13	183	0	0	1	2	3
14	186	3	3	2	1	9
15	191	0	1	0	0	1
16	192	2	1	0	0	3
17	193	0	1	0	0	1
18	195	0	3	0	0	3
19	198	1	4	0	0	5
20	201	0	0	2	1	3
21	203	0	2	0	0	2
22	205	0	1	1	1	3

0	207	VIDEO 02:10				0
23	208	3	0	0	2	5
24	210	0	3	1	0	4
25	213	1	4	0	1	6
26	216	0	1	0	0	1
27	217	2	1	1	0	4
28	219	0	1	0	1	2
29	221	0	2	0	0	2
30	223	2	1	0	0	3
31	224	0	1	0	1	2
32	225	0	0	0	2	2
33	226	2	0	0	3	5
34	228	1	1	0	1	3
35	229	1	3	1	0	5
36	231	0	2	0	0	2
37	233	1	2	0	2	5
38	236	0	0	0	3	3
39	237	0	2	0	0	2
40	238	0	0	0	4	4
41	239	0	2	0	0	2
42	240	0	0	2	0	2
43	241	0	1	0	0	1
44	243	0	0	4	0	4
45	244	0	0	1	0	1
46	246	1	0	1	0	2
47	247	0	0	1	3	4
		33	55	23	39	<u>150</u>

BBC: KeyWord “cyberwar” - Corpus: 47, Items: 150 and 93 pages.

1. 14 July 2011 Last updated at 23:01 GMT

Pentagon admits suffering major cyber attack in March



The deputy defence secretary said future cyber attacks could even cause deaths

The Pentagon has admitted it suffered a major cyber attack in which thousands of files were taken by foreign hackers.

Deputy Defence Secretary William Lynn said that in a March attack and other breaches, hackers had taken information on "our most sensitive systems".

The admission came as the Pentagon rolled out a strategy for strengthening US cyber capabilities and addressing threats and attacks in cyberspace.

The plan would treat cyberspace in a similar manner to land, air and sea.

"In the 21st Century, bits and bytes can be as threatening as bullets and bombs," **Mr Lynn said**, unveiling the plan.

In a speech at National Defense University in Washington, Mr Lynn said about 24,000 files containing Pentagon data were stolen from a defence industry computer network in March, marking one of the largest cyber attacks in US history. [1cm]

Extracting files

He said at least one attack - a previously revealed 2008 penetration of classified computer systems [2cm]- had come from a foreign intelligence service, and in an interview ahead of the speech said the Pentagon believed the March attack had been perpetrated by a foreign government.

Previous cyber attacks have been blamed on China or Russia.

"We have a pretty good idea" who did it, he told the Associated Press news agency.

In his speech, he said some of the stolen data was "mundane, like the specifications for small parts of tanks, airplanes, and submarines.

"But a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols," he said.

Mr Lynn said cyber attacks in the future would not only focus on stealing data but also damaging US defences or even causing deaths. [3in]

He added that virtual intruders have previously tried to extract files related to missile tracking systems and the Joint Strike Fighter.

Though nations like China and Russia have been blamed for many previous cyber attacks, the Pentagon fears terrorist groups could eventually strike American computer networks and steal data.

"Keystrokes originating in one country can impact the other side of the globe in the blink of an eye," Mr Lynn said.

'Too aggressive'

He added that information technology has become so important to the US government that it "virtually guarantees that future adversaries will target our dependence on it". [4in]

Mr Lynn said the **Department of Defense Strategy for Operating in Cyberspace** was defensive, countering earlier criticism that the strategy might be too aggressive.

In a **release** accompanying the new strategy, Defence Secretary Leon Panetta said it was "critical to strengthen our cyber capabilities to address the threats we're facing".

The news comes one month after the Pentagon said it was building its own "scale model" of the internet to carry out cyber war games.

<http://www.bbc.co.uk/news/world-us-canada-14157975>

2. 17 June 2011 Last updated at 14:07 GMT

US builds net for cyber war games



The US system will be used as a test bed for internet security projects

The United States government is building its own "scale model" of the internet to carry out cyber war games.

Several organisations, including the defence company Lockheed Martin, are working on prototypes of the "virtual firing range".

The system will allow researchers to simulate attacks by foreign powers and from **hackers** based inside the US.

More than \$500m (£309m) has been allocated by the Department of Defense to develop "cyber technologies".

The National Cyber Range project is being overseen by the Defense Advance Research Projects Agency (Darpa), which was also involved in **early network research that led to the internet**.

When ready, it will function as a test-bed for defensive and possibly offensive technologies such as **network protection systems**. Having a controllable mini-internet would allow researchers to carry-out experiments "in days rather than the weeks it currently takes," Darpa spokesman Eric Mazzacone told the Reuters news agency.

Unlike the real internet, the in-house version could be wiped or reset between tests, explained Mr Mazzacone.

Development of the National Cyber Range is currently in the hands of several organisations, including Johns Hopkins University in Baltimore and Lockheed Martin.

One of their prototypes will be selected to go into operation later in the year.

Act of war

The United States has been gradually increasing funding for internet security-related projects.



US defence secretary Robert Gates said that the country was under almost constant cyber attacks

In 2008, the US military was the subject of a serious cyber attack when part of its network became infected by a worm known as agent.btz [5cm]

President Obama, in May 2009, declared the cyber threat to be one of the "most serious" challenges facing the country.

Since then, his government claims to have been the subject of several attempted attacks, originating from overseas.

Lockheed Martin, one of the contractors involved in the National Cyber Range project was itself the subject of a security breach in May 2011.

Earlier this month, the Pentagon said it planned to publish proposals to categorise cyber attacks as acts of war.

<http://www.bbc.co.uk/news/technology-13807815>

3. 14 June 2011 Last updated at 01:34 GMT

Lulz attacks: US orders review as Senate site hacked



Lulz Security said the intrusion was "just-for-kicks"

US officials said they have ordered a security review after hackers managed to break into the Senate website at the weekend.

An official said the incident had been "inconvenient", but had not compromised the security of the staff.

The confirmation came after Lulz Security, a loosely aligned group of hackers, said it had carried out the attack for fun and **posted files online**.

Lulz has previously targeted Sony, Nintendo and Fox News.

Senate Deputy Sergeant-at-Arms Martina Bradford said the hacking had been noticed at the weekend, and that officials were now reviewing all the sites hosted on **Senate.gov**.

"Specifically, there is no individual user account information on the server supporting senate.gov that could have been compromised," she said in a statement.

Lulz Security posted files online which indicated they had been in the Senate network. However, none of the files appeared to be sensitive.

"We don't like the US government very much," [6wb] Lulz Security said at the top of a release.

"This is a small, just-for-kicks release of some internal data from Senate.gov - is this an act of war, gentlemen? Problem?" it added.

The US recently said it would consider cyber attacks an "act of war", and reserved the right to respond to attacks with conventional means if they were found to have been orchestrated by a nation state.

Lulz is a reference to internet-speak for "laugh out loud".

<http://www.bbc.co.uk/news/world-us-canada-13758361>

4. 13 June 2011 Last updated at 20:42 GMT

IMF cyber attacks signal new spying era



Before the IMF, Sony and Citibank were also victims of cyber attacks

We don't know who hacked into the International Monetary Fund or whether they got away with anything.

But within weeks, the Pentagon is to announce plans to treat some cyber attacks as an act of war.

A Pentagon spokesman **said at the beginning of this month**: "A response to a cyber-incident or attack on the US would not necessarily be a cyber-response. All appropriate options would be on the table."

When it comes to sophisticated attacks many think the finger points in one direction: towards China.

I've just stumbled across **a fascinating US government report** on the problem. OK, it's a couple of years old. But I've never read it before so there's a chance some of you might have missed it as well.

It argues that many recent intrusions must be by a state because they are beyond the capability of any criminal enterprise. Moreover, criminals would have not use for the sort of information nicked.

The report is by the **US-China Economic and Security Review Commission** and details more than a decade of China's probable involvement in cyber attacks.

Part of their argument is that the People's Liberation Army would use cyber warfare **to knock out an enemy's communications, intelligence and logistics operation [7in]** before any conventional act of aggression.

China going to war is perhaps a remote possibility. But the report claims they are already **masters of high-tech spying**. In the old days they would have to have a carefully cultivated agent, an American motivated by money, ideology or blackmail, in place to steal sensitive information. Micro cameras and all that jazz.

[PHOTO] Criminals and state spies are a few clicks away from success

Not these days. An innocent employee opens a **dodgy e-mail** about a real conference he or she is going to, and hey presto, the backdoor to their **computer is wide open to a foreign power**. One case study of a real event, heavily disguised in the report, claims that **a huge amount of information was taken in a matter of hours. [8cm]**

Once access is achieved by one team, another team takes over to plunder the information. They target particular files selected in advance rather than just take everything they can.

The report finds that it is likely China is "conducting a long-term sophisticated, computer network exploitation campaign" against US

government and industry characterised by "disciplined, standardised operations, sophisticated techniques, access to high-end software development resources, a deep knowledge of the targeted networks..." [9in]

It is fascinating stuff. But it makes me eager for another report, perhaps written by the Chinese, spelling out what the UK and the US are up to and how far they go in cyber-spying. [10cm]

<http://www.bbc.co.uk/news/world-us-canada-13754496>

0. Page last updated at 07:36 GMT, Thursday, 2 June 2011 08:36 UK

~~Cyber war's 'death and destruction'~~

~~[RADIO]~~

~~A cyber attack uncovered by Google appears to have been aimed at a large number of government officials and journalists, mainly but not exclusively in the United States, and to have originated in China.~~

~~Security correspondent Gordon Corera reports on the "offence and defence" of cyber security.~~

~~And Lt General Harry Raduege chairs the Deloitte Centre for Cyber Innovation in Washington DC, and who has written reports on cyber security, analyses the threat of further attacks.~~

~~http://news.bbc.co.uk/today/hi/today/newsid_9502000/9502671.stm~~

5. 1 June 2011 Last updated at 16:24 GMT

US Pentagon to treat cyber-attacks as 'acts of war'



US retaliation for cyber-attacks could take many forms

[Continue reading the main story](#)

The US is set to publish plans that will categorise cyber-attacks as acts of war, the Pentagon says.

In future, a US president could consider economic sanctions, cyber-retaliation or a military strike if key US computer systems were attacked, officials have said recently.

The planning was given added urgency by a cyber-attack last month on the defence contractor, Lockheed Martin.

A new report from the Pentagon is due out in a matter of weeks.

"A response to a cyber-incident or attack on the US would not necessarily be a cyber-response. All appropriate options would be on the table," Pentagon spokesman Col Dave Lapan told reporters on Tuesday.

Col Lapan confirmed the Pentagon was drawing up a cyber defence strategy, which would be ready in two to three weeks.

Cyber-attacks from foreign nations that threaten widespread US civilian casualties, like cutting off power supplies or shutting down emergency-responder networks, could be treated as an act of aggression under the new policy. [11in]

But the plan does not mention how the US may respond to cyber-attackers, such as terrorists, who are not acting for a nation state.

'All necessary means'

The Pentagon's planning follows an international strategy statement on cyber-security, issued by the White House on 16 May.

American strategists are wrestling with the big, new questions of cyber war. What constitutes cyber attack? What laws, definitions and principles should governments use to formulate their response?

How do you tell the difference between a virtual annoyance perpetrated by criminals and hackers and an act of war perpetrated by a nation state? This question is perhaps the biggest difficulty facing those who are charged with writing the doctrine of cyber war.

It's often referred to as the "attribution problem". When an American entity - a government department, the military or a corporation - becomes aware they are under cyber-attack when their networks start malfunctioning, how do they know who is doing the attacking?

Savvy Computer Network Defence (CND) specialists may be able to track the attack to a specific country, even to a specific internet address. But who is operating the computer terminal? An operative of a rival state acting under orders? Or a hacker acting on her own initiative? Or something in between?

"Whose fingers are on the keyboard?" ask the CND specialists. When you don't know who your attacker is, finding a legal and ethical response becomes very difficult.

The US would "respond to hostile acts in cyberspace as we would to any other threat to our country", stated the White House in plain terms.

"We reserve the right to use all necessary means - diplomatic, informational, military, and economic - as appropriate and consistent with applicable international law, in order to defend our nation, our allies, our partners and our interests."

The Wall Street Journal quoted a military official as saying: "If you **shut down our power grid** [12in], maybe we will put a missile down one of your smokestacks."

White House officials said consideration of a military response to a cyber-attack would constitute a "last resort", after other efforts to deter an attack had failed, the New York Times newspaper reported.

Sophistication of hackers

One of the difficulties strategists are grappling with is how to track down reliably the cyber-attackers who deliberately obscure the origin of their incursions.

The sophistication of hackers and frequency of the attacks came back into focus after an attack on arms-maker Lockheed Martin on 21 May.

Lockheed said the "tenacious" cyber-attack on its network was part of a pattern of attacks on it from around the world.

The worst cyber-attack against the US military occurred in 2008, when **malicious software on a flash drive commandeered computers at US Central Command**. [13cm]

The US defence department estimates that more than 100 foreign intelligence organizations have attempted to break into American networks.

The US is also accused of using cyber warfare against other nations. In 2010 Iran accused the US of helping to **develop Stuxnet, a software worm aimed at controlling systems in Iranian nuclear plants**. [14cm]

<http://www.bbc.co.uk/news/world-us-canada-13614125>

6. 17 March 2011 Last updated at 01:05 GMT

US cyber war defences 'very thin', Pentagon warns



US officials say government and private systems are attacked millions of times per day

The US military lacks the people and resources to defend the country adequately from concerted cyber attacks, the head of the Pentagon's cyber command has warned.

"We are very thin, and a crisis would quickly stress our cyber forces," Gen Keith Alexander told Congress.

The US says government systems are attacked millions of times a day.

Disputes over budgets are holding up a new cyber protection system ordered by the Department of Homeland Security.

However, some argue the threat of cyber warfare is greatly exaggerated.

'Potential adversaries'

Gen Alexander, head of the US Defence Department's Cyber Command, told a Congressional Committee that he would mark as a "C" the military's ability to protect Pentagon networks, although he acknowledged improvements in recent years.

"We are finding that we do not have the capacity to do everything we need to accomplish. To put it bluntly, we are very thin, and a crisis would quickly stress our cyber forces," he said.

"We cannot afford to allow cyberspace to be a sanctuary where real and potential adversaries can marshal forces and capabilities to use against us and our allies. This is not a hypothetical danger."

US officials say cyber criminals, terrorists and other nations are getting better at penetrating state and private networks, whether to spy, to steal data [15cm] or damage critical infrastructure [16cm].

But speaking last month, leading security expert **Bruce Schneier** told the BBC that the emotive rhetoric around "cyber warfare" did not match the reality.

"What we are seeing is not cyber war but an increasing use of war-like tactics and that is what is confusing us. We don't have good definitions of what cyber war is, what it looks like and how to fight it," Mr Schneier said.

<http://www.bbc.co.uk/news/world-us-canada-12768617>

7. 16 February 2011 Last updated at 16:48 GMT

Cyber attacks 'acts of war' - Sir Richard Mottram

By Brian Wheeler Political reporter, BBC News



There have been repeated warnings about the threat of cyber attack

A cyber attack by one state on another could be considered an "act of war", Tony Blair's former top national security adviser has said.

Sir Richard Mottram told a House of Lords inquiry new "laws of war" were needed to cope with such a threat.

He also criticised the EU after the multi-million pound theft of carbon credits, saying its apparent lack of cyber security "took my breath away".

It comes amid claims the threat of cyber war is being exaggerated.

Earlier this month, Foreign Secretary William Hague called for countries to come together to agree a set of rules to prevent cyber war.

He revealed that the Foreign Office IT system had come under attack from a "hostile state intelligence agency" as recently as January.

Sir Richard, a former top civil servant at several government departments, who ended his Whitehall career in 2007 as chairman of the Joint Intelligence Committee, appeared to back Mr Hague's call for new

international rules in evidence to the Lords EU sub-committee on Home Affairs.

"Could a cyber attack constitute an act of war? Absolutely. If you could establish who had done it of course... is it feasible to imagine laws of war that could apply in relation to cyber attack? Answer - it is feasible," said Sir Richard, who was also in charge of the previous government's counter-terrorism strategy.

'No confidence'

He was also asked for his reaction to the theft last month of 7m euros (£5.9m) of emission permits from the European Commission's carbon trading system.

According to the Financial Times, it was believed to have been the work of computer hackers who used a hoax bomb threat to get a building in Prague evacuated before **stealing codes and allowances from computers.** [17cm]

The allowances could be sold on the open market for "millions of euros" before anyone would have noticed, **the newspaper said.**

It said there have been at least six attacks on operators of the EU emissions trading system in eastern and central Europe in the past three months - with thieves taking more than 50 million euros - before trading was suspended.

Asked if he had confidence in the EU's cyber security systems following these incidents, Sir Richard said: "I wouldn't have generalised confidence in those systems - no."

He said the Prague incident, in particular, highlighted the vulnerability of EU-wide computer systems.

"These are all systems issues where people seek out the weakest point. So it's no use the UK having the most fabulous security, which I don't suggest it has, but it has in many areas adequate security, if it is also sharing information with others who aren't anywhere near our level," he said.

Commenting specifically on the carbon credits theft, he said: "They (the EU) don't seem to have realised until quite recently that they were an attractive target, which rather took my breath away."

Exaggerated threat

Committee chairman, crossbench peer Lord Hannay, also criticised the EU's cyber security systems following the Prague incident.

"We have asked the government to give us the best knowledge they have about what happened in this case.

"But I think it is pretty clear that cyber security is inadequate both in a number of the national offices that run the emission trading scheme and in Brussels.

"That would not be a particularly surprising discovery but it does have important implications for the need for the EU to do something about its own security, its own institutions' security, as well as looking into the wider issue of all the member states."

The Lords EU Home Affairs sub-committee **is investigating the EU's internal security strategy.**

It comes as one of Britain's leading cyber security experts, BT's head of security Bruce Schneier, told BBC News the threat of cyber war had been exaggerated and was based on only a handful of incidents around the world.

His view appeared to be backed by Howard Schmidt, cyber security co-ordinator for the White House, who called for an end to the use of inflammatory language when talking about internet security.

"Cyber war is a turbo metaphor that does not address the issues we are looking at like cyber espionage, cyber crime, identity theft, credit card fraud," [18cm] he told reporters at a conference in San Francisco.

<http://www.bbc.co.uk/news/uk-politics-12485147>

8. 16 February 2011 Last updated at 09:21 GMT

Cyber war threat exaggerated claims security expert

By Maggie Shiels Technology reporter, BBC News, Silicon Valley



Electronic attacks will play a part in conventional conflict, but they are not wars, says Mr Schneier

The threat of cyber warfare is greatly exaggerated, according to a leading security expert.

Bruce Schneier claims that emotive rhetoric around the term does not match the reality.

He warned that using sensational phrases such as "cyber armageddon" only inflames the situation.

Mr Schneier, who is chief security officer for BT, is due to address the RSA security conference in San Francisco this week

Speaking ahead of the event, he told BBC News that there was a power struggle going on, involving a "battle of metaphors".

He suggested that the notion of a cyber war was based on several high-profile incidents from recent years.

They include blackouts in Brazil in 1998 [19in], attacks by China on Google in 2009 [20wa] and the Stuxnet virus that attacked Iran's nuclear facilities [21in].

He also pointed to the fallout from Wikileaks [22wb] and the hacking of Republican vice-presidential candidate Sarah Palin's e-mail. [23wb]

"What we are seeing is not cyber war but an increasing use of war-like tactics and that is what is confusing us.

"We don't have good definitions of what cyber war is, what it looks like and how to fight it," said Mr Schneier.



Casualty of war? Attacks such as Sarah Palin's e-mail hack have been lumped into the debate

His point of view was backed by Howard Schmidt, cyber security co-ordinator for the White House.

"We really need to define this word because words do matter," said Mr Schmidt.

"Cyber war is a turbo metaphor that does not address the issues we are looking at like cyber espionage, cyber crime, identity theft, credit card fraud.

"When you look at the conflict environment - military to military - command and control is always part of the thing.

"Don't make it something that it is not," Mr Schmidt told a small group of reporters on the opening day of the conference.

A report last month by the Organisation for Economic Cooperation and Development also concluded that the vast majority of hi-tech attacks, described as acts of cyber war, do not deserve the name.

Tanks and bombs

The issue is likely to receive a lot of attention at RSA this week as a number of panels seek to define what is and what is not cyber warfare.

"Stuxnet and the Google infiltration are not cyber war - who died?" asked Mr Schneier.

"We know what war looks like and it involves tanks and bombs.

"However all wars in the future will have a cyber space component.

"Just like we saw in the Iraqi war we [the US] used an air attack to soften up the country for a ground offensive.

"It is probably reasonable you will see a cyber attack to soften up the country for an air attack or ground offensive," he added.

Mr Schneier claimed that the heated rhetoric is driving policy in ways that might not be appropriate.

"The fear is that we are going to see an increased militarisation of the internet," he said.

Recently the FBI and Department of Defence squared off over who got to control defence in cyber space and the multimillion dollar budget that goes with the job.

Mr Schneier said that battle was won by the defence department.

He also claimed there was a worrying trend of politicians who try to introduce legislation as a way to deal with the issue as nothing short of knee-jerk politics.

Last week the Cybersecurity Enhancement Act was introduced in the Senate, following confirmation by oil companies and Nasdaq officials that their computer systems were repeatedly hacked by outsiders

"My worry is these ill thought-out bills will pass," said Mr Schneier.

Treaty talk

Talk of drawing up the equivalent of a Geneva Convention for cyber space has been gaining attention.

The proposal was raised by international affairs think-tank, the EastWest Institute at a security conference in Munich last week.

Mr Schmidt said he is sceptical because he does not believe every country will sign up to an agreed set of norms or standards.

"I don't know that a treaty is going to solve anything at this juncture.

"Not everyone thinks about this unilaterally around the world. We can't do this by ourselves," he said.

Industry commentator Declan McCullagh, who is chief political writer for online news site CNET.com, believes the idea of doing nothing is untenable.

"Before we get to the stage of having to launch a cyber war, and that will eventually come, let's have a public discussion about what this involves," he said.

"A Geneva Convention for cyber war makes sense at least to start that discussion.

"What that would do is put certain types of attacks off the table like you are not going to target the enemy's hospitals or certain types of civilian systems that innocents depend on for their livelihood. [24in]

"I don't think everyone is going to respect it, and maybe the US won't respect it at times, but at least it starts the discussion and will probably have a positive effect," said Mr McCullagh.

This year marks the 20th anniversary of the RSA event, which began as a purely technical cryptography conference and has evolved into a broader forum that includes issues of policy and governance as well as technology.

<http://www.bbc.co.uk/news/technology-12473809>

0. 4 February 2011. Last updated at 02:47 GMT

Calls for 'rules of engagement' for cyber conflict

[VIDEO: 10.05]

When world leaders meet in Munich on Friday for their annual security conference, for the first time cyber warfare will be on the agenda.

UK Foreign Secretary William Hague will make a major speech in Munich, warning that cyberspace has "created new means of repression for undemocratic governments", and raised new fears of a "cyberwar".

But what is cyber war? How will it be fought? and with what weapons?

BBC Newsnight has obtained a copy of US-Russian proposals for Friday's meeting that call for new "Rules of Engagement" for cyberspace.

In the first of a two-part investigation into cyber threats, Newsnight's Science Editor, Susan Watts, looks at the new cyber battleground.

<http://www.bbc.co.uk/news/technology-12362236>

0. 3 February 2011. Last updated at 15:57 GMT

US cyber warfare expert on threats which exist now

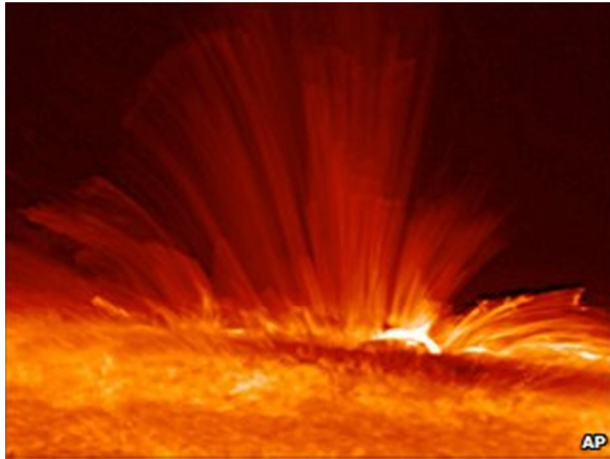
John Bumgarner, research director for security technology at the US Cyber Consequences Unit, talks to Newsnight's Susan Watts about the kind of cyber attack capabilities which already exist.

Watch Susan Watts' full report on the threat posed by cyber warfare on Newsnight on Thursday 3 February 2011 at 10.30pm on BBC Two, then afterwards on the BBC iPlayer and Newsnight website.

<http://news.bbc.co.uk/2/hi/programmes/newsnight/9386804.stm>

9. 17 January 2011 Last updated at 10:33 GMT

Risks of cyber war 'over-hyped' says OECD study



A huge solar flare could give rise to a global cyber shock, warns the report

The vast majority of hi-tech attacks described as acts of cyber war do not deserve the name, says a report.

The Organisation for Economic Cooperation and Development study is part of a series considering incidents that could cause global disruption.

While pandemics and financial instability could cause problems, cyber attacks are unlikely to, it says.

Instead, trouble caused by cyber attacks is likely to be localised and short-lived.

However, it warns that governments need to plan for how it could mitigate the effects of both accidental and deliberate events.

'Great confusion'

Attempts to quantify the potential damage that hi-tech attacks could cause and develop appropriate responses are not helped by the hyperbolic language used to describe these incidents, said the OECD report.

"We don't help ourselves using 'cyberwar' to describe espionage [25cm]

or hacktivist blockading [26wb]

or defacing of websites, as recently seen in reaction to WikiLeaks," [27wb]

said Professor Peter Sommer, visiting professor at LSE who co-wrote the report with Dr Ian Brown of the Oxford Internet Institute.

"Nor is it helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt **critical national infrastructure**," [28in] added Prof Sommer.

The report acknowledged the risk of a catastrophic cyber incident, such as a solar flare that could knock out satellites, base stations and net hardware, but said that the vast majority of incidents seen today were almost trivial in comparison as they did not last long and only hit a few people or organisations.

Attempts to decide how to deal with the wide variety of potential attacks and attackers were being hampered because words used to describe incidents meant different things to different groups.

For instance, it said, an "attack" could mean **phishing e-mails trying to steal passwords, a virus outbreak or a concerted stealthy attempt to break into a computer system**. "Rolling all these activities into a single statistic leads to grossly misleading conclusions," said the report. "There is even greater confusion in the ways in which losses are estimated."

The report also played down the risk of a conflict between nation states being played out over the net.

"It is unlikely that there will ever be a true cyberwar," said the report, most likely because no aggressor would stick to one class of weaponry. Also, it said, existing defences and the unpredictable effects of such an attack could limit its effectiveness.

However, it noted, that even if a cyberwar is unlikely to ever happen, there was no doubt that the weapons used in such a theatre of war were becoming ubiquitous and would likely be used in the future alongside conventional weapons as "force multipliers".

Under the heading of cyber weapons the report included **viruses, worms, trojans, distributed-denial-of-service using botnets and unauthorised access to computers ie hacking**. [29cm]

Finally, it said, while the net may be a vector for attack it might also help in the event of a large-scale event.

"If appropriate contingency plans are in place, information systems can support the management of other systemic risks," it said.

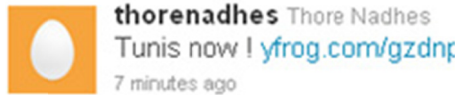
"They can provide alternate means of delivering essential services and disseminate the latest news and advice on catastrophic events, reassuring citizens and hence dampening the potential for social discontent and unrest."

<http://www.bbc.co.uk/news/technology-12205169>

10. 14 January 2011 Last updated at 16:47 GMT

Tunisia protests: Cyber war mirrors unrest on streets

By Aidan Lewis BBC News



Tunisia turmoil

- **Broken dreams**
- **Doubts about martyr**
- **Hunting Ben Ali's treasure**
- **'Speakers' corner'**

A crescendo of protest has shattered Tunisia's calm over the past few weeks, with crowds spilling onto the streets in a way previously unimaginable.

Unions and other professional groups have played a role, as have text messages and satellite TV. But it is on the internet that a generation of activists has been credited with enabling the movement to take off. [30wb]

This has happened despite increasingly strict controls by a government that, even before the demonstrations, was regarded as unusually zealous in its online censorship. [31wa]

A steady flow of protest videos, tweets, and political manifestos has continued to make its way onto the web in a variety of languages: Arabic, the Darija Tunisian dialect, French and English.

Some encouragement has come from abroad, including France and other Arab countries. But much has been generated from within Tunisia.

"Our part as tweeples/bloggers or simple social media users is to pass the info, share it and spread the word: when, where it's happening," one Tunisia-based woman who requested anonymity told the BBC by e-mail.

"Then, once the demonstrations take place, we report live on twitter & FB [Facebook] and if some have pictures or videos, we share!" [32wb]

One reason the internet has played a central role is that Tunisia has long led North Africa in levels of internet access.

More than 34% of Tunisia's 10 million people are online. Nearly two million people, or more than 18% of the population, **use Facebook** - a far higher proportion than in neighbouring countries.

But the Tunisian authorities have also built up a formidable firewall, the censor gaining the nickname of Amaar404 - a reference to the 404 message seen when a page cannot be accessed. [33wa]

Press freedom organisation Reporters Without Borders **ranks Tunisia 164th out of 178 countries in its press freedom index**. The group lists Tunisia as one of its 15 **enemies of the internet**, saying it has set up a "very effective system of censoring" the web.

Operation Tunisia

A sort of warm-up to the recent cyber war came with **the release by Wikileaks of a number of US diplomatic cables on Tunisia** [34wb] in late November and early December.



Social media have been used to help get people out on the streets

A Lebanese news website that published the cables, Al-Akhbar, was blocked in Tunisia, and attacked by hackers. [35wa]

When the demonstrations started on 17 December, they were given little coverage in the domestic media, and were widely reported outside Tunisia as a protest over unemployment.

But the overtly political campaign on the internet escalated with **Operation Tunisia**, in which **activists targeted government sites** with **Distributed Denial of Service (DDoS) attacks**. [36in]

There followed **reports of widespread counter-attacks against bloggers by the Tunisian government**.

Internet users within Tunisia say these included capturing their passwords and blocking or taking control of blogs and other web pages.

Stories about the protests on international news websites such as the BBC or Al-Jazeera have also been blocked, they say, though there were reports that some sites had become accessible on Friday after President Zine al-Abidine Ben Ali pledged a loosening of controls. [37wa]

As many as five bloggers were arrested, along with a rapper, Hamada Ben Aoun, who sang the song President, Your People Are Dead - **an internet video hit**. Three of the bloggers and the rapper have been released.

The US government, which has expressed its **deep concern at the use of "excessive force"** by Tunisian authorities during the protests, **also said it was worried about reports of government-directed attacks** on Tunisian users of American companies such as Facebook, Yahoo and Google.

While Facebook access has been restricted within Tunisia, the authorities have not tried to pull the site completely - apparently out of fear of the possible reaction from the rapidly growing number of Tunisians who rely on it.

It remains the primary vehicle for posting information about the protests.

'Hide and seek'

Bloggers have been able to instruct others how to get round controls, by using proxies or other devices. They have also offered guidance on how to avoid putting themselves, or others, in danger.

"It's like a game of hide and seek," says one blogger who goes by the name of Foetus.

He is one of two people who founded Tunisia's opposition **Takriz cyber group** in 1998, and now operates out of another North African country, which he declined to name for fear that he could be identified and his family targeted.

A recent instruction on one of the most popular internet forums, **Nawaat**, read: "We remind all users of Facebook, especially if they are connecting from Tunisia: DO NOT CONNECT from an unsecure page."

Farooq Ferchichi, a 24-year-old software engineer, said he thought the authorities had become overwhelmed by the protests, and had simply become unable to censor everything.

"We did a page called: 'Mr President, the people of Tunisia are burning,' he said by e-mail.

"It was in the beginning of the events, it was censored. People did a second page: 'Mr President, the people of Tunisia are burning 2'. After some hours many thousands joined, and it was censored. Activists did the same five times, until the government gave up."

Some videos and posts are being uploaded outside Tunisia, but according to Lucie Morillon, head of new media at Reporters Without Borders, "the level of internet activity within Tunisia is still very strong".

She thinks the impact of social media use may be greater than during protests in Iran in 2009, where the significance of what was dubbed the "Twitter revolution" was later questioned. [38wb]

There has also been a growing amount of disinformation posted - partly by opposition bloggers, but also, they suspect, by government operatives trying to discredit the protesters.

On Thursday a fake statement was posted announcing the foreign minister's resignation, a hoax that Foetus claimed was his doing.

Amid the online postings, anger and resentment against President Ben Ali and the perceived corruption of his regime has been clear on the web.

The government initially blamed the protests on a small fringe of extremists, though Mr Ben Ali appeared to change tack on Thursday, announcing he would stand down in 2014, expressing deep regret over the deaths of civilians, and promising media freedoms.

But many on the internet appeared sceptical, urging people to follow the line posted in one appeal on Nawaat: "All the slogans will have to reflect one demand only: Ben Ali to step down and be put on trial," it said.

<http://www.bbc.co.uk/news/world-africa-12180954>

11. 16 December 2010 Last updated at 08:59 GMT

EU could turn to 'crowd sourcing' in cyber crime fight

By Brian Wheeler Political reporter, BBC News



The public could help track down criminals operating in cyber space

Millions of internet users across the EU could be encouraged to join the fight against cyber crime if a ground breaking experiment in "crowd sourcing" goes ahead.

The director of Europol told peers he wants to get net users directly involved in catching cyber crime gangs.

Rob Wainwright briefed a Lords EU sub-committee on plans for a European cyber crime centre.

He said the extent of the problem was often underestimated in the EU.

And criminal gangs were becoming more sophisticated in their use of technology, which was spreading into the world of "offline" crime such as drug and people trafficking and VAT fraud, which netted criminals in the EU 100bn euros (£85bn) last year alone.

Scams

Europol officials say criminals are increasingly communicating with each other through online phone services in the mistaken belief that they are untraceable.

They are also carrying out more "traditional" cyber crimes such as botnets, malicious software that can secretly steal credit card details, and phishing scams, in which people are tricked into handing over confidential details.

Mr Wainwright, a former senior official with the UK's Serious and Organised Crime Agency, said Europol was stepping up its fight against internet-based crime ahead of the opening of a planned cyber crime centre, funded by the European Commission.

Europol, an EU-wide police intelligence agency based in The Hague, already had a "dedicated intelligence project designed to identify the most significant cyber criminals operating in Europe", Mr Wainwright told the committee.

He said the next stage was to launch an "internet crime reporting online system".

This initiative, originally conceived by the French Presidency of the EU in 2008, would, for the first time, "collect all internet crime reported online at a national level, in a harmonised way across the EU," he told the committee.

'Empower citizens'

It would have the ability to alert police in the 27 member states to "connections between different investigations".

"For the first time the EU will have a comprehensive overview of reported cyber crime from within its own borders and this could even include, in the future, a component of direct engagement with the public," said the Europol chief.

Europol strategic analyst Victoria Baines later explained to BBC News that the organisation was interested in eventually using a form of "crowd sourcing" to gather examples of suspected cyber crime so it could build up a fuller picture of illegal activity.

This would involve concerned net users scouring the net for possible examples of crime and reporting it, possibly through a dedicated website.

It could operate along similar lines to America's **Internet Crime Complaint Center (IC3)**, a joint venture between the FBI and the National White Collar Crime Centre, which for the past 10 years has allowed victims of cyber crime to make a complaint online.

But the Europol system could potentially go further because it would not be restricted to people who had themselves been the victim of cyber crime or who wanted to make a formal complaint to a law enforcement agency.

'Empower citizens'

Ms Baines said the idea was to raise awareness of crimes such as the "online solicitation of children", payment card transaction fraud or "social engineering", in which people are tricked into giving their passwords or other personal details.

And then "to empower citizens not only to look out for themselves but to report criminal activity".

But Mr Wainwright stressed in his evidence that Europol's first priority was to involve private industry and academia in the fight against cyber crime.

The crowd sourcing plan is in its embryonic stages, and will depend on the setting up of the European cyber crime centre, which is planned by 2014, if funding can be secured.

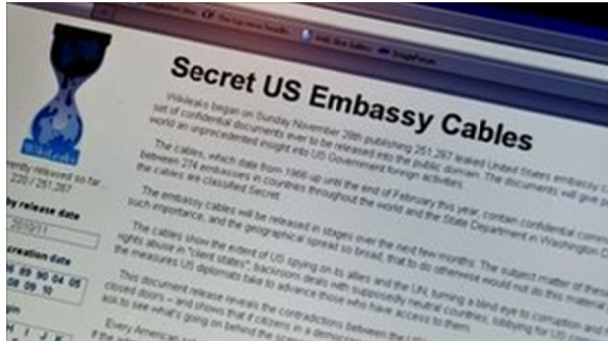
But Mr Wainwright told BBC News he was keen to "scope out" crowd sourcing and saw it as a potentially vital part of the war on cyber crime.

The Lords EU Home Affairs sub-committee **is investigating the EU's internal security strategy**.

<http://www.bbc.co.uk/news/uk-politics-12004134>

12. 14 December 2010 Last updated at 12:43 GMT

UK Government websites may be next pro-Wikileaks focus



The diplomatic cables released by Wikileaks have been the focus of world attention.

The UK's national security adviser Sir Peter Ricketts has warned that **government websites could become the next target for pro-Wikileaks hackers.**

He told civil servants that websites used to file tax returns or claim benefits could be the most vulnerable.

So far attacks from the Anonymous group of hacktivists have concentrated on firms perceived to be anti-Wikileaks. [39wb]

Wikileaks founder Julian Assange has been granted bail by a London court.

A spokesperson for the Prime Minister told a press briefing that Sir Peter had spoken to permanent secretaries about the security of government websites in the light of pro-Wikileaks attacks.

"The priority would be websites that dealt with information that belonged to members of the public such as the DWP [Department for Work and Pensions] and HMRC [Revenues and Customs], he said.

The government did not want to speculate on the scale of the problem.

Data flood

UK web attacks could be likely because Mr Assange has appeared in court.

He has been granted bail but will remain in prison pending an appeal against the decision. He is wanted by authorities in Sweden for questioning over two sex crimes.

He denies the crimes and will fight extradition, his lawyer said.

His mother Christine Assange, who has visited him in prison, said he remained committed to the ideals of Wikileaks.

She also passed on his thoughts on the firms which have withdrawn services from the whistle-blowing site.

"We now know that Visa, Mastercard, PayPal and others are instruments of US foreign policy. It's not something we knew before," Mr Assange said.

The US government has denied that it wrote to individual firms, asking them to stop doing business with Wikileaks.

To date, members of Anonymous - a loose-knit group of net campaigners - have focused their distributed denial-of-service attacks on these firms rather than governments.

The attacks, which flood websites with so much traffic that they fall over, have had some success.

Both Mastercard and Visa, which have stopped processing payments to the Wikileaks site, experienced web outages last week. [40in]

The attacks are co-ordinated via an online tool which members of Anonymous are being encouraged to download.

The tool, which volunteers people's computers to become part of the attack, has now been downloaded more than 80,000 times.

The attacks are a protest against attempts to close down Wikileaks and end the publication of 250,000 secret US diplomatic cables. [41wb]

'Cyber mob'

Some have described the fight between Anonymous, Wikileaks and the US government as the "first infowar".

But security experts have downplayed the conflict.

"It was a demonstration, a protest, nothing more than political theatre - entertaining and influential but not war," James Lewis, a specialist in cybersecurity at the Washington think-tank the Centre for International and Strategic Studies, CSIS, told BBC News.

Allan Friedman, a research director at the US Brookings Institution's technology innovation centre, agreed.

"It's very much not a cyberwar. If we are calling it war, we are devaluing what war is. It's a cyber mob.

"Mobs can be destructive but they tend not to have a long lasting impact."

Some members of Anonymous are also keen to distance themselves from the attacks.

"Many of us are law-abiding citizens of our respective countries around the world," Anonymous member Phill Midwinter told BBC News.

"We're currently involved in more forward-thinking projects that help to spread our message of internet transparency in a more open and productive manner," he added.

This includes a **new venture dubbed Operation Leakspin, which aims to release details from the leaked cables that the mainstream media has overlooked** and summarise them "into chunks that everyone can understand".

Meanwhile the US government remains determined to bring Mr Assange and Wikileaks to book.

It is exploring a nearly century-old spy law as a way to prosecute Mr Assange.

<http://www.bbc.co.uk/news/technology-11990288>

0. 10 December 2010 Last updated at 07:41

[VIDEO 2.41]

The conflict between Wikileaks supporters and the companies withdrawing their services from the whistle-blowing website has been dubbed a "cyber war".

Activists have targeted firms such as PayPal, Mastercard and Visa for their opposition to the site's publication of thousands of secret US diplomatic messages.

But there are fears the online battle could lead to everyday internet use becoming much more heavily regulated.

Click's Dan Simmons reports.

<http://www.bbc.co.uk/news/technology-11966628>

13. 9 December 2010 Last updated: 15:33 GMT

Why are hacktivists 'Anonymous' defending WikiLeaks?

Interview by Debbie Randle Newsbeat reporter



A group of "hacktivists" who crippled websites in revenge for cutting off services to whistle-blowing website WikiLeaks are warned they will continue their "digital sit-in" in a campaign for total internet freedom. [42wb]

The group, known as Anonymous, has disrupted sites belonging to finance giants including MasterCard and Visa.

They bombarded their websites with millions of bogus visits during a campaign called "Operation Payback".

Coldblood is from Anonymous and explains why he's supporting WikiLeaks.

What is Anonymous?

Anonymous is a group of individuals who get together to decide they want to do something.

One of the main goals of Anonymous is keep the internet free and open for everyone to use and not to censor data or anything that goes through the internet.

Why have you suddenly come to our attention?

Anonymous had been defending WikiLeaks by attacking the companies which have decided not to do business with WikiLeaks any more.

That includes Amazon, PayPal, Visa and MasterCard.

What are you hoping to gain from this?



Julian Assange, the man behind WikiLeaks, has been arrested in the UK

What Anonymous is hoping to gain from it is to push the picture to these companies that if they bow down to government pressure they still have to respond to the user.

The person that uses that service.

I feel the way the US government in particular is trying to stop the flow of data from WikiLeaks, it's a vital step the government's taking to censor and be able to control what's on the internet. [43wa]

Do you think that by attacking something that the public uses, especially in the run-up to Christmas when many people are online shopping, do you think that is the best way to get your point across?

We could try to talk to these companies but the odds are they wouldn't listen.

By doing this, we're forcing them to listen.

If people can't access these websites, it's bringing people's attention to the cause and why we're doing it.

Do you think it's just going to anger the public?

It probably has angered some of the public but we feel that it's a necessary evil.

Would you call yourself a computer hacker?

I wouldn't describe myself as a computer hacker.

I'm just quite tech savvy personally.

Anonymous is made up from people everywhere.

We've got some teachers, we've just got people from all walks of life who are participating in it.

What kind of campaigns have you been involved with in the past?

Some of the major campaigns we've done are against the Church of Scientology.

We helped with the flow of data out of Iran when there were all the riots and protests in Tehran over their election.

We also attacked the Australian government when they decided to put a giant firewall to censor the internet.

Is this going to turn into an all out cyber war?

I don't think it's going to turn into an all out cyber war.

The main goal of that is, if you take down WikiLeaks there are still more than a thousand websites you have to take down to stop the flow of information

Coldblood from Anonymous

It's maybe one battle in a very, very long uphill struggle.

What we feel is that, if we let the government continue doing what they're doing to WikiLeaks more and more websites will fall when governments say, 'Ah, I don't like this organisation.'

By standing up for WikiLeaks we're feeling we're helping to pave the way for the future so that websites like WikiLeaks or any website can carry on on the internet without fear of the government shutting them down.

If this doesn't work, how far are you prepared to go? What happens next?

We don't really know.

Anonymous works on a day by day basis.

All the ideas are from the members of Anonymous.

People throw idea out there, and they like it enough and it sticks, the idea becomes reality.

Lots of people have been working on the long-term.

For example, people are making mirrors of WikiLeaks.

The last time I checked the stats, there were 1,247 copies of WikiLeaks out there.

The main goal of that is, if you take down WikiLeaks there are still more than a thousand websites you have to take down to stop the flow of information.
[44wb]

<http://www.bbc.co.uk/newsbeat/11961594>

14. 24 November 2010 Last updated at 09:40 GMT

Should Obama's 'internet kill switch' power be curbed?

By Daniel Nasaw BBC News, Washington



The US Congress hopes to curb the president's authority to order computer systems off the internet

Under a World War II-era law, the US president appears to have authority to disconnect computer systems and servers from the internet in the event of a national emergency. But the next US Congress is poised to change that. [45wa]

The law was passed in 1942. The Japanese attack on Pearl Harbor had provoked fear of a foreign invasion of US soil, and Congress responded by giving President Franklin Roosevelt broad power to commandeer or shutter telephone and telegraph networks.

Nearly 70 years later, telegraph networks have disappeared, and the telephone is only one of many means of communication.

But although the 1942 law makes no mention of the internet - merely of "any facility or station for wire communication" - the Obama administration in June **told Congress** it would cite it in an emergency.

It has not been tested in court, but experts say **section 706(d)** of the Communications Act could give the president wide-ranging authority to shut down key computer systems.

With typical Washington hyperbole, the law has become known as the presidential "internet kill switch".

'Clear rules needed'

The next US Congress will be under pressure to strengthen the nation's cyber defences, and a spectrum of security analysts, internet freedom advocates and senators say lawmakers must update those emergency war powers to limit or at the very least more clearly define the president's authority.



The Pentagon's William Lynn has acknowledged foreign spies have infiltrated secret US military computers

"The time is ripe for some articulation of this authority so we don't have presidents going off into the wild, but actually have a set of pretty clear rules," said Paul Rosenzweig, a former homeland security official under President George W Bush, now a fellow at the conservative Heritage Foundation.

Uncertainty over the interpretation of the current laws has left analysts speculating about how the president would use the "kill switch", and to what end.

One analyst told the BBC that if, for example, computer systems at Washington's natural gas and electric utilities became infected by a powerful internet worm, the president could order them to power down or disconnect from the internet to protect physical infrastructure, stem the infection, and allow them to be cleared. [46in]

Recent major cyber attacks

- 2010 - Stuxnet infects personal computers used by Iranian nuclear scientists [47cm]
- 2009 - A major South Korean bank and newspaper and the country's spy service are slammed with co-ordinated attacks, which some blamed on North Korea [48cm]
- 2008 - Foreign spies infiltrate secret US military computers in an attack launched from an infected flash drive [49cm]
- 2007 - Estonian government and commercial computers bombarded with cyber attacks the country blamed on Russia [50in]
- 2000 - Major websites including Amazon.com and eBay crippled by "denial-of-service" attacks [51wb]

In another hypothetical scenario described to the BBC, the president might order the shutdown of networks hosting Wall Street financial services infrastructure in order to avoid an imminent cyber attack. [52wa]

'Unlimited authority'

In both cases, the actions would have far-reaching consequences for the companies and individuals relying on the systems - for power, or to move money, analysts said.

Civil liberties campaigners are concerned at the potential for the power to be abused.

"It's unlimited," said Michelle Richardson, legislative counsel for the American Civil Liberties Union in Washington, about the president's current power.

"They have the authority, and we've seen since 9/11 that the executive branch has always pushed its power to the limit."

Privacy advocates say the law must be adjusted to ensure the president cannot use emergency war powers to snoop improperly on Americans' e-mail or other information.



Senators Susan Collins and Joseph Lieberman are spearheading the Senate cyber security reform bid

It is unclear whether the disconnection of US networks would affect the internet elsewhere in the world, aside from blocking users from, say, a popular web page or service, technical experts say.

But Greg Nojeim, of the Center for Democracy and Technology, said there was "a high risk" of "a spillover effect in other countries".

However, it is nigh on impossible for the US president - or any single actor - to shut down the whole internet - a virtue of its globally distributed nature, analysts say.

"There's no plug to be pulled," John Kneuer, a former telecommunications policy official under President Bush, told the BBC.

Stuxnet feared

Among several shortcomings in the 1942 law's application to the online world, it does not specify what constitutes cyber war - as opposed to a commercial hacking job. Nor is it even clear the law would treat a cyber attack by a foreign power as an act of war - a precondition of the president's use of the emergency powers.

Nevertheless, the debate over the president's cyber war authority comes amid growing evidence that nations are deploying cyber weapons against adversaries.

The powerful internet worm Stuxnet, discovered this year to have infected computers across the globe, appears to have been designed specifically to target Iranian nuclear sites, causing alarm within the US and UK governments. [53 in] Some analysts say it was so sophisticated it could only have been launched by a sovereign nation state.

In all, attacks on US government facilities this year topped 1.8 billion per month, **according to the US Senate sergeant-at-arms.**

US officials also fear cyber attacks on the private sector, which operates as much as 85% of the nation's critical infrastructure - power plants, major internet service providers, telephone companies and more.

The bipartisan group of US senators currently engaged in rewriting many US cyber security laws is keenly aware of the threat posed by such attacks. But the senators argue the president's emergency war powers must be better defined and delimited.

Legislation backed by Senators Susan Collins, a Maine Republican, and Joseph Lieberman, an independent from Connecticut, would allow the president to declare a "national cyber emergency" and permit the administration to direct a threatened system's operators to take action. The government would have to ensure the mandatory emergency measures were "the least disruptive means feasible".

No advance warning

"The president's authority to deal with a catastrophic cyber attack aimed at critical infrastructure would be carefully defined - and constrained," Ms Collins **said last week.** "The president would not have the authority to take over critical infrastructure."

Some question the need for emergency presidential cyber authority.

Greg Nojeim says internet companies are better equipped than the government to decide whether to shut down their systems or remove them from the internet.

"Nobody has yet identified an actual real life circumstance in which an owner or operator decided not to isolate a network and the government thought it should be isolated," he said.

James Lewis, director of the technology and public policy programme at the Center for Strategic and International Studies in Washington, questions whether emergency shut-down power would be effective considering internet worms are usually discovered after they have struck.

"We almost never have advance warning," he said.

<http://www.bbc.co.uk/news/world-us-canada-11736545>

15. 4 November 2010 Last updated at 16:49 GMT

Europe simulates total cyber war



The cyber war simulation will steadily cut off net links

Essential web services have come under simulated attack as European nations test their cyber defences.

The first-ever cross-European simulation of an all out cyber attack was planned to test how well nations cope as the attacks slow connections.

The simulation steadily reduced access to critical services to gauge how nations react.

The exercise also tested how nations work together to avoid a complete shut-down of international links. [54in]

Neelie Kroes, European commissioner for the digital agenda, said the exercise was designed to test preparedness and was an "important first step towards working together to combat potential online threats to essential infrastructure".

The exercise is intended to help expose short-comings in existing procedures for combating attacks. As the attacks escalated, cyber security centres had to find ever more ways to route traffic through to key services and sites.

The exercise also tested if communication channels, set up to help spread the word about attacks, were robust in the face of a developing threat and if the information shared over them was relevant.

Overseeing the exercise was the European Network Security Agency which has been given new powers to help member states handle cyber security

incidents. In all, 22 member states plus Iceland, Norway and Switzerland took part.

A report into how the simulation went and how different nations coped is due to be published on 10 November.

<http://www.bbc.co.uk/news/technology-11696249>

16. 14 October 2010 Last updated at 16:24 GMT

Call to define rules of cyber war



Cyber attacks, like nuclear weapons, should force a change in defence policy

Nations need to define the rules of engagement for acts of cyber terror.

The call for clarity was issued by Michael Chertoff, former head of the US Department of Homeland Security, at the RSA security conference in London.

He said the lack of direction was giving the initiative to criminals and hampering co-ordinated responses to the growing number of hi-tech attacks.

Countries should be able to defend themselves, he suggested, if an attack posed imminent danger to human lives.

"It's the least understood threat and the one where our doctrine is least developed," said Mr Chertoff.

Graded response

The need for such a doctrine was as pressing now as it was in 1950s, he said, when the emergence of nuclear weapons rendered irrelevant earlier policies governing when and why conflicts were fought.

That vacuum was filled by the policy of deterrence which defined what response could be expected from the US depending on how its territory or citizens were threatened.

"It was very clear to an adversary the consequences of an attack," he said.

In a similar way, said Mr Chertoff, a nation's cyber defence doctrine would lay out a range of responses depending on the severity of the attack.

"We have to treat espionage [55cm] as different from attack or massive fraud or theft of information [56cm]," he said.

Theft and espionage could be dealt with through the legal system, he said, with the strongest responses being reserved for the most serious cases.

"If you cause imminent danger of loss of life by attacking a network that's a different story," he said. "Theft is bad but murder is worse."

International laws of self-defence would allow a nation to respond to remove the threat posed by an imminent or unfolding attack, he said.

He admitted that such serious attacks on national infrastructure, such as rolling blackouts that led to deaths in hospitals, [57in] had not happened yet, but added: "I would not like to experience the first one."

"There seem to be very few entities that are perfectly immune from these types of attacks," said Mr Chertoff who now heads the Chertoff Group, which advises nations and governments on risks and security.

By defining a doctrine, he suggested, all nations would be encouraged to police domestic networks better to avoid incurring a strong response.

"The greatest stress you can have on security is when there is uncertainty," he said. "We are now in a state of uncertainty."

The need to develop response scenarios and an over-arching doctrine was becoming pressing, he said, as those involved in hacking for money carried out ever more attacks.

"It's a real problem and it's growing," he said, "If we do not address it then we are going to be confronted by an event that's so catastrophic that it cannot be shrugged off."

<http://www.bbc.co.uk/news/technology-11545040>

17. 21 June 2010 Last updated at 18:20 GMT

Defence review to look at all potential conflicts - Fox

By James Landale BBC News deputy political editor



Dr Fox said the UK's military capability must be flexible

Liam Fox has warned that Britain should prepare for the possibility of war with another state as part of the government's strategic defence review.

The defence secretary told MPs the coalition should not simply assume that future conflicts will be like that currently taking place in Afghanistan.

The review, the first since 1997, will examine what sort of armed forces are needed in future and the cost involved.

Labour said it backed the review and "difficult" decisions would be needed.

Outlining the terms of the review, the defence secretary told MPs that the armed forces should not assume that future wars will be like the current counter insurgency in Afghanistan.

New threats

There could be conflicts over energy and water, new threats from failed states and a nuclear Iran [58in] - and even, he said, the return of state versus state conflicts.

There would therefore be, he said, a thorough stock-take of current contingency plans.

Britain must maintain a flexible capability to adapt to future threats and there should be a break from the military and political mindset of cold war politics, that prepared for war in space and cyber space.

He confirmed that the coalition remained committed to a continuous at sea nuclear deterrent but was scrutinising Trident to ensure value for money, a process that would be complete by July.

He said the threat of nuclear proliferation was something Britain shall face in the future and was not simply a by-product of the Cold War.

As for defence spending, Dr Fox said the review would have to confront the harsh facts of the economic climate

There needed to be a step change, he said, not the usual salami slicing and Britain's commitments will have to balance its resources.

His comments suggest the UK's defence capability is facing cuts as well as change.

Mr Fox has refused to rule out a cut in troop numbers as a result of the defence review but has insisted that all requested resources will be made available for British forces in Afghanistan.

For Labour, shadow defence secretary Bob Ainsworth agreed that "difficult decisions" would have to be taken on budgets and it was clear that a Cold War capability was not suitable to meet future threats.

However, he questioned the transparency of the Trident review and how the coalition partners would be able to accommodate their "separate views on the shape of the deterrent".

<http://www.bbc.co.uk/news/10370838>

18. 17 June 2010 Last updated at 11:59 GMT

Cyber-war a growing threat warn experts

By Clark Boyd Technology Correspondent, BBC World Service



Only one person, a student living in Tallinn, was ever charged over the 2007 Estonia cyber attacks. He was fined £1000.

In 2007, Estonia was the subject of a series of cyber attacks which crippled the internet across the country.

Banks, government departments and the national media all found their websites swamped by a tidal wave of spam which took them down. [59in]

The perpetrators were never caught.

Some evidence pointed to Russian government involvement in the attacks, but no definitive link to the Kremlin was found.

So was it the first ever act of cyber-war?

Defining cyber war

Experts from nearly 40 countries gathered in the Estonian capital Tallinn to discuss the latest issues in the fight against virtual attackers.

Estonian President Toomas Hendrik Ilves opened the conference with a stark warning about the seriousness of cybercrime.

"Our critical infrastructure, electricity grids, transportation networks and mobile phone networks are so enmeshed and tied to the internet that any open society is open to complete and utter failure," [60in] he said.

Worse still, it's not easy for a country to protect itself from such an attack, added Estonia's Minister of Defence Jaak Aviksoo.

"There are no smoking guns, no foot or fingerprints in virtual reality," he said.

"The computers used in the (Estonia) attacks were distributed worldwide, in more than 100 countries. The attackers can hide very easily, and that is a problem."

For Mikko Hypponen, chief security officer at F-Secure, what happened in Estonia was not an act of war, especially as the country's military systems were not targeted.

"In my book, real cyber-war would be when the army of Country A attacks the computer systems of Country B. And that hasn't happened, yet," he said.

"In the attacks we've seen so far, there's no way to prove direct government involvement."

They were certainly classed as a national security threat though.

In Estonia, the vast majority of all banking is done online. And when the attackers took the banks down, there was pressure on the Estonian government to do something, and fast.

"If people can't access their money, if they can't buy milk and bread, then you're going to have problems," said Kenneth Geers, a US Navy representative.

"Data packets via the internet are fired all the time in anger. However, if no one dies, then according to the laws of war, we're not in conflict."

For the experts in Tallinn, the threats were all too real, and many believed the motivation for cyber attacks had moved beyond politics.

"In real space, there are real lines between criminals and soldiers," said Heli Tiirmaa-Klar, Estonia's national cyber-defence coordinator.

"But in cyberspace, the criminals could be used as mercenaries and proxies to fulfill the tasks others have told them to do."

Easy hacking

Skilled hackers at the conference said malware designed to be used in attacks could be purchased for a few hundred dollars online, or even downloaded for free.

Haroon Meer is a hacker and lead researcher at thinkst, a company that does penetration testing for clients.

He helps companies and organisations determine their own online weaknesses by breaking into them.

But he has also done a lot of thinking about how he would attack an entire country.



One expert said his government network is attacked 60,000 times per second.

"When people talk about cyber-defence, they instantly say, 'we'll protect control systems.' But what about banks, what about the internet service providers? Should the United States protect Amazon or eBay, which are huge financial income for the country?" [61in] he said.

Security consultant Dr Charlie Miller demonstrated just how quickly and easily he could take control of a single machine through a programming flaw he'd found in a web browser.

In less than 10 seconds, Dr Miller, who once worked for the US National Security Agency, took complete control of a machine remotely. He gained access to e-mail, activated the laptop's built-in camera and took a picture of the victim.

He said that with a budget of \$100m (£67m) he could train a team to carry out a major cyber attack on an industrialised nation, with targets including military systems, critical infrastructure and banks.

"We would be able to get into many sensitive systems and cause disruption," he said.

"It's certainly not the same thing as dropping a bomb, but with a few years and enough money, we could cause havoc."

But consumers are not deterred by the magnitude of the potential threat, and even in Estonia e-services have continued to grow at a healthy rate since the attacks.

"Estonians were not frightened by what happened in 2007," said Heli Tiirmaa-Klar.

"We don't think dependency on IT is a bad thing. It's a good thing, and we are used to it."

<http://www.bbc.co.uk/news/10339543>

19. 15 March 2010 Last updated at 09:27 GMT

Meet USCybercom: Why the US is fielding a cyber army

By Patric Jackson



Peacetime role: 24th Air Force personnel recently set up satellite communications in Haiti as part of the earthquake relief effort

The US is in the process of creating a unified cyber command, to fight the wars of the future. The Pentagon has no doubt that the next conventional war will include a cyber element.

Looking out of a window in London's Canary Wharf, Daniel Kuehl gestures randomly towards a high-rise.

"Let's just assume that somewhere in that building there are a bunch of cyber systems, networks, routers, that are militarily important to take out," he said.

"Which would you think would be the better way of doing it in terms of this neighbourhood? To make it stop working through a bunch of key strokes [62in] or to put a laser-guided, 1,000-lb weapon through the third floor and blow it to shreds?"

"We're really good at that second operation - but there might be some advantages to doing it the first way."

The Pentagon is creating its first fully fledged cyber command - USCybercom - to improve its ability to wage war with key strokes.

'Precision disruption'

There will be "one guy in charge of cyber defence and offense", says Mr Kuehl, who helped plan the air campaign for the first Gulf War before becoming the professor of information operations at the National Defense University in Washington.

Amit Yoran, a former cyber security director at the Department of Homeland Security, and now head of Netwitness Corp, defines cyber war as "the use of information technologies for the purposes of conducting warfare".

"That could be using a computer network or a cyber attack to take systems out and make them inoperable and deny access to the legitimate users of those systems at a critical point in time," [63in] he says.

"It could also be cyber system exploitation which I would define as compromising systems, accessing data and using that information but in a more covert way, not necessarily tipping off what you have access

[64cm] to and how you are using it, perhaps for later attack purposes."

Dr Kuehl, in London recently for the Cyber Warfare 2010 conference, believes the day may come when Pentagon computer experts will enjoy the same kind of combat status as jet pilots or frigate commanders. Their weapon of "precision disruption" has the potential to be more efficient, more effective, less damaging, less life-threatening than a kinetic weapon," he says.

But as with pilots and warship commanders, as US cyber warriors get stronger, so may their potential adversaries.

Hitting banks

Summer of 2008, Beijing Olympics. As the world settles down to watch the Games, war erupts deep in the Caucasus Mountains. Georgian rockets fly, Russian tanks roll - and Russian hackers storm Georgian websites [65in].

Some experts regard this as the first cyber war.

"We saw a military mobilisation by Moscow into South Ossetia accompanied by clearly orchestrated cyber attacks against the Georgian government's communication systems and the banking system," says Nigel Inkster, director of transnational threats and political risk at London think tank The International Institute for Strategic Studies (IISS).

The planners in Moscow were quite careful, he says, calibrating the "proportionality and focus" of the cyber attack to remain "broadly in line with the law of armed conflict (LOAC)".

The law does not permit attacks on civilians or civilian infrastructure that does not directly contribute to the state's ability to prosecute the conflict, and while the attacks on the banking system arguably target civilians unduly, Mr Inkster says, "in a country which still predominantly operates a cash economy that would be debatable".

While the exact level of Russia's cyber military organisation is not clear, and China does not have a formal cyber arm, the creation of USCybercom is clearly a response to the two countries' "greatly increased activity in this arena", says Mr Inkster, a former deputy head of the British foreign intelligence agency MI6.

So, are we witnessing the first steps in a new arms race?

"There is a lot of concern in both countries [China and Russia] that the US is seeking to achieve in cyberspace the same dominance it is perceived to have in the realms of conventional and nuclear weapons, and space," says Mr Inkster.

USCybercom will cover all four armed services, each of which recently gathered its cyber components into one unit: 24th Air Force, 10th Fleet, Army Forces Cyber Command and Marine Corps Cyber Command.

The oldest of these, 24th Air Force, describes itself as an "operational warfighting organization that establishes, operates, maintains and defends [US Air Force] networks and exploits and attacks threat networks" [66in].

Headquartered in Texas, it comprises 3,339 military, 2,975 civilian and 1,364 contractor personnel and one of its key units, 67th Network Warfare Group, prides itself on having a presence "on every continent except Antarctica", which is a demilitarised zone.

'Significant target'

Brig Gen Charles Shugg, vice-commander of the 24th, explains that the very nature of the air force requires strong cyber defences.

"We have become dependent on our information networks to accomplish our mission, and while those information systems have greatly improved our capabilities, they have become a significant target for our adversaries," he says.

Some sense of its area of operations was given in February, when it announced awards for five of its "cyber warriors".

One was honoured for leading an anti-virus script initiative "that reduced risk to personal computers by 85%" and "crafting 17 courses of action in response to adversary tactics, which countered a major threat".

Another "secured 425 gateways, 650,000 personal computers and 300,000 users and identified a flaw in the policy governing use of USB drives in the force, thus "protecting the network from a viable threat". Not everyone is convinced of USCybercom's military value. One US official at the London conference said that if cyber warfare was a WMD it was only a weapon of "mass disruption, not destruction".

But the US Senate is expected to confirm Lt Gen Keith Alexander, who also heads the US National Security Agency (NSA), as head of USCybercom in the near future.

If this happens, he will rise to the rank of a four-star general, and his new command will get its badge and take its place in the military.

"Believe me, creating an organisation led by an officer of that rank is not easy," says Daniel Kuehl.

"It's not simple and it's not done unless there are perceived to be very, very pressing reasons for doing so. We are deadly serious about this."

<http://news.bbc.co.uk/2/hi/technology/8511711.stm>

20. 11 February 2010 Last updated at 08:37 GMT

How Iran's political battle is fought in cyberspace

By Jon Leyne



International media were banned from reporting on protests in June, so pictures on Twitter filled the gap.

They called it the "Twitter revolution". Iran's post-election protests showed the world the power of new media to organise and publicise [67wb] opposition in a controlled society.

On the anniversary of the Islamic revolution in 1979, once again Twitter, Facebook and other internet tools could be crucial in helping the opposition organise another major protest.

Since Iran's disputed election in June of last year, the cyber war between government and opposition has taken on a whole new dimension.

"Absolutely extraordinary and unprecedented" - that was the role of the internet in Iran's election dispute according to Hamid Dabashi, who presents an opposition webcast to Iran from New York every week. His webcast is broadcast on YouTube, and his staff say it then goes "viral" - spread across Iran by other websites, CDs and Bluetooth links between mobile phones.

Mr Dabashi described the role of the internet in helping to organise the huge post-election demonstrations.

"Nobody called for it except on the internet," he said.

"Cyberspace was buzzing with information that there was to be a demonstration from this square to that square. As a result if there is a leadership... it is really the networking that the internet has made possible."

Raw power

Just over a week after the election, the footage of a young woman, Neda Agha Soltan, bleeding to death from bullet wounds was sent from a mobile phone and relayed around the world.

The opposition believes she was shot by one of the government's Basij militia.

The Iranian government continues to deny responsibility, but the pictures have swayed opinion internationally.

That raw power has been noticed by governments.

The US Secretary of State, Hillary Clinton, hosted a conference recently on it in Washington and proposed new support to try to free the internet from censorship.

The Iranian government has become far more sophisticated in its handling of the internet as well.

A day after the election, Iran closed the internet down entirely for half an hour, then slowly loosened its grip, as the authorities struggled to gain control. [68wa]

"If you look at what was going on after the election, it was very clear that they had no solid plan in place," explained Austin Heap of the Censorship Research Center in San Francisco.

"The way they were filtering, what they were filtering. Just basic things like the speed the internet was operating at would change day by day, week by week. And if you look at just the past three months their filtering attempts have become more co-ordinated and organised."

Crude blocking

Mr Heap has been writing an anti-censorship program, Haystack, which he hopes to spread to internet users in Iran.

My experience from two years in Iran was that both sides struggled to gain the upper hand.

Any program to prevent filtering would have a limited life, as the government eventually found a way to block it.

But at the same time the filtering system was crude and ineffective. In the turmoil that followed the election, that "mood swing" became even more dramatic.

One morning the whole BBC website would be inaccessible, and even usually secure connections were blocked.

On other days the controls would be mysteriously lifted, enabling us to use the internet to broadcast live from our office in Tehran.

Now Iran says it has organized a new "cyber army" with a more sophisticated approach.

Supporters tracked

According to experts I spoke to in the United States, the Revolutionary Guards have drafted, sometimes against their will, some of Iran's bright young internet-savvy generation.

Not only are they helping to block opposition communications and track down opposition supporters from their use of the web, they have taken the battle to the enemy.

The cyber army claimed responsibility recently for what Mr Heap said was a well co-ordinated attack on Twitter and other websites.

"The attacks were very well organised," [69wa] he told me.

"They had back-up plans and back-up back-up plans, all of which got enacted. It was clear with the timing and the co-ordination that people had planned this ahead and were trying to make a statement."

The battle for control of the web is carried out between governments and individuals.

Each new censorship tool used by Iran or other authoritarian countries is taken up as a challenge by many thousands of young computer experts around the world.

It is a game of cat and mouse, likely to change the face of the internet for the indefinite future.

Cyber battle has become cyber war, and there is no sign of a ceasefire.

Leyne is the BBC's Tehran correspondent. He is reporting from London after being forced to leave by the Iranian government for reporting on protests in June

http://news.bbc.co.uk/2/hi/middle_east/8505645.stm

21. 17 November 2009 Last updated at 08:18 GMT

Age of cyber warfare is 'dawning'

Digital Planet Alka Marwaha BBC World Service

Cyber war has moved from fiction to fact, says a report.

Compiled by security firm McAfee, it bases its conclusion on analysis of recent net-based attacks.

Analysis of the motives of the actors behind many attacks carried out via the internet showed that many were mounted with a explicitly political aim.

It said that many nations were now arming to defend themselves in a cyber war and readying forces to conduct their own attacks.

While definitions of what constitutes cyber war are not shared, it was clear that many nations were preparing for a future in which conflict was partly conducted via the net [70in].

"There are at least five countries known to be arming themselves for this kind of conflict," said Greg Day, primary analyst for security at McAfee Europe.

The UK, Germany, France, China and North Korea are known to be developing their own capabilities.

The US is known to have an operating manual governing the rules and procedures of how it can use cyber warfare tactics. It is known to have used hack attacks alongside ground operations during the Iraq war and has continued to use this cyber capability while policing the nation.

Mr Day said there was evidence of a growing number of attacks that could be classed as "reconnaissance" in advance of a future conflict. The ease with which the tools of such attacks can be gathered and used was worrying, said Mr Day.

"To go to physical war requires billions of dollars," he said. "To go to cyber war most people can easily find the resources that could be used in these kind of attacks."

The targets of such future conflicts were likely to be a nation's infrastructure, said Mr Day, because networks of all kinds were now so embedded in peoples' lives.

In response, he said, many nations now have an agency overseeing critical national infrastructure [71in] and ensuring that it is adequately hardened against net-borne attacks.

Chris Wysopal, chief technology officer at Veracode which advises many governments on security, said cyber war presented its own problems when it came to deciding motive and finding the perpetrators.

"In physical warfare it's pretty clear who has which weapon and how they are using them," he said. "In the networked world that attribution is incredibly difficult."

The same is true for cyber crime, he said, where following a trail of money can lead investigators back to a band of thieves.

"If it is someone stealing information or planting logic bombs, it's far more difficult to find them," he said.

Mr Wysopal said many governments had woken up to the threat and were starting to put in place systems and agencies that could help protect them.

However, he said, they still had some weaknesses.

"The thing about governments doing this is that they have a time horizon of many years," he said. "But the criminals are doing it in a matter of months."

<http://news.bbc.co.uk/2/hi/technology/8363175.stm>

22. 24 June 2009 Last updated at 12:00 GMT

What rules apply in cyber-wars?

Digital Planet Alka Marwaha BBC World Service



Iran has blocked many social networking sites and blogs

As protests and violence continue in Iran so do the attacks and counter-attacks online.

Pro-reform campaigners have targeted Iranian websites like that of President Ahmadinejad, [72wb] while the state continues to clamp down on social networking sites, blogs and mobile networks in the country [73wa].

BBC World Service's technology programme, Digital Planet spoke to journalist Cyrus Farivar who recently attended the international conference on cyber warfare in Estonia.

"Over in Iran there has been a lot of activity trying to organise very crude cyber attacks to bring down the websites of opponents of the reformist candidate Mr Mousavi and to take down for example, the website of President Ahmadinejad, and other Iranian government websites as a way to protest against them.

"These types of attacks are a minor version of other types of cyber attacks that have been going on for many years around the world," he said.

Estonia's own web infrastructure was blitzed from outside in 2007 and the attack was thought to have originated from Russia.

Cyber centre

After that experience, Estonia established a body called the Cooperative Cyber Defence Centre of Excellence, in order to enhance Nato's cyber defence capability.

"A number of government websites, Estonian banks and media websites were brought down by a massive flood of artificial traffic, [74in]

that was brought in from the outside, bringing down a number of websites over the course of a few weeks," he added.



The Estonian President discussed cyber-war with US president

The Estonian President, Toomas Hendrik Ilves has just returned from a brief tour of the United States where he met with President Obama in Washington to discuss cyber issues.

"Ultimately I would say that the attacks actually back-fired because Estonia had been talking about cyber-security for a variety of reasons, even telling Nato that we ought to have a cyber-centre of excellence," said President Ilves.

Nato agreed that it was a serious issue and the centre was set up in Estonia's capital city Tallinn.

Defining war

One of the major issues in cyber warfare is defining what it actually means, thinks Mr Farivar.

"After the Estonian attack there was a lot of rhetoric that was thrown around, cyber-war, digital pearl harbour, cyber 9/11, these kinds of hyperbolic phrases," he said.

"We need to be careful with how we describe these types of issues because when you talk about war, it has a very specific definition in a political and legal context.

"Should we invoke Article Five of the Nato Charter which says that an attack against one Nato country is an attack on all Nato countries and should all the Nato countries then attack back at some unknown entity through cyber means?" he asked.

The 2007 attacks in Estonia were launched via a botnet, a network of computers that have been subverted by malicious code so they fall under someone else's control.

At the conference, a couple of graduates from the University of Bonn in Germany showed off a technique they had developed to counter the effects of botnets.

Botnets are networks of computers which have been subverted by malicious code so they fall under someone else's control.

Owners of machines forming a botnet typically do not know their computer has been hijacked and home users account for 95% of all attacks mounted by botnets, according to figures from security firm Symantec.

"These two graduate students basically said, we now know how to counter-attack these botnets, we can undo them and use their own software against them.

"However, whilst they may want to launch their counter-attack against a botnet, they might want to counter these effects, as there are legal issues that they have to deal with first," said Mr Farivar

"The legal and political frameworks that exist around the world, haven't quite yet caught up to these technological realities," he added.

<http://news.bbc.co.uk/2/hi/technology/8114444.stm>

0. Page last updated at 08:44 GMT, Monday, 22 June 2009 09:44 UK

West 'seeks Iran disintegration'
BINTEO [2.10]

Iran's foreign ministry spokesman, Hassan Qashqavi, has accused Western media of attempting to "disintegrate" Iran.

He claimed journalists from CNN had been trained to hack into government websites and said this was a "cyber war".

<http://news.bbc.co.uk/2/hi/8112341.stm>

23. 15 June 2009 10:07 Last updated at 09:07 GMT

Israel and foes in internet war

By Ahmad Budeiri
BBC Arabic, Jerusalem

The battlefield in the Middle East may be changing. Israeli intelligence agencies have warned citizens of the risks in using social networking sites such as Facebook.

They say that the internet is a war zone between Israel and its enemies including Hamas, Hezbollah and Iranian groups,



Israeli intelligence sees using Facebook as a potential threat to security

According to the Israeli intelligence analyst, Dr Ronen Bergman, Israel's concerns are twofold: first, that Israeli internet sites might be breached and sabotaged; second, that Israeli soldiers might be enticed to give away secrets. [75wb]

Israeli intelligence officials are worried that Israelis risk leaking sensitive information or may even be kidnapped if they speak too openly with Palestinians and Lebanese online.

They fear that Israelis might be encouraged to leave Israel to meet someone they meet in the virtual world of Facebook and then be kidnapped in the hope that they can be exchanged for some of the thousands of Palestinians held in Israeli jails.

Many national governments issue advice to their citizens about using the internet safely. But Israeli intelligence tips are more like strict orders.

National service is an obligation of Israeli citizens and many have knowledge of information which is secret or at least highly sensitive.

Dr Ronen Bergman says that Hamas claims that it got important information via the internet about intelligence networks and spies and also about some of the elite units in the Israeli army.

Of particular concern are social networking sites such as Facebook.

The fear is that people who use Facebook may let their guard down in a way they would never do if they were speaking face-to-face. [76wb]

Virtual Training Camps

But Israel cannot just rely on giving advice.

A battle is being fought day and night by trained "soldiers" fighting an enemy they cannot see.

Private companies are involved in this war to provide protection for government and financial websites which are constantly under attack and sometimes breached. [77cm]

Safenet Aladin was formed in the United States 26 years ago and now has branches in over 100 countries

It has a specially designed laboratory in Israel to conduct experiments and simulate electronic attacks.

The laboratory is a kind of virtual training camp where engineers are taught how to use the most sophisticated programs to repulse electronic invasions.

The manager of security technology at the Israeli branch of the company, Ofer Alzam, told BBC Arabic Radio about the laboratory and how the battle is fought on the internet.

One of the tools they use in the battle is an electronic key which contains encrypted data and is provided to a number of clients to help protect vital secret information. [78cm]

The key not only protects secret information but also foresees computer threats.

"First, we have to foresee the threat. If we can anticipate it we can normally deal with it. In one or two percent of cases however, we have to minimise the threat window to provide protection and security against new threats, particularly for major internet providers" says Mr Alzam.

Bullet proof

The most sensitive Israeli strategic sites are those housing electronic databases.

The companies that provide these for individuals, the government and private companies pride themselves on the level of security they provide their clients.

Saji Maysar, the marketing manager of on such internet security company, Samial, took me to a room secured by strong doors and bullet-proof glass.

Over the loud hum of the computer servers housed there he said that if there was ever a successful attack on this room it would be the equivalent of a strike on a key military base.

He said the room held sensitive information which not **only had to be protected against cyber-attack** but also against physical attack by those who wanted to harm Israel and its citizens.

The Israeli army itself has a division trained to fight cyber warfare to protect military secrets. [79cm]

When intelligence officers resign from the army, some take their knowledge to one of the prestigious computer companies.

Many analysts now believe that the Israeli capability in this cyber war may now be as strong as more traditional Israeli defences built up over the past half-century.

It is difficult to judge who is winning this war, or sometimes to even find out where the battles are being fought.

But Israel's considerable intelligence resources need to be constantly on full alert to prevent a successful attack by nimble enemies who are becoming increasingly astute in fighting a virtual war from their laptops.

http://news.bbc.co.uk/2/hi/middle_east/8079774.stm

24. 31 March 2009 09:17 Last updated at **08:17 GMT**

The Tech Lab: Ken Silva



The engine of the internet could come to halt unless security is sorted out

Ken Silva, chief technology officer at Verisign, warns about the dangers that threaten the open internet.

Ask internet users what they want from their service and 99 times out of 100 the answer will be the same: more - more speed, more bandwidth and more flexibility of use.

Nobody knows this better than internet infrastructure providers, who for years have devoted the vast majority of their development budgets to meeting consumer demands for faster, more flexible networks. Security has often been an afterthought.

For the most part, this market-driven approach has been a boon to the internet and its users, but recent events have begun to illustrate the dangers of this single-minded focus.

In the past couple of years, two serious incidents have sent ripples throughout the global internet, causing real damage and painting a troubling picture of vulnerabilities that could someday bring this vital engine of commerce and communication to a grinding halt, imperilling billions of dollars in commerce and worse, as the internet becomes an ever more critical component of our daily lives. **[80in]**

The simple truth is that our global investment in the security and stability of the internet has not kept pace with our relentless pursuit of greater speed and flexibility. If we don't correct this growing imbalance, and soon, we face the possibility of a global online incident, the impact of which could be felt for years to come.

In April 2007, a spat between Estonia and Russia over a Soviet-era war memorial erupted into what has been described as the first modern "cyber war" as Russian-based attackers effectively took the entire nation of Estonia offline for a period of weeks. **[81in]**

In February 2008, the Pakistani government, responding to an anti-Islamic video clip appearing on YouTube, unintentionally set in motion a series of events that prevented most of the world's internet users from visiting the site - one of the internet's most popular - for a period of hours. **[82wa]**

Perhaps the most remarkable thing about both of these incidents is how unremarkable they were - at least from a technical standpoint.

Although remarkably well coordinated, the Estonian attack was not the largest ever recorded, nor was it particularly novel in its methods. More than anything, the incident demonstrates just how damaging even a "typical" attack can be when timed properly to strike vulnerable targets.



Silva: More can be done to secure the open internet

As is the case in the hundreds of similar attacks that take place each day, the perpetrators harnessed the power of corrupted personal computers to swamp their targets in a sea of bogus internet traffic, effectively cutting off whole neighborhoods of the Estonian internet from legitimate traffic.

Millions of these infected "zombie" computers exist. Used in concert, they can generate attacks that few systems on earth are capable of withstanding.

The Pakistan-YouTube incident was even more commonplace - the result of two seemingly benign errors and a quirk in an internet protocol designed at a time when most of the global network ran on trust and virtual handshakes.

The details of the incident are less important than the fact that the circumstances that allowed it to occur remain unchanged, as do scores of similar vulnerabilities endemic to the internet's open architecture.

The message is that these sorts of incidents can - and almost certainly will - happen again. And if history tells us anything, it's that the next time will be worse. More powerful computers hooked up to more robust internet connections translate into more severe and disruptive attacks.

Also, as we rely on the internet to a greater and greater extent, the likelihood that such an incident will cause real harm to our lives and livelihoods only increases.

It would be wrong to suggest that this is entirely preventable. The openness and interconnectedness that are the internet's hallmarks ensure that there will always be vulnerabilities for attackers to exploit.

But we can do a much, much better job of securing the critical internet infrastructure on which we all rely.



Many home computers are part of zombie networks

Stability and security must become a higher priority for everyone involved in the development and stewardship of the global internet. Companies may not be able to monetise security in the same way that they monetise speed, but nobody in this space can afford to remain ignorant of the costs associated with getting it wrong.

The "choice" between speed and flexibility on one hand, and stability and security on the other is more a product of cost than anything else. The cost of providing secure, stable network infrastructure is equal to, and in some cases, greater than the cost of increasing network speeds. [83in]

The good news is that there isn't, for the most part, a fundamental technological tension between flexibility and stability on the internet. Indeed, one of the most critical components of stability - excess capacity - is also essential to providing greater speed and flexibility.

This challenge doesn't require technological breakthroughs or dramatic paradigm shifts. We know what needs to be done if we are to bring the security and stability of this global network up to par with its stunning speed and flexibility.

The choice is so simple that it isn't a choice at all: invest the time and resources necessary to safeguard the internet against known dangers, or face the sort of failure that could permanently change the face of the internet for the worse

<http://news.bbc.co.uk/2/hi/technology/7972393.stm>

25. 14 August 2008 Last updated at 07:11 GMT

Caucasus foes fight cyber war

By Neil Arun BBC News

Armed with computers, unseen ranks of hackers are fanning conflict in the Caucasus.

Internet users in Russia and Georgia have attacked vital websites in each other's countries, [84in] in a virtual echo of battles being fought on the ground by troops and tanks.

Several Georgian government portals have been defaced [85in] or forced offline by hackers allegedly based in Russia.

Visitors to Georgian President Mikhail Saakashvili's website were recently routed to a page portraying him as a modern-day Hitler. [86wb]

Georgia's parliament and foreign ministry sites have also repeatedly been disabled, allegedly by attacks from networks of hijacked computers.

Hackers from Georgia have meanwhile been blamed for targeting the websites of Russian news outlets and the separatist government of South Ossetia, which Russia supports.

Internet security experts say it was inevitable that a conflict fired by separatism in the Caucasus should spill into cyberspace.

The republics of the former Soviet Union are, along with China and Brazil, major centres of cyber-crime, according to Alex Shipp of the email security firm, MessageLabs.

While the Chinese specialise in industrial espionage and the Brazilians are adept at online financial fraud, Mr Shipp says Russian criminals dominate the market in online tools tailored for amateur hackers. [87cm]

"Several Russian sites specialise in selling software that would-be cyber-criminals can download," he says.

'Dark side'

Russia's association with cyber-crime dates back to the demise of the former Soviet Union - an event that roughly coincided with the dawn of the internet era in the early 1990s.

For thousands of youths who came of age as communism collapsed, computers symbolised the new spirit of enterprise.

Treating programming as a tool for self-empowerment, these eager amateurs eventually became skilled software engineers.

They learnt their expertise, in part, from a brilliant earlier generation of Soviet-era developers, says the BBC News website's technology correspondent, Mark Ward.



Hackers created a defamatory collage comparing Mr Saakashvili to Hitler

These older programmers had devised clever software to sidestep the shortcomings of the clunky communist computers they had been forced to use.

Although Russia's new engineers had skills to match the brightest minds of Silicon Valley, they earned far smaller sums than their peers in the West.

Bored and underpaid, many turned their talents to hacking.

Gradually, they attracted new paymasters from the thriving post-Soviet underworld. As the gangsters harnessed the hackers' skills, the profits from cyber-crime grew.

The result, according to technology critic Bill Thompson, is a business that today resembles the "dark side of Silicon Valley".

Hacking made easy

The people accused of attacking government websites in Georgia's war with Russia are using many methods pioneered by the cyber-criminals.

However, it is far harder to trace hackers who are driven by patriotism rather than profit.

"Where extortion or fraud is involved, you can follow the money trail," Bill Thompson says. "But politically-motivated attacks are almost impossible to police."

Hacking technology is also becoming increasingly accessible.

The most common form of attack uses networks of hijacked computers, or botnets, that besiege a site with more traffic than it can handle, eventually forcing it offline.

Such "denial of service" attacks are often the work of amateurs, following instructions downloaded from the internet. [88in]

Experts are more commonly responsible for "deface hacking" - attacks that manipulate the content on a secure website or divert traffic from it.

Lawless space

According to Anton Nosik, a Russian businessman and internet pioneer, most hackers tend to be teenagers with broadband internet and limitless time on their hands.

He says websites hosted in countries with relatively small, under-developed networks are often most vulnerable to attack.

The Georgian government, he says, ought to consider moving its websites to providers in the US or Western Europe if it hopes to reduce its exposure to attack.

In doing so, it would follow an example set by websites that support separatists from the Russian republic of Chechnya - also frequently targeted by hackers.

"Websites run by Chechen militants are hosted in western European countries with relatively large, secure networks - capable of handling larger volumes and less easily taken off air," Mr Nosik says.

But, he warns, there is no foolproof defence against the most determined hackers, for whom Russia remains a haven. [89in]

"The very notion of crime only exists in places where you have the law and the law is applied," he says.

Global laws governing cyberspace are still being devised. In nations waging war, they are least likely to be applied.

<http://news.bbc.co.uk/2/hi/europe/7559850.stm>

26. 14 May 2008 17:00 Last updated at 16:00 GMT

Estonian cyber defence hub set up

Seven Nato nations have backed a new cyber defence centre in Estonia, which last year blamed Russia for weeks of attacks on its internet structure.

Germany, Slovakia, Latvia, Lithuania, Italy and Spain will staff and fund the hub in the Estonian capital Tallinn.

Estonia came under cyber attack in 2007 after its decision to remove the bronze statue of a Red Army soldier from the centre of Tallinn.

Moscow denied involvement in the flood of data which crashed computers.

"We have seen in Estonia that a cyber attack can swiftly become an issue of national security," Nato spokesman James Appathurai said after a signing ceremony in Brussels.

"Cyber attacks can cripple societies." [90in]

The US will initially send an observer to the project, which will have some 30 staff when fully operational in August.

The centre will provide research, consultation and training on the development of cyber defences for participating national governments.

<http://news.bbc.co.uk/2/hi/europe/7401260.stm>

27. 25 April 2008 14:48 Last updated at 13:48 GMT

Hackers warn high street chains

High street chains will be the next victims of cyber terrorism, some of the world's elite hackers have warned.

They claim it is only a "matter of time" before the likes of Tesco and Marks & Spencer are targeted.

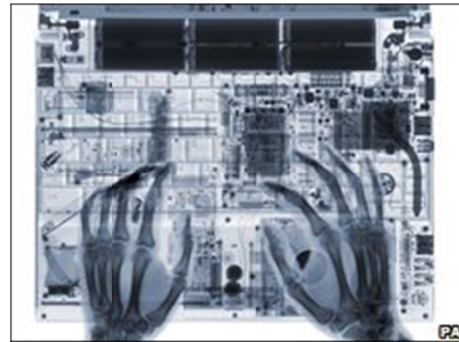
Criminals could use the kind of tactics which crippled Estonia's government and some firms last year, they warned.

The experts were members of the infamous "Hackers Panel" which convened in London this week at the InfoSecurity Europe conference.

The panel includes penetration testers [91cm] and so-called "white hat" hackers, who help companies tighten up their digital security by searching for flaws in their defences.

Previous panellists include Gary McKinnon, known as Solo, alleged by the US government to have hacked into dozens of US Army, Navy, Air Force, and Department of Defense computers.

The "hackers" usually remain anonymous, "for security reasons", but this year's panellists agreed to break cover.



The hackers panel is one of the highlights of InfoSecurity Europe

Common cause

First up was Roberto Preatoni, the founder of the cyber crime monitoring site, Zone-H, and WabSabiLabi, a trading site for security researchers. His appearance came just a few months after he was arrested by Italian authorities on charges of hacking and wiretapping, as part of the ongoing investigation into the Telecom Italia scandal.

Mr Preatoni told the audience that the attacks in Estonia were a harbinger

for a new era of cyber warfare.

"I'm afraid we will have to get used to this," said Mr Preatoni, also known as SyS64738. "We had all been waiting for this kind of attack to happen.

"Estonia was just unfortunate to be the first country to experience it. But very soon, our own [western] companies and countries will be getting attacked for political and religious reasons.

"This kind of attack can happen at any time. And it will happen."

During the two week "cyber war" against Estonia, hackers shut down the websites of banks, governments and political parties using "denial-of-service" (DoS) attacks, which knock websites offline by swamping servers with page requests. [92in]

As many of the attacks originated from Russia, the Estonian government pointed the finger at the Kremlin. But Mr Preatoni said that, having spoken to contacts in the hacking community, he was clear that "Putin was not involved".

"In my opinion, this was a collection of private individuals who spontaneously gathered under the same flag.

"Even though Estonia is one of the world's most advanced countries in IT technology, the whole economy was brought to its knees.

"That's the beauty of asymmetric warfare. You don't need a lot of money, or an army of people. You can do it from the comfort of your living room, with a beer in your hand.



Notorious hacker Gary McKinnon has previously taken part in the panel

Gate control

His warning was echoed by Steve Armstrong, who teaches seminars in hacking techniques, at the SANS Institute for information security training.

"If someone wants to have a pop at the UK, they are unlikely to go for the government web servers. They will go for the lower hanging fruit - companies which are seen as good representatives of the country.

"The likes of Tesco, Marks & Spencer and B&Q can be seen as legitimate targets. We have to get the message across to companies [to invest in information security].

"At the moment Chief Executives are only interested in the bottom line. But remember - if tesco.com goes down, that's a lot of shopping."

Mr Preatoni said that the Estonian government's repeated failure to thwart the attacks was proof that we still have "no good solutions" for denial of

service attacks.

The panellists then argued over whether Internet Service Providers should do more to tighten security, by helping customers' protect their computers from being "zombified" by hackers for use in distributed DoS attacks.

"Actually, I don't think the ISPs should have any role in security," said Preatoni.

"In my opinion, that's like asking the Royal Mail to be responsible for the quality of your post."

But his view was immediately challenged by the third panellist, Jason Creasey, head of research at the independent Information Security Forum.

"I believe ISPs can play a phenomenal role in security, with a little bit of legal pressure," he claimed.

Net weakness

He was backed by an audience member, Angus Pinkerton, of Lynks Security Consulting. "The only way to defend against a distributed attack is with a distributed defence," he argued.

"I think it's unacceptable that ISPs are content to let their customers be part of bot-nets."

He challenged Steve Armstrong's view that asking ISPs to perform security duties was "fundamentally, censorship." [93wa]

"This is not about free speech," said Mr Pinkerton. "Free speech does not entitle you to shout fire in a crowded theatre."

In the meantime, Mr Preatoni warned the audience it is "only going to get easier" to carry out a DoS attack, because he claimed the latest net address system, known as Internet Protocol Version 6 (IPv6), is actually more amenable to DoS.

Later, he told the BBC that the rise in cyber attacks originating in China was a convenient cloak for western countries to disguise their own cyber espionage activities [94cm].

"It's too easy to blame China," he said. "In fact, legitimate countries are bouncing their attacks through China. It's very easy to do, so why not?"

"My evil opinion is that some western governments are already doing this."

<http://news.bbc.co.uk/2/hi/technology/7366995.stm>

28. 25 January 2008 Last Updated: 10:31 GMT

Estonia fines man for 'cyber war'

A 20-year-old ethnic Russian man is the first person to be convicted for taking part in a "cyber war" against Estonia.

Dmitri Galushkevich was fined 17,500 kroons (£830) for an **attack which blocked the website**. of the Reform Party of Prime Minister Andrus Ansip.

The assault, between 25 April and 4 May 2007, was one of a series by hackers on Estonian institutions and businesses.

At the time, Estonia accused the Russian government of orchestrating the attacks. Moscow denied any involvement.

Kremlin spokesman Dmitry Peskov told the BBC in May 2007 that the allegations were "completely untrue".

Minority attacks

The attacks took place against a backdrop of riots by ethnic Russian Estonians prompted by the removal of a Soviet war memorial from the centre of Tallinn.

During the unrest, one person was killed and more than 150 injured.

Moving the so-called Bronze Soldier was seen as an affront to the memory of Russian soldiers who died during World War II.

Prosecutors said Mr Galushkevich, a student, had claimed the attack was an act of protest against Mr Ansip, who became a hate figure for Estonia's Russian minority.

Ethnic Russians make up about a quarter of Estonia's population of 1.3 million.

Other websites that were crippled by the denial-of-service attacks, which knock websites offline by swamping servers with requests, included those of the state government, political parties and leading newspapers. [95in]

Some sites also redirected users to images of Soviet soldiers and quotations from Martin Luther King about resisting "evil". [96wb]

'No record'

Most of the hackers were believed to be based in Russia - the Estonian government said at the time that Kremlin computers were used to carry out a number of the attacks.

The tiny Baltic State enlisted the help of Nato to help defend their networks in what was described as a "cyber war".

But David Emm, senior technical consultant at Moscow-based antivirus software company Kaspersky Lab, told the BBC website that he believed the most likely culprits were "younger types who, in other days, would have been writing and spreading viruses".

Mr Galushkevich is the first individual to be fined in connection with the attacks.

"The young man admitted his guilt," Gerrit Maesalu, spokesman for the regional prosecutor's office in north-east Estonia, told AFP.

"In deciding the verdict, the court took into account the fact that he had no criminal record," he said.

Several other investigations into the events are under way, but no-one else has yet been brought to trial.

<http://news.bbc.co.uk/2/hi/technology/7208511.stm>

29. 17 May 2007 Last Updated: 15:21 GMT

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.

"In the 21st century it's not just about tanks and artillery," Nato spokesman James Appathurai told BBC News.

"We have sent one of our experts at the request of the Estonian authorities to help them in their defence."

'Paperless government'

Estonia wants to put the issue at the top of Friday's EU-Russia summit agenda.

The head of IT security at Estonia's defence ministry, Mikhail Tammet, told BBC News that the attacks had affected a range of government websites, including those of the parliament and governmental institutions.

He said the country was particularly vulnerable as much of its government was run online.

"Estonia depends largely on the internet. We have e-government, government is so-called paperless... all the bank services are on the internet. [97in] We even elect our parliament via the internet," Mr Tammet said.

The memorial's removal also triggered riots amongst mostly ethnic Russian living in Estonia, during which one person was killed and more than 150 injured.

Estonians say the memorial symbolised Soviet occupation of the Baltic state. Russians say it is a tribute to those who fought the Nazis.

Spam avalanche

The Estonian government says its state and commercial websites - including a number of banks - are being bombarded by mass requests for information - overwhelming their computer servers.

Targets of the so-called denial-of-service attacks have also included the Estonian foreign and defence ministries and leading newspapers and banks.

In some cases, officials have simply blocked access to the servers from outside Estonia, to prevent them from being attacked.

"A couple weeks ago when the whole thing started we had some problems in our online services and then our mail server was absolutely inundated with spam e-mails as well," Estonian journalist Aet Suvari told the BBC.

"In the past few weeks it has been quite difficult for some government officials to read their e-mails on the web, to get access to the banks."

The defence ministry says that the cyber attacks come from all over the world, but some have been hosted by Russian state servers.

It says that instructions on how to carry out cyber warfare are circulating in Russian on Russian websites.

Estonian Prime Minister Andrus Ansip has directly accused Russia of being responsible, pointing the blame at the Russian government.

Nato and EU internet experts are all helping to track down the culprits, but Estonian officials say that they have had no co-operation from Russia.

'Internet pioneer'

While technical experts say that the initial wave of attacks came from official structures in Russia, they now say it might be very difficult to track the perpetrators down, the BBC's Steven Eke says.

He says that experts point out that botnets - the term given to the groups of computers that mount denial-of-service attacks - can be located across several countries, or even continents. [98 in]

Russia - which has a large community of hackers and computer virus-writers - has been accused of mounting such attacks before in the US and Ukraine.

Moscow denies any involvement in the internet attacks on Estonia.

Kremlin spokesman Dmitry Peskov told the BBC that the allegations were "completely untrue".

<http://news.bbc.co.uk/2/hi/europe/6665145.stm>

30. 17 May 2006 Last Updated: 15:06 GMT

Web attacks end anti-spam effort

A series of web attacks by spammers have forced a security firm to end an initiative to curb junk mail.

Israeli start-up Blue Security used a variety of tactics to make spammers clean up the lists of addresses to which they sent junk mail.

The firm also automatically filled in forms on spammers' websites to get names taken off the mailing lists. [99cm]

But escalating attacks from spammers annoyed by the initiative's success has led to its closure.

Widespread attack

Blue Security set up the Blue Frog anti-spam scheme in July 2005 and since then has signed up more than 500,000 members.

The scheme involved users reporting to Blue Security every spam message they received. The security firm would then contact the

spammers who sent the mail and ask them to remove the name of that user from their mailing list.

If this method of stopping spam failed, Blue Security would then visit the spammer's websites advertising the products seen in junk mail and fill in any forms asking for users' names be removed from the list.

This could mean that some spammers' websites were getting thousands of requests for mailing lists to be cleaned up every day. [100cm]

Blue Security claimed that the scheme reduced spam for many of those that signed up.

The tactic of bombarding spammers' websites was controversial among many anti-spam workers.

Sense of responsibility

The first indication that some junk mailers had taken exception to the anti-spam efforts came in early May when Blue Security was hit by a large so-called Distributed Denial of Service attack. [101in]

In such attacks websites get bombarded with huge amounts of data that their servers cannot handle.

At the same time some of those that had signed up for Blue Security's anti-spam system started getting threatening messages.

Blue Security realised that if it re-started its anti-spam campaign the attacks would get worse as the spammers seemed to have a huge network of remotely-controlled computers under their control.

"We cannot take the responsibility for an ever-escalating cyber war through our continued operations," said a statement on Blue Security's website.

As a result the company has decided to discontinue its anti-spam efforts.

"We believe this is the responsible thing to do," said the statement.

The company said it would now explore other ways to use its technology although for non-spam uses.

<http://news.bbc.co.uk/2/hi/technology/4990622.stm>

31. 12 February 2006 Last Updated: 14:54 GMT

'Cyber Storm' tests US defences

Vital US infrastructure including power grids and banking systems have been put under simulated attack in a week-long security exercise called Cyber Storm.



Cyber Storm took place on computers isolated from the net

The war game drew in 115 agencies from the FBI and CIA to the Red Cross, the Department of Homeland Security said.

IT companies and state and foreign governments also played a role in responding to the mock attacks.

The exercise had given the US "an excellent opportunity to enhance our nation's cyber security," the US said.

"Cyber security is critical to protecting our nation's infrastructure," [102in] George Foresman of the Department of Homeland Security added in a statement.

The US has been accused of being unprepared for a determined attack by hackers.

Cyber Storm reportedly not only tested against attacks by hackers, but also by bloggers - who deliberately spread misinformation in the exercise.

It was carried out on secure computers in the basement of the Secret Service in Washington DC. [103wb] There was no effect on the internet.

The exercise was the latest in a series of simulated attacks, including a gas attack on the New York subway.

<http://news.bbc.co.uk/2/hi/americas/4706316.stm>

32. 4 December 2005 Last Updated: 13:22 GMT

Militants' new tack in cyber war

By Sebastian Usher

BBC News world media correspondent

A new twist has surfaced in the cyber war being waged by Islamic militants.

A message has been posted to several radical Islamist - or jihadi - websites announcing a competition to design a new site for a militant group in Iraq.

The prize offered is the chance to fire missiles remote-controlled by computer at a US military base in Iraq.

Whether the competition is genuine or not, it shows again how jihadis are using the internet both to organise attacks and to drum up publicity.

The internet provides not just a vital means of organisation for Islamic militants but also a huge opportunity for propaganda. [104wb]

That is presumably the intention of the message that has recently shown up on several jihadi websites with details of a competition to design a new website for a militant group in Iraq, calling itself Jaish Al-Taifa Al-Mansura, to showcase its messages and videos.

The winner will be given the chance, the group says, to fire three long-range missiles at an American army base in Iraq by - in the words of the announcement - "pressing a button on his computer with his own blessed hand, using technology developed by the jihad fighters".

Bravado

The authenticity both of the group and the announcement has not been verified - but it is the sense of self-confidence that it is sending out that is perhaps its key message.

It is similar to an advertisement recently put out on radical Islamist websites by a group called the Global Islamic Media Front (GIMF) - asking for applications for posts as video editors, writers and translators for a weekly TV bulletin presenting news from a jihadi perspective. [105wb]

The GIMF aims to be a clearing-house for information from and about groups linked to al-Qaeda.

But despite the bravado shown by such recent announcements, analysts of jihadi sites on the internet say that recently many have gone unusually

quiet - perhaps a sign of increased international pressure being put on them.

<http://news.bbc.co.uk/2/hi/technology/4497078.stm>

33. 21 March, 2003 Last Updated: 11:41 GMT

Anti-war hackers target websites

The number of web defacements has leapt up since the US-led war against Iraq began.

According to security firm F-Secure, more than 1,000 sites have been hacked in direct relation to the Iraq conflict.

Many of the hack attacks contain anti-war slogans and some have direct anti-USA or anti-Iraq slogans. [106wb]

Sites hacked to date include the US National Centre for Agricultural Utilization Research and the US Navy.



Peace campaigners are among the hackers

Three groups of hackers are believed to be responsible according to F-Secure; US-based patriotic hackers, Islamic extremist groups and peace activists who were against the war.

Pro-peace

While politically motivated hackers are nothing new, it is an interesting development to have peace campaigners turning to the net to get across their message said General Manager of F-Secure Jason Holloway.

"In the past hack attacks have been about the kudos of breaking into a website and proving yourself the best hacker, [107cm]" he said.

"But this seems to be using the web as a soapbox and a way of spreading a message. The vast majority of these attacks have been pro-peace and that is unusual," he added.

US security firm iDefense has also reported hundreds of websites have been daubed with anti-war graffiti since the beginning of the conflict.

The firm believes a pro-Islamic hacking group the Unix Security Guards is responsible.

The cyber graffiti promises that the defacements are the beginning of "the new era of cyber war". [108wb]

Limited damage

Political hacking known as hacktivism is not a new phenomenon and in the run-up to the Iraq war there has been increased activity from pro-Islamic hackers.

Israel has also been under bombardment from hackers as tensions rise in the region.

The bomb in Bali caused a rash of cyber attacks against South Asian targets, originating from Indonesia and Malaysia. [109wb]

And tensions between Pakistan and India over the disputed territory of Kashmir caused a series of to and fro attacks from groups representing both sides.

The Ganda e-mail worm was the first example of a virus exploiting the ongoing war, luring computer users with the promise of satellite pictures of Iraq and screensavers mocking President Bush. [110cm]

Both the web defacements and the Ganda virus have caused limited damages.

At the moment the attacks has been against fairly low key sites.

But as more sophisticated hackers get involved as the conflict intensified then more sensitive US military sites could be targeted, warned Mr Holloway.

<http://news.bbc.co.uk/2/hi/technology/2871985.stm>

34. 13 March, 2003 Last Updated: 14:19 GMT

Indian hackers target Pakistan

A new e-mail virus has been released on the internet in the latest cyber war of words between rival hackers in India and Pakistan.

A variant of the Yaha internet e-mail worm has been written by a group of hackers calling themselves the Indian Snakes.

It has been attacking websites in Pakistan, including government sites, internet service providers and the Karachi Stock Exchange, said anti-virus firm Sophos. [111cm]



E-mail worm is revenge in cyber squabble

Yaha-Q arrives as an e-mail attachment and can send itself to people listed in the recipient's e-mail address book.

Cyber squabble

It then launches a denial-of-service attack - where the ear-marked servers are overloaded by multiple requests - on Pakistani websites. [112in]

The worm has also been leaving anti-Pakistani messages on hard drives, although one such message suggests that the hack is not politically motivated. [113wb]

Rather the spat seems to an attempt to see who is the better hacking group.

"Unfortunately childish squabbles like this are being fought on the computers of innocent computer users, uninterested in the disagreement," said Graham Cluley, Senior Technology Consultant at Sophos.

The damage done by the worm has been fairly limited, said Mr Cluley, and protection is available from anti-virus firms.

An earlier version of the Yaha worm appeared in January affecting computers in over 100 countries.

According to e-mail filtering firm MessageLabs one in around every 200 e-mails sent in 2002 contained a virus.

<http://news.bbc.co.uk/2/hi/technology/2847455.stm>

35. 7 February, 2003 Lust Updated: 16:31 GMT

US ponders cyber war plans



Will cyber war ever replace convention military tactics?

The US is reportedly drawing up guidelines for cyber attacks against countries such as Iraq.

According to the Washington Post, President Bush has already laid the foundations for the US Government to develop a strategy on how and when it can penetrate and disrupt enemy computer systems.

There has also been speculation in Washington that the Pentagon is considering some form of cyber war in conjunction with any military action against Iraq the paper said. [114in]

The US army is always on the lookout for new forms of weaponry and much consideration has been given to how cyber weapons can sit alongside conventional ones.

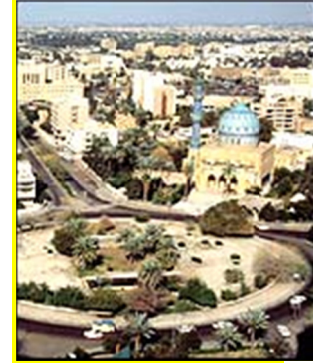
Information warfare

Some so-called smart bombs already have the capacity to knock out electricity supplies when detonated.

Any cyber war against Iraq would have to take into account how crucial computers are to the running of the country.

"Iraq has a relatively advanced telecommunications infrastructure and any cyber attack could cripple emergency services and prevent both the military and civilians from talking to each other," said DK Matai, Chief Executive of security firm mi2g. [115in]

"It would play an important part in shaking citizens' confidence in the government," he added.



Baghdad is not particularly wired

There is nothing new in disabling communications and information warfare has always been a part of any military strategy.

Topography of networks

More sophisticated targeting of computer systems is unlikely, said Mike Knights, a cyber warfare expert for specialist military publisher Jane's.

"Iraq is a non-wired economy and all Iraqi computers with sensitive information will be stand-alone and not connected to the internet and therefore invulnerable to attack," he said.

The US military has never regarded computer hacking as a particularly useful part of information warfare, he said.

"It will be some decades before it becomes an important strand of military strategy."

"It is not always easy to see the effects such computer attacks are having and it is difficult to understand the topography of computer networks especially primitive ones such as in Iraq," he added.

That has not prevented the US from shipping computers with backdoor snooping facilities to Iraq and engaging in psychological warfare via e-mail said Mr Knights.

"Iraqi generals have been sent e-mails saying 'we know you personally' and requesting they send light signals to show the positions of weapons of mass destruction," he said. [116wa]

US vulnerable

Iraq has about 12,000 of its 23.5m people online and was one of the last countries in the Middle East to join the net community.

It only has a tiny amount of international bandwidth.

The US on the other hand is very dependent on computer systems.

Following the 11 September terrorist attacks, the US Government has stepped up its own cyber security.

President Bush ordered a \$1.5bn increase in spending on computer and network security as well as training an army of workers to thwart any cyber attack that terrorists might launch. [117cm]

"Ironically the US are the people that are most effective at information warfare but also are the most vulnerable to it," said Mr Knights.

Credible threat?

Opinion differs widely on how likely such an attack is.

Some commentators point to nightmare scenarios in which power supplies, telecommunications and financial systems are severely disrupted by an attack.

Mr Knights does not think Iraq would be a serious player in any cyber war despite giving some consideration to such attacks.

Security firm mi2g takes the threat more seriously.

"The Slammer worm paralysed Korea, disrupted 13,000 ATMs in the US and disabled the emergency services in Seattle," said Mr Matai.

He imagines a scenario where a piece of malicious software is released onto computer networks, causing serious disruption in the cyber equivalent of a dirty bomb.

And any such attack would require state sponsorship. [118in]

"To bring a nation to its knees any cyber warfare attack would require nation state backing," he said.

<http://news.bbc.co.uk/2/hi/technology/2737885.stm>

36. Wednesday, 17 April, 2002, 13:43 GMT 14:43 UK

Indian hacker turns cyber cop



Net security is an increasing concern in India

By Brajesh Upadhyay
of the BBC Hindi service

The clock had just struck midnight when users logged onto a popular chat site noticed a rather short message flashing up on their **monitors: "DOS attack".**
[119in]

To the majority, it may not have meant much, but to 16-year-old Ankit Fadia sitting in front of his PC in the Indian capital Delhi it was a "Denial of Service" attack - someone somewhere was trying to hack into a website.

Within seconds, he had managed to track the location of the sender - from somewhere in Pakistan. Minutes later he had also found the target of attack - the website of a top Indian firm.

They were soon alerted and a major hack was averted.

Early start

Ankit Fadia is one of the many "ethical hackers" now employed by businesses all over the world to protect against such attacks.

"It was my **first anti-hacking operation** and it was successful," says Ankit, who was only 10 days into a job as an intelligence consultant with a US Government agency when he saved this website.

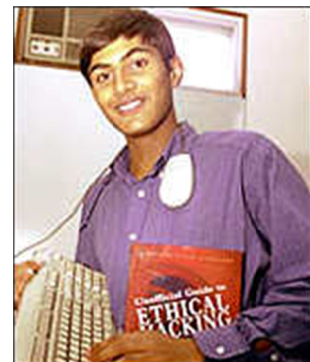
He refuses to divulge the name of the agency he is employed by or the firm whose website he saved for security reasons.

At 14, Ankit defaced the front page of an Indian magazine and sent an e-mail to the editor confessing to the hack and suggesting counter measures.

He wrote a book on "ethical hacking" at the age of 15, becoming the youngest ever author to be published by Macmillan India.

"The term hacking leaves a negative impact on people," he says.

"In reality, hackers are actually good, pleasant and extremely intelligent people who could keep computer criminals on the run."



Ankit Fadia: Now advising governments and business

India catches up

Employing ethical hackers to protect against malicious ones has become common practice in the US, but has only recently caught on in India.

It only really got going when the Reserve Bank of India directed its banks to use "ethical hackers" last year, according to Pavan Duggal, President of Cyberlaw.net, a law firm with expertise in cyber laws.

"It was done after several Pakistan-based hackers launched some sort of cyber war against India and the sites belonging to the Ministry of External Affairs and the Atomic Energy Research Board were hacked, [120in]" says Mr Duggal.

However, there is still no organised body to guard against such practice.

"We don't have a strong legal regime to protect against such violations," says Pavan Duggal.

As for Ankit Fadia, Pavan Duggal says he is now so well known in the net community, that there are even some in the corporate world who fear his success might encourage others to turn to hacking.

http://news.bbc.co.uk/2/hi/south_asia/1934874.stm

37. 23 October, 2001 Last Update: 11:07 GMT

Hacktivists take sides in war



GForce is one of the most prolific hacker groups



BBC News Online's Kevin Anderson
in Washington

Online graffiti artists are taking the war on terrorism to cyberspace.

It is not the kind of cyber-warfare that some have envisioned with state-sponsored super hackers targeting key networks and wreaking offline havoc as water, power and transportation systems go down [121in]. Instead, it is a virtual war of words between home-grown hackers - so-called hacktivists - who mix hacking with political activism [122wb].

And as with many other conflicts and causes in recent years, hacktivists are bringing their messages to a website near you.

Cyber jihad

One of the most prolific participants in recent bouts of hacktivism has been a group of Pakistani hackers calling themselves GForce Pakistan.

Their main focus is the conflict in Kashmir, and they have left anti-Indian screeds across hundreds of Indian websites.

But they also have supported other causes like the Palestinian intifada, and now, according to some of its most recent defacements, Afghanistan and Osama Bin Laden.

Last week, they defaced a server belonging to the US National Oceanic and Atmospheric Agency.

"You call it terrorism? We call it Jihad," the group wrote in the lengthy message left in place of the site's homepage.

The group said that although it condemned the 11 September attacks on the US, "we also stand by al-Qaeda. Osama Bin Laden is a holy fighter, and whatever he says makes sense".

Ultimatum

The group issued an ultimatum saying it would attack US and British military websites unless a number of demands were met. These included:

- the departure of US troops from Saudi Arabia
- an end to the bombing campaign in Afghanistan
- evidence linking Osama Bin Laden to the attacks in the US.

The group said it had "very high confidential US data that will be given to the right authorities of Al-Qaeda".

The group then hacked three military sites associated with the US Defence Test and Evaluation Professional Institute.

In a message left on the defaced sites, the group threatened to hack more than 1,500 major US, British and Indian sites.

Hackers fight back

In the past, these types of attack have led to hacking tit-for-tat battles between pro-US and anti-US hackers.

Earlier this year Chinese and American hackers declared a trans-Pacific cyber war following a collision between a US spy plane and a Chinese fighter. [123cm]

However, in a new twist, a group of hackers calling itself YIHAT, Young Intelligent Hackers Against Terror, are waging a completely new kind of cyber counterattack.

The group was founded by Kim "Kimble" Schmitz, a German hacker turned computer entrepreneur.



In September, YIHAT said it had hacked into computers belonging to the Al Shamal Islamic Bank in Sudan to get information on accounts held by Osama Bin Laden and his al-Qaeda organisation.

YIHAT now says it has obtained the real name of the leader of the GForce Pakistan hacking group.

YIHAT said he works for an online business in Karachi.

FBI warning

The FBI warned last week that political events were increasingly leading to cyber protests.

The most common form of protest has been defacing web pages.

The FBI said protests had had little impact on US network infrastructure. [124in].

But they warned that as the power of computing and sophistication of hacking tools increases, "cyber protesting and hacktivism will become more significant to US national interests". [125wb].

The FBI said "future attacks could bring about large economic losses as well as potentially severe damage to the national infrastructure, affecting global markets as well as public safety".



The FAS site fell victim to the hackers

Nuisance more than threat

But people in the hacking community like to put the threat in perspective.

Shortly after the 11 September attacks, Brian Martin of the security site attrition.org wrote: "First, let's put 'cyber-war/jihad/whatever' in perspective to the very real, physical attacks of September 11, 2001. Thousands of people were killed. No one was ever killed from a 'cyber attack'."

Right now it is more of a nuisance.

Peter Voth, the webmaster for the Federation of American Scientists (FAS) can attest to that.

He spent most of Tuesday morning restoring the FAS site after it was hacked by someone referring to himself as Pakistani's son.

Instead of the normal FAS homepage, Mr Voth found the message, "stop bomb !! stop kill !! pls bless my homestead !!"

FAS is a non-profit, non-governmental organisation conducting analysis and advocacy on science, technology and public policy, according to its website.

That includes national security, nuclear weapons, arms sales and biological hazards.

"We get a lot of traffic from people interested in terrorism and foreign affairs," Mr Voth said, adding, "not all of whom are aware that we are not an intelligence agency or wing of federal government".

Preliminary investigations showed no files appeared to have been tampered with, he said.

This was the first successful defacement of the site, to his knowledge. He said the FAS was working with a security company to make sure it did not happen again.

<http://news.bbc.co.uk/2/hi/americas/1614927.stm>

38. 7 March, 2001 Lust Updated: 16:40 GMT

Hamas hit by porn attack



Another blow appears to have been struck in the hacking war that has broken out on the sidelines of the current conflict in the Middle East.

This time the victim is the Muslim militant group Hamas, with visitors to its home page being diverted to a hard-core pornography site called Hot Motel Horny Sex Sluts. [126wb]

The cyber attack comes after Hamas said it had carried out a deadly bomb attack in the Israeli town of Netanya on Monday, which killed two Israelis and the suicide bomber.

Sheikh Ahmad Yassin, spiritual leader of the political wing of Hamas, accused Israeli intelligence of being behind the hack.

"I'm telling them to die of their own fury," said the sheikh. "They are trying to disfigure the image of Islam and Muslims.

"These are the people who are shedding our blood and massacring our people every day, so it is not difficult for them to do something like this. As much as their anger and fire rises, they will try all and crazy ways to extinguish it."

It is not yet clear who hacked the Hamas website, which usually carries information about the group and its opposition to Israeli-Palestinian peace moves.

Sheikh Yassin said Hamas would seek advice from internet specialists to block any further hacking attempts.

Hackers at war

Middle East "hacktivism" - as political hacking is called - has been a common feature of the past five months, during the Palestinian uprising to protest against Israel's occupation of the West Bank and Gaza. [127wb]

There have been numerous successful and unsuccessful hacking attempts - many of them recorded on the computer security site Attraction.com - and website administrators on all sides are reported to have been busy defending their sites against attack from enemy hackers.

In November, an anti-Israeli hacker managed to penetrate the site of one of Washington's most powerful lobbying organisations, the American-Israeli Public Affairs Committee (Aipac), replacing it with critical e-mails from Aipac's own database, as well as publishing credit card numbers and e-mail addresses of Aipac members.

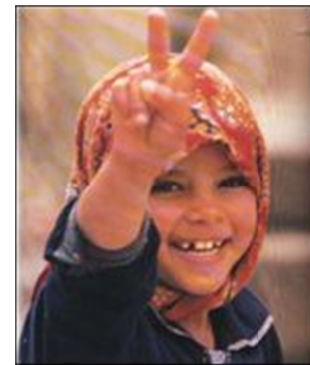


A hack which did not seem to harm Sharon's poll standing

"The hack is to protest against the atrocities (sic) in Palestine by the barbarian Israeli soldiers and their constant support by the US Government," the raider - Doctor Nuker, founder of the Pakistan Hackerz Club - wrote.

Hackers have also targeted the websites of Israel's Parliament, its foreign ministry and an Israeli internet provider, as well as several sites run by the Hezbollah guerrillas.

But hacktivism does not always seem to have the desired effect - just before Israel's election, the campaign website of Ariel Sharon was replaced temporarily with pro-Palestinian material parodying Sharon's site under the headline "the world's biggest murderer". [128wb]



He went on to win the election by a landslide and was due to be sworn in on the day after the Hamas hack was reported.

This image was placed on Israel's embassy site in New Zealand

http://news.bbc.co.uk/2/hi/middle_east/1207551.stm

39. 26 October, 2000, Last Updated: 18:39 GMT

Israel under cyber attack



Several official Israeli web sites have crashed after falling prey to a concerted jamming campaign by Islamic groups around the world.

The website of the Israeli parliament was paralysed on Thursday morning after being penetrated by hackers believed by officials to be based in Saudi Arabia.

And the foreign ministry website has been down since Wednesday after being overwhelmed by floods of incoming mail.

The Prime Minister's Office and the Israeli Defence Forces (IDF) have also come under attack. [129in]

Attack call

Local newspapers had previously reported that Israeli teenagers had sabotaged a website of the Lebanese guerrilla movement Hezbollah. [130in]

Reports say Islamic groups provided access to computer programmes which allowed users to flood Israeli sites with huge amounts of electronic mail.

Prime Minister Ehud Barak's office was the first to be affected but the site was later restored.

The IDF web site avoided collapse by switching from the local Netvision server to one connected to United States communications giant AT & T.



Ehud Barak: web site jammed

Cyber wars are not unusual in the Middle East.

An Israeli teenager who claimed to have destroyed an Iraqi Government internet site was hailed as a hero in Israel last year.

http://news.bbc.co.uk/2/hi/middle_east/992879.stm

40. 1 September, 2000 Last Updated: 21:58 GMT

Draskovic website hoax



Draskovic has faced bullets as well as cyber tricks

By south-east Europe analyst Gabriel Partos

One of Serbia's leading opposition parties, the Serbian Renewal Movement (SPO), has become the victim of a cyber hoax. [131wb]

An internet website bearing the name of the party's charismatic leader, Vuk Draskovic, is being used to publicise President Slobodan Milosevic's governing Socialist Party.

The hoax has come to light on the day Serbia's main opposition bloc - the SPO's rivals - launched its own official campaign for Yugoslavia's presidential and parliamentary elections.

There are just over three weeks to go before President Milosevic faces re-election, and the race for the Yugoslav presidency is beginning to hot up.

Domain name bought

According to senior SPO officials, the domain name www.VukDraskovic.com was bought by the leader of the Socialist Party's youth wing in the small western town of Loznica.

Lawyers have been in touch about the matter, and it now appears that the Socialist Party publicity material will be removed from the website on Saturday.

This is by no means the first occasion that cyberspace has been used for a robust form of propaganda in and around Yugoslavia. [132wb]



President Milosevic faces a challenge in the polls

Last year's conflict over Kosovo was quickly dubbed the first internet war when rival cyber activists hacked into the official websites of NATO member countries and of the Yugoslav Government. [133wb]

Football websites disrupted

The return of peace has not put an end to such activities.

In April, the websites of several prominent Western organisations - including leading football clubs - were disrupted when pro-Serb messages were posted on them.

And two months ago Serbia's leading pro-government newspaper, Politika, became a target for hackers when its website carried a report claiming President Milosevic had died in a bomb explosion. [134wb]



Draskovic heads one of three main opposition groupings

Although internet usage may not be as widespread in Serbia as it is in the West, the scope for causing mischief is no less extensive.

<http://news.bbc.co.uk/2/hi/europe/907081.stm>

41. 7 August, 2000 Last Updated: 20:41 GMT

Taiwan plays cyber war games



Taiwan war games coming soon to a PC near China

Taiwan is to include drills in cyber warfare in its largest annual military exercises later this month, according to a defence ministry official.

The step is an effort to strengthen its defences against a possible computer virus [135in] attack from mainland China.

A Taiwanese military spokesman said "red" (communist Chinese) and "blue" (Taiwanese) combat forces would use nearly 2,000 computer viruses to attack each other's information networks during the Han Glory war games.

Taiwan's economy relies heavily on computers and a successful cyber attack could cause serious damage on the island.

Virus offensive

Chief of the Taiwan General Staff Tang Yao-ming has warned that China might launch an "information war," including the use of computer viruses to paralyse military command, energy, transportation and banking systems, before an invasion of the island. [136in]

The protection tactics developed against cyber virus includes a large list of computer bugs, including those from the ILOVEYOU family which swept the world a few months ago.

Taiwanese media have previously said the China's People's Liberation Army had simulated computer virus offensives in exercises in Shenyang, Beijing, and Nanjing over the past two years.



Taiwan soldiers will also make manoeuvres in a cyber battle field

<http://news.bbc.co.uk/2/hi/asia-pacific/870386.stm>

42. 23 March, 2000 Last Updated: 14:46 GMT

Liberian radio ban lifted



The Liberian authorities have lifted a recent controversial ban on an independent radio

station - but restrictions remain in place on a second broadcaster. [137wa]

The information ministry said that a broadcasting suspension on Catholic station Radio Veritas would be lifted, and the question of the closure of Star Radio would be resolved "through diplomatic channels".

The government has changed its position after the United States took the matter up at diplomatic level.

The information ministry statement said that "Radio Veritas has assured continued co-operation with the government of Liberia in the field of communication, education, health and religion.

"The parties have also agreed that they will be available to exchange views on issues of a controversial nature to ensure factual and balanced reporting at all levels," the statement continued.

The government banned transmissions by the two broadcasters last week, saying they posed a threat to state security.

Critical

The two stations, which broadcast views critical of President Charles Taylor's government, have been described as the most credible and the most independent in the country.



President Charles Taylor:
Wanted to impose conditions
on Radio Veritas

Radio Veritas's broadcasting licence was suspended, though the president said the station would be allowed to continue as long as it kept to religious matters.

The Catholic archbishop of Monrovia said the station could make no such undertaking, arguing that the matter should be resolved in court.

President Taylor had accused Star Radio - which also runs an internet-based news service - of "cyber war" against Liberia, and said it would never operate again during his administration. [138wa]

The US ambassador to Liberia met Mr Taylor on Monday to discuss the closure of Star Radio, which was set up by US and Swiss agencies.

Amnesty International has also condemned the government's action against the broadcasters.

<http://news.bbc.co.uk/2/hi/africa/688266.stm>

43. August 18, 1999 Last Updated: 13:45 GMT

World: Asia-Pacific Timor activists warn of cyber war



Gunmen shot at the offices of the main independence group on Tuesday

Computer hackers plan to sabotage Indonesia's banking system if Jakarta rejects an East Timor vote for independence, resistance leader Jose Ramos Horta has warned. [139in]

Mr Horta said about a dozen viruses were being designed to infect computers if there is fraud in the 30 August ballot on the territory's future. The Nobel laureate warned that a 100-strong team of hackers in Europe and North America had prepared a campaign that would cause economic devastation to Indonesia.



Their targets would include computers controlling banking, finance, the military and aviation, he said in a commentary in Australia's Sydney Morning Herald.

"One computer wizard recently told me, 'We will terminate their banking system. We will invade their sites and destroy them...We will cause them to lose hundreds of millions of dollars'," he added.

Electoral fraud

The warnings come as East Timor prepares to choose between Jakarta's offer of autonomy or full independence.

Mr Horta: Barred from East Timor during campaigning

The United Nations which is overseeing the ballot says it is confident there will be a free and fair vote.

But Mr Horta has warned that the ballot could turn into the biggest electoral fraud in modern times.

He said Indonesia's army intended to get a pro-integration vote through by terror and fraud.

Mr Horta alleged that a violent campaign by pro-Jakarta militias had already

- cost over 1,000 lives
- razed entire villages
- uprooted 80,000 people

He said the vote was also compromised by

- a ban on detained resistance leader Xanana Gusmao and himself during the campaigning
- continued Indonesian army support for the militias
- a biased Indonesian controlled East Timorese media

"All this makes for an extremely dangerous situation. Full-scale violence before or after the ballot is now almost certain," Mr Horta added.



Militiamen hand in weapons

"The next phase of resistance will be much more desperate and ferocious and will not be contained to East Timor," he added.

Mr Horta's comments came as Amnesty International also warned that Indonesia's failure to halt the bloodshed in East Timor - mainly by pro-Jakarta militias - threatened to prevent a fair ballot.

Indonesia invaded East Timor, a former Portuguese colony, in 1975 and annexed it the following year in a move not recognised by the UN.

Human rights groups say more than 200,000 people died, many of them from starvation, in the years since the invasion.

<http://news.bbc.co.uk/2/hi/asia-pacific/423549.stm>

44. August 4, 1999 Last Updated: 22:52 GMT

Sci/Tech China accused of cyber war



Falun Gong publications have been burned by Chinese authorities

By BBC Internet Correspondent Chris Nuttall

The Chinese Government has been blamed for **cyber attacks on Websites and Internet Service Providers supporting the Falun Gong movement.**

Some of the attacks, which appeared to be aimed at **blocking access to information** on Falun Gong, have been traced back to Beijing, where authorities are becoming increasingly **sophisticated in restricting the influence of the Internet on Chinese society.** [140wa]

China has been a victim of so-called hacker attacks in the past; now it appears to have gone on the offensive.

Last year, a human rights Website it set up was hacked and pages were replaced with a link to Amnesty International.

Hackers have also targeted government computers to try to stop them blocking access to Websites such as the BBC's.

Info-warfare

Now some direct attacks on Falun Gong Websites in the United States and Canada have been traced to government-backed technology institutes in Beijing.

They have used the same weapons as hackers - bombarding computers with requests for information that have either slowed down or blocked access for people wanting to visit the sites.

The Chinese Government has also set up an anti-Falun Gong Website filled with articles saying the movement is a threat to the mental and physical health of society.

Propaganda sites such as these are not unusual, but the cyber attacks are the hardest evidence yet of a government indulging in info-warfare [141wa].

This trend has long been predicted, and Indonesia was accused of attacking an East Timor Website in Ireland earlier this year [142wa].

That was not proved, and neither were attacks on Nato's computer systems traced to Belgrade during the Kosovo campaign [143wa].

They seemed more the work of individuals - but the Falun Gong cases are being sourced to a major institution directly supported by the Chinese Government.

<http://news.bbc.co.uk/2/hi/science/nature/412296.stm>

45. March 1, 1999 Last Updated: 19:14 GMT

World: Africa Eyewitness: Reporting the war in the Horn



Ethiopian militia: Some audiences have been hard to please

By East Africa Correspondent Cathy Jenkins



It's a Saturday night. I'm in the departure hall of Nairobi's international airport, along with half a dozen or so other correspondents and television crews.

Across the cafeteria we spot the Ethiopian ambassador. He's saying goodbye to a colleague, and when he's finished we call him over. He is extremely genial.

"Where are you going?" he asks. - "Mm, well, actually we're going to Asmara."



Cathy Jenkins

Through the day we have all been monitoring the worsening situation on the Ethiopian-Eritrean border, and we've got the go-ahead from our offices to scramble to the airport to catch the overnight flight to Eritrea. Other correspondents are going, or have already gone to Addis Ababa.

"Oh yes" says the Ethiopian ambassador, to everyone in general.

And then to me: "You already have a BBC reporter in Ethiopia, don't you".

Reassured that the BBC will have correspondents on both sides of the border, he takes his leave, still extremely affable.

Propaganda and spin doctors

Once in Eritrea, the attitude from Addis Ababa towards those on the other side is noticeably less polite.

I use the satellite phone to check with my BBC colleague in Ethiopia what the government-backed newspapers and state radio have been saying about me.

Various spin doctors have already said the BBC has banned me from reporting on the conflict because my reports were so biased. Now I hear that I've apparently been sacked. This must be rather confusing to anyone tuning in to a radio to find me still reporting.

The vitriol gets worse: we hear that all the correspondents in Asmara are being paid by the Eritrean government to write their propaganda.

Then, and this is my favourite: "The BBC female correspondent is having an affair with an Eritrean government official."

I relay the comment to my bosses in London and remark that the Ethiopians obviously don't know how working for a 24-hour news channel like the BBC seriously limits one's quality time.

Getting access

When the border fighting first flared in the summer of 1998, the **Eritreans felt they lost the propaganda war. This time they're determined to win it.** So in the first few days of our stay in Asmara, everything we ask for, we get:

"You want to go to a front line - fine, go to a front line".

"You want to see some prisoners of war - fine, we'll take you and you can talk to them for as long as you want."

Consequently, on the Eritrean side the journalists are churning out story after story of what we've seen, whom we've talked to.

Our colleagues in Addis Ababa are being given no access, despite their pleas. They find they can't write so much, and there are no television pictures from the Ethiopian side.

The Ethiopians don't like turning on the television and finding all the reports coming from the enemy side. Their hatred of us seems unlimited.

War by e-mail

Alongside the battles on the ground, the cyber war has swung into top gear. Every day London tells me that more complaints have been e-mailed in from Ethiopia about the BBC's one-sided reporting. [144wa].

I'm actually rather pleased when an Eritrean writes in to complain that I'm pro-Ethiopian.

It's impossible to win. However many times one writes "Eritrea says this, Ethiopia denies it" or "Ethiopia says this, Eritrea denies it", someone will be unhappy - extremely unhappy.

It's not only the Ethiopians who are bombarding cyberspace with complaints about one-sidedness. An Italian colleague in Asmara tells me that his counterpart in Addis Ababa has been receiving pretty strong e-mail attacks - presumably because he's writing out of Ethiopia.

One day, however, this Italian journalist writes a story from Addis Ababa which the Ethiopians hate, and the Eritreans love.

Suddenly, for the Eritreans, he is an excellent writer with an excellent understanding of the conflict. His article is translated into English on the Internet. In the hotel in Asmara, a copy of it is placed in the pigeon hole of every journalist.

Back in Nairobi, I contact the secretary of the Ethiopian ambassador to arrange a meeting. I'm a reporter. I like to see all sides of the story.

Next time, if I'm given a visa, I may like to report from the Ethiopian side of the front lines

<http://news.bbc.co.uk/2/hi/africa/288239.stm>

46. February 7, 1999 Last Updated: 17:26 GMT

World: Asia-Pacific

China casts a cyber net



China: Fighting a war in cyberspace

By Duncan Hewitt in Beijing

Officials in China have vowed to crack down on unauthorised Internet telephone services.

The country's ministry of information industry said such services were costing it hundreds of millions of dollars and warned that they amounted to the smuggling of information [145cm].

The Internet draws mixed signals from the Chinese Government. It has praised it as a tool for economic growth but at the same time it has blocked politically sensitive Websites, increased controls on Internet cafes and recently jailed a man for providing a list of e-mail addresses to exiled dissidents. [146wa]

A court case in south-eastern Fuzhou has highlighted official anxiety at the impact of the Net. Two brothers who offered an alternative to China's notoriously expensive international phone calls through the Internet found their business closed, their equipment confiscated and were accused of harming national security.

The men appealed against their arrests and to general surprise the court found in their favour, saying no relevant law existed at the time. Yet the brothers are still in detention while the authorities seek to have the ruling overturned.

"There are some illegal operators who have been colluding with foreign companies and have seriously eroded China's income from international telecommunications", said an official at the ministry of information industry.

"The figures are huge, several billion yuan so far. In fact this is information smuggling. These people are evading official controls and we're going to crack down very hard on them."

The spokesman said the authorities would respect the court's final ruling on the Fuzhou case. He also said that China would license a number of officially approved Internet phone services this year.

But the brothers' action has won support from unlikely quarters, including the official English-language newspaper, the China Daily.

An opinion piece said the Fuzhou court decision had been welcomed by local people, who were tired of the government's telephone monopoly and at the unreasonably high prices for international calls.

The state-run China Telecom currently controls 95% of the market.

<http://news.bbc.co.uk/2/hi/asia-pacific/274433.stm>

47. February 1, 1999 Last Updated: 01:42 GMT

World: Middle East Teenage hacker 'destroys anti-Israeli Website'



Nir Zigdun has been hailed a cyber-hero in Israel

A teenager who claims to have destroyed an Iraqi government Internet site containing anti-US and anti-Israeli "propaganda" has been hailed as a hero in his native Israel. [147wb]

But the operator of the US-based Website insists he caught 14-year-old Nir Zigdon's computer virus in time.

The boy has been feted in Israel after he sent a virus by e-mail to the site - www.iraq.com - after reading about allegedly anti-Semitic sites in PC-Media magazine.

He said: "I destroyed the site because it contained lies about the United States and Israel and propaganda against Jews." [148wb]

Congratulated by fellow Israelis

Nir said he had received more than 100 phone calls on Sunday from Israelis congratulating him after his story was published in the daily Maariv newspaper.

He said he sent Fawzi el-Faramawy, a New York-based Egyptian who runs the site, an e-mail six months ago under an assumed name.

The boy said he was a Palestinian admirer of Iraq who had created a virus to destroy all the Israeli sites on the Internet.

The e-mail encouraged Fawzi el-Faramawy to click a designated batch file twice and Nir said when he followed the instructions it destroyed the Iraqi site.

The www.iraq.com site now defaults to www.arabia.com, a popular but non-partisan news website.

'Virus was stopped'

Fawzi el-Faramawy, who now runs www.iraq.org, an Iraqi government site says the default is for "security reasons". He says he caught Nir's virus before it caused any damage.

He says the boy's e-mail pretended to be an advertisement promising enhanced access to the Net.

Fawzi el-Faramawy, a 26-year-old student who volunteers his time, says he scanned the batch file and saw a crude program formatted to destroy his hard disk. He says he then destroyed the file.

He admits he e-mailed the boy back and told him to "go to Hell".

Cyber wars

Nir says he is working on destroying several other "anti-Israeli" sites.

He says the Internet is "a place for different kinds of wars, like against Nazis who are against Jews and Arabs against Jews."

Several Israeli companies reported last year that neo-Nazis had hacked into their sites to avenge the destruction of their sites by Israeli hacker Ehud Tenenbaum [149wb], known as The Analyser. Mr Tenenbaum has destroyed several neo-Nazi, paedophile and anti-Israeli Websites [150wa].

http://news.bbc.co.uk/2/hi/middle_east/269399.stm

Πίνακας κειμένων CNN

A	ΣΕΛ.	ΗΜΕΡ/ΝΙΑ	ΤΙΤΛΟΣ	ΛΕΞΕΙΣ
1	253	11/10/2011	Virus infects program that controls U.S. drones	822
2	254	6/10/2011	Arab Spring galvanizers, WikiLeaks among Nobel...	966
3	256	3/10/2011	The Pentagon's cyberstrategy, one year later	1.709
4	260	15/8/2011	Cybertheft could destroy the U.S. economy	1.940
5	264	15/8/2011	'Mafiaboy' breaks silence, paints 'portrait of a hacker'	1.085
6	267	15/7/2011	Pentagon makes love, not cyber war	765
7	269	23/6/2011	Cyberwarfare finds a captive audience	829
8	270	18/1/2011	U.S. strategy on Iran is working	920
9	273	16/12/2010	The Sweep: WikiLeaks stirs anarchy online	1.961
10	277	10/12/2010	Why WikiLeaks hackers are a glitch, not a cyberwar	1.003
11	279	9/12/2010	Is WikiLeaks engaged in 'cyber war'?	1.158
12	282	3/10/2010	Iran arrests 'nuclear spies,' intelligence chief says	338
13	283	29/9/2010	Iran denies cyberattack hurt nuclear program -- but...	640
14	284	7/7/2010	Threat of 'cyberwar' has been hugely hyped	905
15	286	19/3/2010	Dismantling of Saudi-CIA Web site (...)	80
16	286	28/9/2009	CNN Student News Transcript [<i>Face book</i>]	31
17	290	21/9/2009	Facebook gets caught in Golan Heights dispute	489
18	291	7/8/2009	Rus.-Geor. tensions still high one year on from conflict	354
19	292	8/7/2009	U.S. government sites among those hit by cyberattack	818
20	294	17/6/2009	Briton's software a surprise weapon in Iran cyberwar	420
21	295	21/8/2008	Experts: Internet filtering and censorship rife	902
22	297	18/8/2008	U.S. at risk of cyberattacks, experts say	1.070
23	299	4/3/2008	China denies U.S. computer hacking agenda	696
24	301	3/3/2008	<i>Report</i> : China trying to crack U.S. computers, buy nukes	577
25	303	26/9/2007	Sources: Staged cyber attack	952
26	305	24/8/2007	Anarchy on-line	1.414

27	308	29/5/2007	Cyber-spies tracking terror on Web	822
28	310	29/5/2007	Is it time to crack down on the blogosphere?	1.720
29	313	12/4/2007	Security crucial as intruders grow sophisticated	625
30	314	1/12/2006	Advisory on al Qaeda cyber threat issued out of caution	159
31	315	24/10/2006	Ronald Sugar, Chairman and CEO, Northrop Grumman	775
32	316	3/10/2006	Social networking fuels new Web boom	581
0	317	29/9/2006	Cyber-spies tracking terror on Web	0
33	319	13/10/2005	A convicted hacker debunks some myths	1.841
34	321	16/2/2005	The Internet war	952
35	323	19/1/2005	Uncertain state of security	1.479
36	326	20/7/2004	Review: A fresh 'Angle' on the spy novel	518
37	327	20/3/2003	Are we vulnerable to cyber-attacks?	775
38	328	20/11/2002	Military intelligence system draws controversy	622
39	330	17/11/2002	Indonesians take protests to the net	405
40	331	12/4/2002	Hack attack, how you might be a target	824
41	333	11/11/2002	Indonesian cyberprotesters target Australia	299
42	334	4/2/2002	Rumsfeld: Cyberwar among possible threats	456
43	335	8/1/2002	Report: Cybervandalism jumped in 2001	416
44	336	17/7/2001	Decoy PCs give hackers a security lesson	759
45	338	11/5/2001	Analysis: U.S.-China 'cyberwar' fires blanks	1.174
46	340	10/5/2001	Epic cyberattack reveals cracks in U.S. defense	675
47	342	2/5/2001	U.S., Chinese hackers continue Web defacements	405
48	343	24/1/2001	Special Report: Crime on the Internet	298
49	344	24/1/2001	Could a cyberwar cripple the U.S.?	1.624
50	348	22/11/2000	U.S. Army kick-starts cyberwar machine	603
51	349	2/11/2000	Mideast fighting spills onto the Internet	493
52	350	3/11/1999	Derailing the vision of a truly digital government	347

Πίνακας ευρημάτων CNN

A	Σελ.	Διείσδυση	Υποδομές	Λογοκρισία	Προπαγάνδα	Σύνολο
1	253	3	0	0	0	3
2	254	0	0	0	2	2
3	256	2	8	0	0	10
4	260	3	1	0	0	4
5	264	4	0	0	1	5
6	267	1	1	0	0	2
7	269	4	2	0	2	8
8	270	2	0	0	0	2
9	273	0	0	0	6	6
10	277	1	0	2	1	4
11	279	1	1	0	2	4
12	282	2	0	0	0	2
13	283	3	0	0	0	3
14	284	2	3	2	1	8
15	286	1	0	0	0	1
16	286	0	0	0	1	1
17	290	0	0	2	1	3
18	291	0	0	1	0	1
19	292	0	1	0	0	1
20	294	0	0	0	1	1
21	295	1	1	5	1	8
22	297	0	5	1	1	7
23	299	1	0	0	0	1
24	301	1	1	0	0	2
25	303	0	3	0	0	3
26	305	0	0	1	0	1

27	308	0	0	1	2	3
28	310	0	0	2	0	2
29	313	1	0	0	0	1
30	314	0	1	0	0	1
31	315	1	0	0	0	1
32	316	0	0	0	1	1
0	317					0
33	319	4	0	0	0	4
34	321	0	1	1	2	4
35	323	1	1	0	0	2
36	326	0	1	0	0	1
37	327	1	2	0	1	4
38	328	1	0	1	0	2
39	330	1	1	0	1	3
40	331	4	0	0	0	4
41	333	0	0	0	2	2
42	334	0	3	0	0	3
43	335	3	0	0	0	3
44	336	1	0	0	1	2
45	338	1	2	0	1	4
46	340	2	0	0	0	2
47	342	0	0	0	1	1
48	343	1	1	0	0	2
49	344	1	7	0	2	10
50	348	3	1	0	0	4
51	349	0	1	1	3	5
52	350	0	1	0	0	1
		58	50	20	37	<u>165</u>

CNN: Keyword “cyberwar” - Corpus: 52, Items: 165 and 100 pages.

1. October 11, 2011

Virus infects program that controls U.S. drones

From **Chris Lawrence**, CNN

Washington (CNN) -- They've become a linchpin of projecting U.S. military power into war zones around the world. But now those same unmanned aerial vehicles have been **infected by a computer virus [1cm]**, according to a U.S. defense official.

The drones are still flying missions in places like Afghanistan and Iraq, where as many as 150 of them can be involved in various surveillance missions each day. The official says the virus infected the classified military computer systems that control the drones, but it has not "stopped the drones from flying worldwide."

"Military officials are more concerned than panicked by this virus," said Danger Room Editor Noah Schactman, who first reported the story last week for Wired magazine. "They're just really not sure what's going on. They're not sure if it's a deliberate attack. They're not sure if it's something accidental."

The drones fly all over the world, but they are remote-piloted from American soil by pilots at Creech Air Force Base in Nevada. That's where the virus was first detected.

The virus is logging each keystroke that the remote pilots input, and officials are trying to determine whether any classified information is actually being lost or sent outside the network. Schactman says the military has had a hard time wiping out the virus.

"They've tried over and over again to get rid of this thing using some fairly conventional methods, and they haven't worked. And so it seems **the only thing to get rid of this virus is to basically wipe the hard drives of these computers entirely and sort of rebuild the computers from scratch,**" **[2cm]** Schactman said.

But that can be an exhausting process: In 2008 **removable hard drives introduced a virus into thousands of Defense Department computers [3cm]**, and to this day the Pentagon is still purging some machines. In the case of the computers that help coordinate the drones, care also has to be taken to back up all the information, so it isn't lost during rebuilding.

The UAVs have become indispensable for military planners who depend on constant combat air patrols. But current and former Pentagon officials admit that technology cuts both ways. At the confirmation hearing for Defense Secretary Leon Panetta, former Deputy Defense Secretary William Lynn said bluntly, "In the 21st century, bits and bytes can be as threatening as bullets and bombs." Lynn says even the National Defense University has been breached, and in a single intrusion this year 24,000 files were taken from a defense company. He says these are just some examples of a number of cyber intrusions over the past several years.

In June Lynn testified that "Some of the stolen data is mundane, like the specifications for small parts of tanks, airplanes and submarines. But a great deal of it concerns our most sensitive systems, including avionics, surveillance technologies, satellite communications systems and network security protocols. The cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs and the Joint

Strike Fighter." Perhaps most alarming, Lynn admitted that up till now, the US military had not been able to secure its systems. "Current countermeasures have not stopped this outflow of sensitive information," Lynn said. "We need to do more to guard our digital storehouses of design innovation."

Officials have not determined whether the virus introduced into the drone program is benign, or doing actual harm. An investigation is ongoing. Despite the fact the controls are not linked into any outside network, and therefore seemingly impervious to intrusion, the drone systems do have security issues. Noah Schactman says they still use external hard drives, and when they're attached to the top-secret computers it can open them up to infection. He says the true danger of this virus comes not from an ability to "bring down a drone," which is unlikely. Schactman says it comes down to trust. And he surmises that if officials come to think that the data they're receiving from the unmanned vehicles has been compromised, they're much less likely to view the information as safe and valuable. Perhaps most alarming: the worst is yet to come. Even top Pentagon officials admit that more destructive tools are being developed, cyber weapons that have not yet been used. Former Deputy Secretary Lynn says, "And the most malicious actors have not yet obtained the most harmful capabilities. But this situation will not hold forever. There will eventually be a marriage of capability and intent, where those who mean us harm will gain the ability to launch damaging cyber attacks. We need to develop stronger defenses before this occurs."

In August, a drone attack killed al Qaeda No. 2 Atiya Abdul Rahman in Pakistan. The most recent high-profile drone strike resulted in the death of U.S.-born militant cleric Anwar al-Awlaki in Yemen last month.

<http://edition.cnn.com/2011/10/10/us/drone-program-virus/index.html?iref=allsearch>

2. October 6, 2011

Arab Spring galvanizers, WikiLeaks among Nobel contenders

By **Moni Basu**, CNN

(CNN) -- Twitter was abuzz Thursday with the death of Apple visionary Steve Jobs but another topic was gathering steam as the day progressed. Who will win this year's coveted Nobel Peace Prize?

Not Jobs, though many among his huge global following posted messages that he should. The Nobel is never awarded posthumously and that rule also eliminates Mohamed Bouazizi, the unemployed college graduate whose self-immolation in Tunisia sparked a popular uprising that led to the fall of Zine al-Abidine Ben Ali's government. The Tunisian revolt began this year's so-called Arab Spring.

Some years, there are clear frontrunners -- Martin Luther King, Jr., Mother Teresa, Nelson Mandela, Aung San Suu Kyi.

This year, it's anyone's guess with a record number of nominations -- 241 -- received by the Nobel committee. Of those, 53 are organizations, including WikiLeaks -- the website founded by Julian Assange that facilitates the publication of classified information and made headlines for leaking documents and videos related to the wars in Iraq and Afghanistan [4wb]. It also released thousands of U.S. diplomatic cables.

"Liu Xiabao was awarded the Nobel Peace Prize last year for his struggle for human rights, democracy and freedom of speech in China," blogged Norwegian lawmaker Snorre Valen of the Socialist Left Party, who nominated WikiLeaks. "Likewise: WikiLeaks have contributed to the struggle for those very values globally, by exposing (among many other things) corruption, war crimes and torture -- some times even conducted by allies of Norway."

Liu's win upset the Chinese and set off a diplomatic squabble. The year before, the world gasped collectively at Barack Obama's win, a shocker that the U.S. president had won even before he had completed his first year in office.

Despite the controversy that has swirled around perhaps the world's most prestigious prize, some experts say this year is a no-brainer, given the seismic events that have gripped the Arab world.

Kristian Berg Harpviken, director of Norway's Peace Research Institute Oslo shortlisted men and women who did their share in fomenting peaceful revolts against repressive regimes.

Harpviken's top choice is Israa Abdel Fattah, who helped organize Egypt's online April 6 Youth Movement in 2008.

She was arrested by Egyptian security that year and soon became a symbol of defiance against Hosni Mubarak's government. She has earned the monikers "cyber dissident" and "Facebook girl" and was named one of Arabian Business Magazine's 100 most powerful women in 2011. [5wb]

The peace research institute's website said that Fattah is a good choice because the Nobel committee "has emphasized its wish to be relevant, to speak to dominant themes of the present, and to see the prize giving leverage in unfolding processes. Secondly, Harpviken believes that the prize is likely to be awarded to a female leader or activist who has been an innovator of new tools for bringing about peace."

Another potential winner is Wael Ghonim, the former Google executive who used social media to jump-start social change in Egypt. Ghonim fired off a steady stream of messages on Twitter and Facebook and worked behind the scenes to galvanize thousands to march on the streets to demand change.

Tunisian blogger Lina Ben Mhenni is also on many top lists. Censored in her own country, she criticized the regime long before the uprisings began, dispersing information to the outside world.

"A prize to Mhenni would be a prize to independent reporting, in the form of social media, as well as recognition of the peaceful protests of the Tunisian people at large," the peace institute website said.

Some experts think that Gene Sharp, an American scholar who founded the Albert Einstein Institution in Boston, could be recognized for his work on the principles of non-violence, including "From Dictatorship to Democracy." The downloadable writings in many languages have proved a source of inspiration around the world, including the uprisings in the Middle East and North Africa.

Harpviken also named Memorial, a Russian civil rights group known for its fight for to protect refugees and victims of political persecution and human rights violations in war zones.

Natalya Estemirova, Memorial's lead researcher in the Chechen republic, was abducted and killed in July 2009. Human Rights Watch said it "appeared to be clearly connected to her work uncovering human rights violations in Chechnya."

Bookmakers Paddy Power listed Sima Samar, head of the Afghan Independent Human Rights Commission, as a favorite at 5/4 odds.

A physician and trailblazer for women's rights, Samar was named deputy premier after the toppling of the Taliban in 2001, the first woman to win such a high government post. She has been threatened with death and harassed for questioning conservative Islamic laws and practices, including the burqua, the head-to-toe garment Afghan women have been forced to wear.

Paddy Power picked the right winner last year. That bodes well for Samar. Other names on global shortlists include:

-- Aung San Suu Kyi, the Burmese pro-democracy leader who was released from house arrest last year. Suu Kyi is already a Nobel laureate -- she was awarded the peace prize in 1991. No individual has won it twice, though two organizations -- the International Committee of the Red Cross and the United Nations High Commissioner for Refugees -- are repeat winners.

-- German Chancellor Helmut Kohl

-- Cuban dissident Oswaldo Payas Sardinias

-- Ghazi bin Muhammad, a Jordanian advocate of interfaith dialogue

The winner will be announced Friday. Until then, the speculation continues to heat up.

Twitter user Alu Abunimah (@avinunu) offered one last candidate for consideration to his more than 16,000 followers.

"Maybe the Nobel Peace Prize will go to The Markets, to help Calm them and make them Feel Better," he said. "Also they need the money."

The Nobel Peace prize laureate will win about \$1.5 million.

<http://edition.cnn.com/2011/10/06/world/norway-nobel-peace-prize/index.html?iref=allsearch>

3. October 3, 2011

The Pentagon's cyberstrategy, one year later

Editor's Note: William J. Lynn III is U.S. Deputy Secretary of Defense.

By **William J. Lynn III**, Foreign Affairs

For almost all of human history, man has waged war on land and at sea. Air and space emerged as potential battlefields only in the past few generations. Now, the danger of cyberwarfare rivals that of traditional war. The advent of more destructive technologies - and of their inevitable proliferation among actors willing to use them - means that the United States must strengthen its **critical national networks against ever worse threats [6in]**.

In "**Defending a New Domain**" (September/October 2010), I announced that the Pentagon had officially recognized cyberspace as an operational domain and went on to describe the military's cyberstrategy. One year later, U.S. military networks are better defended, the U.S. Cyber Command is fully operational, and we have made progress working with **private industry to secure critical infrastructure [7in]**.

Meanwhile, the Obama administration has committed half a billion dollars to develop advanced defensive technologies, including novel approaches to improving network security. But much remains to be done, and the window for doing it is short.

CYBERCONFLICT

Our assessment is that cyberattacks will be a significant component of future conflicts. Over thirty countries are creating cyber units in their militaries. It is unrealistic to believe that each one will limit its capabilities to defense. Moreover, the centrality of information technology to the U.S. military and society virtually guarantees that future adversaries will target it.

Putin's Return and Washington's Reset With Russia

The United States is now in the midst of a strategic shift in the cyberthreat. Until now, intrusions have largely been for the purpose of exploitation: stealing intellectual property from commercial networks or spying on the government. There have also been disruptive cyberattacks, for example on **Estonia, in 2007, and Georgia, in 2008**. In a development of extraordinary importance, cyber technologies now exist that are capable of destroying **critical networks**, **[8in]** causing physical damage, or altering the performance of key systems. In the twenty-first century, bits and bytes are as threatening as bullets and bombs.

The cyberthreat is also intensifying in a second direction: toxic technologies are proliferating among actors willing to use them. At present, sophisticated cyber capabilities reside almost exclusively in the hands of advanced nation states. For them, U.S. power - both military and cyber - is a strong deterrent. Although attribution of a cyberattack is difficult, the risk of discovery is likely too great for a major nation to mount a major attack. But circumstances can change. The United States must guard against the possibility of a future adversary who is not deterred from launching a cyberstrike.

Terrorist groups and rogue states must be considered separately. With few assets the United States can hold at risk, they are more willing to provoke. To advance their radical agendas, they are intent on acquiring, refining, and expanding their cyber capabilities. A burgeoning market for cybercrime services, with settled price lists for botnet rentals and denial-of-service attacks, already exists in the murky underworld of organized crime. If a terrorist group does obtain destructive cyberweapons, it could strike with little hesitation. Faced with these threats, the United States must guard **against both a cyber Pearl Harbor [9in]**, as Secretary of Defense Leon Panetta has warned, and the possibility of a cyber 9/11. Indeed, Panetta recently noted how the disruptive effects of a cyberattack may well be worse than 9/11 and Pearl Harbor combined.

In short, more destructive tools are being created every day, but have not been widely used. Similarly, the most malicious actors have not yet obtained the most harmful technologies. But this situation will not hold forever. There will eventually be a marriage of capability and intent, where those who mean to harm the United States will gain the ability to launch a damaging attack. The United States must develop stronger defenses before this occurs.

To meet this growing threat, the Department of Defense developed a strategy for operating in cyberspace that has five pillars: treating cyberspace as an operational domain, like land, air, sea, and outer space; **employing active defenses to stop malicious code before it affects our networks [10cm]**; **protecting commercial networks that operate the critical infrastructure that our military relies upon [11in]**; joining with allies to mount a collective cyberdefense; and mobilizing industry to redesign network technology with security in mind. (The strategy is available at www.defense.gov/cyber.)

CRITICAL INFRASTRUCTURE

Extending advanced cyberdefenses to critical infrastructure is one of the strategy's most crucial objectives. [12in] Cyber intrusions have been directed at nearly every sector of our economy. Victims include the IMF, Citibank, Sony's PlayStation network, the secure data provider RSA, Google, and NASDAQ. The United States' critical infrastructure has also been probed. Because much of this infrastructure supports military operations, its failure could compromise national defense. Ninety percent of U.S. military voice and Internet communications, for example, travel over the same private networks that service private homes and offices. The U.S. military relies on the civilian transportation system to move its personnel and freight, on commercial refineries to provide its fuel, and on the financial industry to process its payments. Ensuring the integrity of the networks that undergird critical infrastructure must therefore be a part of the United States' cyberstrategy.

The Department of Homeland Security has the primary responsibility for protecting U.S. critical infrastructure. In the past year, the Defense Department and DHS have agreed to coordinate cybersecurity efforts, established a joint planning capability, and have exchanged cyber personnel. The Defense Department is also helping DHS deploy advanced defensive technologies on networks in the .gov domain.

How the Haqqani Network is Expanding From Waziristan [13in]

Partnering with DHS carries the long-standing tradition of military support for civilian authorities into the cyber domain. During a natural disaster, such as a hurricane, FEMA often uses military troops and helicopters to help deliver relief. Similarly, the military's cyber capabilities will be available to civilian leaders to help protect the networks that support government operations and critical infrastructure. At all times, these resources will be under civilian control and used according to civil laws.

DIB CYBER PILOT

Within critical infrastructure, the private defense companies that build the equipment and technology the U.S. military uses are especially important to protect. Their networks hold valuable information about U.S. weapons systems and their capabilities. Alarming, foreign intruders have already extracted terabytes of data from defense industry networks in recent years. In a single intrusion in March, 24,000 files were taken. Some of the data stolen during this and other attacks is mundane, but a great deal concerns the United States' most sensitive systems, including aircraft

avionics, surveillance technologies, satellite communications systems, and network security protocols.

Current countermeasures have not stopped this outflow of sensitive information.

[**14cm**] In response, the Department of Defense, in partnership with DHS and a handful of defense companies, has established a pilot program to provide more robust protection for private networks. In the Defense Industrial Base (DIB) Cyber Pilot, the government shares classified threat intelligence with private companies or their Internet service providers. The intelligence is then integrated into companies' own network defenses. Because it builds off commercial technologies, the DIB Cyber Pilot provides additional protection for only an incremental increase in cost.

Moreover, the project does not entail U.S. government monitoring, intercepting, or storing of private sector communications, and it is voluntary for all participants.

The Defense Department is only beginning to evaluate the pilot's effectiveness, but it has already stopped hundreds of intrusions at participating industry partners. Building off this initial success, the Department is hoping to expand the pilot to more defense companies. The Pentagon is also working with the White House and the Department of Homeland Security to evaluate applying **the concept to other critical infrastructure sectors** [**15in**]. With intrusions over the last year into the networks of the financial sector, of transportation networks, of a national laboratory run by the Department of Energy, and even of top-notch cybersecurity firms, there is much left to do. But by establishing a lawful and effective framework for the government to help the operators of critical infrastructure defend their networks, the DIB Cyber Pilot will provide a means to measurably enhance the security of the nation.

DEFENDING CYBERSPACE RESPONSIBLY

The steps the Pentagon has taken to respond to the cyberthreat have prompted discussion about cyberwar and its implications. Commentators have asked whether and how the United States would respond militarily to attacks on its networks. Some are concerned that cyberspace is at risk of becoming militarized. The concern here, as in other areas, is that the measures put in place to prevent hostile actions will negate the very benefits of cyberspace the government seeks to protect. The Department of Defense has designed its cyberstrategy to address this concern. We need to ensure that a domain overwhelmingly used by civilians and for peaceful purposes is not fundamentally altered by the military's efforts to defend it.

Overturning Lee Kuan Yew's Legacy in Singapore

It should come as no surprise that the United States is prepared to defend itself in all domains. It would be irresponsible, and a failure of the Defense Department's mission, to leave the nation vulnerable to a known threat. Just as the military defends against hostile acts from land, air, and sea, it must also be prepared to respond to hostile acts in cyberspace. Accordingly, the United States reserves the right, under the law of armed conflict, to respond to serious cyberattacks with an appropriate, proportional, and justified military response.

The ability to identify and respond to a serious cyberattack, however, is only part of U.S. strategy. The focus on building robust defenses aims to change adversaries' incentives in a more fundamental way. If the United States increases the resources needed to mount a successful attack, minimizes the impact of attacks when they do occur, and quickly attributes them to their sources, it may be able to change a potential attacker's decision calculus.

Far from militarizing cyberspace, U.S. cyberstrategy will make it more difficult for military actors to use cyberspace for hostile purposes. Indeed, establishing robust cyberdefenses no more militarizes cyberspace than having a navy militarizes the ocean. This commitment to peace through preventive defense is at the heart of the Pentagon's cyberstrategy and the administration's overall approach to cyberspace.

The views expressed in this article are solely those of William J. Lynn III

<http://globalpublicsquare.blogs.cnn.com/2011/10/03/the-pentagons-cyberstrategy-one-year-later/?iref=allsearch>

4. August 15th, 2011

Cybertheft could destroy the U.S. economy

Editor's Note: The following is reprinted with permission of the Council on Foreign Relations.

By **Jonathan Masters**, CFR.org In August 2011, the cybersecurity firm McAfee released an eye-opening report (PDF) detailing its investigation into a multi-year, most likely state-sponsored cyberattack that includes intrusions into the U.S. federal government and defense contractors, resulting in the theft of massive stores of intellectual property.

The report's author and McAfee's vice president of threat research, Dmitri Alperovitch, describes these attacks, known as Operation Shady RAT, as a profound threat, indicative of a larger trend that may result in "the complete destruction" of the U.S. economy. Rather than focus on the potential for a theoretical "cyber Pearl Harbor," he says that U.S. policymakers should use all of the nation's power to stem **the steady theft of national secrets [16cm]**.

Jonathan Masters: What do you see as the broader implications for U.S. cybersecurity policy given these Shady RAT attacks?

Dmitri Alperovitch: The policy discussion up to date, at least in open circles, has been a bit misfocused. The challenge has been that everyone has been talking about waiting for this massive event—a "cyber Pearl Harbor"—but what's really happening is that we're suffering a "death by a thousand cuts."

It's not one event, such as our electric grid going down, but rather a wholesale transfer of wealth from our economy (PDF) to our adversaries' economies that's been going on

for the last six years or more. The results of these activities, especially theft, will manifest itself in dramatic ways over the years with reduced economic growth, reduced competitiveness, a loss of jobs and everything that comes with that.

While we should be worried about destructive attacks that can cause widespread damage, physical damage, and even potentially loss of life, **the massive espionage (WSJ) that's been taking place is really the more pressing issue.** [17cm]

What's the first step to getting at this problem?

The first thing that needs to happen is an admission of the problem. One of the most striking things about the [Shady RAT] report is that seventy-two organizations are compromised, and not a single one of them - many had known about these infections - had ever reported it. You have this massive activity taking place, and yet our policymakers don't know about it, the public doesn't know about it, and the news media doesn't know about it.

The first thing we need to do is to address the fact that these companies absolutely have to report this. Some of the regulations that require them to do so already exist, at least if they are a public company. The SEC mandates disclosure of any material event. Now there's debate if someone hacks into a system and steals all of your intellectual property: Is that a material event? Most companies have unfortunately decided that it is not. That's one of the things that needs to change in order to make sure everyone in the country understands the magnitude of this problem. When there's a Shady RAT [attack] every single week that's being disclosed in the media, then perhaps we will be much more willing to act to solve this problem.

The scale and volume on which **this espionage and theft is taking place** is really unprecedented and presents an existential threat to the U.S. economic well-being. While it's true that every government engages in some form of espionage, this exceeds any acceptable norms. You cannot equate strategic espionage - such as trying to determine the disposition of an adversary's strategic nuclear deterrent - to this **wholesale theft of every sector of the economy** [18cm].

Generally speaking, who are the perpetrators of cyberattacks?

I divide them into four categories based on capabilities.

At the low end of the scale you have the **hacktivist groups, such as Anonymous**, and **terrorist groups, such as al-Qaeda and Hezbollah**. And we're very lucky today - and this may change over time - but these groups do not have significant capabilities to do major damage to our country. Most of what they are doing is a distraction.

The second on that scale is **cyber criminals**. They certainly range in capabilities, but their motivation is primarily **financial**. They are not out to destroy the system; they benefit from the system like a parasite benefits from attacking its host. They don't want to destroy the host because it's their livelihood.

On the third end of that scale you have what the industry calls **APT (Advanced Persistent Threat)** - though not all these threats are advanced - effectively nation-states

performing **cyber espionage or operations like Shady Rat and Night Dragon**. These are much more insidious and much more damaging to our economy than either the cyber-criminal actors, or certainly the hacktivists or terrorist actors. But so far they are not interested in destruction.

Finally, on the top end of the scale you have the military destructive operations or cyber network attack operation (CNA), and those today, on a significant scale, will only be conducted by foreign militaries. And if you think about that prospect, no one is out there to destroy our energy grid for example, unless we're already at war with that country or about to enter into kinetic conflict. So while we should absolutely worry about it, it's highly unlikely that out of the blue that sector gets attacked in a catastrophic way.

What percentage of cyberattacks - the ones discovered by the target entities - are reported?

Below 1 percent. And we've been involved in hundreds of investigations over the years. The reason we could not disclose most of them publicly is because of nondisclosure agreements. None of the companies have ever come forward. Most of the disclosures you've seen in the media, even this year, have been accidental leaks.

What do you say to the critics who claim that this notion of cyberwarfare is exaggerated and that organizations like MacAfee are potentially engaging in hyperbole because they stand to profit?

You can accuse us of whatever intentions you want, but try to dispute the facts that we're reporting - that massive sectors of our economy have been compromised and valuable intellectual property has been stolen (NYT). We're not the only ones saying that.

Google was very courageous in announcing their intrusions back in January 2010, and just recently RSA has announced intrusions (Bloomberg), as have Lockheed [Martin] and others. We're not the only ones pointing a finger at this problem. And when you go and talk to an official off-the-record, or even on the record, some will tell you the exact same thing - that it's a massive problem.

I'm not a fan of the cyberwar analogy: Are we at a war? It's a difficult question. Typically when you talk about wars, you expect to see dead people on the streets. We're clearly not seeing that. But is it an existential threat to our country from an economic perspective? Absolutely.

What do you think is missing from the U.S. government's various cyber strategies?

They're very much focused on defense, which is the first step. But this problem is not going to be solved by defense alone. To be clear, I'm not arguing that we go on offense. But I am arguing that we need to raise the level of conversation in bilateral and multilateral discussions with our potential adversaries [such as China and Russia] and make it a major issue on the agenda. We need to bring to bear all of our national

power: economic power, political power, and, if it makes sense, perhaps even military power.[19in] What is happening today is completely unacceptable and needs to stop.

On that note, is there any progress with identifying the perpetrators of these attacks?

That problem is much more theoretical than practical. Most of the time, you know who's doing it. It may be classified, but the government is fully aware who these actors are in most cases. Even when you don't have technological proof of their culpability, you do have the *cui bono* argument of who benefits. While there are circumstances in which rapid real-time attribution may be difficult, in hindsight virtually every case that is serious in nature can be tracked down and attributed.

How much of the problem of cyber criminals and cyber espionage is technical and how much is human error? For example, people falling victim to these spear-fishing scams and so on.

It's both. But [the attacks] are getting better and better to the extent that you can't blame the victim for this. One of the problems we have in this industry and the reason we don't have more disclosures is this mentality [of] "If you get hacked it's your fault."

This is the equivalent of virtual assault. And in the physical world, we would never blame the victim of the assault for that assault taking place, but yet we do so all the time in the cyber world. I think that's completely misguided. While certainly mistakes occur and they need to be rectified, it's the attackers' fault.

What's trending with regard to cybersecurity that you or McAfee are positive about?

Some of the trends are positive where we've seen significant law enforcement wins in recent years and making progress in addressing the cyber-crime problem. There aren't many of these top-notch cyber criminals out there in the world - my guess is less than a thousand are responsible for 90-plus percent of the problem.

Law enforcement has made tremendous efforts, building relationships with other law enforcement agencies across the globe, including in places like Russia, where you wouldn't have thought in a million years that there would be collaboration. There is collaboration now. Is it ideal? No. But it's a lot more than there was even five years ago.

We're seeing arrests: A bunch of people from Anonymous [were] arrested in the last couple of weeks. The number of top Russian cyber criminals and those in the United States and other Western countries have been arrested in the last year. I'm seeing a lot more progress on the deterrent aspect in dealing with cyber crime.

Where do you see the evolving threat in five years?

I see complete destruction of our economy. One of the things that really worries me is whether it's already too late. We've had this activity for the last six or seven years.

Have they already stolen enough and now are just busy taking those schematics and plans and basically rebuilding entire sectors of our economy over there [i.e., China]. We will start to see the answer to that in a few years.

The challenge is that, quite frankly, a lot of this has been painless thus far because when someone goes into a company and steals your intellectual property, it's not like they stole your car - you still have your intellectual property. Until someone does something with it that damages you, you really haven't experienced that loss in many ways. That's why a lot of these companies have been hesitant to come forward.

The other thing that worries me is the risk that some of these cyber warriors who are currently doing espionage for a U.S. adversary - we don't know how much control their own militaries or intelligence agencies have over them, and what rules of engagement they operate under.

It could be that they go home and decide to work for their own benefit using very similar tools and, instead of stealing data, they may modify or destroy that data or the systems that are hosting that data. That's a big problem. They may collude with cyber criminals or terrorists and loan out their skills.

<http://globalpublicsquare.blogs.cnn.com/2011/08/15/cybertheft-could-destroy-the-u-s-economy/?iref=allsearch>

5. August 15, 2011

'Mafiaboy' breaks silence, paints 'portrait of a hacker'

(CNN) -- Michael Calce once briefly shut down this site.

It was February 8, 2000, and the then-15-year-old was egged on by a fellow hacker who believed CNN.com would be impossible to bring down because of its "advanced networks" and "huge traffic numbers." It took Calce just a few minutes.

"The sense of power I felt was overwhelming," he wrote later of the attack, which **slowed CNN.com's news operations for nearly two hours**. "It was also addictive."

By then, the Canadian teen better known as "Mafiaboy" had already made national headlines by toppling Yahoo!, eBay and E*TRADE with a brazen series of denial-of-service attacks, which usually involve barraging a website with so many requests that its servers are overrun [20cm].

It's a story he tells, breaking years of silence, in "**Mafiaboy: A Portrait of the Hacker as a Young Man**," which chronicles Calce's rise to becoming arguably the most famous, or infamous, computer hacker ever.

The book, co-written by Craig Silverman, takes Calce from the day he got his first computer at age 6 to the secretive chat rooms of a then-burgeoning hacker community.

Along the way he single-handedly prompted then-President Bill Clinton to convene a cybersecurity summit at the White House. Attorney General Janet Reno swore her office wouldn't rest until he was arrested.

Those are deep political and legal waters for a kid who, when the police finally busted him, was having a sleepover at a friend's house, staying up late eating junk food and watching "Goodfellas."

"My attacks of 2000 were illegal, reckless and, in many ways, simply stupid," Calce writes. "At the time, I didn't realize the consequences of what I was doing."

Calce eventually pleaded guilty to 56 counts stemming from hacking and attacking the sites. He was sentenced to eight months in "open custody" at a rehabilitation home for youths and spent another year on probation.

Calce's message now, a decade later? It's way easier to do what he did now than it was then.

"Twelve years ago, they actually were real hackers. You had to work and build your arsenal of tools," he said. "These days, they make hacker desktops that you just download and you have every tool out there on the market. If you're interested and you want to be a hacker, you can be a hacker in 30 minutes."

And while Calce and many of his compatriots hacked more out of curiosity than anything else, he said many of **today's generation of hackers have crime, or even espionage, in mind [21cm]**.

"I could have launched those attacks and tried to make money off of it," said the former online bad boy, now a Montreal, Canada-based Internet security consultant. "I was more (about) running tests. Everyone at that point in time was running tests and seeing what they could do and what they could infiltrate."

Calce talked with CNN.com recently about hacking, Internet security and why Facebook, Twitter and other popular online sites can be a bad thing. Below are excerpts from that conversation.

On misconceptions about the term "hacker"

"The problem is that, over the years, it's been misconstrued. The media has used it a couple of times improperly. The problem now is that anything associated with hackers or hacking is in the malicious sense when that's really not true. A hacker is anybody looking to manipulate technology to do something other than its original purpose. That's not necessarily a bad thing."

On recent hacking by "Anonymous" and "Lulzsec"

"They're a different breed. They're considered 'hacktivists.' They hack for a lot of political reasons. They believe information should be free. But some of them do have malicious intent.

"It's really hard to classify them in the white-, black- or gray-hat hacking, but if I had to pick one, I'd probably go with gray. And you're going to see a lot more of these groups.

Technology being where it is, it allows people to fight back. (Compared to traditional political protests) what Lulzsec and Anonymous are doing is way more potent in actually trying to awaken people and raise awareness. [22wb]

"Not that I really condone what they're doing, but I understand their point."

On the risks of Facebook

"I do have a Facebook account, but it's very, very limited. I don't use it in the same fashion that other people would. There are people putting up hundreds of pictures of themselves, updating their status every 10 minutes and adding people they don't know just so they can say they have 1,000 friends."

"We're putting too much information online. I understand the networking part. But the way it's being utilized right now is not going in the right direction. People are data-mining. (Facebook) is such a viable spot for hackers to launch viruses and Trojans [23cm]. People just don't understand the ramifications."

On the prospects of "cyberwar"

"We're going to see a lot more cyberattacks... It probably could be the next world war for all we know. It could be online."

"Places like China actually have hacker camps. They're training you to infiltrate government secrets and whatnot [24cm]. The government is going to have to realize that they're going to need to fight dirty the same way. You're going to need hackers to fight hackers; that's just how the world is evolving right now."

"You're going to have to set up hacker schools to train people. Hacking can be in the positive fashion. There is a white-hat side to hacking and I think we're going to need to breed a lot of white-hat hackers right now to fight the black-hat hackers. Right now, they're winning the war."

On how to stay safe online

To be safer online Calce suggests the following:

_ Stronger passwords:

"The No. 1 problem is strength of passwords," he said. "A lot of people don't use strong passwords. It's getting a bit better, because websites are forcing you now to make longer passwords."

_ Adding firewalls

Calce suggests protecting your computer with "after-market" firewall software, meaning not just relying on the ones already installed on your computer. "Without having a firewall, it's basically like leaving your home with the doors unlocked and the windows open," he said.

_ Be wary of open Wi-Fi:

"Almost every router is installed with Wi-Fi now," Calce said. "Wi-Fi is so incredibly easy to crack or manipulate and people fail to realize this. Even if you are on password-protected Wi-Fi, it's so buggy to the point where it's very easy to crack wireless passwords."

<http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html?iref=allsearch>

6. July 15, 2011

Pentagon makes love, not cyber war

The Pentagon has revealed an unclassified version of its "**Strategy for Operating in Cyberspace**." And despite a drumbeat of scare talk and digital sabre-rattling in Washington, the document takes a measured, reasonable approach -- focusing on good network hygiene and data-sharing, rather than bombing hackers into submission.

The question is whether this public summary conveys what's actually in the classified strategy, or reflects the real mood of the Department of Defense.

"DoD would like to be much more aggressive in what it says and how it acts," says a source familiar with the development of the strategy. "But that tendency to be aggressive has been reined in by the State Department, Treasury, and the White House, and not in an unreasonable way."

Listen to the talk inside the Washington Beltway -- and especially within the Pentagon -- and you'd think hackers were about to reach their hands through our computers, and strangle us all in our sleep.

WIRED: Insiders doubt 2008 Pentagon hack was foreign spy attack

"The United States is fighting a cyber-war today, and we are losing," retired admiral and former National Security Agency chief Mike McConnell **wrote in the Washington Post** last year.

Defense Secretary Leon Panetta **claimed** cyber attacks could be the "next Pearl Harbor we confront." Or perhaps the next Hiroshima.

Senator Carl Levin declared that "cyberweapons and cyberattacks potentially can be devastating, approaching weapons of mass destruction in their effects" during an April 2010 (.pdf) hearing.

According to the **Wall Street Journal**, the Pentagon has come to the conclusion that "computer sabotage... can constitute an act of war." As one military official tells the paper: "If you shut down our power grid [25in], maybe we will put a missile down one of your smokestacks."

Yet the Pentagon strategy uses tones of cooperation, not confrontation, in the strategy it released today.

"By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense," the document notes. "Cyberspace is a network of

networks that includes thousands of ISPs [Internet Service Providers] across the globe; no single state or organization can maintain effective cyber defenses on its own."

WIRED: Cyber war hype intended to destroy the open Internet

Yes, there are all kinds of bad guys out there on the internet, the strategy adds. But many of them are out for money, not for blood.

"The tools and techniques developed by cyber criminals are increasing in sophistication at an incredible rate, and many of these capabilities can be purchased cheaply on the internet."

And the best way to stop these crooks is through strong passwords, up-to-date software, and keeping unclassified disks and drives off of secret systems.

"Most vulnerabilities of and malicious acts against DoD systems can be addressed through good cyber hygiene," document adds.

If there was a nod to the McConnell crowd -- who'd like to "**reengineer the internet**" to make everyone trackable online -- it was in the declaration that "DoD will pursue revolutionary technologies that rethink the technological foundations of cyberspace." But the nod was a subtle one.

Behind closed doors, some Pentagon officials take a much harder line. There have been calls to massively shift Defense Department spending from defensive measures to online offense.

Other countries -- especially the Chinese, they believe -- had infiltrated every corner of the military-industrial complex, and need to be shoved back. Every fresh online break-in brings a fevered call to declare the intrusion an "act of war."

But that view is not universally shared in Washington. "There is no cyberwar," White House cyber czar Howard Schmidt has **repeatedly said**. And those more rational voices helped keep the rhetoric in this Pentagon strategy from overheating.

As one source who watched the strategy develop, says: "This the result of a long, political process."

But this is hardly the final document, Gen. James "Hoss" Cartwright tells reporters.

"This strategy talks more about how we are going to **defend the networks**, [26cm]," **says Cartwright**, the Vice Chairman of the Joint Chiefs of Staff and one of the most **influential voices** on cybersecurity in the Defense Department. "The next iteration will have to start to talk about here's a strategy that says to the attacker, 'If you do this, the price to you is going to go up. It's not just free.'"

"Today, we are on a path that is way too predictable. It's purely defensive. There is no penalty for attacking right now," Cartwright adds. "We've got to figure out a way to change that."

<http://edition.cnn.com/2011/TECH/innovation/07/15/pentagon.cyber.war.wired/index.html?iref=allsearch>

7. June 23, 2011

Cyberwarfare finds a captive audience

(CNN) -- From scanning news headlines over the last couple of months, you might think the walls around Internet strongholds are made of rotting wood.

Yet the frequency of data breaches actually hasn't increased dramatically, according to security experts and reports compiled by nonprofit advocacy group **Privacy Rights Clearinghouse**.

What appears to be changing is how quickly companies are publicly disclosing network intrusions and the breadth of information stolen in each case. Those factors, in turn, spur the rabid media attention that's being given to digital security.

More personal info is being nabbed as part of these break-ins because, simply, each company is taking in **reams of data from more customers**. [27cm] As Web usage grows and becomes more personalized, so too do the databases that store the names, addresses and, in worse instances, credit card numbers that are routinely dispensed over Internet lines.

Still, the incidents, with new targets popping up every week, are no less frightening.

Several national governments are on the defensive, while simultaneously exploring ways to use cyber tactical strikes to their own ends.

Google said last year that a **widespread intrusion** into its system originated in an area that's home to a national security branch of the Chinese army and then blamed the **Chinese government for slowing access** to its services. A U.S. diplomatic cable made public by WikiLeaks [28wb] charged that the **Chinese government ordered the computer hacking** [29cm], according to a report in **The New York Times**. Chinese officials denied any involvement in the attack.

Hackers from China, Russia and other countries reportedly **penetrated the U.S. electrical grid** in 2009. [30in] U.S. federal agencies have used digital detective work in countless investigations. President Barack Obama signed executive orders more than a month ago that provide guidelines for how extensively U.S. international military forces can use cyberwarfare, The Associated Press reported on Wednesday.

But the cyberattacks that directly affect millions of people (Whoops! Bank account is empty!) are also getting attention from regulators. [31in] The FBI is pitching in to help companies make sense of system intrusions, as in the case of Sony.

The Japanese tech giant has become a recent poster child for data mismanagement. Sony's systems have been breached 20 times in the last two months or so. Hackers accessed 177,000 e-mails from the French website of Sony Pictures last weekend. About two weeks earlier, hacker group Lulz Security obtained more than 1 million e-mail addresses, passwords and other **personal info from the U.S. Sony Pictures**. [32cm]

Those, of course, pale in comparison to the more than 100 million accounts, many of which had credit cards on file, from **PlayStation and other Sony game networks**.

The PlayStation hack was the biggest on record (many institutions have never publicly disclosed the details of past data theft) since a combined 130 million credit and debit card numbers were taken from Heartland Payment Systems and some retail chains, including T.J. Maxx, several years ago. [33cm]

Before that, 26.5 million people's information and some Social Security numbers were taken from U.S. Department of Veterans Affairs computers in 2006. A year before that, CardSystems fumbled info from 40 million accounts.

The scope of these intrusions wasn't fully understood until years after they had happened.

But U.S. regulators have become less patient. A congressional inquiry to Sony executive Kazuo Hirai asked why the company took so long (a week or two) before releasing details about stolen subscriber info or the fact that **credit card numbers were taken**.

"As soon as you figure out there's a breach, you have to put it out right away," said Jeff Carter, the development chief for security firm Hoyos Group. "After the Sony breach, it finally reached a maturity level that caught everyone's attention."

Security consultancies, including Carter's, began receiving calls after the Sony incidents from companies suddenly more concerned about locking down their systems. For example, Carter said his group saw an influx in requests from video-game makers, as well as from financial institutions.

Banks and credit card processors are typical targets for rogues proficient in circumventing computer security who are trying to find a big payday. But entertainment companies, not traditionally hoarders of customers' info, have found themselves in the crosshairs of high-profile hacker collectives that identify themselves as nerdy gamers and purveyors of Web culture.

The hacker group LulzSec, fresh off its raid on Sony Pictures, offered to help Sega investigate a recent break-in that exposed 1.3 million accounts. "We love the Dreamcast," a spokesperson for the group wrote, referencing Sega's cult classic game console. "We want to help." [34wb]

Sony uncovered a file after one of its incidents that suggested the group Anonymous might be behind the attacks. Anonymous denies the charge. Sony says it still hasn't uncovered the names of the culprits.

As this novelty plays out -- the prominent and enigmatic cyberpunks, the flailing conglomerates, the superpower nations issuing declarations on cyberwar -- interest in the data-hacker phenomenon grows. Even though it's all been an open secret for years.

<http://edition.cnn.com/2011/TECH/web/06/23/hacks/index.html?iref=allsearch>

8. January 18, 2011

U.S. strategy on Iran is working

Editor's note: Joe Cirincione is president of *Ploughshares Fund*, a global security foundation that seeks to make progress toward a world free of nuclear weapons and author of *"Bomb Scare: The History and Future of Nuclear Weapons."*

(CNN) -- The strategic calculus for dealing with Iran's nuclear program has shifted dramatically in the past month.

First, came news that the **Stuxnet computer worm [35cm]** had apparently wrecked more than one fifth of the centrifuges Iran has used over the past five years to enrich uranium.

Then came new estimates from leading Israeli authorities that Iran is three to five years away from having a nuclear weapon, a sharp shift from earlier assessments. On Sunday, The New York Times **reported** the U.S. and Israel may be behind the computer virus, confirming what many had suspected.

The nuclear clock is still ticking in Iran. Its scientists and engineers are smart and dedicated, and the regime seems determined to acquire nuclear technology that can be used to make fuel for reactors or the cores of nuclear weapons. But the clock has slowed. Time is now on the side of efforts to negotiate an end to Iran's program.

Credit must be given to the Obama administration. The president's critics have blasted his Iran strategy, portraying him as weak and naive. Some have been campaigning for military strikes as the only solution to a threat they have claimed was urgent and otherwise unstoppable.

Weekly Standard Editor Bill Kristol, for example, has long **urged U.S. and Israeli attacks on Iran** and blasted President Obama for having "done nothing effective [and] pressuring Israel not to act to stop Iran from getting nuclear arms."

The president, however, now appears to have been playing a deeper game than critics understood.

The strategy could be called "Engage, Sanction and Sabotage." It began two years ago with Obama's offer to talk directly to the Iranian regime as he extended the hand of friendship in his **inaugural address**.

When Iran rebuffed his calls, Obama used their refusal to build the case for tougher international sanctions, an effort greatly aided by his exposure in September 2009 of a covert enrichment facility near the city of Qom. The U.N. Security Council last year passed the toughest sanctions ever enacted on a member state. The European Union, Japan, South Korea and other states piled on their own sanctions, as did the United States.

Concurrently, the administration, as the Times reports, was developing the most sophisticated cyberweapon ever deployed in "a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own." It worked.

The **centrifuge program** was already problematic, working with a decades-old Pakistani design that is notoriously temperamental, resulting in hundreds of machines breaking down. The **Institute for Science and International Security** concludes that the virus

caused new "major problems," forcing the Iranians to remove an additional 984 machines -- known as IR-1 centrifuges -- from their main facility at the city of Natanz.

The sanctions make it much harder for Iran to recover from the cybersabotage. [36cm]

They hamper Iran's ability to import the high-tech materials, such as carbon fiber and maraging steel, needed to replace these machines or build the more advanced centrifuges Iran desires.

A senior European official told the Wall Street Journal, "We believe they are experiencing critical shortages" of the materials for the centrifuges program.

U.S. expert David Albright adds, "They seem to be approaching their limit on the number of IR-1 centrifuges they can build."

Israel's retiring intelligence chief, **Meir Dagan**, said the international sanctions and covert actions have slowed the Iranian program.

He estimated Iran could not have a nuclear bomb before 2015, while **Deputy Prime Minister Moshe Yaalon** puts the danger date at 2013. This is a sharp break from **previous Israeli estimates** that have warned Iran could get a nuclear bomb within months.

The Israeli estimates are a vote of confidence in Obama's Iran strategy. It is by far the most successful Iran policy in decades. The question now is how to use the time?

The nuclear program has been slowed but not stopped. The sanctions are hurting Iran's economy, but the regime has a high pain threshold.

Sanctions and sabotage alone cannot coerce Iran into either compliance or collapse. The 2012 presidential campaign will likely spur renewed calls for military strikes on Iran, as may hearings in the Republican-controlled House of Representatives.

Now is the time to emphasize the engagement component of the strategy.

A new report from the Henry L. Stimson Center and the U.S. Institute of Peace concludes that the administration "must rebalance" its approach.

"U.S. and European leaders should communicate a comprehensive picture of what Tehran has to gain from a mutually acceptable agreement," say authors Barry Blechman and Daniel Brumberg.

In other words, give the Iranian regime a face-saving way out. Pressures are building on Iran and within Iran, but unless the regime believes there is a negotiated solution that can guarantee its security and allow a resumption of normal diplomatic and economic relations -- including with the United States -- the leadership will persist with its current course.

Diplomatic solutions have their risks. But they are far preferable to the risks of war with Iran. Or the risks of **an Iranian response to the cyberwar** we are apparently now waging. Now is the time to press the U.S. advantage and capitalize on the gains the administration has won.

<http://edition.cnn.com/2011/OPINION/01/18/cirincione.iran.nuclear/index.html?iref=allsearch>

9. December 16, 2010

The Sweep: WikiLeaks stirs anarchy online

In "The Sweep," CNN dives deep into issues that are making news and explores why they're in the headlines.

Washington (CNN) -- WikiLeaks' avalanche of U.S. State Department cables had just hit the internet when Secretary of State Hillary Clinton boarded a plane for a meeting of European countries in Kazakhstan. [37wb]

Descending the stairs from her plane in the biting Central Asian cold, she was braced for what wasn't officially on the agenda: apologizing to some of the 52 leaders she was about to see who were the targets of highly embarrassing comments by U.S. diplomats contained in those cables.

Cables by a U.S. Embassy official described the meeting's host, Kazakh President Nursultan Nazarbayev, the man whose hand she was about to shake, as having a lavish lifestyle, his prime minister as dancing the night away in a disco. There were some tough moments, but a top Kazakh diplomat who attended the meeting in Astana says that Clinton "kept her face. She didn't run away from difficult questions."

One by one Clinton and her top aides met with each of the ministers, explaining, apologizing, cajoling and trying -- in spite of the harsh words in the cables -- to salvage the relationships that she and the Obama administration had worked hard to establish.

In Washington, the State Department went into "war room" mode, pulling together an emergency round-the-clock team to handle the fallout.

While embarrassing to both U.S. diplomats and the foreign leaders mentioned in the cables, there haven't been any bombshells out of the small percentage of cables released so far. But the implications of the leaks -- not just for America's relations with countries around the world but for politics worldwide, security of information and the future of an unregulated cyberworld -- are enormous and not yet fully known.

The practical effects already are being felt at U.S. embassies overseas.

In foreign capitals, some countries are limiting the number of American diplomats who can attend meetings. Those who are invited are asked to leave their notebooks behind. Several foreign diplomats said this lingering distrust of American officials is likely to remain for some time. Few leaders, they said, will feel comfortable expressing honest views, fearing they will be quoted in cables that will be splashed across the internet.

American diplomats also have been burned by comments they made about world leaders.

Negative impressions of Afghan President Hamid Karzai by Karl Eikenberry, U.S. ambassador to Afghanistan, were already well-known, thanks to cables he wrote to Washington leaked last year. But scathing new cables in which Eikenberry calls Karzai

"paranoid," "weak" and an "overly self-conscious" leader have further aggravated already strained relations with the Afghan leader and are sure to make it more difficult for the U.S. diplomat to do his job.

Similarly, future meetings between German Chancellor Angela Merkel and Philip Murphy, the U.S. ambassador to Berlin, won't be all that comfortable after a leaked dispatch by Murphy dubbed the German leader "risk averse and rarely creative."

Leaks damage relationships with U.S. allies

The leaks also have been a cold shower for some U.S. allies who felt they had a warm embrace from Washington.

Perhaps Polish President Bronislaw Komorowski put it best when he said he had no more illusions about his country's ties with the U.S. after reading WikiLeaks cables that show the United States puts relations with Russia ahead of Poland's security interests. This month in Washington, Komorowski said he told President Obama, "I simply believe that very much has gone the wrong way in Polish-American relations. And this can be testified to by leaks from different American cables." [38wb]

Clinton went to great lengths to make clear that the opinions of diplomats expressed in the cables don't reflect official U.S. policy. The authors, she and other U.S. officials said, are simply giving unvarnished feedback to Washington about the situation in other countries, something all diplomats are accustomed to doing.

More damaging, however, are revelations about the views of America's interlocutors about their own countries.

In Germany, the chief of staff in the foreign minister's party headquarters was forced to resign over a leaked cable that showed he was regularly briefing U.S. officials on the political situation inside his country. Such valuable intelligence from insiders may be hard to come by post-WikiLeaks.

The ability to get insightful perspectives about third countries is likely to suffer as well.

Both Saudi King Abdullah and Mohammed bin Zayed, crown prince of the United Arab Emirates, were cited in the cables for making blunt and harsh assessments of Pakistan's civilian leaders. While their views were no surprise, would they do it again if they can't trust their confidences will be kept? Prospects for future candid conversations that provide a window into other countries look bleak.

Beyond relationships with allies, the WikiLeaks disclosures also have the potential to affect critical foreign policy issues now that the world's diplomatic cards have been laid on the table. [39wb]

It was no surprise to read that Saudi Arabia's and Bahrain's fear of the threat posed by Iran's nuclear program. But when Abdullah is quoted as asking Obama to "cut the head off the snake" or the king of Bahrain is seen telling American officials that the Iranian nuclear program "must be stopped," it reinforces Iran's suspicions and could force Tehran to make more trouble in the region.

Officials lament that any hope U.S. allies in the Gulf would endorse tougher measures against Iran are even less likely now.

Clinton: 'An attack on the international community'

And how will China react to comments to Clinton by then-Australian Prime Minister Kevin Rudd, captured in a cable, that force might be needed to contain Beijing? The candid conversation between the two leaders in which Rudd said Australia's intelligence community was keeping a close watch on China's growing military power and Clinton, concerned about China's economic rise, asked, "How do you deal toughly with your banker?" leave the U.S. exposed and the Chinese paranoid.

It is no wonder Clinton argued WikiLeaks' disclosure of the cables is "an attack on the international community." The message to wounded countries that might take delight in U.S. discomfort is that their dirty laundry could be aired, too. [40wb]

Clinton has taken a dual approach to responding to the cables.

As the WikiLeaks cables were hitting newsstands and websites, Clinton angrily said, "There is nothing laudable about endangering innocent people, and there is nothing brave about sabotaging the peaceful relations between nations on which our common security depends."

But a few minutes later, she tried to downplay the cables' contents as part of diplomatic "give-and-take." Clinton joked that at least one of her counterparts said, "Don't worry about it. You should see what we say about you."

As the U.S. makes its case against WikiLeaks' founder Julian Assange, it faces charges of hypocrisy that its own commitment to democracy and a free press is no stronger than the countries it criticizes. In a January speech, Clinton championed the case of internet freedom, saying, "The more freely information flows, the stronger societies become."

Clinton said, "Even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable."

The Obama administration is arguing that Assange is neither a journalist nor a whistleblower. But Clinton's arguments about internet freedom have become less convenient for Washington post-WikiLeaks, a fact not lost on Russian President Vladimir Putin, who took the opportunity to score political points at the U.S. expense. Even as he was dubbed an "Alpha dog" and his country a "mafia state" in the cables, Putin fired back by saying, "If you have a democracy, then it should be full."

Referring to the case against Assange, Putin, still smarting from previous U.S. lectures to him about democracy, retorted, "We have a saying here: 'Whoever's cow it was that mooed, yours should remain quiet.' So I would like to shoot the puck back at our American friends."

State Department disconnects from central database

As the U.S. seeks to contain the diplomatic fallout, it also is trying frantically to ensure such a breach doesn't happen again.

Before 9/11, the State Department operated its own internal cable system and encrypted documents to ensure security. After the attacks, it was merged into a new digital records system controlled by the Defense Department to which more than 1 million government employees had access. Since the WikiLeaks disclosures, the State Department temporarily has severed its connection to that database while it works to prevent the future unauthorized downloading of material.

The administration has even prohibited U.S. government employees from reading the cables on the internet. And it has demanded the return of what it calls stolen property.

But it knows, in reality, that it's too late. The cables are spreading like weeds across the internet, with about 1,300 mirror sites so far copying the dispatches and reposting them in a seemingly endless cyber cycle.

Moreover, the WikiLeaks saga has turned the internet into the Wild West. While Assange fired the first volley -- what is being referred to as the first "cyberwar" -- armies of both supporters and opponents are in open combat on the Web.

In the initial moments after the cables' release, hackers tried to shut WikiLeaks down, with the site experiencing denial of service attacks. While it is unclear whether these cyber mercenaries were working on behalf of the U.S. government, they seemed to be supporting the U.S. claims that the disclosures were dangerous to national security.

Assanges' supporters shot back with anonymous "hacktivists" attacking the sites of companies such as Amazon, which threw WikiLeaks off its servers, and MasterCard and PayPal, which froze WikiLeaks accounts and prevented Assange's supporters from donating to his cause.

These cyber vigilantes, launching what they called "Operation Payback," even sought to attack the website of the Swedish prosecutor who issued Assange's arrest warrant on sexual-abuse allegations. [41wb]

WikiLeaks sought to distance itself from these hackers, saying there is no affiliation with a loosely knit online movement known as "Anonymous," which took credit for the attacks.

Cyberwar taking a sinister turn

The cyberwar has taken an even more sinister turn in foreign capitals, with some countries generating fake cables to bolster their political agendas.

Already one Pakistani news agency had to retract cables, published in Pakistani newspapers about India meddling in Pakistani affairs. One, revealed to be a forgery, spoke of India's role in supporting insurgents in Pakistan's tribal regions, while another talked about rifts in India's top army command and yet another mentioned "Bosnianlike genocide" by the Indian army in Kashmir. The potential for diplomatic missteps based on erroneous information is enormous.

Many have wondered why the U.S. government, with its own sophisticated cyberwarfare capabilities, has not moved to shut WikiLeaks down if, as Clinton has argued, the leaks threaten national security.

With cyberspace still a new battleground, the administration is struggling with rules to govern such warfare, especially against an unconventional enemy. A cyber-attack on WikiLeaks might not even work, given the prolific spread of the cables to countless other sites. It also could expose U.S. cyber capabilities to much more lethal enemies, such as Iran or terrorist groups such as al Qaeda.

While the cables are embarrassing and are likely to cause discomfort with allies for some time to come, officials acknowledge the threat posed by their release does not warrant a cyberwar using the full scale of the U.S. cyber arsenal.

The administration eventually will recover from this embarrassment, but cyber experts warn the anarchy spawned by WikiLeaks could mark the beginning of uncharted waters online. With the lack of regulations on the internet, this popular rebellion of tech-savvy activists is hard to trace and even harder to stop. Nobody knows where they will strike next. [42wb]

<http://edition.cnn.com/2010/POLITICS/12/15/sweep.wikileaks/index.html?iref=allsearch>

10. December 10, 2010

Why WikiLeaks hackers are a glitch, not a cyberwar

Editor's note: Douglas Rushkoff is the author, most recently, of "Program or Be Programmed," and "Life Inc: How Corporatism Conquered the World and How to Take it Back"

(CNN) -- Like a momentary glitch on a flat-panel display, the attacks by hackers calling themselves "Anonymous" came and went. Visa, PayPal, MasterCard and Amazon report no significant damage, and business goes on as usual. The corporations acting to cut off WikiLeaks remain safe.

Although many are unsettled by the thought of a site such as WikiLeaks revealing state secrets or a group of anonymous hackers breaking the security of the banking system, events of the past week reveal that such threats are vastly overstated. [43wb]

If anything, the current debacle demonstrates just how tightly controlled the net remains in its current form, as well as just what would have to be done to create the sort of peer-to-peer network capable of upending corporate and government power over mass communication and society itself. [44wa]

While in the short term, WikiLeaks managed to create a public platform for a massive number of classified cables, the site itself was rather handily snuffed out by the people actually in charge of the internet. That's because however decentralized the net might feel when we are posting to our blogs, it was actually designed around highly centralized indexes called domain name servers.

Every time we instruct our browsers to find a web page, they ping one of these authorized master lists in order to know where to go. Removing WikiLeaks or any other site, group, top-level domain or entire nation is as easy as deleting it from that list.

The durability of WikiLeaks' disclosures rests less in the willingness of many rogue websites to attempt to host them in WikiLeaks' stead than in the sanctity of traditional news outlets such as The New York Times and Guardian of London, which were also sent the complete package of classified documents and can't be turned off with the online equivalent of a light switch.

Likewise, the server space on which our websites appear is owned by corporations that have the power -- if not the true right -- to cut anyone off for any reason they choose. It's private property, after all.

Similarly, our means of funding WikiLeaks is limited to companies such as Visa and PayPal, which immediately granted government requests to freeze payments and donations to WikiLeaks. It's the same way a rogue nation's assets can be frozen by the banks holding them.

Hackers, angered at this affront to the supposed openness of the internet, then went on the attack. They used their own computers -- as well as servers they had been able to commandeer -- to wage "denial of service" attacks on the websites of the offending companies.

Most of those companies, already armed with defensive capabilities designed to fend off intrusions from the likes of the Russian mob or the Red Army, survived unscathed. Only MasterCard was noticeably, if only temporarily, disrupted. Meanwhile, Facebook and Twitter quickly disabled accounts traced to those using the services to organize their minions.

And all this tamping down occurred on today's purportedly "net neutral" internet, which offers no real advantage to one corporate-owned server over any other. [45cm]

We can only imagine the effect of these events on those who will decide on whether to maintain net neutrality or give in to the corporations that argue the internet's distributive capabilities should be reserved for those who can pay for such distribution, by the byte.

No, the real lesson of the WikiLeaks affair and subsequent cyberattacks is not how unwieldy the net has become, but rather how its current architecture renders it so susceptible to control from above.

It was in one of the leaked cables that China's State Council Information office delivered its confident assessment that thanks to "increased controls and surveillance, like real-name registration ... The Web is fundamentally controllable." [46wa]

The internet's failings as a truly decentralized network, however, merely point the way toward what a decentralized network might actually look like.

Instead of being administrated by central servers, it would operate through computers that pinged one another, instead of corporate-owned server farms, and deliver web pages from anywhere, even our own computers.

The FCC and other governing bodies may attempt to defang the threat of the original internet by ending net neutrality. But if they did, such a new network -- a second, "people's internet" -- would almost certainly rise in its place.

In the meantime, the internet we know, love and occasionally fear today is more of a beta version of modeling platform than a revolutionary force.

And like any new model, it changes the way we think of the way things work right now. What the internet lacks today indicates the possibilities for what can only be understood as a new operating system: a 21st century, decentralized way of conducting political, commercial and human affairs.

This new operating system, even in its current form, is slowly becoming incompatible with the great, highly centralized institutions of the 20th century, such as central banking and nation states, which still depend on top-down control and artificial monopolies on power to maintain their authority over business and governance.

The ease with which PayPal or Visa can cut off the intended recipient of our funds, for example, points the way to peer-to-peer transactions and even currencies that allow for the creation and transmission of value outside the traditional banking system.

The ease with which a senator's phone call can shut down a web site leads network architects to evaluate new methods of information distribution that don't depend on corporate or government domain management for their effectiveness.

Until then, at the very least, the institutions still wielding power over the way our networks work and don't work have to exercise their power under a new constraint: They must do so in the light of day.

The opinions expressed in this commentary are solely those of Douglas Rushkoff.

<http://edition.cnn.com/2010/OPINION/12/10/rushkoff.hacking.wikileaks/index.html?iref=allsearch>

11. December 9, 2010

Is WikiLeaks engaged in 'cyber war'?

(CNN) -- Media outlets and a Twitter feed this week lobbed a controversial term into the public debate about cyber attacks over WikiLeaks:

"CYBERWAR," the WikiLeaks' European Twitter feed declared, linking to a blog post of the same title.

"WikiLeaks Cyberwar!" read a CBS blog headline.

"Cyberwar erupts over WikiLeaks funding cut," wrote RFI, the international public radio network.

Despite these bold proclamations, internet security experts said the WikiLeaks-related attacks are anything but cyber war -- not that these same experts are exactly sure what a cyber war would look like, or if one has ever occurred.

The WikiLeaks saga reads like a high-tech spy novel -- one packed with government secrets, icy Cold War bunkers, shady networks of anonymous hackers and, most recently, the disruption of American financial institutions.

The battle over the site -- which has come under fire from the United States for publishing private diplomatic communications -- escalated this week as apparent WikiLeaks' supporters crashed the websites of PayPal, Visa and MasterCard, which had stopped processing donations to WikiLeaks. [47cm]

"There are some things WikiLeaks can't do. For everything else, there's Operation Payback," wrote a Twitter user claiming responsibility for the attacks -- and giving them a snappy name.

That scared plenty of people, even though the credit card companies continued to operate without their Web presence. To many, it also felt unprecedented, like these attacks were a new way to rattle core institutions of the American economy.

But is this kind of thing really new? And what does one call this type of digital battle, where attacks result in the unwanted movement of 1s and 0s online rather than bombed-out buildings and wounded soldiers?

Maybe anything but a cyber war.

Calling the WikiLeaks back-and-forth a cyber war is "completely idiotic," said **Bruce Schneier**, chief security technology officer of BT, a communications company.

"War. W-A-R. It's a big word," Schneier said. "How could this be a cyber war? It's certainly a cyber attack, right? It's certainly politically motivated. But this stuff has been going on for a couple of decades now. Do you mean there have been thousands of wars that haven't been noticed? It doesn't make any sense at all. If there was a war, you'd know it, and it would probably involve tanks and artillery -- as well as cyber weapons."

Only cyber attacks between two warring nation-states count as cyber war, he said.

WikiLeaks is, of course, a website -- not a sovereign nation.

"War isn't just nameless attacks between parties that are not nation-states to begin with," said **Mikko Hypponen**, chief research officer at F-Secure. "WikiLeaks is not a country. MasterCard is not a country."

But perhaps that definition still isn't quite good enough. In war, it's usually pretty easy to tell who's doing the shooting. In cyber attacks, it's almost always impossible to determine the origins of an attack unless it's "perpetuated by the slip of the tongue" on the part of the attacker, said Don DeBolt, director of threat research at CA Technologies, a computer security company.

In the WikiLeaks case, for example, no one knows -- or may ever know -- who is behind the attacks on financial websites. The same goes for hackers standing on the other side

of the digital battlefield, who have been trying to take WikiLeaks down so that it can't share any more state secrets.

The United States government has denied involvement, but the situation raises a question: If it's almost impossible to know who's behind a cyber attack, how can you say whether one has taken place between two nation-states or not?

Another issue with cyber war is the type of attack that's used.

Security researchers said the tactics of cyber warfare have been deployed in the WikiLeaks saga, but they're by far not the most drastic measures a hacker would take if he or she really wanted to cause real damage.

Schneier compared the pro-WikiLeaks attacks on MasterCard and Visa to a bunch of protesters standing in front of an office building, refusing to let workers in. It's annoying, but it didn't shut down the operation. And it didn't start a war. [48wb]

Cyber attacks start to become war-like when they purposefully attack real-world targets, causing actual damage to property or death, Hypponen said.

That had never been shown to be possible until this year, when the **Stuxnet worm** showed that it could attack factory systems and alter mechanical processes, he said. That kind of virus could, in theory, be used to shut down power grids, halt public transportation or blow up factories, he said. [49in]

The WikiLeaks attacks are more like political protests, he said.

There's an insider term for this: "hacktivist," or hacker plus activist. [50wb]

"I see it mostly as a demonstration of their dissatisfaction with the system and how things are going," he said of the hackers who are defending WikiLeaks by targeting big-name American sites. "There are other points you'd want to hit if you wanted to inflict monetary damage or retribution."

The type of attacks pro-WikiLeaks hackers have been carrying out are not at all sophisticated; they actually have been going on for at least 10 years, he said. Called "direct denial of service" attacks -- or DDoS in geek-speak -- these attacks essentially try to overload a website with so much internet traffic that they can't handle the load and temporarily are shut down.

DDoS attacks have been used as a **form of protest** before.

What's new with WikiLeaks, Hypponen said, is that DDoS attacks have gotten so easy to carry out that almost anyone can participate. There's evidence that "hundreds" of WikiLeaks supporters have volunteered their computers to be used as weapons in these online assaults, said **Jose Nazario**, senior manager of security research at Arbor Networks, another security firm.

To sign up, you just have to find the right people on Facebook or Twitter and download a simple program with another spy-novel name: a "low-orbit ion cannon."

"Ten years ago you had to be pretty skilled and know the right people to gain entry into this sort of event. Now it's easy," he said.

Still, that doesn't completely settle the "cyber war" issue either. In real-world war, you can fight with swords -- old tools -- or remotely operated drones -- new tools -- and still be engaging in battle. Perhaps part of the definition of cyber war lies in exactly how those tools are used to inflict damage, said **Herbert Lin**, a computer science and security expert at the National Research Council of the National Academy of Sciences.

"Soldiers use M16s. And they can use them in a prosecution of a war," Lin said. "But policemen also use M16s, and they're not prosecuting a war. So the question here is, does it count to say if you're using cyber warfare techniques against WikiLeaks in various forms, is that cyber warfare?"

Lin answered his own question: "I'd say no."

<http://edition.cnn.com/2010/TECH/innovation/12/09/wikileaks.cyber.attacks/index.html?iref=allsearch>

12. October 3, 2010

Iran arrests 'nuclear spies,' intelligence chief says

(CNN) -- Iran arrested a number of "nuclear spies," its intelligence minister said, in the wake of widespread reports of a sophisticated new computer virus that may have been aimed at Iran. [51cm]

Intelligence Minister Heydar Moslehi made the announcement Saturday, without giving any details, Iran's semiofficial Mehr news agency reported.

Iran is widely thought to have been the most likely target of the Stuxnet virus, which a top computer security expert told CNN was "the most complex piece of malware in the history of computing."

Tehran has insisted its controversial nuclear program had not been compromised by the virus.

Moslehi, the intelligence chief, did not mention Stuxnet in his statement, but said his ministry has "absolute control over the virtual networks and will foil all acts of sabotage."

Ralph Langner, who was among the first to identify and study Stuxnet, told CNN last week that it would have required insider information to deliver.

"In order to do the attack as Stuxnet did, you also need to have very detailed and specific knowledge about the targeted application and process," he said. "So you also need insider knowledge from a process control system person."

The virus, which he called "a cyberwar weapon," is designed to attack industrial control systems. [52cm]

It is so sophisticated, he said, that it is designed to attack a specific machine only when it fulfils specific conditions, such as reaching a particular temperature or pressure, he said. He said it had to be the work of a government, rather than a hacker group, because of the resources required to build and test it.

He did not speculate in an interview with CNN about who might be behind it, but asked mischievously last month on his website if there would be Israelis at the conference where he was presenting his Stuxnet findings.

Israel and the United States are both deeply concerned about Iran's nuclear program. They believe Iran aims to build a nuclear bomb. Iran denies it.

<http://edition.cnn.com/2010/WORLD/meast/10/03/iran.nuclear.arrests/index.html?iref=allsearch>

13. September 29, 2010

Iran denies cyberattack hurt nuclear program -- but expert isn't sure

(CNN) -- Iran denied Wednesday that its nuclear systems had been infected with a virus, after days of reports that a new kind of malware had struck the Bushehr nuclear plant. [53cm] But the head of its nuclear program admitted that a virus had been found on the personal laptops of some staff at the reactor, the Iranian Students News Agency reported.

"We succeeded in preventing the enemy from achieving its objectives," IRNA quoted Ali Akbar Salehi as saying on Wednesday.

But a top computer security expert who analyzed a new kind of virus called Stuxnet says Iran is the most probable target of the malware, which he says could only have been designed by "the best of the best."

"We have never seen anything like this before," said Ralph Langner. "It's the most complex piece of malware in the history of computing."

"What the thing does, is actually it's designed to blow something up, it's as simple as that," he said. "The virus is a cyberwar weapon." [54cm]

Langner, who was among the first to study the virus, presented his findings at a cyber security conference in Maryland last week.

The virus is designed to attack only a specific machine at a specific time, Langner told CNN Wednesday.

Langner has detected "the highest number of infections" in Iran, suggesting that Tehran's controversial nuclear program is the target.

"If you look at all the sophistication that went into Stuxnet, if you look at the fact that it's about sabotage, about destroying a specific piece of machinery, then the only target that makes sense given the target region... would be the Iranian nuclear power program," he said.

A government is almost certainly behind it, he said.

"You can take for granted that a hacker group is not able to create anything like Stuxnet, because the development requires much more resources than any such hacker group could afford," he said.

To use it as a weapon would require insider information, he said.

"You need to have very detailed and specific knowledge about the targeted application and process," he said.

"You will need to build up a lab model to test all that and if you take all that together into account, the only background that makes any sense is to assume that a nation-state is behind it."

It was probably delivered via infected USB sticks, he said, speculating that a Russian engineering firm that worked on the Iranian nuclear program had been infiltrated.

That would explain the pattern of infections around the world, he said -- anywhere the company worked would end up with the virus. [55cm]

But only one specific target would be affected by it.

It's as if a virus were designed not only to target a computer running Microsoft Word, he said, but to search for a specific document created with Word.

And it's designed to hit industrial control systems, he said, activating itself only once its target reaches a certain state, like a designated temperature or pressure.

"When it finds a specific match, let's say in specific temperatures or pressures to reach certain thresholds, then the attack routine is executed," he said.

Stuxnet itself is no longer a cause for concern, he said.

"Don't worry about Stuxnet any longer," he said. "Obviously it hit its target. It is so specific it won't attack anything else."

But now that it's out there, other people will try to replicate it, he warned.

"Everybody will be able to study exactly what Stuxnet does and how it is done," he said.

"So we must assume that Stuxnet will now act as a template for any kind of hackers, organized crime, terrorists in order to study how it can be done.

"Stuxnet is history," he said. "We need to work on what will come next."

<http://edition.cnn.com/2010/WORLD/meast/09/29/iran.cyberattack/index.html?iref=allsearch>

14. July 7, 2010

Threat of 'cyberwar' has been hugely hyped

Editor's note: Bruce Schneier is a security technologist and author of "Beyond Fear: Thinking Sensibly About Security in an Uncertain World." Read more of his writing at <http://www.schneier.com/>

(CNN) -- There's a power struggle going on in the U.S. government right now.

It's about who is in charge of cyber security, and how much control the government will exert over civilian networks. And by beating the drums of war, the military is coming out on top. [56wa]

"The United States is fighting a cyberwar today, and we are losing," **said** former NSA director -- and current cyberwar contractor -- Mike McConnell. "Cyber 9/11 has happened over the last ten years, but it happened slowly so we don't see it," said former National Cyber Security Division director Amit Yoran. Richard Clarke, whom Yoran replaced, wrote an entire **book** hyping the threat of cyberwar.

General Keith Alexander, the current commander of the U.S. Cyber Command, **hypes** it every chance he gets. This isn't just rhetoric of a few over-eager government officials and headline writers; the entire national debate on cyberwar is plagued with **exaggerations** and **hyperbole**.

Googling those **names** and **terms** -- as well as "cyber Pearl Harbor," "**cyber Katrina**," and even "cyber Armageddon" -- gives some idea how pervasive these memes are. Prefix "cyber" to something scary, and you end up with **something** really scary.

Cyberspace has all sorts of threats, day in and day out. Cybercrime is by far the largest: fraud, through identity theft and other means, extortion, and so on. Cyber-espionage is another, both government- and corporate-sponsored. [57cm] Traditional hacking, without a profit motive, is still a threat. So is cyber-activism: people, most often kids, playing politics by attacking government and corporate websites and networks. [58wb]

These threats cover a wide variety of perpetrators, motivations, tactics, and goals. You can see this variety in what the media has mislabeled as "cyberwar." The attacks against Estonian websites in 2007 were **simple hacking** attacks by ethnic Russians angry at anti-Russian policies; these were denial-of-service attacks, a normal risk in cyberspace and hardly unprecedented. [59in]

A real-world comparison might be if an army invaded a country, then all got in line in front of people at the DMV so they couldn't renew their licenses. If that's what war looks like in the 21st century, we have little to fear.

Similar **attacks** against Georgia, which accompanied an actual Russian invasion, were also probably the responsibility of citizen activists or **organized crime**. [60in] A series of power blackouts in Brazil was caused by criminal extortionists [61in] -- or was it **sooty insulators**? China is **engaging** in espionage, not war, in cyberspace [62cm]. And so on.

One problem is that there's no clear **definition** of "cyberwar." What does it look like? How does it start? When is it over? Even cybersecurity experts don't know the answers to these questions, and it's dangerous to broadly apply the term "war" unless we know a war is going on.

Yet recent news articles have claimed that **China declared cyberwar on Google** [63wa], that Germany attacked China, and that a group of young hackers declared cyberwar on Australia. (Yes, cyberwar is so easy that even kids can do it.) Clearly we're not talking about real war here, but a rhetorical war: like the war on terror.

We have a variety of institutions that can defend us when attacked: the police, the military, the Department of Homeland Security, various commercial products and services, and our own personal or corporate lawyers. The legal framework for any particular attack depends on two things: the attacker and the motive. Those are precisely the two things you don't know when you're being attacked on the Internet. We saw this on July 4 last year, when U.S. and South Korean websites were **attacked** by unknown perpetrators from North Korea -- or perhaps England. Or was it Florida?

We surely need to improve our cybersecurity. But words have meaning, and metaphors matter. There's a power struggle going on for control of our nation's cybersecurity strategy, and the NSA and DoD **are** winning. If we frame the debate in terms of war, if we accept the military's expansive cyberspace definition of "war," we feed our fears.

We reinforce the notion that we're helpless -- what person or organization can defend itself in a war? -- and others need to protect us. We invite the military to take over security, and to ignore the limits on power that often get jettisoned during wartime.

If, on the other hand, we use the more measured language of cybercrime, we change the debate. Crime fighting requires both resolve and resources, but it's done within the context of normal life. We willingly give our police extraordinary powers of investigation and arrest, but we temper these powers with a judicial system and legal protections for citizens.

We need to be prepared for war, and a Cyber Command is just as vital as an Army or a Strategic Air Command. And because kid hackers and cyber-warriors use the same

tactics, the defenses we build against crime and espionage will also protect us from more concerted attacks. But we're not fighting a cyberwar now, and the risks of a cyberwar are no greater than the risks of a ground invasion. We need peacetime cyber-security, administered within the myriad structure of public and private security institutions we already have.

The opinions expressed in this commentary are solely those of Bruce Schneier.

<http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html?iref=allsearch>

15. March 19th, 2010

POLITICAL HOT TOPICS...

The CNN Washington Bureau's morning speed read of the top stories making news from around the country and the world.

Washington Post: Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies

The use of computers to gather intelligence or to disrupt the enemy [64cm] presents complex questions: When is a cyberattack outside the theater of war allowed? Is taking out an extremist Web site a covert operation or a traditional military activity? Should Congress be informed?

<http://politicalticker.blogs.cnn.com/2010/03/19/political-hot-topics-march-19-2010/?iref=allsearch>

16. September 28, 2009

CNN Student News Transcript

THIS IS A RUSH TRANSCRIPT. THIS COPY MAY NOT BE IN ITS FINAL FORM AND MAY BE UPDATED.

CARL AZUZ, CNN STUDENT NEWS ANCHOR: How did Facebook become part of a geographic controversy? We're to map out the answer to that in today's edition of CNN Student News! Hello, everyone. I'm Carl Azuz.

First Up: Iranian Nuclear Fears

AZUZ: Missile tests. Nuclear plants. Accusations and denials. All part of the rising tension between several western nations and Iran. Yesterday, the Middle Eastern country fired two types of missiles - part of a series of exercises that it says are designed to promote the country's military defense capabilities. Those tests are expected to go on for the next 10 to 11 days. The missiles fired yesterday are short-range. Iran is scheduled to test a long-range missile today.

All of this comes after Friday's announcement that Iran is building a uranium enrichment plant. That would be the country's second one. Here's why that's controversial. Enriching uranium is part of the process to create nuclear power, and that's what Iran says the facility will do. Okay, fine. But enriching

uranium is also part of the process for creating nuclear weapons. The U.S. and Israel believe that is the ultimate goal of Iran's nuclear plants. Iran says it will allow the International Atomic Energy Agency to inspect the new facility. But as Elaine Quijano tells us, the country's nuclear program is the focus of international concern.

(BEGIN VIDEO CLIP)

ELAINE QUIJANO, CNN CORRESPONDENT, WASHINGTON, D.C.: One day after the U.S., Britain and France called out Iran for building a secret nuclear site, Iranian officials insisted they have nothing to hide and will comply with demands to let international inspectors into the facility.

ALI ASGHAR SOLTANIEH, IRAN'S AMBASSADOR TO THE IAEA: And there is no nuclear material in this new site. And we are arranging, and inspectors will confirm my assertion.

QUIJANO: Secretary of State Hillary Clinton welcomed the Iranians' pledge to allow inspectors in, but made clear the U.S. expects concrete action at key nuclear talks on Thursday.

HILLARY CLINTON, U.S. SECRETARY OF STATE: We are hopeful that in preparing for the meeting on October 1st, Iran comes and shares with all of us what they're willing to do, and gives us a timetable on which they're willing to proceed.

QUIJANO: The United States has long suspected Tehran of trying to develop nuclear weapons, and in his weekly address, President Obama warned Iran's leaders the U.S. is not alone in its suspicions.

U.S. PRESIDENT BARACK OBAMA: Yesterday, I stood shoulder-to-shoulder with our European allies in condemning Iran's program. In our meetings and public statements, President Medvedev of Russia and I agreed that Iran must pursue a new course or face consequences.

QUIJANO: That means possibly tougher sanctions, and President Obama says the U.S. is keeping all options on the table, including a military one. But in an interview for CNN's "State Of The Union" with John King, Defense Secretary Robert Gates said even that has its limits.

ROBERT GATES, U.S. DEFENSE SECRETARY: The reality is there is no military option that does anything more than buy time.

QUIJANO: Next up is that crucial meeting Thursday in Geneva. That is when Iranian diplomats will sit down with officials from the U.S. and the other permanent members of the U.N. Security Council, as well as Germany, to discuss Iran's nuclear program. Elaine Quijano, CNN, The White House.

(END VIDEO CLIP)

Downloadable Maps: Iran - Germany - Golan Heights

I.D. Me

BRENDAN GAGE, CNN STUDENT NEWS: See if you can I.D. Me! I'm a European nation that was split into two countries from 1949 to 1990. I'm Europe's second-most populated nation, but I have the continent's largest economy. My capital city is Berlin. I'm Germany, and the head of my government is Angela Merkel.

Germany Elections

AZUZ: And Chancellor Merkel will be keeping that title based on the results of yesterday's election. According to exit polls taken after the voting, Merkel's political party defeated the one led by Frank-Walter Steinmeier, who currently serves as the country's foreign minister. That means a second, four-year term for German Chancellor Merkel, who was first elected in 2005.

When voters headed to the polls yesterday, they actually cast their ballots not for chancellor, but for members of Germany's lower house of Parliament, which is called the Bundestag. It's those members who then pick the head of government. Most observers had predicted a win for Chancellor Merkel. But there was some suspense leading up to the election. Al Qaeda and the Taliban had released videos warning Germans not to vote for leaders who want to keep the country's troops in Afghanistan.

Philippines Flooding

AZUZ: Meanwhile, rescue workers in the Philippines are struggling to reach victims of deadly flooding. This was caused by the heaviest rainfall in the Asian country in more than 40 years. The severe weather claimed at least 75 lives, although some officials have said it's hard to determine the exact impact because so many roads were left impossible to pass. You can get an idea of that by these pictures. The heavy rains left more than 80 percent of the capital city of Manila under water. Not entirely surprising because it was a month's worth of rain that fell on the city in just six hours Saturday.

Fast Facts

MARY ELLEN HOPKINS, CNN STUDENT NEWS: Time for some Fast Facts! The Golan Heights is a Middle Eastern region that's located between Israel and Syria. It's about 444 square miles in size. Syria controlled the area at first, but Israel occupied the heights in the 1967 Arab-Israeli War, and Israel controls it today. Currently, the region is home to about 20,000 Arabs and 20,000 Israelis.

Golan Heights

AZUZ: So, let's say you're one of those 40,000 people, and you're setting up your profile on Facebook. When you get to that section about what country you live in, what do you put? That question sparked a controversy. And as Paula Hancocks explains, it's put Facebook and residents of the Golan Heights in the middle.

(BEGIN VIDEO CLIP)

PAULA HANCOCKS, CNN CORRESPONDENT, JERUSALEM: This is the Shouting Hill. Before mobile phones and the Internet, this is how Druze families split between Syria and the Golan Heights communicated. But times have changed. Behind this fence is Syria. Where I'm standing right now is Israeli-occupied Golan Heights. Now, this border has been disputed for more than 40 years, and now Facebook has found itself caught in the middle. The social networking site, up until recently, followed international consensus, designating the Golan Heights as Syria. The Golan was captured by Israel in 1967 and has been considered occupied territory ever since. But pro-Israel Web site HonestReporting started a campaign to add an Israeli option, a campaign it says that's non-political.

ALEX MARGOLIN, HONESTREPORTING.COM: You know, it's totally possible that at some day in the future the Golan will change hands, go to Syria. It's not really what this campaign was about.

HANCOCKS: Ofri Baza lives in Odem in the Golan Heights, and always kept her country of origin blank. Thanks to Facebook, she now has the choice of Israel or Syria.

OFRI BAZA, ISRAELI GOLAN RESIDENT: Odem, Israel, woo!

HANCOCKS: Ofri's happy, but her neighbors in this Druze town of Magdil Schams are not. They consider themselves Syrian under Israeli occupation. Shopkeeper Sakur abu Sabit thinks Syria should be the only Facebook option.

SAKUR ABU SABIT, SYRIAN GOLAN RESIDENT [TRANSLATED]: We fought against all the occupiers. We fought against the French for our freedom as well as against the Turks. Here we will never give up our Syrian citizenship.

HANCOCKS: Across the border in Syria, the backlash is likely to be muted because Facebook has already been banned there for a couple of years.

AMMAR ABDULHAMID, SYRIAN SCHOLAR: The real reason for that, however, has nothing to do with the Arab-Israeli conflict. It has nothing to do with interaction between Syrians and Israelis. It's because these sites are really very popular with Syrian activists

HANCOCKS: The Israeli-Syrian fight for the Golan Heights is 42 years old; the cyber-war has only just begun. Paula Hancocks, CNN, in the occupied Golan Heights.

(END VIDEO CLIP)

AZUZ: A spokeswoman from Facebook tells CNN, "We deal with the listings for disputed territories on a case-by-case basis, and with Golan Heights, we decided a dual listing made sense in this instance." The company also notes that it has the same dual-listing policy with respect to the West Bank, which is listed in both Palestine and Israel.

Promo

AZUZ: No matter where you live, you can always check us out on Facebook. Watch our videos and find out what's going on behind the scenes. Just head to Facebook.com/cnnstudentnews. Or if you're logged on to the site, search for "CNN Student News official." Remember, if it's not official, it's not us.

Before We Go

AZUZ: Before we go, you've heard of speed reading, speed dating, speed skating? Check out speed mapping! Ok, we sped this up a little bit, but Terry Downing can actually draw all 50 states in just 90 seconds! He says he starts with his home state of Kansas, and then the rest just falls into place. But his map mastery isn't the end of terry's geographic genius. State nicknames, capitals, largest cities: all stored in his head.

Goodbye

AZUZ: Where he can draw on the information at a moment's notice. I kinda like that one. Log onto Facebook and tell us what you think of today's pun. CNN Student News returns tomorrow. You guys have a great day. Hope everything goes well for you and hope to see you then. **[65wb]**

<http://edition.cnn.com/2009/LIVING/studentnews/09/27/transcript.mon/index.html?iref=allsearch>

17. September 21, 2009

Facebook gets caught in Golan Heights dispute

By Paula Hancocks

JERUSALEM (CNN) -- Logging onto Facebook as a resident in the Golan Heights, should you enter Syria or Israel as your home country?

Decades of war and occupation have not provided an answer to that question -- but the social networking Web site now permits both options, sparking fears about an anti-Facebook cyber-war [66wa].

The Golan Heights is Syrian territory that was captured by Israel during the Six-Day War in 1967. Since then it has been internationally classified as Israeli-occupied territory.

Up until recently, Facebook fans in the **Golan Heights** could only choose Syria as their country of origin or else leave it blank. Pro-Israel Web site honestreporting.com sought to change that, starting a group called "Facebook, Golan residents live in Israel, not Syria. [67wb]"

Alex Margolin says the campaign was never political. "It was never a question of the future of Golan... it's totally possible that at some time in the future the Golan will change hands and go to Syria."

The group welcomed 2,500 members in the first week. Shortly afterwards **Facebook** policy changed. **Do you think Facebook was right to change policy?**

"We have enabled users in Golan Heights to choose either Syria or Israel in the listings," a Facebook spokesperson told CNN. "We currently have the same dual-listing options for the West Bank settlement, which is listed in both Palestine and **Israel**."

"We deal with the listings for disputed territories on a case-by-case basis, and with Golan Heights we decided a dual listing made sense in this instance."

Eighteen-year old Ofri Bazaz is delighted she can finally change her profile to Israel, squealing with delight as she tries it for the first time. She said: "It's very important on the Internet when somebody comes to my profile on Facebook they will see Israel and not Syria. I'm not Syrian."

But a 20-minute drive away in the Druze town of Majdal Shams, the reaction is very different. Facebook users here consider themselves **Syrian** and refuse to accept the change, as they fear it undermines their peaceful resistance to the Israeli occupation.

Shopkeeper Sakar abu Sabit said: "Even if it's just on the computer, I want people to always recognize me in the Golan Heights as a Syrian citizen."

Reaction from Syria is likely to be muted according to Syrian scholar, Ammar Abdulhamid. He told CNN that Facebook and other social networking sites have already been banned in Syria. **"The Syrian**

government has really taken a strong stance on Internet activism and social networking sites." [68wa] he said.

"The real reason is nothing to do with the Arab-Israeli conflict, it's because these sites are very popular with Syrian activists."

But with 300 million users worldwide and an estimated 120 million logging in every single day according to Facebook, there will inevitably be fears about a backlash against the site that now finds itself at the center of a 40-year-old conflict

<http://edition.cnn.com/2009/TECH/09/21/israel.syria.facebook/index.html?iref=allsearch>

18. August 7, 2009

Russia-Georgia tensions still high one year on from conflict

(CNN) -- One year after Russian tanks rolled into the former Soviet republic of Georgia, the conflict that erupted over a breakaway territory continues to stoke tensions in the region, with repercussions around the world.

Earlier this month, Georgia and the Russian-backed enclave of South Ossetia accuse each other of violating a cease-fire that ended the brief conflict.

In another development with global consequences, an attempt to silence a pro-Georgia blogger with a cyber attack resulted in severe disruptions to social networking sites Twitter and Facebook. [69wa]

Though confined to a relatively small area, last year's conflict also threatened to spill beyond the region, as frictions elevated between **Russia** and Ukraine, and Georgia tried to drag in NATO, the European Union and the United States.

The conflict erupted after days of sporadic clashes between both sides led to a Georgian assault on South Ossetia's capital Tskhinvali on August 7, 2008.

A day later Russian troops poured into South Ossetia -- a region which declared its independence from **Georgia** in the early 1990s after a bloody ethnic war.

During the days of fighting that followed, the Georgian city of Gori came under heavy fire, with reports of Russian jets shelling parts of the city, buildings on fire and numerous casualties.

About 192,000 people were displaced by the violence. Some 38,500 people were reported to have left South Ossetia for Russian territory, of whom all but an estimated 4,000 are now said to have returned.

An EU-brokered cease-fire was struck on August 12 after Russian troops had driven Georgian forces out of South Ossetia and Abkhazia, another Russian-backed breakaway -- and pushed into Georgian government-controlled territory.

Russia claimed it had pulled out its troops by August 22, but left in place "peacekeeping" forces in "buffer zones" to prevent further violence.

Despite the cease-fire, Russia has yet to withdraw its troops to pre-conflict positions and allow unhindered humanitarian access to Abkhazia and South Ossetia, according to the U.S. State Department.

Last year's conflict came as Georgia had been cultivating closer ties with the United States and western Europe and was seeking admission to NATO despite fierce Russian opposition.

<http://edition.cnn.com/2009/WORLD/europe/08/07/goergia.background/index.html?iref=allsearch>

19. July 8, 2009

U.S. government sites among those hit by cyberattack

WASHINGTON (CNN) -- U.S. government Web sites -- including those of the White House and the State Department -- have been under attack since the Fourth of July, along with financial and commercial sites like Yahoo Finance and the New York Stock Exchange, cybersecurity experts said Wednesday.

The Department of Homeland Security, which is one of the targets, according to a security expert, confirmed that the attacks were taking place.

Web sites in South Korea, including the president's, were targets of the same attack [70in], said Jose Nazario, manager of security research at Arbor Networks in Ann Arbor, Michigan.

The Washington Post said it, too, had been attacked.

There is some indication that the attack comes from China, Nazario said, but he added that he could not be certain of the origin. Even if it is coming from China, it would be difficult to determine whether officials or individual hackers were responsible.

He said the attack was of moderate size, involving "a few tens of thousands" of infected computers "around the world."

"We measured a peak of 25 megabits/second" in data transmission, he said, calling it "about the size of a big PowerPoint presentation, well in the garden variety of what we see."

But other cybersecurity experts said that even if the current attack was not particularly worrisome, it was a window into potentially more serious problems.

Jim Lewis of the Center for Strategic and International Studies in Washington said that the attack was simple and primitive but that the fact that it worked on some agencies shows the government is still "disorganized."

Some parts of the government were able to "beat this off," while others haven't, he said.

"That's a problem. Everyone is marching to a different drummer," he said. "We should have been able to beat this back. Someone needs to step back and say why not."

Alan Paller of the Sans Institute said the attack "is not a small thing."

"This is a harbinger of how people who are angry or at war with us can affect government Web sites," he said, adding that he did not have direct knowledge of the current attacks.

Disabling a Web site matters, he said. "If people rely on that Web site for information, it's important. If it stops government from functioning, it matters."

The top U.S. military officer said Wednesday that cybersecurity is "a growing concern."

"I grow increasingly concerned about the cyber world and the attacks, whether they're from individual hackers or state entities, and that's something we all need to be concerned about," said Adm. Mike Mullen, chairman of the Joint Chiefs of Staff.

The Web sites are facing a "distributed denial of service" attack or, more specifically, an "http flood attack," in which computers are infected with a virus that makes them repeatedly try to access a Web page. The increased demand can overload the page's servers, cutting off access.

The malware, or the program that is running the attack, does not seem to be stealing information from the computers it infects or the ones it attacks, Nazario said.

Amy Kudwa, a **Department of Homeland Security** spokeswoman, said no data has been stolen from any of the government Web sites. She stressed that the attacks were against some of the government's public Web sites, not internal ones.

People trying to access the affected sites might have had difficulty getting into them or may have found the sites sluggish, she said.

Kudwa would not say which government agency sites were affected.

The department warned other federal departments and agencies, as well as partner organizations, about the activity and advised them of steps to take to help mitigate such attacks, she said.

"We see attacks on federal networks every day, and measures in place have minimized the impact to federal Web sites," she said.

White House spokesman Nick Shapiro said the "attacks had absolutely no affect on the White House's day-to-day operations" but added that some "visitors from regions in Asia may have been affected."

A South Korean presidential office spokesman said the attack on their computers only slowed down the system and caused no damage.

Workers are in the process of figuring out where the attack came from, the spokesman said.

Unnamed South Korean parliamentary sources said Wednesday that North Korea appeared to have orchestrated the attack, the official South Korean news agency reported. The sources cited informal reports by the country's top spy agency.

But Nazario said he had seen "nothing that would suggest that North Korea is an accurate claim."

He said his company was one of many working with "appropriate authorities around the world" to stop the attack.

He said that progress was being made but that the attack was not over.

"This is being beaten back, but I see an indication that it might still be going on," he said. "It appears to be ongoing."

<http://edition.cnn.com/2009/TECH/07/08/government.hacking/index.html?iref=allsearch>

20. June 17, 2009

Briton's software a surprise weapon in Iran cyberwar

LONDON, England (CNN) -- A Web designer in London was amazed to discover that Iranian election protesters are attacking the Iranian president's Web site using software he developed in his spare time, he told CNN Wednesday.

With anti-government activists in Iran sidestepping official attempts to silence them on the Internet by posting photos, videos and blogs on sites like Facebook and Twitter, others are using a site that automatically refreshes a Web page every few seconds, potentially overloading the host server.

[71wb]

The page reboot software means that dissidents can "attack" sites with a barrage of hits -- known as a denial of service attack -- causing them to appear to users as "unobtainable."

Iranian President Mahmoud Ahmadinejad's Web sites was one of those displaying this message on Monday, according to Britain's Channel 4 News, although on Tuesday it was loading correctly.

The freely available page refresh site was partly developed by Ryan Kelly for use with sports results sites and eBay. He said he was unaware it was being used by Iranian protesters to stop the government from getting out its message until Tuesday when he received an email from an unknown source asking him to take the site down.

"Can you please shout (sic) down the website for few weeks. Currently they are using that website to attack other websites," stated the anonymous e-mail seen by CNN.

Kelly, who works for contract publisher Wardour, then discovered that hits on his own site had risen from 700 on a normal day to 41,000 on Monday.

"I was shocked when I heard my site was being used in this way," the 25-year-old told CNN.

"This exemplifies the power of the Internet that something happening in London can affect events thousands of miles away in Tehran. It's great it's being used in this way."

The heavy traffic forced Kelly to temporarily suspend his site, but only because it was exceeding the volume of traffic on his server. He said he later received dozens of e-mails requesting him to restore the site, and he did so.

One message seen by CNN said: "Please bring your site back up as fast as you can. We need your help in Iran against Ahmadinejad."

Kelly said he supported the protesters in their battle to have the results of the disputed presidential election overturned. "I suppose I am taking sides because I've put the site back up, but I have no problems with it being used in this way."

<http://edition.cnn.com/2009/WORLD/meast/06/17/iran.elections.hackers/index.html?iref=allsearch>

21. August 21, 2008

Experts: Internet filtering and censorship rife

LONDON, England (CNN) -- Believe the conspiracy theories: Out of sight and without your knowledge, governments truly are filtering what you see on the Internet.

The recent conflict between Georgia and Russia has highlighted many of the issues at play with Internet filtering, as its increasing use by governments raises serious doubts about the freedom of the Web.

[72wa]

Georgian authorities blocked most access to Russian news broadcasters and Web sites after the outbreak of the conflict, and both sides reported Web sites being blocked, removed or attacked as the situation unfolded.

According to one of CNN's iReporters in Georgia, the situation has been very frightening for citizens.

Andro Kiknadze said an online forum he used to organize supporters appeared to have been taken down, and he described a "cyberwar" in which some Web sites appear to be blocked.

"Please, please help us. We are losing our treasure, our freedom. I am almost crying because I'm seeing my country is falling," Kiknadze said.

So, what is Internet filtering, and why all the fuss?

Filtering simply means restricting access, blocking or taking down Web sites.

Karin Karlekar, senior researcher at freedom promoter Freedom House, said there were several ways in which content could be "filtered."

She said governments could use purpose-built filtering technology, censor Web sites, filter search results -- with the assistance of multinational corporations, and block applications and circumvention tools -- to stop online applications like Facebook, YouTube or Voice Over IPs that enable social networking. [73wa]

And the use of these tactics appears to be quite widespread.

According to a 2007 report by the OpenNet Initiative, which surveyed more than 40 countries, almost two-thirds of the states involved were filtering content to some degree.

Ron Deibert, director of the Citizen Lab at the Munk Centre for Internet Studies at the University of Toronto, said in the research, "states are applying ever more fine grained methods to limit and shape the information environment to which their citizens have access."

"Some states block access to a wide swathe of content, while others tend to concentrate on one or two narrow baskets. South Korea, for example, tends to block access only to sites related to North Korea, [74wa]" Deibert said.

Although countries such as Iran and China -- home to the "Great Firewall of China" -- are obvious examples of where filtering is prevalent, other countries are also restricting content for varying reasons. [75wa]

Ian Brown, research fellow at the Oxford Internet Institute, said the Internet in some European countries, including the United Kingdom, was also filtered. However, this was mostly to block child pornography and content that incited or glorified terrorism, he said.

Most democracies, and particularly those of the U.S. and India, had unrestricted Internet, though more than 40 countries were known to filter content, he said.

And it's not just governments involved in filtering. Search engine Google has been heavily criticized for working with the Chinese government to block searches for material about Taiwan, Tibet, democracy and other sensitive issues on its Chinese portal. **Share your views on filtering and censorship of Web sites.**

Don't Miss: Just Imagine: 2020 - Cyber-spies tracking terror on Web - U.S. at risk of cyberattacks,

With recent developments in Georgia and Internet restrictions during conflict in Estonia [76in] last year, there are concerns that filtering could be further utilized in future "cyberwarfare."

Brown believed that filtering would be used more commonly in repressive states in the future. Although he didn't have exact figures, Brown understood the Chinese military had more than 100,000 people employed to look at cyber warfare.

Jonathan Zittrain, co-founder of Harvard Law School's Berkman Center for Internet and Society, said the tactic was very powerful.

"Filtering can help shape the message a country's citizens see, including, as may have happened recently when Georgia filtered some Russian Web sites, for the purpose of preventing enemy propaganda from reaching one's citizens. [77wa]"

Although Karlekar agreed that filtering was a strong aspect to cyber warfare, she said other trends were more concerning.

"Filtering isn't the primary technological way that Internet freedom can be compromised. The kind of 'cyberwarfare' that we hear about usually isn't filtering as much as 'denial of service' attacks that disable servers hosting particular Web sites, either of opposition media outlets or of foreign governments.

"Another type of 'cyberwarfare' that occurs more regularly is hacking into computers and stealing information, [78cm] as well as planting Trojans or viruses," Karlekar said.

So, if governments are stepping up their Internet filtering and the threat of cyberwarfare is increasing, how can citizens sidestep the restrictions?

Zittrain said tech-savvy citizens are using a variety of tools to circumvent filtering.

"They range from the Electronic Frontier Foundation's Tor software to commercial anonymizers and virtual private networks and 'buddy system' software like Psiphon, which allows a person in one place to handle requests for Web sites from someone in a place that filters."

In Iran, some citizens were overcoming Internet restrictions by using Freedom House's Gozaar Web site.

Karlekar said the site offered news and debates with a plurality of voices and gave Iranians an opportunity to participate. [79wb] The domain name was changed weekly to keep ahead of Iranian authorities, she said.

Zittrain, a founder of the OpenNet Initiative, which tracks Internet filtering around the world, said the organization is working on a free tool that will let people easily report blockages as they find them.

<http://edition.cnn.com/2008/TECH/08/21/internet.filtering/index.html?iref=allsearch>

22. August 18, 2008

U.S. at risk of cyberattacks, experts say

CNN -- The next large-scale military or terrorist attack on the United States, if and when it happens, may not involve airplanes or bombs or even intruders breaching American borders.

Cyberattackers shut down one Georgian government site and defaced another with images of Adolf Hitler. [80wa]

Instead, such an assault may be carried out in cyberspace by shadowy hackers half a world away. And Internet security experts believe that it could be just as devastating to the U.S.'s economy and infrastructure as a deadly bombing. [81in]

Experts say last week's attack on the former Soviet republic of Georgia, in which a Russian military offensive was preceded by an Internet assault that overwhelmed Georgian government Web sites, [82in] signals a new kind of cyberwar, one for which the United States is not fully prepared.

"Nobody's come up with a way to prevent this from happening, even here in the U.S.," said Tom Burling, acting chief executive of Tulip Systems, an Atlanta, Georgia, Web-hosting firm that volunteered its Internet servers to protect the nation of Georgia's Web sites from malicious traffic.

"The U.S. is probably more Internet-dependent than any place in the world. So to that extent, we're more vulnerable than any place in the world to this kind of attack," Burling added. "So much of what we're doing [in the United States] is out there on the Internet, and all of that can be taken down at once."

"This is such a crucial issue. At every level, our security now is dependent on computers," said Scott Borg, director of the United States Cyber Consequences Unit, a nonprofit research institute. "It's a whole new era. Political and military conflicts now will almost always have a cyber component. The chief targets will be critical infrastructure, and the attacks will emerge from within our own computer systems. [83in]"

Don't Miss

'Pentagon hacker' loses extradition appeal

Hackers mounted coordinated assaults on **Georgian** government, media, banking and transportation sites in the weeks before Russian troops invaded. Known as distributed denial of service, the attacks employ multiple computers to flood networks with millions of simultaneous requests, overwhelming servers and crippling Web sites. **[84in]**

Hackers shut down the Web site of the Georgian president, Mikheil Saakashvili, for 24 hours and defaced the Georgian parliament site with images of Adolf Hitler. Saakashvili blamed Russia for the attacks. **[85wb]** although the Russian government said it was not involved.

Web sites and computer networks have been targeted by hackers for decades, although large-scale, coordinated cyberattacks are still a relatively new phenomenon. Some **Internet-security** experts believe that the Georgia conflict marks the first time a known cyberattack has coincided with a ground war, but others said that similar computer attacks have accompanied military operations in the Middle East and elsewhere.

The challenge to U.S. security experts is that such attacks can be mounted anonymously, and relatively cheaply, from anywhere in the world. Georgia's attackers employed "botnets," or malicious automated programs that take root undetected in far-flung computers and barrage their targets with useless data. By last Friday, some of those botnets were originating from Comcast Internet addresses in the United States, Burling said.

"It only takes a couple of experts; it doesn't take a whole cyber infantry division to pull something like this off," said Don Jackson, director of threat intelligence for SecureWorks, an Atlanta-based computer security firm. "For a very small investment in resources, you can have a huge impact."

In the United States, government computer networks parry millions of attempted intrusions every day, Internet-security experts say. The **U.S. Department of Homeland Security** created a National Cybersecurity Center this year to coordinate federal cyberdefense efforts and quicken responsiveness. However, a recent Homeland Security Department intelligence report, obtained by The Associated Press, concluded that there are no effective means to prevent a coordinated attack on U.S. Web sites.

"When it comes to our government IT security, we're pretty strong in protecting against [attacks]," Homeland Security spokesman William R. Knocke told CNN. "But I wouldn't say ... we're 100 percent impenetrable."

So what would a cyberattack on the United States look like? And where is the U.S. most vulnerable? It depends on who you talk to.

Borg does not believe that the U.S. is susceptible to the kind of attacks launched at Georgia.

"We can command so much bandwidth that it's hard to overwhelm our servers," he said. "We are vulnerable to more sophisticated attacks, but right now most of the people who want to do us harm don't have those capabilities."

The Web sites of key government security agencies, such as the Pentagon and the Central Intelligence Agency, are difficult to bring down, experts said. So are the computer networks of large American

banks. But experts say a successful, large-scale attack on U.S. computer systems could hobble electric-power grids, transportation networks and industrial-supply chains.

"You'd see some disruption of essential services, like electricity. [86in] You'd definitely see espionage," said James A. Lewis, a senior fellow at the Center for Strategic and International Studies in Washington. "Would it be decisive? No. Nobody's going to win a conflict with the United States in cyberspace. But would it be disruptive and irritating? Yes."

Federal researchers who launched an experimental cyberattack last year in Idaho caused a generator to self-destruct, prompting fears about the effect of a real attack on the nation's electrical supply.

And a May report by the Government Accountability Office found that the Tennessee Valley Authority, which supplies power to almost 9 million people in the southeastern U.S., had not installed sufficient cybersecurity measures. Spokesman Jim Allen said the TVA, the nation's largest publicly owned utility company, is "on track" to correct the problems.

What frustrates computer-security experts is that the features that make the Internet such an invaluable resource -- its openness and interconnectedness -- also make it easier for hackers to do harm. As a staple of 21st-century warfare, cyberattacks will become increasingly sophisticated, forcing governments and private industry to build ever-stronger firewalls and other defenses, experts said.

Also, vague international laws and a lack of accountability will continue to make tracking down and prosecuting cyberattackers difficult.

"We don't know quite what the rules are for this kind of conflict. If it's spying, it's illegal. But is it an act of war? And who do you arrest?" Lewis asked. "We're much safer [in the U.S.] than we were a year ago. But we still have a long way to go."

<http://edition.cnn.com/2008/TECH/08/18/cyber.warfare/index.html?iref=allsearch>

23. March 4, 2008

China denies U.S. computer hacking agenda

BEIJING, China (CNN) -- China rejected a U.S. report concluding that the Chinese military is secretly increasing spending to break into U.S. military computer systems [87cm], expand its Navy, and invest in intercontinental nuclear missiles and weapons to destroy satellites.

The United States must "abandon Cold War thinking" and adopt a better understanding of China to "promote a constructive Sino-U.S relationship," Chinese Foreign Ministry spokesman Qin Gang said Tuesday.

An annual Pentagon report to Congress said Monday that China's total military spending in 2007 was between \$97 billion and \$139 billion, but because of a lack of transparency, it's hard to tell exactly how much was spent and on what.

Xinhua -- China's official news agency -- said Tuesday that the country's 2008 military budget would rise by nearly 18 percent to \$57 billion.

In comparison, the U.S. military budget request for 2008 is \$481.4 billion, not including war requests.

Pentagon officials said a chunk of China's spending went to cyber warfare, as 2007 saw continued several "intrusions" believed to be from the Peoples Liberation Army (PLA). In the incidents, U.S. military unclassified computer systems were broken into and information was taken, according to Pentagon officials.

The Chinese spokesman said the Pentagon report was "interfering with China's internal issue and violating the standard of international relationship.

" He said China's policies are peaceful and defensive.

"We are playing the crucial role to maintain peace in the Asia Pacific region and the world, and we are not a threat to any countries," Qin Gang said. "We require the United States to abandon the Cold War thinking, understand China and its development in the right way, redress the misunderstanding on China's military report, and conduct action to promote constructive Sino-U.S relationship," he said.

He said the United States should "stick to the promise on opposing Taiwan independence, stop selling weapons to Taiwan and any kind of contact between the two militaries.

"Stop giving any wrong signals to Taiwan independence force, stay with China to maintain stability in Taiwan sea and Sino-U.S relationship," he said.

The **Pentagon** report said China was investing heavily in and fielding improved nuclear intercontinental ballistic missiles and anti-satellite missiles.

The United States expressed its concern last year after **China** fired a missile at one of its old satellites and destroyed it, sending thousands of dangerous pieces of space debris around orbit.

The United States conducted a similar strike last month on a broken U.S. spy satellite before it re-entered the Earth's atmosphere. U.S. officials said the satellite was hit and broke into thousands of small pieces that burned up as they re-entered the Earth's atmosphere.

The United States is also concerned about the purchase of more submarines by the Chinese navy as well as plans for more aircraft carriers. The Chinese once had a small Navy. Now the United States is keeping an eye on the growing service amid concerns over Taiwan.

The concerns include "China's near-term focus on preparing for contingencies in the Taiwan Strait, including the possibility of U.S. intervention, which is an important driver of its modernization," the report says.

Additionally, the Chinese have placed about 100 more short-range missiles on the shore opposite Taiwan in the past year, it says.

Pentagon officials worry that the continued increase in Chinese military spending is slowly tipping the balance of power between China and Taiwan in China's favor. The United States has said it would help defend Taiwan if China invaded.

The report also says the PLA is "pursuing comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short-duration, high-intensity conflicts along its periphery against high-tech adversaries."

Such an army, the report says, would have "the greatest potential to compete militarily with the United States and field disruptive military technologies that could, over time, offset traditional U.S. military advantages."

The United States says that the lack of transparency by the Chinese on its spending poses "risks to stability by increasing the potential for misunderstanding and miscalculation," and that China has yet to explain to the international community the purpose of its military expansion, Pentagon officials said

<http://edition.cnn.com/2008/US/03/04/pentagon.china/index.html?iref=allsearch>

24. March 3, 2008

Report: China trying to crack U.S. computers, buy nukes

WASHINGTON (CNN) -- The Chinese military continues to increase spending on efforts to break into U.S. military computer systems, expand its Navy, and invest in intercontinental nuclear missiles and weapons to destroy satellites, according to the latest U.S report on China's military power.

The annual report from the Pentagon to Congress says China's total military spending in 2007 was between \$97 billion and \$139 billion, but it is hard to tell exactly how much was spent and on what.

In comparison, the U.S. military budget request for 2008 is \$481.4 billion, not including war requests.

Pentagon officials said a chunk of China's spending went to cyberwarfare, because 2007 saw several "intrusions" believed to be from the Peoples Liberation Army. In the incidents, unclassified U.S. military computer systems were broken into and information was taken, according to Pentagon officials.

While the information taken was not classified, **Pentagon** officials said the worry is the Chinese hacking [88cm] required many of the skills and capabilities that would also be required for a computer network attack.

Last summer, a cyber-attack on Department of Defense computer systems took down the e-mail capability of hundreds of staffers for weeks, but the Pentagon still will not comment on who initiated the attack [89in]. It is widely believed among the military to have been the Peoples Liberation Army.

China is also investing heavily in and fielding improved nuclear intercontinental ballistic missiles and antisatellite missiles, according to the report.

The United States expressed its concern last year after China fired a missile at one of its old satellites and destroyed it, sending thousands of dangerous pieces of space debris into orbit.

The United States conducted a similar strike last month on a broken U.S. spy satellite before it re-entered the Earth's atmosphere. U.S. officials said the satellite was hit and broke into thousands of small pieces that burned up as they re-entered Earth's atmosphere.

The United States is also concerned about the purchase of more submarines by the Chinese navy as well as plans for more aircraft carriers. The Chinese once had a small Navy. Now the United States is keeping an eye on the growing service amid concerns over Taiwan.

The concerns include "China's near-term focus on preparing for contingencies in the Taiwan Strait, including the possibility of U.S. intervention, which is an important driver of its modernization," the report says.

Additionally, the Chinese have placed about 100 more short-range missiles on the shore opposite Taiwan in the past year, it says.

Pentagon officials worry the continued increase in Chinese military spending is slowly tipping the balance of power between China and Taiwan in China's favor. The United States has said it would help defend Taiwan if China invaded.

The report also says the Peoples Liberation Army is "pursuing comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short-duration, high-intensity conflicts along its periphery against high-tech adversaries."

Such an army, the report says, would have "the greatest potential to compete militarily with the United States and field disruptive military technologies that could, over time, offset traditional U.S. military advantages."

The United States says the lack of transparency by the Chinese on its spending poses "risks to stability by increasing the potential for misunderstanding and miscalculation," and that China has yet to explain to the international community the purpose of its military expansion, Pentagon officials said

<http://edition.cnn.com/2008/US/03/03/pentagon.china/index.html?iref=allsearch>

25. September 26, 2007

Sources: Staged cyber attack

WASHINGTON (CNN) -- Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix. **[90in]**

CNN has honored a request from the Department of Homeland Security not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho lab

In a previously classified video of the test CNN obtained, the generator shakes and smokes, and then stops.

DHS acknowledged the experiment involved controlled hacking into a replica of a power plant's control system. Sources familiar with the test said researchers changed the operating cycle of the generator, sending it out of control.

The White House was briefed on the experiment, and DHS officials said they have since been working with the electric industry to devise a way to thwart such an attack.

"I can't say it [the vulnerability] has been eliminated. But I can say a lot of risk has been taken off the table," said Robert Jamison, acting undersecretary of DHS's National Protection and Programs Directorate.

Government sources said changes are being made to both computer software and physical hardware to protect power generating equipment. And the Nuclear Regulatory Commission said it is conducting inspections to ensure all nuclear plants have made the fix. [91in]

Industry experts also said the experiment shows large electric systems are vulnerable in ways not previously demonstrated.

"What people had assumed in the past is the worst thing you can do is shut things down. And that's not necessarily the case. A lot of times the worst thing you can do, for example, is open a valve -- have bad things spew out of a valve," said Joe Weiss of Applied Control Solutions.

"The point is, it allows you to take control of these very large, very critical pieces of equipment and you can have them do what you want them to do," he said.

Adding to the vulnerability of control systems, many of them are manufactured and used overseas. Persons at manufacturing plants overseas have access to control system schematics and even software program passwords, industry experts say.

Weiss and others hypothesize that multiple, simultaneous cyber-attacks on key electric facilities could knock out power to a large geographic area for months, harming the nation's economy. [92in]

"For about \$5 million and between three to five years of preparation, an organization, whether it be transnational terrorist groups or nation states, could mount a strategic attack against the United States," said O. Sami Saydjari of the nonprofit Professionals for Cyber Defense.

Economist Scott Borg, who produces security-related data for the federal government, projects that if a third of the country lost power for three months, the economic price tag would be \$700 billion.

"It's equivalent to 40 to 50 large hurricanes striking all at once," Borg said. "It's greater economic damage than any modern economy ever suffered. ... It's greater than the Great Depression. It's greater than the damage we did with strategic bombing on Germany in World War II."

Computer experts have long warned of the vulnerability of cyber attacks, and many say the government is not devoting enough money or attention to the matter.

"We need to get on it, and get on it quickly," said former CIA Director James Woolsey on Tuesday.

Woolsey, along with other prominent computer and security experts, signed a 2002 letter to President Bush urging a massive cyber-defense program.

"Fast and resolute mitigating action is needed to avoid a national disaster," the letter said.

But five years later, there is no such program. Federal spending on electronic security is projected to increase slightly in the coming fiscal year, but spending in the Department of Homeland Security is projected to decrease to less than \$100 million, with only \$12 million spent to secure power control systems.

Despite all the warnings and worry, there has not been any publicly known successful cyber-attack against a power plant's control system. And electric utilities have paid more attention to electronic risks than many other industries, adopting voluntary cyber-standards.

"Of all our industries, there are only a couple -- perhaps banking and finance and telecommunications -- that have better cyber-security or better security in general than electric power," Borg said.

And DHS notes that it uncovered the vulnerability discovered in March, and is taking steps with industry to address it.

While acknowledging some vulnerability, DHS's Jamison said "several conditions have to be in place. ... You first have to gain access to that individual control system. [It] has to be a control system that is vulnerable to this type of attack."

"You have to have overcome or have not enacted basic security protocols that are inherent on many of those systems. And you have to have some basic understanding of what you're doing. How the control system works and what, how the equipment works in order to do damage. But it is, it is a concern we take seriously."

"It is a serious concern. But I want to point out that there is no threat, there is no indication that anybody is trying to take advantage of this individual vulnerability," Jamison said.

Borg notes that industry will have to remain forever vigilant at protecting control systems.

"It will always be an ongoing problem. It's something we will have to be dealing with [for] lots of years to come," he said.

<http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=allsearch>

26. August 24, 2007

Anarchy on-line

Late last year the avatar Anshe Chung, a property developer in the virtual world Second Life who is said to have made more than \$1 million dollars on virtual real estate deals, was assaulted by flying phalluses in a 'griever' attack during a live media interview. The attack brought to attention the increasing phenomenon of anti-social behavior on the web.

We expected so much from the internet in the early days. It was to be a libertarian's paradise, where people could meet and form lasting relationships with other individuals from around the globe, free from the constraints of daily existence - all without having to leave their bedroom.

But it seems cyberspace may just be a magnification of the worst aspects of human nature.

In the online world, users are bullied, assaulted, even raped. In the expanding world of online gaming and social networking, anti-social and malicious behavior has become universal enough to give birth to a whole new vocabulary of terms such as "griefing" and "trolling". But can the worst aspects of cyberspace be regulated or is it a universe that is impossible to control?

What is griefing?

A recent report by **Pew Research's Internet & American Life Project** found that 32 percent of all teenagers who use the internet have experienced some form of "cyber-bullying". And it is not limited to adolescents, where you would expect it.

Griefing, which is often used to describe behavior on multi-player online games in which individual players intentionally frustrate others by disregarding the rules of etiquette has become so widespread that it has even generated sub genres -- terms such as kill stealing, corpse camping, spamming and ninja looting.

But griefing can also describe any form of anti-social and malicious activity performed within the confines of the internet. "If you are going to be technical about it [griefing] should be defined as harassment that one couldn't do in real life," explains Steven Davis of IT GlobalSecure, a security adviser to producers of online multi-platform games.

"I place mines in front of planes," an anonymous griever told G4 TV, describing his behavior on the multi-player games Battlefield 1942. "When someone tries to take off, they're blown to bits. I also take advantage of a glitch in the game that allows me to ride the wings of a plane. Then I kill the unsuspecting pilot midair and parachute to safety."

While examples such as this might prove little more than an annoying hindrance to the enjoyment of other players, some griefing can have far more damaging consequences.

One of the earliest recorded incidences was the now infamous "Rape in Cyberspace", as described by the journalist Julian Dibbell in the Village Voice in 1993. Dibbell had been part of LambdaMOO, a text-based virtual world (the world was described with words on the screen rather than with graphics).

One of the members of the world, Mr Bungle, managed to run a "voodoo doll" subprogram which controlled the actions of other characters within the room, and two of the characters were forced to perform sexual acts upon him, and themselves, against their will.

While no physical sexual act took place, the user whose character was a victim described to Dibbell how "post-traumatic tears were streaming down her face" as she discussed the incident with other members of the group. It only demonstrates how the boundaries between what's real and what's virtual can often blur.

It's true to say that anti-social and behavior occurs frequently within the real world but it would appear that the internet acts not just as a mirror to the real world but as a magnifying glass, exaggerating malicious tendencies.

Griefing -- why does it happen?

Most observers of the problem agree that the main contributing factor is the anonymity behind which users can hide on the web.

"We've known for a long time from the fields of psychology, anthropology and other areas of social studies that peer pressure is probably a more significant driver of human behavior than laws," says Raph Koster, a game designer and creative director behind **Star Wars Galaxies**.

The internet can act as an amplifier for bad behavior; the increased reach can encourage griefers to perform to an audience. "In computer science there's this term -- an N^2 problem," explains Koster. "This is where, as you add more things to a system, each new thing interacts with all the existing things so that problems scale exponentially rather than lineally. Human behavior is a kind of N^2 problem."

Judith Donath, a professor in media, arts and sciences at the Massachusetts Institute of Technology and director of the **Sociable Media Group**, agrees that anonymity of the perpetrator and an ensuing lack of peer pressure are key contributing factors to the increasing growth of cases of griefing, but also believes that the problem is exacerbated by the dehumanizing effect of the Internet.

"[The internet] changes people's perceptions of what the rules and constraints are. Obviously people do pull pranks and do mean things to each other in real life but online not only are they anonymous and feel safer doing things like that but there's also less of a sense of the humanity of the other that might make some people stop and think: 'I really shouldn't do this.' It's very easy to think of the people they are corresponding with as not quite human."

Donath believes that while in the early days of the web, cases of trolling -- deliberately inciting arguments by posting controversial messages on discussion boards and forums -- did exist, the problem was kept in check partly because most of the early users knew each other, but also because the size of the chat groups reduced the chances of true anonymity.

Solutions

The British anthropologist Robin Dunbar formed the theory **Dunbar's Number**, which proposes that 150 is the maximum number of individuals with whom a set of people can maintain a social relationship. The

theory concludes that beyond a group size of 150, civil society breaks down because individuals no longer feel a connection with other members of the group. In much the same way, as the volume of traffic on the web has increased and sites have become more populated, so acceptable behavior has deteriorated.

Koster believes that one of the solutions to stemming an epidemic of grieving or trolling is to break down online communities into smaller numbers where individuals within the group can exercise influence over destructive participants.

Another path is the one forged by countries such as South Korea, where any South Korean citizen who wants to post comments on a blog or forum, or take part in an online game, must submit their National ID number. [93wa] This reduces the potential for anonymity and consequently the inclination for anti-social behavior. But human rights groups have condemned such policies, claiming it impinges on free speech.

Ultimately, Koster believes the solution lies in an '**Avatar Bill of Rights**' which would give players in online communities a measure of protection against the power wielded by administrators -- and against fellow players. He proposes a structure by which users are empowered to take action against griefers and are given the chance to collectively ban someone. Users should also be able to file grievances against each other in a more organized fashion than currently exists.

"There's a whole raft of things like this that don't currently exist as infrastructure," he says. "They have them ad hoc, every community does it differently and most of them don't offer the full sweep. There's almost nothing out there that offers the array of things that the real world does for dealing with similar problems."

But some are more skeptical about such a proposal, believing that the internet is too large and too diverse to police and that it would be difficult to apply rules that will stick and remain relevant to such a rich variety of worlds. "I don't think there's going to be a universal set of laws like that carried out across the net," says Judith Donath. "Right now we tend to see these spaces as markedly different and I think that over time it will be about having spaces that are a little more transparent."

As virtual worlds become more popular and more intricate -- some games even offer players the chance to win real world money - it is plain that the brave new world of the internet will eventually have to find some way of regulating itself.

<http://edition.cnn.com/2007/TECH/08/23/virtual.bullying/index.html?iref=allsearch>

27. May 29, 2007

Cyber-spies tracking terror on Web

(CNN) -- There is an unconventional war being waged on the Internet. The battles here know no boundaries; and are fought from homes and offices from small Midwestern towns to Europe and the Middle East.

For the fighters in these battles weapons usually consist of no more than collected intelligence and computer programming skills.

It's no secret anymore that active terrorist cells are currently operating freely and openly on the Internet, using propaganda tactics to illicit prospective recruits [94wb].

The emergence of these terrorist groups has spawned their nemesis: groups of researchers, hackers, and maverick computer geeks who cyber-stalk terrorist networks online and take them down.

Aaron Weisburd, founder of Internet Haganah and director of the Society for Internet Research, is a fighter on the frontline in this new type of warfare.

Weisburd, who works out of his Carbondale, Illinois home, describes his organization as a "global non-governmental ad-hoc intelligence network" which he's modeled after al Qaeda's network.

Internet Haganah has assisted in the shutting down of hundreds of sites it says were linked to networks affiliated with groups such as Hezbollah, Hamas -- considered a terrorist organization by Britain, the U.S. and Israel -- and the insurgency in Iraq.

Weisburd recently led a panel on terror informatics and data mining at an annual conference at the Institute for Counter Terrorism in Herzliya, Israel. [95wb]

Resembling a modern-day Clark Kent, Weisburd is a boyish 40-something former computer programmer who decided to use his background and skills to track terrorists following the terrorist attacks of 9/11.

He's proved himself a force to be reckoned with, fighting -- and winning -- a war waged against the "dark side" of the Internet.

To do this, Weisburd poses as a member of the Islamic Brotherhood, using what he's learned from al Qaeda's terrorist networks to glean information and then pass it on to the appropriate people -- whom he calls "associates."

These "associates", says Weisburd, may or may not necessarily be affiliated with law enforcement.

To emulate and catch the bad guys, Weisburd adopts their language and behavior, noting that it's rare to be kicked out of a terrorist community forum for being "too radical."

"If somebody reports on the latest terror attack, then the Brothers usually think that's a cool thing, so they'll respond with praise for the bombers. That would be appropriate behavior," says Weisburd.

Weisburd's reputation has earned him the nickname "the vigilante" in cyber space, a legacy he's eager to shrug off.

"If I was a vigilante running a Web site, I would hurt you," says Weisburd.

"If I find that you're running a Web site for al Qaeda, I'm not going to hurt you. I'll report you to people that will ask you to come quietly, and if you don't go quietly, they may hurt you," he says.

Gabriel Weimann, also a panelist at the ICT Counter Terrorism Conference in Herzliya, is a professor, researcher, and author of "Terror on the Internet."

Weimann says most active terrorist groups have established their presence on the Internet.

"When we started this research," says Weimann, "we had around 12 terrorist Web sites. Now we have more than 5,000 Web sites."

Weisburd and Weimann agree that these terrorist groups should not be underestimated and have proven to be Web-savvy enough to gain strength and popularity on the Internet.

"Every time you see video tape of a sniper, there's someone holding a camera there," says Weisburd.

By all accounts, the Internet remains a free and unmitigated arena where terrorists can operate with little or no regulation, censorship, or government control.

Leading international Web log hosting service BlogSpot -- owned by Google -- is currently hosting several sites for terrorist networks such as al Qaeda in Iraq, who are using the free service to post their blogs in German, English, and Arabic.

After receiving complaints about these sites, Google posted a disclaimer that reads: "Some readers of this blog have contacted Google because they believe this blog's content is hateful. In general, Google does not review nor do we endorse the content of this or any blog."

Google maintains a policy of free expression, even if some of their blogs are unpopular or deemed offensive, moving to take down a site only if there's a threat against a specific individual.

"We put up warnings in front of blogs in some instances when users have complained, and the blogs include hate speech and hateful content, [96wa]" says Google spokesperson Steve Langdon.

With terrorist groups growing and gaining strength on the Internet, hackers like Weisburd may have their work cut out.

Some experts argue the phenomenon of burgeoning terrorist cells online is still in its infancy. While Weisburd's work may slow them down, they claim, ultimately it won't remove them as they simply re-emerge in other domains.

Still, Weisburd vows to continue the fight, saying he feels rewarded knowing he's making a difference in the intelligence community.

<http://edition.cnn.com/2007/TECH/05/29/internet.spying/index.html?iref=allsearch>

28. May 29, 2007

Is it time to crack down on the blogosphere?

By Linnie Rawlinson for CNN

LONDON, England (CNN) -- I blog, therefore I am: the Internet has become the place where "citizen journalists" broadcast their thoughts to all. This haven of free speech is treasured by thousands of online writers, each ready to leap onto their virtual soapbox and broadcast to the world.

But the blogosphere may not be the electronic utopia that we thought. It has been wracked by cyber-bullying, hate mail and even anonymous death threats. Are the golden days of the Internet over? Is it time to curb more extreme behavior -- and start to regulate what people write online?

Death threats

In March this year, high-profile technology blogger Kathy Sierra found herself the victim of cyber-bullying. She received anonymous death threats in her blog, and violent and sexual threats towards her were posted on other sites. Kathy was so affected by the threats that she stopped blogging and locked herself in her house. She told CNN, "I feel horrible, I feel frightened, I'm ready to just quit the whole industry."

Sierra says that her situation is not unique. She reports that after posting about the harassment in her blog, she received support from hundreds of people who have also been threatened by cyber-bullies.

While it's likely that Sierra's harassers could have been Internet "trolls" (people who randomly seek to provoke a hostile reaction with crude insults) there are elements of the Web that set it aside from other media, and increase the opportunity for personal attacks.

Beautiful chaos

The beauty of -- and the challenge for -- the Internet is that anyone can publish. Kids can instant message each other while doing their homework; enthusiasts create plethoras of fansites and forums; people with niche interests build communities online and connect on a global level.

The results can be chaotic. As the Internet spans traditional societal and geographical boundaries, the vast majority of people will connect in a civil manner (albeit with some heated debate.) But, as with any large gathering of people, groups with conflicting ideas can clash, while those with more sociopathic tendencies may start out with a trouble-making agenda.

It's also easy to provide an alias online, and with a little skill, Internet users can mask their identities further and target their victims from behind a veil of secrecy. This can give people the sense that they are separated from their words - as computer publishing supremo Tim O'Reilly says in his blog, "When people are anonymous, they will often let themselves say or do things that they would never do when they are identified."

Sticks and stones

Defenders of Internet freedom are quick to quote the "sticks and stones" defense -- they say that words, especially in the virtual world, are extremely unlikely to translate into physical attacks. They believe that offensive or aggressive verbal threats -- threats that people might never consider making offline -- should be ignored.

Blogger Mark Hughes, responding to Tim O'Reilly, writes, "Anything you write will offend someone sooner or later. That's not your problem, that's their problem. If you don't like what someone else writes on their own blog, don't read that blog anymore."

It can be hard to imagine the flesh and blood behind words on a screen. There is a sense that people online aren't "real," and it's ok to vent frustration at them.

But the Internet is not an alternative reality. It's a technological extension of the real world, populated by real people, and virtual attacks have an all too real result.

Victims of online attacks who don't know the identity of the perpetrators are left in a state of insecurity, always looking over their shoulder wondering where the next dose of vitriol will come from. As Kathy Sierra said to CNN,

"If I don't know for sure and I can't feel safe, am I willing to bet with my life that it's just a random Internet jerk? No."

The psychological damage from attacks such as those on Sierra can be chronic and severe. Ignoring trolls works to a point, but as a commenter posting as "Shelley" writes in O'Reilly's blog, "If a serious threat occurs, anonymous or not, it should be investigated by the police."

So should we start cracking down on what people are allowed to post online? [97wa]

Spirit of the Internet

Proponents of Internet freedom say that severe cases of cyber-bullying amongst adults are still not the norm; that heavy-handed legislation and increased governance are unnecessary and would see the spirit of the Internet die.

David Weinberger, from Harvard University's Berkman Center, told CNN that while attacks such as those on Kathy Sierra are deplorable, they also need to be seen in proportion. "The sort of violence of the threats that we see occasionally, we do see just occasionally," he said. "If that were pervasive, nobody would be on the Internet."

Weinberger has a point.

The Internet has brought people together in an unprecedented way. It is a lifeline to friendship and community, especially for those at risk of becoming isolated by society -- older people and disabled people, for example -- and has also given people like stay-at-home parents the chance to interact as well as work online.

Millions of people take part in online activities every day without encountering extreme mob action or personal attacks. Flame wars die out; people move on. The attention span on the Internet is very short.

Self-moderating

And many bloggers would argue that the virtual world, while predominantly not regulated, is far from lawless. Since its inception, Internet communities have been largely self-moderating, and this is generally successful.

Most communities and blogging sites will see their share of verbal conflict, but many have their own rules and guidelines as to what behavior is acceptable. These social mores, or "netiquette," are promoted and enforced by community owners and elders.

Some, such as longstanding community the Well, ban anonymity; others boot out users who break their rules; others simply ignore them. Some even advise victims to open a dialogue with the perpetrators -- if known -- to reach resolution, or as O'Reilly puts it, "We connect privately before we respond publicly."

And while anonymous attacks are prevalent, web users are reluctant to give up the right to remain hidden, even if it were to create a safer online environment: and with good reason.

The case for anonymity

Bloggers have pointed out that job applicants might not want prospective employers to Google them and discover their political or religious beliefs, embarrassing photographs or their frank thoughts about their workplace. And employers are checking.

Jackie Thompson, HR manager at PR agency Brands2Life, has rejected a candidate based on what she found out about them online. She told CNN, "I looked up a person and found some content about their previous employers which I didn't think was suitable. I decided not to go ahead with the application."

More seriously, bloggers cite the right of those in oppressed countries to write about their situation without fear of governmental recrimination. As the Pakistani Spectator said on Tim O'Reilly's blog, "Blogging is the great and unique way of protest for the oppressed people against such regimes."

But many Internet users also believe that people using the Internet need to act responsibly online, and realize that their words and actions can -- and do -- affect other users.

A commenter in O'Reilly's blog posting as "Groucho" says, "Vitriol really gives me the pip. Freedom of speech implies universal responsibilities - to respect the other fellow, to present rationally, and in good faith."

Code of conduct

And do those who run forums, blogs and messageboards have further responsibilities? Tim O'Reilly has called for bloggers to subscribe to a voluntary code of conduct where they take responsibility not just for their own words but also for the comments placed on their sites.

His six guidelines include: not saying anything you wouldn't say in person; considering disabling anonymous comments; and ignoring trolls. He also urges people to whistleblow on anonymous bullying rather than staying silent.

"It's the broken windows problem," he says. "If you don't look after your neighborhood, it gets worse, and eventually you have to move out."

O'Reilly's suggestions have received a mixed response from bloggers, many of whom fear a code of conduct would be the first step towards greater regulation of web publishing. Commenter Michael Mahoney replied, "The slippery slope here is more dangerous to civil discourse, by far, than the enforced civility that it strives to achieve."

O'Reilly's critics also point out that a voluntary code of conduct will have no effect on "trolls" and other troublemakers.

Responding to O'Reilly's draft code, Kathy Sierra wrote, "This Code of Conduct would have had no effect on what happened to me ... Anyone who would support a code of conduct doesn't *need* one, and anyone who we *wish* would adopt it never would."

Freedom implies responsibility

Others have greeted the draft code enthusiastically, saying that as an example of good Internet citizenship, it could encourage more positive behavior online and provide clarity on what conduct is expected on certain sites.

Chris Howard backs the code, commenting, "I can't see how or why anyone would object to people's right to be treated with respect in favor of their right to say what ever they like."

And that's the key. The tension lies between those who view the Internet's freedom as prized above all else; and those who feel that civility and responsibility are every web user's duty.

It's too soon to tell if voluntary codes of conduct will take off amongst bloggers and, if they do, whether they will be effective. But given the diversity on the Internet, it's unlikely that a solution that fits all will be found. Codes of conduct would make it clear what behavior is acceptable where; firm moderating would back that up. That won't stop trolls, but may help to prevent misunderstandings, and thereby unnecessary conflict. And of course, the authorities should continue to intervene when heated discussion turns to hate speech.

But although attacks on individuals cannot be condoned, the feeling amongst bloggers is that curbing freedom of expression online to prevent future attacks is too high a price to pay: the richness of an unrestricted Internet is too great. [98wa]

http://edition.cnn.com/2007/TECH/05/17/blog_crackdown/index.html?iref=allsearch

29. April 12, 2007

Security crucial as intruders grow sophisticated

What technology gadgets do the experts love, or would love to have? CNN.com is asking experts in several fields about their favorite high-tech toys. This week, we asked security expert Heath Thompson.

(CNN) -- Heath Thompson is vice president, product development for IBM Internet Security Systems.

The 25-year computer industry veteran says security is going to be increasingly important since consumers are spending more of their lives online and intruders are growing more sophisticated.

Here, he shares with CNN.com some of the key weapons in the security cyberwars [99cm].

1) Biometrics: Biometric readers are the key to the future, literally. Not only do they reduce the number of passwords the average consumer has to remember, but they are truly a unique identifier and one of the strongest forms of security. Today fingerprint readers are built into laptops, but in the near future, I believe these readers will replace the traditional lock and key and be built into smart phones, handheld devices and door locks for the car and home.

Eventually, I also anticipate that people will be able to store biometric information over the Internet so they can identify themselves from any location.

For instance, rather than carrying keys for safety deposit boxes, mailboxes and office entry, people will be able to access any secure device at any time through identification over the Internet.

2) Filters: My children are coming into their preteens, and with the popularity of MySpace and YouTube (and the uncertainty of what my children will find) I've begun to think about stronger content filtering that would prevent children from viewing violence, hate, pornography, etc.

Unfortunately, content filtering available through the computer's operating system isn't sufficient. Children are relentless and have figured out how to bypass security settings. Parents need industrial-strength content filtering, and the most economical way to get this would be through their Internet service provider. This type of security would allow parents to control individual usage throughout the home.

3) Portable security: It's getting to the point where encrypted sites are not sufficient for financial and confidential transactions because Internet attackers have coaxed users to download Trojans unknowingly. The Trojans sit dormant on the computer and wait for the user to authenticate to the network. Once a secure connection is established, the Trojans awaken and capture consumers' identities that can be reused or sold.

Consumers need their banks or ISPs to provide dynamic, downloadable security clients to ensure the machines being used, be it at home or at an airport kiosk, are free of Trojans and other malicious software. Consumers need dynamic protection that follows them to provide security regardless of location.

4) Secure Internet connections: Today, the Internet is connected to everything -- game consoles, digital video recorders, printers -- even refrigerators are now Web-enabled. Oftentimes these devices have no security settings installed, much less enabled. And even more often people are unaware these devices present an on-ramp into their home network.

The No. 1 targeted source for attacks is the consumer. When it comes to gaining easy access to user account data, Internet attackers have learned the consumer is much more susceptible and accessible than corporations.

For years corporations have been deploying intrusion prevention technology to keep the bad guys off corporate networks. Considering 68 percent of corporations experience six losses of sensitive data every year due to human error, according to IT Policy Compliance Group, employees need consumer-grade intrusion prevention equivalent to what their corporations have to secure their home Internet connections.

Corporate IPS systems would be cost-prohibitive and excessive for consumers and small business owners; however, if consumers could buy secure Internet connectivity through their ISPs, they would be able to protect their Internet Protocol-enabled devices, from today's ever-evolving threats.

<http://edition.cnn.com/2007/TECH/biztech/04/12/thompson/index.html?iref=allsearch>

30. December 1, 2006

Editor's Note: The CNN Wire is a running log of the latest news from CNN World Headquarters, reported by CNN's correspondents and producers, and The CNN Wire editors. "Posted" times are Eastern Daylight.

DHS: Advisory on al Qaeda cyber threat issued out of caution

WASHINGTON (CNN) -- A Department of Homeland Security advisory cautioning that al Qaeda may be planning **cyber attacks on banking and financial institution Web sites** [**100in**] was issued out of an abundance of caution, although there is no corroboration, a DHS spokesman told CNN Thursday.

The threat apparently was posted on a jihadist Web site, the spokesman said. It was discovered Nov. 27 by DHS and translated. The department decided to send an advisory out to financial institutions out of caution.

The Web site warned that denial-of-service attacks would be launched against stock and banking sites during the month of December through what the Web site called the "infidel New Year's." (Posted 7:55 p.m.)

...

<http://edition.cnn.com/2006/WORLD/europe/11/30/thursday/index.html?iref=allsearch>

31. October 24, 2006

Transcript: Ronald Sugar, Chairman and CEO, Northrop Grumman

LONDON, England (CNN) -- From under seas. To cyber space. To outer space. U.S.-based defense contractor Northrop Grumman is there. Armed with a doctorate in electrical engineering, Chief Executive Ron Sugar leads the company that is one of the top five defense contractors in the world. With 125,000 employees and annual sales of almost \$31 billion dollars, the company is at the forefront of the warfare revolution. CNN's Todd Benjamin caught up with him in London and began by asking about his thoughts on leadership.

Sugar: When I was a kid growing up I think I always wanted to be in charge and the only difficulty was that I discovered people didn't always want to follow me. One of the reasons for that was I didn't really understand that to be a leader you needed followers who are willing followers.

Benjamin: What philosophy did you take away from that?

Sugar: You really have to have a sense of where you're going otherwise you can't be a leader, and then you want to surround yourself with really good people, the right appropriate people for the task and you want to empower them and bring them into the process with you and trust them and say hey this is where we want to go, what are your thoughts. And they're always astonished when I say to them "what can I do for you, how can I work for you so you can get your job done"?

Benjamin: The defense industry has changed radically from when you first started in it and changed again since the end of the cold war. Where do you see the future?

Sugar: I read a piece just a couple of days ago that indicated that we really have begun a next world war. We didn't realize it but in fact we are in a next world war. And it's a different kind of war than the kind of wars we've experienced in World War I or World War II or even the Cold War and the rules are going to be different. But the one thing which I think is going to be necessary is for technological advantage wherever possible because we don't have human advantage in this country. There are many more people outside this country who would probably do us harm than we have that we can defend. The only differentiator we have is the quality of our technology.

Benjamin: How will this manifest itself?

Sugar: A great deal of digitalization of the battlefield. The greater use of improved intelligence gathering, sensing, unmanned aircraft, spacecraft, information processing, information warfare where you have a better understanding of what the other guy is saying to himself before he can actually act on it. **You can interrupt it, you can disrupt it. [101cm]** And of course you cannot deny the need for kinetic weapons and the actual ability to strike something which is the target.

Benjamin: Now technology is a powerful weapon for the military, but ideology and insurgency is also a very powerful weapon, so can the war on terror ever be won?

Sugar: Well, I think it has to be, but it's going to have to be won on more than just purely a military basis. Clearly there are many dimensions. And if you're able to create more terrorists than you can somehow neutralize overtime, you're not going to win. So, there are some fundamental structural issues in terms of poverty, in terms of class structure, clashes, cultural clashes, religious clashes which are really big issues and these things are going to go on for many, many generations.

Benjamin: The defense industry by nature of what it makes is a very different industry from several other industries. How do you respond to critics who would say that you make weapons which maim and kill?

Sugar: Our purpose is to provide the technological firepower so people don't maim and kill us. And that we can protect our way of life. And while it would be nice to live in a world where there are no weapons, and it would be nice to live in a world where everybody has the same values and respect that we might have; that is not the world we live in. And so it becomes a simple imperative of do we want our way of life, our society, our families, our civilization, the structure of the civilized world as we know it to prevail, or do we want something else to prevail? And, fundamentally, because the world is a dangerous place, we need the kind of technology that we provide.

<http://edition.cnn.com/2006/BUSINESS/10/20/boardroom.sugar/index.html?iref=allsearch>

32. October 3, 2006

Social networking fuels new Web boom

By Ravi Agrawal for CNN

(CNN) -- If you haven't already created a cyber profile on a social networking Web site like MySpace.com or Facebook.com, you're part of a rapidly shrinking minority.

With growth rates unheard of since the online boom of the late 90s, the question every investor worth his bandwidth secretly wants to know the answer to is whether the gold rush is going to last.

After NewsCorp. acquired MySpace last year for \$580 million, and with news last month of Yahoo bidding \$1billion for Facebook, new social networking sites are mushrooming every week.

According to the latest figures released by comScore World Metrix, Web 2.0 -- a vague moniker for newer internet companies started with less capital and focusing on open business models and the customers -- companies are growing at an unprecedented rate.

While older sites run by Yahoo!, eBay, and Amazon continue to be among the top 10 sites with the most unique visitors, they have grown in single digit figures in the last year.

Meanwhile MySpace (243% annual growth in unique visitors to 79.6m) and Facebook (86% growth to 15.5m) are fast pushing to become the most trafficked Internet destinations.

But when Facebook has approximately a fifth of the users MySpace can boast of, how can Yahoo! justify paying almost double the price NewsCorp paid out?

According to Caris and Company's analyst Tim Boyd, \$1bn is a "reasonable price" for Facebook. In a research note, Boyd suggests that the perceived value of social networking sites has increased by six to eight times in the last year.

Due to Facebook's "lack of public company expenses" and its' "far-more-targeted user demographic" the deal could well be a sound one for Yahoo!, says Boyd.

Many analysts are confident that the new boom won't explode like the 90s bubble burst.

"The 90s bubble was fueled by investors' money being pumped into the economy and forcing it to rise without any real justification," said Bob Ivins, the managing director of comScore Europe.

"Now investors have rigorous financial models and a vision of how to monetize Web traffic and engagement statistics. They're conducting the due diligence to make sure the mathematics makes sense."

For some founders of social networking sites, the end goal isn't necessarily to start a bidding war and cash out fast. The bigger bucks may just lie in advertizing in the long term.

Facebook signed an online advertizing deal last month with Microsoft Corp., guaranteeing the software giant at least \$200m over the next three years. MySpace too signed a \$900m three-year deal with Google, almost double what NewsCorp. paid out to buy the social networking site.

"The Google-MySpace deal shows that the mathematics [behind potential bids] makes sense if investors can monetize user traffic," added Ivins.

Michael Birch, the co-founder of Bebo -- a social networking site with 27m users which claims to have overtaking MySpace in the UK -- is just one of many start-up gurus who might not sell anytime soon.

"We're not looking to sell. I've spent all these years trying to get to this point. To sell out as soon as I get to it just seems a little bit silly," he told The Times in an interview last week.

And if the competition to survive wasn't intense enough already, a Microsoft spin-off called Wallop announced last week it expects to take on MySpace and Facebook by touting tools users can buy to craft better-looking web pages [102wb]

<http://edition.cnn.com/2006/TECH/internet/10/03/social.networking/index.html?iref=allsearch>

0. September 29, 2006

Cyber-spies tracking terror on Web

By Dana Rosenblatt for CNN

(CNN) -- There is an unconventional war being waged on the Internet. The battles here know no boundaries; and are fought from homes and offices from small Midwestern towns to Europe and the Middle East.

For the fighters in these battles weapons usually consist of no more than collected intelligence and computer programming skills.

It's no secret anymore that active terrorist cells are currently operating freely and openly on the Internet, using propaganda tactics to illicit prospective recruits.

The emergence of these terrorist groups has spawned their nemesis: groups of researchers, hackers, and maverick computer geeks who cyber-stalk terrorist networks online and take them down.

Aaron Weisburd, founder of Internet Haganah and director of the Society for Internet Research, is a fighter on the frontline in this new type of warfare.

Weisburd, who works out of his Carbondale, Illinois home, describes his organization as a "global non-governmental ad-hoc intelligence network" which he's modeled after al Qaeda's network.

Internet Haganah has assisted in the shutting down of hundreds of sites it says were linked to networks affiliated with groups such as Hezbollah, Hamas -- considered a terrorist organization by Britain, the U.S. and Israel -- and the insurgency in Iraq.

Weisburd recently led a panel on terror informatics and data mining at an annual conference at the Institute for Counter Terrorism in Herzliya, Israel.

Resembling a modern-day Clark Kent, Weisburd is a boyish 40-something former computer programmer who decided to use his background and skills to track terrorists following the terrorist attacks of 9/11.

He's proved himself a force to be reckoned with, fighting -- and winning -- a war waged against the "dark side" of the Internet.

To do this, Weisburd poses as a member of the Islamic Brotherhood, using what he's learned from al Qaeda's terrorist networks to glean information and then pass it on to the appropriate people -- whom he calls "associates."

These "associates", says Weisburd, may or may not necessarily be affiliated with law enforcement.

To emulate and catch the bad guys, Weisburd adopts their language and behavior, noting that it's rare to be kicked out of a terrorist community forum for being "too radical."

"If somebody reports on the latest terror attack, then the Brothers usually think that's a cool thing, so they'll respond with praise for the bombers. That would be appropriate behavior," says Weisburd.

Weisburd's reputation has earned him the nickname "the vigilante" in cyber space, a legacy he's eager to shrug off.

"If I was a vigilante running a Web site, I would hurt you," says Weisburd.

"If I find that you're running a Web site for al Qaeda, I'm not going to hurt you. I'll report you to people that will ask you to come quietly, and if you don't go quietly, they may hurt you," he says.

Gabriel Weimann, also a panelist at the ICT Counter Terrorism Conference in Herzliya, is a professor, researcher, and author of "Terror on the Internet."

Weimann says most active terrorist groups have established their presence on the Internet.

"When we started this research," says Weimann, "we had around 12 terrorist Web sites. Now we have more than 5,000 Web sites."

Weisburd and Weimann agree that these terrorist groups should not be underestimated and have proven to be Web-savvy enough to gain strength and popularity on the Internet.

"Every time you see video tape of a sniper, there's someone holding a camera there," says Weisburd.

By all accounts, the Internet remains a free and unmitigated arena where terrorists can operate with little or no regulation, censorship, or government control.

Leading international Web log hosting service BlogSpot -- owned by Google -- is currently hosting several sites for terrorist networks such as al Qaeda in Iraq, who are using the free service to post their blogs in German, English, and Arabic.

After receiving complaints about these sites, Google posted a disclaimer that reads: "Some readers of this blog have contacted Google because they believe this blog's content is hateful. In general, Google does not review nor do we endorse the content of this or any blog."

Google maintains a policy of free expression, even if some of their blogs are unpopular or deemed offensive, moving to take down a site only if there's a threat against a specific individual.

"We put up warnings in front of blogs in some instances when users have complained, and the blogs include hate speech and hateful content," says Google spokesperson Steve Langdon.

With terrorist groups growing and gaining strength on the Internet, hackers like Weisburd may have their work cut out.

Some experts argue the phenomenon of burgeoning terrorist cells online is still in its infancy. While Weisburd's work may slow them down, they claim, ultimately it won't remove them as they simply re-emerge in other domains.

Still, Weisburd vows to continue the fight, saying he feels rewarded knowing he's making a difference in the intelligence community.

<http://edition.cnn.com/2006/WORLD/europe/09/28/internet.spying/index.html?iref=allsearch>

33. October 13, 2005

A convicted hacker debunks some myths

(CNN) -- To many, the name Kevin Mitnick is synonymous with hacking, the cinematic sort where a snot-nosed kid thumbs his nose at authority. But, Mitnick says, the characterization is a bit overdone and the legend untrue, if not libelous.

It is true, he says, that **he broke into corporate computer systems and stole source code** to satisfy his curiosity, but he denies the stories that he hacked into NORAD -- North American Aerospace Defense Command -- or that he wiretapped the FBI.

After a well-publicized pursuit that made him notorious, the FBI arrested Mitnick in 1995. He served five years in prison after pleading guilty to charges of wire and computer fraud. He was released in 2000 and today runs a computer security firm. In a telephone interview with CNN's Manav Tanneeru, Mitnick talks about his past, the state of online security today, and how he handles what his name has come to mean.

CNN: There is a certain myth of Kevin Mitnick, but you seem to disavow a lot of it. Why exactly did you become so famous and what specifically was reported that was inaccurate?

MITNICK: [The claims] that I wiretapped the FBI or something like that were something out of a movie like "War Games" or "Enemy of the State" or something. There were fictional events that were tied to real events, like when I took code from Motorola and Nokia when I was a hacker to look at the source code. I took a copy, which is essentially stealing, to look at the information. [103cm] That was true, that was the truth ... in the story, but there were a lot of libelous statements. ...

I'm the one that got myself into trouble, but because the reporting in the [New York] Times portrayed me as this very dangerous character, the government stepped up the prosecution of the case.

At the end of the day, I would have been prosecuted, but I wouldn't have been held in solitary confinement for a year for the fear that I could launch nuclear missiles by whistling through a pay phone.

I was powerless because I was represented by a publicly appointed attorney who had a very limited budget. But a lot of accusations I wasn't charged with. If I hacked into NORAD or wiretapped the FBI, I certainly would have been charged with it. I got into trouble largely because of my actions. However, because of the media reporting, I was treated as "Osama bin Mitnick."

CNN: You were once the most famous and sought after hacker in the country. After your release from prison you were asked to testify before the Senate, and you now run a Web security firm, which is a fascinating evolution.

MITNICK: It's kind of interesting, because hacking is a skill that could be used for criminal purposes or legitimate purposes, and so even though in the past I was hacking for the curiosity, and the thrill, to get a bite of the forbidden fruit of knowledge, I'm now working in the security field as a public speaker. Twenty-five percent of my revenue is actually doing security assessments, so people actually hire [me] to break into their systems to find their security failures and patch them before the bad guys find them [104cm].

So, it's kind of interesting, because what other criminal activity can you ethically practice? You can't be an ethical robber. You can't be an ethical murderer. So it's kind of ironic. But it is really rewarding to know that I can take my background and skills and knowledge and really help the community.

CNN: The fact that you are back in the online world, especially the cyber security sector, may give many reason for a certain insecurity and paranoia. How has your firm been received?

MITNICK: There are several in the security field that don't trust me. They're my competitors, and right there, there is an agenda. But I'm sure that our company does not receive phone calls because they're concerned about my past, and then again, there are a lot of people that do make those calls, and they keep the business going pretty good. I never got a phone call saying, "Hey, we're not hiring your firm because of x, y and z."

I don't know what the percentage is, but I'm sure there are people that don't want to use our firm because they really don't know much about the case. They just know me as a hacker that went to jail.

CNN: Compared to the time you were an illegal hacker, and the contemporary landscape, how easy is it to hack a computer? Has security improved much? Would you still be able to do what you did years ago?

MITNICK: I get hired to hack into computers now and sometimes it's actually easier than it was years ago. It really depends on who the client is -- or if you're doing ethical hacking, who the target is. It could be a difficult target or an easy target. The security landscape, the only thing that's changed in regards to vulnerability are technical issues, but with social engineering, it's all remained the same. So, it depends how vigilant the owners and the operators of the computer systems and the network are, and it really doesn't go to the question of are we living in a more secure world?

CNN: Then, how vulnerable is the common user? Sure, it depends on how many safeguards they've installed, but if they have the most effective of security, how easy is it?

MITNICK: I did a study USA Today was involved with and another marketing firm in San Francisco was involved with within the last year, and we set up a honeypot network, which was six different networks running various different operating systems. We plugged them into a DSL line in San Francisco, and we just watched them to see how quickly these systems could get broken into without having any protection. And one of the computers was broken into four minutes after plugging it into the Internet, which is quite astounding.

CNN: You previously mentioned social engineering. What exactly does that term mean to you?

MITNICK: Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a Web site, which exploits a technical flaw and allows the hacker to take over the computer. [105cm]

CNN: And how do contemporary hackers use social engineering in what they do?

MITNICK: Well, how about Paris Hilton? She was attacked on her cell phone, and she was attacked two ways. One was because of a T-Mobile's Web site, and the other guy was able to compromise it by getting her phone number by going on T-Mobile's Web site, doing a password reset, which SMS-ed her new password because, presumably, only the owner would have the handset.

And then what they did was, they did a technique called caller ID spoofing, which allows a person to change the number they're calling from on their calling phone number display. So, they were posing as T-Mobile customer service, and they called her phone, and on the caller ID it showed as T-Mobile customer service, and then they told her, "There are some network difficulties. Have you been getting any SMS [messages] about a password reset, and what were the contents of the message?" and she freely gave it out, and that's how these guys were able to get to her T-Mobile Sidekick, and her e-mail, and whatnot.

In another example, the IRS just did a security audit under the office of the inspector general and called 100 managers posing as IT people at the IRS, and 35 of those managers freely gave out their password and user name over the telephone. [106cm]

So, it's a significant threat. A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted. It's essentially meaningless.

CNN: How much do you trust online banking and the usage of credit cards online?

MITNICK: I trust online banking. You know why? Because if somebody hacks into my account and defrauds my credit card company, or my online bank account, guess who takes the loss? The bank, not me.

CNN: Then what about other transactions? Do you pay bills online or shop online? I'm just curious if Kevin Mitnick is worried about ID theft?

MITNICK: Somebody already stole my identity once and used it to apply for a cell phone account. And it's too bad. I wish they stole my identity 10 years ago when I was a fugitive -- that would have been cool. It was a \$400 bill, and they used my mom's address in Las Vegas when I was living in California under my name. That's really easy, because all you need to steal someone's identity is the Social Security number. It's not really rocket science.

But, I don't have a problem at all using my credit card online. There are attacks that can be done, but it's unlikely that I'll be targeted as an individual. It's more likely the attackers will target the bank. So that way they can get many user names and passwords, and get access to many accounts, rather than just targeting me. I think it's safer to use a credit card over the Internet than it is to go to a Macy's and use it where an employee can simply skim off the card, or go into a bar, or a restaurant where they have your credit card number.

CNN: You've become something of a star, a cult one, at least, even appearing on an episode of "Alias" as a hacker. What do you make of your celebrity?

MITNICK: It's kind of interesting, because I went through a horrific, horrendous experience and became the hacker poster boy, and it had a negative effect on my trip through the criminal justice system. But now that I've turned over a new leaf and people are interested in my skill-set, now the notoriety of my name helps me in my business. Not because of what I did in the past, but because I'm a known entity with my skill-set.

CNN: Do you miss being on the run?

MITNICK: No, no, I don't miss it all. I like my life now. I made some really stupid mistakes in the past as a younger man that I regret. I'm lucky that I've been given a second chance and that I could use these skills to help the community.

<http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnn/index.html?iref=allsearch>

34. February 16, 2005

The Internet war

(CNN) -- By now, you've probably heard how some alleged Iraqi insurgents kidnapped a doll last week and claimed it was a U.S. soldier. Not G.I. Joe, but Special Ops Cody, an action figure put out by Dragon Models USA.

The punch lines were quick to follow: Barbie was negotiating his release. G.I. Joe was the kidnappers' next target.

It's an Internet hoax, yes. At least one Islamist Web site admits it was taken in because, its moderator wrote, it wanted to believe the story. **[107wb]**

Hoax or not, it is an important window into the Internet war that's going on between al Qaeda, its supporters and those who are fighting against them.

There are a vast number of Web sites -- a few of them significant -- that carry the postings of al Qaeda and Iraqi insurgents, as well as their sympathizers.

Web sites monitored

Government agencies monitor the increasing output of Web sites. **[108wa]** We at CNN spend quite a bit of time doing that as well, as do other journalists -- trying to sort fact from fiction and deciding what is appropriate to report and what video to show, a sensitive task when hostages or killings are shown.

There are also numerous private citizens who have made it their business to monitor these sites.

Jeremy Reynolds is one of those people. If you didn't see the story we did about him last year on CNN, here's his background.

His day job is running Joy Junction, a faith-based homeless shelter in Albuquerque, New Mexico. But he spends his spare time -- as do others in the United States and Britain -- combing the Internet for the latest postings by these groups.

Reynolds got into this avocation after the September 11 attacks, saying it was a way he could join the fight against terrorism.

After I mentioned the doll story to him, he and his colleagues began to trace back the links. They discovered it had been posted to a message board that regularly carries postings from al Qaeda and Iraqi insurgents.

The site, which has a disclaimer that it cannot vouch for the information posted there, has contained links to material from people like Osama bin Laden and Abu Musab al-Zarqawi.

It was actually another such site that carried the mea culpa about the hoax. Not that it was much of a mea culpa. By the end, the whole thing was being blamed on either the U.S. government or Zionists.

Reynolds found that the doll photo and claim were originally posted to yet another site. He found other photos there, including one titled "Original Picture of Dead American Dog on Road in Iraq" and a portrait of former Iraqi ruler Saddam Hussein.

Internet offers anonymity

This site appears to have been registered to someone in Baghdad that, if true, might ultimately lead us to the kidnapped doll. But given how easy it is to hide identities on the Internet, the truth may never be known.

In the course of his cyber-sleuthing, Reynolds has butted heads not just with the creators of some of these Web sites, but also the Internet service providers (ISPs) that host them. [109in]

He says he has asked a Houston-based company why it continues to host the first Web site mentioned above, adding that he's gotten no answer.

And he's been taking on Yahoo for several months now about a forum it hosts called Global Islamic Media. This site also carries postings from hostage takers and beheading videos from Iraq.

That's what led us to do the story about him last year. He never got a clear answer from Yahoo and neither did CNN, when we asked.

The forum was taken down and then came back up. That's the pattern for most of these sites.

For a while, after September 11, al Qaeda had its own Web site. CNN traced the site to Malaysia and asked the ISP about it. The site was soon taken down.

But it would reappear elsewhere on the Internet, for a few days at a time, then get taken down. These days, most of the groups will post to these various bulletin boards, especially if they want to show off a hostage or beheading video. [110wb]

Osama bin Laden's messages get posted to these sites as well, when they don't show up on Al-Jazeera first. The Internet allows bin Laden, al-Zarqawi and others to get their message out. That's one reason they like to use it.

And it should be noted that unlike the case of the kidnapped doll, bin Laden and al-Zarqawi don't have histories of posting hoax messages. Nevertheless, CNN checks each and every one of them to verify the authenticity of the images or voices.

That's what happened with the doll photo. The posting originally claimed it was an American soldier. But when CNN and other news organizations asked the Pentagon, officials there quickly pointed out that no U.S. soldiers were missing.

Because cyberspace is so tricky and allows identities to be masked, groups can post messages that usually are not traced back to them -- even though Reynolds and, no doubt, agencies like the CIA try their hardest to do so.

It has always been thought that one way to find bin Laden would be to follow the tapes that are either delivered to Al-Jazeera or posted on the Web.

Reynalds, by the way, is still at it. He's gone back to that original Web site, where it looks like the hoax originated -- and this time he's found new pictures on the site.

Not dolls this time, but planes. Model planes! An AC-130H Spectre gunship and an F-15E Eagle fighter. The next hoax perhaps?

He'll keep checking.

<http://edition.cnn.com/2005/US/02/08/schuster.column/index.html?iref=allsearch>

35. January 19, 2005

Uncertain state of security

Complexities abound in protecting homeland

By Greg Botelho - CNN

(CNN) -- The three and a half years since the September 11, 2001, attacks have brought no new terrorist acts on U.S. soil, but questions continue about the state of the nation's security.

Federal, state and local agencies have created new organizations, attempted to coordinate among existing ones along with the private sector, and crafted policies to preempt and respond to attacks. Add in an evolving threat, persistent alerts, fresh scrutiny on intelligence and other complicating factors, and you have a process that security expert Frank Cilluffo compared to "building an airplane mid-flight."

"You can't codify homeland security into a neat box," said Cilluffo, director of George Washington University's Homeland Security Institute and former special assistant to President Bush. "You cannot separate foreign, health, agricultural, economic, energy and other policies. And all of it raises other issues, like freedom of privacy."

Sweeping reforms have not been without controversy. Some claim anti-terror measures, such as the Patriot Act, threaten civil rights or damage the country's credibility and, thus, its security. And for all that's been done, criticisms circulate about a host of perceived holes in the system.

The challenge isn't just catching up to ensure optimal organization and cooperation between pertinent U.S. and international groups, but also keeping up with present and future threats. Knowing how safe the nation is requires knowing the condition, movements, motivations and methods of America's enemies.

"As we get better, so do they. As we get harder, they'll figure out ways to get around hardened targets or go after softer ones," said Jonathan Duecker, Pennsylvania's homeland security director. "This homeland security game is relatively new, and there is a lot of learning."

For now, authorities will build relationships, revamp institutions and infrastructure and hunt down threats in and outside the United States. The greatest danger, they say, is complacency.

"Every day we don't have an attack gives us one day to get better," said James McMahon, head of New York's Office of Public Security. "If we ever decide we're at full preparedness, we're making ourselves very vulnerable."

Current assessment

In a national CNN/USA Today/Gallup poll conducted between January 7-9, 39 percent of respondents said they felt a terrorist attack would likely occur inside the United States over the next several weeks, the lowest such figure since September 11, 2001. About a year earlier, that figure was 46 percent and, in March 2003 after U.S.-led forces invaded Iraq, it was at 73 percent.

"The further away from 9/11 we get, the harder it is to get people engaged," Duecker admitted.

Outgoing U.S. Homeland Security Director Tom Ridge this month attributed a decrease in intercepted terror threat information to coalition military activity, corraling terror leaders and funds, and domestic measures to "harden" prime targets [111cm]. But some experts, noting that recent "chatter" jumps have not equated to domestic attacks, said it would be dangerous to assume terrorists' tactics and means have not evolved in recent years.

To keep up with the threats requires funds to replace outdated equipment, buy new materials and train personnel, money that Duecker says has already begun dropping off incrementally.

New York City received a significant increase in the latest round of funding, for instance, as did Washington. But money for Philadelphia, Pennsylvania, located between these two cities, stayed essentially static, much to Duecker's dismay, while other areas saw drop-offs. Jersey City and Newark, New Jersey, for example, saw 60 and 17 percent decreases, respectively, in the latest round of funding -- two of several municipalities nationwide to face such a shortfall.

Finding a fair funding formula is one of many complex tasks facing the U.S. Department of Homeland Security, as well as state and local agencies charged with safeguarding the nation.

Numerous government divisions -- which handle everything from law enforcement to agriculture, intelligence to health, the military to the economy -- have a stake. Experts say that it is critical that businesses (not just government agencies) have clear, firm security guidelines and up-to-date training to address threats, especially given that many targets are in the private sector.

Convoluted bureaucracies, entrenched interests and large egos could all aggravate an already difficult process. And each group -- public or private -- comes equipped with its own issues, tools and approaches, notes Duecker.

"Not too many people at the state and local level are dedicated full time to homeland security," said McMahon, a former New York State Police superintendent. "They've had to take on new responsibilities in addition to what they do routinely. It's human nature you kind of drop back."

From international to local

For all the meetings, bureaucratic moves and funding spats, the post-September 11 environment puts perhaps the greatest burden on first responders to track down threats and handle emergencies.

"As tough as the federal issues are, it's the men and women in the frontlines ... who will ultimately determine if the battle is won or lost," said Cilluffo.

Duecker, a former DEA agent, noted a "bona fide nexus between common criminals and transnational terrorism" -- saying many terrorists get funds from criminal activity. This makes it important for law enforcement to follow the final destination of funds from larcenies, money laundering, drug deals and other crimes.

Gathering intelligence, "the lifeblood for every facet in the war on terrorism," Cilluffo said, works best when more people, in more communities, contribute.

While terrorism used to be a federal matter, McMahon said, today officials cannot afford to "discount the 680,000 sets of eyes, 70,000 in New York alone" of local fire and police. The September 11 hijackers, after all, used ATMs, were pulled over by police, visited establishments and did other things that might have been spotted by alert authorities or citizens, he added.

This need for quality intelligence has put renewed importance on international cooperation, at a time when America's reputation worldwide is tenuous in some circles.

Invading Iraq without a full United Nations mandate; torture claims; mass detentions of people in Iraq, Afghanistan and elsewhere; and other developments have hurt the United States' credibility, and its security, said Seattle University law professor Ron Slye. Anti-American sentiment may impair international cooperation, as well as spawn new terrorists, he added.

"It gives a lot of fodder to people who don't understand the United States, but say that it is an evil empire bent on dominating the world and only gives lip service to human rights," said Slye. "It's a very serious problem, and the administration and the country as a whole need to be very serious about countering it."

Cilluffo, having recently worked in the White House, dismisses the notion of any international breach, saying countries that may object publicly to U.S. policies cooperate effectively behind the scenes. But he does note difficulty in simultaneously preserving a country's security against terrorists and its civil rights.

"Terrorism first and foremost is a psychological weapon aimed at undermining policies and values," Cilluffo said. "It's a tough balance."

A difficult measure

Reports vary on the likelihood of a nuclear, chemical, biological or other terrorist attack inside the United States in the near future. Regardless, some critics say not addressing a number of prevalent problems could have dire consequences.

Sen. Joe Biden of Delaware called it "criminal" that "there is no basic security" for the U.S. railroad system. The DHS denies that assertion.

An EPA report, meanwhile, found water **supplies vulnerable to cyber-attack [112in]**, according to the Associated Press.

The Department of Homeland Security's Inspector General has been one prominent critic. He recently reported that nonresidents using stolen passports can easily enter the United States, and even faulted the DHS for mismanaging grants intended to bolster port security.

While admitting unresolved issues, "substantial progress" has been made in recent years, said McMahon.

Communication between federal agencies, like the FBI and local authorities, has improved greatly in recent years, said Duecker. Would-be attacks reportedly have been thwarted in Jordan, the United Kingdom and the Philippines, Cilluffo said, adding that other terrorist operations have been averted behind the scenes.

"These are all delicate issues, but there's a success story that hasn't been fully told," he said.

Yet the level of success, like much else related to homeland security, is largely an unknown.

"It's very hard to quantify how successful a counterterrorism operation is because how can you know you foiled something?" Duecker said.

Uncertainty is inherent when targets -- soft and hard -- are everywhere, and the opposition is ephemeral, not clearly perched across a battlefield. That does not mean initiatives to protect America should not continue, experts say, but only that any such efforts and debates must take into account the complicated reality.

"We'll never be in a position where we can protect everything, all the time," Cilluffo said. "We can't afford it, and we don't want to infringe on the values we're trying to preserve."

<http://edition.cnn.com/2005/US/01/18/security.overview/index.html?iref=allsearch>

36. July 20, 2004

Review: A fresh 'Angle' on the spy novel

Bruce Sterling's new book takes author in new direction

By L.D. Meagher - CNN

(CNN) -- The espionage thriller genre has been a bit adrift since the end of the Cold War. The cyberpunk sub-genre of science fiction has been a bit adrift since its dystopian visions of a wired world started to look a lot like the real world.

Bruce Sterling, one of the founders of cyberpunk, has addressed the latter issue in his writings. Now, he addresses the former in his novel "The Zenith Angle."

Sterling has created a new post-Cold War milieu for spy stories. Gone is the us-versus-them paradigm of competing superpowers. In its place is another us-versus-them: the United States against terrorists. The tale begins, fittingly, on September 11, 2001.

Derek Vandevener, uber-techie, is living the good life. He and his wife have a new baby. He's making boatloads of money running research for an Internet company that survived the dot-com bust. He is having breakfast in the suburban mansion he has just purchased when he sees the World Trade Center attacks on television. In that instant, his comfortable existence is over.

Before he knows it, he has signed on with a new, high priority federal project to build defenses around the high-tech U.S. infrastructure [113in].

The protagonist hears a lot of talk about heightened "cyber-security" and a coming "info-war." Mostly, though, he finds himself doing what he did in the private sector -- developing and evaluating new hardware and software.

Cut off from his family by his work, he gravitates into the orbit of a special operations veteran named Michael Hickok. Only then does Vandevener begin to see the true dimensions of the threat facing the United States.

Edgy narrative

Sterling takes his time laying down the background of the story. The technique allows him to explore Cyber Age concepts and constructs, including a new, state-of-the-art telescope that Vandevener's wife, an astrophysicist, is working to bring on line.

"This telescope was polished and elegant," Sterling writes, "bejeweled with buttons, plugs, and switches, like a trophy wife at a Nobel Prize party. It -- she -- was five stories high. A towering complex of struts had delicately tapered arms painted in designer enamel. Her bottom was a great big mirror bowl of glassy blue hexagons in a green plastic case. All the joins and seams were suspiciously perfect. This telescope was like the Hubble's sexier little sister."

About two-thirds of the way through the book, the action kicks in. And once it does, the story rockets toward a violent conclusion that leaves Vandevener -- and everyone he knows -- profoundly changed.

"The Zenith Angle" touches all the bases one would expect from an espionage thriller. And it does so in against a backdrop that is as chilling as it is familiar. Sterling has not lost the narrative edge that gave the cyberpunk movement its vitality. He wields it just as deftly in a very different genre.

This novel may not be the final word on where spy stories are going. But it's a pretty good start.

<http://edition.cnn.com/2004/SHOWBIZ/books/07/20/review.angle/index.html?iref=allsearch>

37. March 20, 2003

Are we vulnerable to cyber-attacks?

Most getting more serious about security, but risks growing

By David Kirkpatrick - FORTUNE.COM

(FORTUNE.COM) -- With war on Iraq underway, the possibility of a terrorist response is on all of our minds. In addition to the other things we have to worry about, this is likely to be the first major war that takes place with the entire world linked together by one continuous **set of electronic signals** [114in]. That creates immense dangers of war-related hacking and cyber-terrorism.

Even without war, the risks of cyber-attack have been growing daily. The British consulting firm mi2g said in a report this week that verifiable digital attacks worldwide have caused economic damage of more than \$16 billion so far this year, almost double a year earlier. And 64 percent of digital attacks worldwide have been against North American targets, compared to about 30 percent a year ago.

The attacks themselves are changing, too. "The new kinds of attacks are more malicious, not kids in the basement hacking," says Jim Kollegger, CEO of BBX Technologies, which makes security software for Windows networks. **"We're seeing arms merchants for digital wars. Some hacker agencies in Bulgaria and China have found holes in the Microsoft fabric and are crafting toolkits to take advantage."**

[115in]. That means anyone can cause trouble. You don't have to be a good programmer anymore.

Protest hackers are an increasingly serious problem. **The website of the American Academy of Diplomacy was defaced with the phrase "NO WAR"** [116wb] earlier this week. The mi2g firm says anger about U.S. policies is generating protest hacking from Brazil, France, Indonesia, Mexico, Morocco, Romania, Saudi Arabia, Turkey, and the UK. Now mi2g says protesters are shifting targets, from government and military to business. Others agree.

Retired Marine Lt. Col. James Emerson, a vice president of Princeton-based ICG (formerly called Internet Crimes Group), says the companies most at risk are those seen as symbols of American global presence. If so, they ought to increase their cyber-security. "Companies should be asking, 'Am I someone who just might end up in the wrong place at the wrong time on the web? And is the risk I was willing to accept this morning the same risk I'm willing to accept at the start of hostilities?'"

The good news, in a way, is that both mi2g and ICG say the vast majority of serious damage from cyber-attacks is caused by organizational insiders. That means disgruntled current and former employees, along with consultants and others with trusted access. What can you do? Monitor and vet your trusted personnel more closely, says mi2g.

Most organizations say they're getting more serious about security. A recent Gartner survey finds that **"data security concerns"** [117cm] are the second most important priority for CIOs, only slightly behind "costs and budget pressures."

Yet vulnerabilities are huge. For instance, contrary to popular perception, open-source software has gaping security problems. A recent Aberdeen Group report stated, "Open-source software...is now the major source of elevated security vulnerabilities for IT buyers."

It added, "Unix- and Linux-based systems are just as vulnerable to viruses, Trojan horses, and worms [as those from Microsoft]. Furthermore, Apple's products are...vulnerable now that it is fielding an operating system [OS X] with embedded Internet protocols and Unix utilities." This Mac user wasn't thrilled by that.

And Microsoft, while taking many steps to increase security for its customers, is also adding to their headaches. In a policy announced late last year, it decreed that henceforth software will no longer be supported indefinitely with free updates and security patches, though support will always last a minimum of five years. Support for MS-DOS, Windows 3.X, Windows 95, and Windows NT 3.5X has already expired.

But users of the world's most popular server software, Windows NT 4.0, face a decision soon. IDC calculates that NT 4, which originally shipped in July 1996, is used in about half of the world's 8.2 million

Windows-based servers (as of year-end 2002). This June, Microsoft begins charging for non-security NT 4 upgrades, and on December 30, 2004 it will stop issuing all fixes and security patches for NT 4. So all those servers need to be upgraded soon. That's a good thing for Microsoft's revenues (and for PC sales), but I'm sure many owners of those increasingly vulnerable NT servers haven't got a clue. Microsoft intends to start telling them loudly this spring when it releases Windows Server 2003.

We've all been bequeathed the near-miraculous gift of one big global network-but we're only starting to recognize how vulnerable it makes us, too, in a time of crisis. As is so often the case, the gift brings with it huge responsibilities.

<http://edition.cnn.com/2003/TECH/ptech/03/20/fortune.ff.cyberattacks/index.html?iref=allsearch>

38. November 20, 2002

Military intelligence system draws controversy

WASHINGTON (CNN) -- The Pentagon said Wednesday that it's working to develop a powerful information-gathering system designed to uncover possible terrorists before they strike, but the plan is already coming under fire from civil libertarians who say it would violate Americans' constitutional rights.

The program, called the Total Information Awareness (TIA) system, would be able to search through "vast amounts" of data -- such as credit card records, passport applications, driver's licenses, arrest records, and the purchases of guns, chemicals or airline tickets [118cm] -- for patterns that could indicate terrorist activity, Defense Undersecretary Pete Aldridge said.

The system would have a rapid language translation feature that would connect domestic databases with ones in other countries, as well as decision-making tools to aid communication and analysis between agencies. Aldridge said agencies such as law enforcement departments, which can already get similar information, would be hooked into the network.

"We are in a war on terrorism, we are trying to prevent terrorists acts against our country. We are trying to give our people who understand and try to track down the terrorists ... a sufficient set of tools," Aldridge said.

Critics of the program have asked how much freedom Americans must give up in the pursuit of potential terrorists -- a debate over civil liberties vs. protecting the homeland.

"If the Pentagon has its way, every American -- from the Nebraskan farmer to the Wall Street banker -- will find themselves under the accusatory cyber-stare of an all-powerful national security apparatus," said Laura W. Murphy, director of the Washington office for the American Civil Liberties Union.

"So much for the presumption of innocence and the right to privacy," said George Getz, a spokesman for the Libertarian Party. "Unless this Orwellian project is dismantled, innocent Americans will suffer under the kind of high-tech, 24-hour surveillance that the Stasi and the KGB would have envied."

Aldridge sharply disputed such claims, and said it is "absurd" to think the Defense Department is "trying to become another police agency."

"The bottom line is this is an important research project to determine the feasibility of using certain transactions to discover and respond to terrorists before they act," Aldridge said.

"If it proves useful, TIA will then be turned over to the intelligence, counter-intelligence, and law enforcement communities as a tool to help them in their battle against domestic terrorism."

He said those agencies would have to use the same processes they use now to make sure that individual rights are protected.

Concerns also have been raised about the project's developer, John Poindexter, the embattled Reagan national security adviser who was indicted and sentenced for giving false testimony to Congress about his role in the Iran-Contra scandal. His conviction was later overturned.

"This is a program that incorporates all of the 'Big Brother' operations that the American public has feared from its government all these years and that the Constitution has protected us from -- spying, invasion of privacy, you name it," [119wa] said Peter Kornbluh, a senior analyst at the National Security Archive at George Washington University. "And Admiral Poindexter, of all people, is now in charge of that program."

Aldridge, however, was quick to note that Poindexter has a doctorate in physics and is more than capable of developing such a project. Aldridge also stressed that Poindexter would not be involved in intelligence gathering if the project is successful.

"What John Poindexter is doing is developing a tool, he is not exercising the tool, he will not exercise the tool. That tool will be exercised by the intelligence, counterintelligence, and law enforcement agencies," Aldridge said.

The new data-gathering technology is being developed under the auspices of the Defense Advanced Research Projects Agency, or DARPA.

<http://edition.cnn.com/2002/US/11/20/terror.tracking/index.html?iref=allsearch>

39. November 17, 2002

Indonesians take protests to the net

From Atika Shubert - CNN Correspondent

JAKARTA, Indonesia -- Anti-Australian protests have been widespread in Indonesia in recent months, and become particularly intense since the October 12 nightclub bombings in Bali.

But the form the protests have taken has transformed from the street rallies witnessed last week in Jakarta when students demonstrated against terror-suspect raids targeting Indonesian families in Australia. Now, political protest is taking a different, high-tech, form.

More than 200 websites have been hacked or defaced by Indonesian hackers, since the Australian security raids.

Hundreds of Australian websites have been vandalized and defaced. Open the bigcountry.com.au site and you get this message instead: "Who is the Terrorist? We or You?". [120wb]

The culprits are Indonesian hackers, often young college students, looking to make a name for themselves in cyberspace. They are increasingly latching onto political protests to gain hacker fame, this time focusing on the Australian terror raids.

"In my opinion they're doing it just for fun," said Budi Rahardjo, an Indonesian computer security analyst.

"Political reason? Yes, probably a little. But mostly for fun. Just for gaining popularity," said Rahardjo.

"I guess they do feel that they are heroes. But most people don't believe that. In my opinion, cracking websites, that's not a hero at all."

Neighbors Indonesia and Australia have often had strained relations, a situation made worse by Australian support for East Timor's independence vote in 1999.

With the majority of the deaths in the Bali tragedy Australian tourists, Canberra has turned its focus to potential terror links within Australian shores.

Commercial targets

In addition to website vandalism, credit card fraud is rampant in Indonesia.

Most of it occurs in cyber cafes where you pay per minute, log on with your favorite computer nickname, hack and leave without anyone knowing who you are. Small businesses with outmoded computer protection bear the brunt of a so-called cyber attacks. [121cm]

Most are simply an easily fixed nuisance. But commercial websites incapacitated by an attack do lose money.

Now, Indonesia's hackers are threatening to step up the cyber war by tampering with routing systems that could shut down commercial sites for days. [122in]

Computer security experts say in a cyber war your best offense is a good defense. Keep your system upgraded, patch the security holes and install a firewall that prevents unwanted users from coming in.

If you don't, they warn, you leave yourself open to a cyber attack.

<http://edition.cnn.com/2002/WORLD/asiapcf/southeast/11/17/indo.hacking/index.html?iref=allsearch>

40. April 12, 2002

Hack attack, how you might be a target

By Pia Turunen

LONDON, England (CNN) -- Imagine waking up one morning to discover all your personal information has been stolen.

Your bank account has been cleaned out. The project you have been working on for the past six months has vanished. Your e-mails have been infected with a virus that has copied itself to all the people you have ever exchanged e-mails with. You try to make a call but your mobile phone's address book has been deleted remotely. [123cm]

Then things start to get really bad.

The computer system protecting your house no longer recognises you because the data containing your retina scan has been stolen. Now you are barred from your home, so you alert the police, but they are very keen to talk to you about your recent credit card purchase in Panama.

It sounds like technophobe's worst nightmare, but it could be reality.

In America, the FBI reports that cybercrime is rising, costing individuals and businesses billions of dollars. And the war on this kind of crime seems hard to win.

Marius Nacht, Senior Vice President at Israeli security technology company Check Point, says: "There is no easy way to say this, but if your PC is connected to the Internet, there is someone trying to attack it within 15 minutes of the connection being made."

Hackers are not looking for individuals, they are looking for any vulnerable computers. [124cm]

Sometimes computer users are helping the hacker unknowingly. Most people do not use complex methods to protect personal information because most people think they have very little a hacker might want.

So they use their birthday as a PIN code to access bank accounts, mobile phones and other personal information, to make it easier to remember.

A recent survey from U.S. security company Pentasafe suggested most people do not know how to set up a password that cannot be easily worked out. Pentasafe's marketing director David Blackman said: "Hackers work very logically. Once they uncover one password to the PC, getting the one to the cash point isn't rocket science. There is software available on the Internet which can calculate passwords."

Even a well chosen password may not be enough to protect digital information as some hackers use sophisticated methods when trying to break into our computers.

Going undercover

Hackers can often get confidential information effortlessly [125cm], according to Neil Barrett, digital crime expert at International Risk Management, a London-based security consultant.

"The most likely way for bad guys to break into the system is through social engineering. This involves persuading administrators or telephonists to give details of passwords or other things by pretending to be staff, suppliers or trusted individuals -- even police officers. They could be even masquerading as a computer repair man to get an access to the premises."

Social engineering a devastating weapon in the hacker's armoury. It targets and exploits computer network's most vulnerable aspect -- people. Barrett added: "As protection measures for companies and individuals become ever more impregnable, social engineering is bound to become more popular among cyber criminals."

And if the hackers do not get you, a virus might.

Last year one in 350 e-mails sent contained a virus, while the notorious "Code Red" alone cost businesses worldwide about \$2.6 billion, according to the Confederation of British Industry (CBI).

Luckily most Web surfers are aware of viruses, the CBI said. But a new, more deadly virus is on the horizon, according to ISS, a UK Internet security firm.

"Hybrid viruses like 'Nimda' and 'Code Red' are especially dangerous because they combine viral spreading capabilities with hack attack techniques," the company said.

Clever hackers can secretly install a back-door "Trojan horse," a small program designed to spy on people's keyboard movements and record the information typed.

"Trojans are different from viruses because they can lurk in PCs without anyone noticing and can spy on the computer user's activities then send this information back anywhere in the world," says technical specialist Graham Cluley at UK-based Sophos anti-virus.

Cybercriminals are targeting desktop computers connected to the Web and the growing array of pocket PCs and hand-held devices. As mobile phones get smarter and carry large amounts of personal data, they too become easy meat for malicious coders.

"People forget that the mobile phone is a small computer with memory, important data and an access to the Internet. [126cm] These devices should be protected equally carefully, if not more, than network computers," says Juha Snellman, vice-president of Finnish wireless security specialist SmartTrust.

Many people in the UK are already suffering from text message spam, or SMS junk mail from rogue mobile firms. The first mobile virus was found more than a year ago. Called "Timofonica," it did not start an epidemic, but Snellman warns: "Wireless security threats grow as the functionality of the handsets increases.

"Hackers are always one step ahead and we must stay vigilant to keep up with them."

<http://edition.cnn.com/2002/TECH/ptech/04/12/hack.dangers/index.html?iref=allsearch>

41. November 11, 2002

Indonesian cyberprotesters target Australia

JAKARTA, Indonesia (CNN) -- In Jakarta last week students gathered to demonstrate raids targeting the homes of Indonesians living in Australia.

Chants, banners, burning the Australian flag -- all normal fare for a demonstration -- but now, political protest is taking a different form.

In cyberspace hundreds of Australian websites have been hacked, vandalized and defaced. [127wb]

One of the targets was www.bigcountry.com.au. Visitors to the website were greeted with the message: "Who is the Terrorist? We or You?"

The culprits? Hackers, often young college students looking to make a name for themselves online, latch on to political protests to gain fame and notoriety.

And this time they are focusing on the Australian terror raids.

"In my opinion they're doing it just for fun," says computer security analyst Budi Rahardjo.

Is there a political reason? "Yes," he says, "probably a little. But mostly for fun -- just for gaining popularity

"I guess they do feel that they are heroes. But most people don't believe that. In my opinion, cracking websites, that's not heroic at all."

Anonymous

In addition to Web site vandalism, credit card fraud is rampant.

Most of it occurs in cyber cafes -- where users pay per minute, log on with a computer nickname, hack and leave without revealing their identity.

Small businesses with outmoded computer protection bear the brunt of a so-called cyber attacks.

Most are simply a nuisance and easily fixed, but commercial websites incapacitated by an attack, do lose money.

Now, Indonesia's hackers are threatening to step up the cyberwar by tampering with routing systems that could shut down commercial sites for days. [128wb]

Computer security experts say in a cyberwar your best offense is a good defense.

System upgrades, security patches and firewalls can help protect Web sites from potential attack.

<http://edition.cnn.com/2002/WORLD/asiapcf/southeast/11/11/indo.aus.internet/index.html?iref=allsearch>

42. February 4, 2002

Rumsfeld: Cyberwar among possible threats

By Martyn Williams

(IDG) -- The vulnerability of U.S. information networks and a belief that a future attack against the U.S. may be launched in cyberspace is high in the mind of U.S. Secretary of Defense Donald Rumsfeld as he plots to change the U.S. armed forces so they can better defend against unconventional threats.

"Our challenge in this new century is a different one," Rumsfeld told an audience at the National Defense University in Washington, D.C., on Thursday, according to a transcript. "It's really to defend our nation against the unknown, the uncertain and, what we have to understand, will be the unexpected. That may seem on the face of it an impossible task but it is not."

"There is a great deal we can learn from this first war of the 21st century, but we cannot and must not make the mistake of assuming that terrorism is the only threat. The next threat we face may indeed be from terrorists, but it could also be cyber-war, a traditional state-on-state conflict or something entirely different," said Rumsfeld.

With this as a background, Rumsfeld said he has six goals for transforming U.S. defense strategy including "to protect our info networks from attack," and "to use info technology to link up different kinds of U.S. forces so they can, in fact, act jointly." [129in]

His speech came just over four months after the attacks on the World Trade Center and the Pentagon -- attacks that served to highlight the vulnerability of key telecommunications and information networks.

In the wake of the attacks, some telecommunication networks in the New York City area were paralyzed after several key exchanges were taken offline, either because of damage to cables, the buildings they are housed in or a loss of power. Beyond New York, where telephone calls went unconnected and bank ATM machines were offline, the effects spread around the world as trading on the New York Stock Exchange and Nasdaq markets was suspended and Internet traffic routed through New York was slowed. [130in]

The growing importance of infrastructure systems, such as telecommunication and non-IT sectors like banking and finance, and the chaos feared if the systems were attacked led to the creation of the National Infrastructure Protection Center [131in] in February 1998. Located at the U.S. Federal Bureau of Investigation's headquarters in Washington, the NIPC brings together representatives of national, state and local agencies and the private sector to work on protecting key sectors.

To date, the NIPC has spent much time on IT issues, tracking large scale outbreaks of computer viruses, such as the "Code Red" worm that hit in early September last year and hacking cases, such as denial of service attacks against major Web sites.

<http://archives.cnn.com/2002/TECH/internet/02/04/military.preparation.idg/index.html>

43. January 8, 2002

Report: Cybervandalism jumped in 2001

(IDG) -- The number of vandalized Web sites recorded by defacement archive Alldas.de jumped in 2001 to 22,379, over five times more than the 4,393 defacements logged in 2000.

Mostly Brazilian cybervandals are responsible for the surge in defacements, according to Fredrik Ostergren, a Sweden-based security analyst and spokesperson for Alldas.de. He also said that more Internet users in general are trying out tools to hack into Web sites.

"Many of the defacers we have in the scene today are located in Brazil," [132cm] he said. "One of the reasons for the increase in defacements is more people getting connected to the Internet, especially in Brazil."

A defacer is a hacker who breaks into a Web server and defaces the Web site by replacing or altering the front page.

Alldas.de has been tracking defacements since 1998 and offers snapshots of defaced Web sites as well as security analyses and statistics. The site gained in popularity after its U.S. counterpart Attrition.org stopped hosting copies of defaced sites in May.

More exposure for Alldas.de helped the Web site increase the number of defacements logged, although Alldas.de had a big network before Attrition stopped archiving, Ostergren said.

Current Events Contribute

The number of defacements was especially high in spring. The organization identified 3003 sites altered in April and 3431 in May. U.S. and Chinese hackers were said to be fighting a 'cyberwar' in those months after a U.S. spy plane crash-landed in China on April 1, and the FBI warned at the time of increased attacks by Chinese hackers.

[133cm]

Most popular among cybervandals are well-known sites. [134cm] For example, last year SANS Institute and Amnesty International fell victim to defacers, Ostergren said.

More than 60 percent of the defaced Web sites logged to date by Alldas.de were hosted on a Microsoft Windows server, and 20 percent were on a server running Linux.

Attackers mostly exploit known vulnerabilities in server software with hack software that is readily available on the Internet. Applying security patches will keep most defacers out, according to Ostergren.

"Mostly well-known exploits are used to penetrate servers. Secure yourself! I can tell for sure that nothing is secure, but please add the latest patches to your Web server, it is not hard, administrators," Ostergren called out.

Defacing will continue in 2002, Ostergren said, but he doesn't expect a big increase in the number of defacements.

"I don't think it will increase much, hopefully decrease as administrators wake up and secure their servers," he said.

<http://edition.cnn.com/2002/TECH/internet/01/08/cybervandal.jump.idg/index.html?iref=allsearch>

44. July 17, 2001

Decoy PCs give hackers a security lesson

(IDG) -- For the best security, hack the hackers, suggest security experts who have spent several months watching malicious intruders break into disguised decoy systems on the Internet.

The informal study found it was only two to four days before hackers attacked an unprotected Windows 98 system with its file sharing enabled. Hackers attacked one such system four times in a five-day period. The fastest takeover was 15 minutes, when a hacker broke into a PC running Red Hat Linux 6.2. [135cm]

An ongoing organization may form out of this informal research, known as the HoneyNet Project. Security researchers created a network of PCs they dubbed honeypots, named for the attractive but troublesome favorite treat of children's book character Winnie the Pooh. In this case, the group placed PCs on the Internet in various states of security and designed to attract hackers, says Lance Spitzner, who described the experiment at the final day of the annual Black Hat Briefings security conference here last week.

Some of the computers ran with the default installations of their operating systems, while team members patched others with the latest security fixes. Then they placed the PCs on the Internet in such a way that HoneyNet Project members could closely observe the systems without being noticed by hackers. They recorded the exact methods hackers used to break into those and other systems, and even recorded the text conversations of a notorious group of Web page defacement hackers known as GForce Pakistan. [136wb]

"Even though the technical proficiency of the [GForce Pakistan] hackers was pretty low, they were able to cause a lot of damage," says security consultant George Kurtz, also a speaker.

Gathering Intelligence

The honeynet served as an intelligence gathering system, says Spitzner, a former Army officer who worked in a tank rapid deployment force.

"It's about teaching people how the attacks spread to other systems," Kurtz says. "You would never find a for-profit company that would say, 'hey, we've been hacked, want to take a look at what they did?'"

Commercial intrusion detection systems can sometimes let you know if you're being hacked, Kurtz adds. But simple detection can't tell you "the mindset or motivations of the hacker."

HoneyNet Project participants encouraged Black Hat attendees to set up honeypots on their own networks, and to share their findings with the HoneyNet Project.

If more honeypots are in place, hackers might think twice before trying to break into a particular network, the speakers suggest. It could be the Internet version of the deterrence that security cameras provide to potential bank robbers.

"If we can make [the hackers] have to keep looking over their shoulders, so much the better," adds group member Edward Skoudis. "A presumption of surveillance goes a long way in preventing hack attacks in the first place."

The Honeynet founding group, composed of security and network information specialists from many of the largest computer networking products companies, plans to continue operations as a nonprofit organization.

Their efforts are just another in the cyberwar on hackers, a recurring theme of the Black Hat event.

Legal Weapons

In fact, international laws of conflict apply even in cyberspace, says Walter Gary Sharp Sr., a former military legal counsel. He spoke on "Key Legal Implications of the Computer Network Defense," addressing a crowd that included people who may have considered defending their networks by hacking the hackers.

The rules of the Geneva Conventions and the United Nations charter apply to international hacker attacks as well, Sharp says. Those rules vary if the hacker's nation of origin is at peace or in armed conflict with the nation where the targeted system resides.

Lawmakers and international agencies are clearly concerned about computer security issues, the speakers suggest. One, cryptographic analyst Bruce Schneier, says he is testifying next week before a U.S. Senate panel on the status of computer security and proposed improvements.

"Security in the real world is all about risk management," Schneier says. He suggests the insurance industry might have a useful role.

"The insurance industry drives security in the real world," he says. "They write policies based on the countermeasures you have in place to protect yourself."

If companies who use software could buy "antihacking insurance," software quality might improve, Schneier says.

"Right now, Microsoft has no financial incentive to make Windows secure," Schneier says.

But if customers held insurance policies against security problems in programs, software developers would need to rapidly plug holes and repair weaknesses in their products -- or face ever-higher insurance premiums.

<http://edition.cnn.com/2001/TECH/internet/07/17/honeynet.project.idg/index.html?iref=allsearch>

45. May 11, 2001

Analysis: U.S.-China 'cyberwar' fires blanks

(IDG) -- What if they gave a cyberwar and nobody came? That seems to be the situation days after the end of what was described by some as a "cyberwar" staged by Chinese hackers against the U.S. in retaliation for the death of Chinese

pilot Wang Wei in early April. Doubts linger in some Internet security experts' minds, however, whether this "cyberwar" was the week's real threat.

A Chinese hacker group, the Honker Union of China, issued a statement to the Chinese portal Chinabyte earlier in the week declaring a truce and saying that they had reached their goal of hacking 1,000 U.S. sites. [137cm]

But a truce was perhaps unnecessary, as nothing approaching a war ever materialized over the 10 days since the U.S. National Infrastructure Protection Center issued a warning [138in] saying that Chinese hackers would take April 30 to May 7 to attack U.S. Web sites to commemorate Wang Wei and celebrate May Day (May 1), Youth Day (May 4) and mark the anniversary of the U.S. bombing of the Chinese embassy in Belgrade, Yugoslavia (May 7).

Rather, the only traces of any conflict are a series of Web page defacements showing pictures of Wang Wei -- who died when his plane crashed into a U.S. spy plane -- and promising to fight "hegemony" and "unify the motherland" on one hand and a good deal of frequently vulgar anti-Chinese sentiment from U.S. hackers on the other. Both were complemented by a pile of press releases from eager computer security firms warning users of the danger from "this new form of terrorism" and offering up sources to reporters, as well as a flurry of news stories. Some security experts say that the real problem that cropped up over the last week was that more computers may be potentially vulnerable to being used in denial-of-service attacks due to the spread of so-called Internet worms.

Web pages defacements are a form of slightly sophisticated digital graffiti. Like graffiti, they involve a hacker leaving a message or an image on a Web site to show that they succeeded in cracking it. However, unlike graffiti, Web page defacement requires that a hacker break into a Web site, a bit harder than simply spraying paint on the side of a building. This sort of attack, however, is equivalent to "pouring paint on some ... person's building," said Alan Paller, director of security research at the SANS Institute.

Two high-profile incidents started the week of defacements when hackers defaced the Web sites for the U.S. Department of Labor and two sites controlled by the U.S. Department of Health and Human Services -- Health.gov and Surgeongeneral.gov -- with pro-China messages [see "Two U.S. government sites hacked over weekend," April 30]. In the days following those hacks, a number of other low-level U.S. government and military sites were hit, with similar postings left on them. [139wb]

U.S. hackers responded in kind, with a flurry of hacks against Chinese government and private sector sites. The mirrors -- or copies -- of defaced pages at security Web site Attrition.org show that U.S. hackers were still going strong Monday, though the efforts of their Chinese counterparts have largely abated.

Such, evidently, is the fate of the most public face of the cyberwar.

The Web page defacements of the last 10 days were business as usual in the computer security field, said Shawn Hernan, the vulnerability handling team leader at

CERT/CC (Computer Emergency Response Team Coordination Center), a computer security research and development facility located at Carnegie Mellon University.

The week's events "were certainly not remarkable in the scope of the activity we saw, regardless of (where the hacks came from)," he said.

The source of the hacks is difficult to establish or trace. Because hackers can take over machines based in locations other than the hacker's own, hacks can appear to be coming from one location, when in fact they are only be routed through that PC from a different source.

"Without police work, you really can't know" the actual source, nationality or motivations of a hacker, Hernan said.

Because of this, there is no way to "distinguish state-sponsored terrorism from bored teenagers from people who have compromised Chinese sites from people trying to impersonate these groups," he said.

Though the defacements add up to only minor incidents with indeterminate origins, there is another, larger issue that has been obscured due to the attention given to the defacements, according to SANS' Alan Paller. The last week has seen a rise in the spread of the Lion worm on Linux systems worldwide, he said [see "Dangerous Linux worm in the wild," March 23]. Data from Incidents.org, an information-sharing organization which boasts over 1000 members, including SANS, shows that at least 5,000 computers have been infected with the worm in the last 12 to 14 days, he said. Computers infected with the worm can then be used in distributed Denial of Service (DoS) attacks, he said. [140in]

The Lion worm was written by Lion, the founder of the Honker Union of China, according to a Web report on the worm by white-hat (i.e., nonmalicious) hacker Max Vision. The Honker Union of China defaced a number of Web pages over the last 10 days. Several worms, including Lion, have code that sends passwords and other information to .cn domain names (.cn is China's country address), but because of the nature of the Net and hacking, it can't be known whether that is actually someone in China or an imposter, CERT/CC's Hernan said.

Though the week's news focused on the defacements, because they were "the only visible part," hackers now have a "strong DoS base" from which to launch attacks, Paller said. The news was about defacements, but the week was about finding Zombies (machines that can be taken over for DoS attacks), he said.

Paller isn't sure that the spread of the Lion worm can be tied to the Wang Wei incident. "You don't know, you never know" why hacking incidents happen, he said. Hackers don't usually offer information about their motivations or affiliations, he said.

The spread of Lion, and thus of zombies, is like an earthquake, Paller said. After rumblings, once tension has built up enough, something will happen, "someone will let loose."

CERT/CC's Hernan agrees that the Web page defacements were not the most serious security issue to arise in the last ten days, instead pointing to the spread of the Lion worm, the flaw found in Microsoft Corp.'s IIS 5.0 and the new sadmind/IIS worm as the most serious threats.

But problems like these are nothing new, Hernan said.

"Everyday large numbers of intruders (try) to break into as many machines as they can," he said. "There are thousands upon thousands of probes and scans."

The proper response to security flaws, he said, is to patch computer systems as soon as holes are identified and fixes are made available, use anti-virus tools and stay informed.

"The key message is vigilance," he said. "I'm not sure it's possible to be too vigilant."

<http://edition.cnn.com/2001/TECH/internet/05/11/china.cyberwar.idg/index.html?iref=allsearch>

46. May 10, 2001

Epic cyberattack reveals cracks in U.S. defense

(IDG) -- Although the feds aren't talking publicly about a three-years-plus cyberattack believed to be coming from Russia, a member of the National Security Agency's Advisory Board said the case, dubbed "Moonlight Maze," reveals huge cracks in the U.S. government's defense system.

"The fact of the matter is our defense is a shambles, really," said James Adams, who also is chairman of security consultancy iDefense, based in Fairfax, Va.

"We need a deterrent strategy for cyberspace just like we have for nuclear war or conventional war," he said. "The Department of Defense has to step up to the plate because they have the capability and the responsibility."

Adams, the author of a book on cyberwarfare as well as a former writer and Washington bureau chief for the London Sunday Times, details the severity of the situation in an article in the latest edition of Foreign Affairs magazine.

The Moonlight Maze stealth attack, which **has targeted sensitive but unclassified information** since it was launched in March 1998, is the "largest sustained cyberattack" on the U.S., according to Adams. He said the U.S. government has since been tracking intrusions into the computer networks of the Pentagon and other government agencies, as well as attacks on private universities and research labs.

The hackers, Adams said, have managed to sneak into those computer networks and leave so-called back doors, which can consist of code or instructions planted into existing systems that easily enable hackers to slip back into a system and steal information or do other damaging things. [141cm]

Investigators don't yet know how many systems have been penetrated, exactly how they've been compromised, or who is responsible, though some of the attacks appear to have originated from Russian Internet addresses, according to Adams.

U.S. officials complained formally to the Russian government last year to no effect, Adams said. Calls to the State Department to confirm this were not returned, and a spokeswoman from the FBI's National Infrastructure Protection Center declined to comment.

Adams said he believes the attacks are a concentrated or coordinated effort. Possible suspects include organized crime or other groups that can make money from selling sensitive U.S. information, but Adams said he thinks the Russian government is involved, or at least tolerating, the actions.

Russian hackers have been linked to a number of cases of online theft of credit cards and extortion, including a case involving the credit card numbers of 300,000 CD Universe customers last year. [142cm] In March, the FBI warned companies conducting business online of the threat posed by organized hackers in Russia, Ukraine and other former Soviet countries. However, the e-commerce-related hacks, investigations into which the Russian government has cooperated in, are not related to the Moonlight Maze case, Adams said.

Reports on the threat of cyberterrorism and cyberwar have been released since at least 1991, when Winn Schwartau, author of several books on security, warned Congress of a "digital Pearl Harbor." However, Schwartau and others warn that exaggerating the risks of such attacks can lead people to dismiss them.

"I'm more concerned with the private sector's ability to deal with" cyberattacks, said Michael Assante, VP of intelligence at Vigilinx, a provider of managed security products and services based in Parsippany, N.J. Private companies don't have the resources the government has in order to protect themselves, he added.

Meanwhile, the Russian president and chief executive of a Dublin, Ohio-based software company said it's almost irrelevant where the attacks are coming from, especially because hackers can so easily masquerade their locations.

"You have to be worried about hackers no matter where they're coming from," said Ratmir Timashev of Aelita Software, which has its primary software-development center in St. Petersburg.

In 1999 and 2000, there were more than 1,300 cyberattacks on the Air Force, Army and Navy sites, and more than 700 of them were "serious," according to the General Accounting Office. The FBI is looking into more than 100 cases involving computer intrusions into more than 1,200 government systems, NIPC Director Ronald Dick told Congress in April.

<http://edition.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/index.html?iref=allsearch>

47. May 2, 2001

U.S., Chinese hackers continue Web defacements

(IDG) -- Two days into what was supposed to be a 'cyberwar' launched by Chinese hackers in retaliation for the death of Chinese pilot Wang Wei, a number of U.S. government Web sites have been defaced. But groups of U.S. hackers have entered the picture as well, hacking Chinese sites.

Attrition.org, a nonprofit security site which hosts mirrors of defaced Web pages for research purposes, has mirrors of dozens of pages that have been cracked by both U.S. and Chinese hackers in the past two days. Among them are a number of U.S. government and military sites, including the U.S. Geological Survey, Eastern Region, the Hurricane Liaison Team of the Federal Emergency Management Agency and the headquarters of the commander of the Naval Surface Force of the U.S. Atlantic Fleet.

These sites, and a number of others, have been altered to include anti-American, pro-China messages, such "Beat down Imperialism of America." A number of sites bear the standard message from the "Honkers Union of China," who hacked into the U.S. Department of Labor's Web site over the weekend. Government sites are not the only ones to be hit, however, as a number of private sector Web sites were also defaced.

[143wb]

A number of other sites, including some associated with the Department of Energy and United Press International, were hit, according to a report in Tuesday's Los Angeles Times.

Over the weekend, a handful of U.S. government sites were hacked, including the U.S. Department of Labor and the Department of Health and Human Services' Health.gov and Surgeongeneral.gov.

Hacks by Chinese groups were expected after the National Infrastructure Protection Center issued a statement last week warning of just such an event. What was, perhaps, less expected was that U.S. hackers would retaliate in kind. A number of Chinese sites, mostly private firms, rather than government sites, have been defaced, according to Attrition's listing.

The defacements indicate that the hacks are in response to Chinese hacks of U.S. sites, and exhort U.S. hackers to work together to hack Chinese sites. One group, called "Project China," promises a coordinated group of hackers will attack Chinese sites over the next two weeks.

Chinese pilot Wang Wei was killed in early April when his plane collided with a U.S. spy plane off the coast of China. The collision touched off a weeks-long international incident that ended with the U.S. flight crew being returned to America.

<http://edition.cnn.com/2001/TECH/internet/05/02/china.hacks.idg/index.html?iref=allsearch>

48. April 18, 2001

Special Report: Crime on the Internet

(CNN) -- As technology becomes more sophisticated, so does cybercrime. U.S. intelligence and law enforcement officials say that the future of national security -- and the personal safety of everyone -- may hinge on how prepared they are to fight crime on the Internet.

FBI officials say that technology-enabled terrorists are looking for new ways to strike at **critical national infrastructure [144in]** and that organized crime rings are extorting companies by **stealing proprietary information from the Web. [145cm]**

Child pornographers have thousands of pictures at their fingertips, and according to law enforcement officials, easy access to Web sites is now attracting a younger audience who have begun experimenting with the production and publication of "peer" pornography.

U.S. government agencies, including the Secret Service, FBI, State Department, Customs Service and the Department of Defense have all committed money and manpower to cybercrime-fighting units. But officials say that despite these efforts, the United States is still not completely up to the task of preventing or dealing with all cyberattacks.

Those on the front lines of the cyberwar cite a number of problems in fighting technology-savvy adversaries. Recruiting people with advanced technological training on government salaries remains difficult -- the salaries are low compared to those at the corporate level.

As soon as law enforcement develops a technological fix for a problem, cybercriminals often have already found new technological strategies.

And deciding where to commit resources can be puzzling: Who would have targeted Oklahoma City as a possible site for a terrorist act before 1995?

How does this affect you? In a three-part series on cybercrime, CNN Justice Correspondent Kelli Arena examines the issues and the steps you can take to protect yourself, whether it's protecting your personal information or restricting your children's time on the Web.

<http://edition.cnn.com/2001/LAW/04/16/cybercrime.overview/index.html?iref=allsearch>

49. January 24, 2001

Could a cyberwar cripple the U.S.?

(IDG) -- It's April Fool's Day, 2002. Glitches in air traffic controller screens nearly cause a collision above New York's LaGuardia Airport. Two weeks later, California Independent System Operator Corp., which controls California's power grid, somehow misplaces an electrical energy order to Southern California Edison, leaving

two-thirds of San Diego in the dark. Then in May, a high-power microwave burst fries the electronics at an abortion clinic in Virginia. [146in]

Hypothetical "information warfare" (IW) exercises like these are being played out around the country in preparation for what politicians, the military and law enforcement officials fear will be an orchestrated cyberattack on critical U.S. infrastructure companies. [147in] The theory goes that if a well-funded, organized series of cyberattacks were to strike at a target's economic and structural nerve centers, it would send the target society into chaos and make it difficult for the military to communicate and move troops.

This particular information war game was played out among 75 IT executives attending an IW workshop at the SANS Institute's Joint Computer Security Conference in Monterey, Calif.

"In the worst-case scenario, every major industry sector would be affected," says Stephen Northcutt, a SANS fellow and a former military IW expert who led the animated workshop at the conference. Note that most of the targets in Northcutt's IW games are private-sector companies.

"When you're talking about information warfare, you're talking about information systems used to cripple the government and economy," says John Tritak, director of the Critical Infrastructure Assurance Office (CIAO) in Washington. "Close to 90 percent of those critical infrastructure companies are privately owned and operated."

The CIAO, formed in 1998 under presidential directive PDD-63, outlines a national infrastructure protection plan to bring better security and reporting to the telecommunications, transportation, emergency services, energy and financial industries [148in]. The directive deems those industries as critical to the nation's operational infrastructure. Although President Bush isn't bound to support the directive, Tritak and others say they hope PDD-63 will remain in effect.

In two years, IW preparedness has moved forward the fastest in the highly regulated and well-organized financial, energy and telecommunications sectors, say Tritak and others. But IT leaders in the private sector say they're hesitant to report incidents to agencies like the CIAO and the FBI. Still, Tritak says the agencies need this information for intelligence and predictive analysis.

While the impact of IW bears the same uncertainty as Y2K, many IW experts say cyberterrorism and cyberwarfare are inevitable. In the past year, hacking hobbyists have shown how easy it is to propagate viruses throughout Internet-connected mail systems [149wb]. They've also shown they can hack armies of unwitting computers and make those computers do their bidding. Now, the U.S. government is thinking about what terrorists with more resources could accomplish. And so are countries like China and Russia, which are developing their own IW capabilities, according to Richard Power in the book Tangled Web.

Moving Mountains The directive that created the CIAO is a national defense document that, ironically, relies on the private sector to accomplish its mission. Telling that to executives hasn't been easy.

"The concept of information warfare doesn't present a compelling case to the CEO and the board, whose responsibility is to their shareholders and customers," Tritak explains. "But as they begin to see that operating in a reliable and secure business environment is part of taking full advantage of the Information Age, they get it."

To make this business connection, the CIAO recruited a private-sector security expert, Nancy Wong, from San Francisco-based Pacific Gas and Electric Co., to help develop a business-friendly framework and get the message out. Wong soon learned she had a third challenge: keeping government, in its zeal to protect, from crossing constitutional lines between public and private sectors.

"We put in place a road map to identify who are the people who have the most influence in business risk management -- financial security analysts, bond raters, corporate executives, even auditors," Wong says. "We're using existing networks by cascading information through their members to the people who communicate it even further."

The networks Wong refers to include industry associations like the Institute of Internal Auditors, the North American Energy Reliability Council and the National Security Telecommunications Advisory Committee. [150in]

The CIAO's strategy of taking advantage of existing networks -- and their built-in emergency preparedness -- helped speed along the formation of the first of two Information Sharing and Analysis Centers (ISAC) for the financial and telecommunications industries. ISACs are privately owned, industry-specific cooperatives through which the government plans to channel warnings out to the private sector. The government also plans to use ISACs to gather intelligence it needs to better predict an orchestrated attack.

Energy and technology centers are expected to be completed by the end of March. The long-standing emergency management methodologies and collaborative networks provide the framework for these infrastructure analysis and reporting structures.

Bruce Moulton, vice president of infrastructure risk management at Boston-based Fidelity Investments, explains, "If a failure occurs in the Northwest power grid, for example, the energy sector has processes to keep that power failure from rippling across the United States." [151in]

And because its core business is consumer trust, the financial services industry has particular impetus for security and disaster planning, says Moulton, who chairs the financial services ISAC. "We've already got a good framework of controls to protect against disruption and customer privacy violations," [152cm] he adds.

A Matter of Trust

But the biggest problem with this infrastructure plan is that businesses have a hard time visualizing the return on investment in risking corporate privacy by reporting breaches.

"The risks in reporting are clear: the fear of negative publicity, proprietary information shared in court, loss of public confidence or reduced trust in the economy itself," Harris Miller, president of the Information Technology Association of America, told an infrastructure panel last month at SafeNet 2000. [153in]

The question of reporting was one of the most nettlesome issues tossed around at SafeNet, where leading privacy and security professionals, educators, vendors and infrastructure companies met with government infrastructure protection heavyweights at Microsoft Corp.'s conference center in Redmond, Wash.

Meanwhile, industry leaders are awaiting the passage of a House bill, the Cybersecurity Information Act, that would reduce liability and antitrust action, along with actions brought under the Freedom of Information Act that are related to cyberinformation sharing.

Who Responds?

Such complexities spotlight the precarious relationships being forged among defense agencies, law enforcement bodies and the private sector, which all have stakes in the national infrastructure. On top of that, there's the sticky issue of jurisdiction.

Who responds to an orchestrated attack, particularly one that affects military operations and crosses state lines? The answer differs from region to region. But, absent a declaration of martial law, it wouldn't be the military.

"When we're at war, we just go blow up the bad guys. But domestically, our mission is different. We can't trespass [into private systems] when we chase the bad guys. And we can't blow up the bad guys, because the bad guys are an unknown," explained Jim Christy, a supervisory special agent at the Defense Department's Information Assurance Office, to a group of 400 officials at a state summit on cybercrime in Mesa, Ariz., in October.

So the burden of responding to private-sector calls for help will most likely fall to the FBI's InfraGard program, which itself is fishing for intelligence from corporations and private citizens. Many IT leaders say they don't trust the agency, especially given its poor sensitivity to business issues, including efforts to limit encryption exports, and most recently, its controversial Carnivore e-mail wiretapping system.

Meanwhile, Arizona has unveiled perhaps the most unusual plan on the drawing board today: Make the Air Force National Guard the nerve center for private-sector reporting and response, an idea that comes from Christy and Republican State Rep. Wes Marsh, who's also a member of the Air Force Reserve. Marsh says that because

members of the National Guard work full time in the private sector, they'd make excellent liaisons between the government and private sector.

Better Today

No matter how you look at these issues, the net result of the presidential directive is that security awareness is rising, ISACs are forming and executives are more clued in. In spite of raised awareness, internal and external cyberthreats continue to rise, according to a joint survey by the FBI and the San Francisco-based Computer Security Institute. And, in a nonscientific online poll by Computerworld last month, only 17 percent of 150 respondents said their companies were prepared to respond to an orchestrated, warlike cyberattack.

But is this work moving fast enough? "This is a race. If the industry doesn't learn to manage its risk in a prudent way and something like an Exxon Valdez happens, then you'll see a chilling effect as laws get passed during the crisis," says Tritak. "At the same time, if you try to overlay the risks and threats, you could lose your audience."

Already, international IW efforts are moving forward.

The U.S. military has publicly announced the formation of IW units. Cyberclashes between Israeli and Palestinian factions that shut down Israeli and Palestinian government Web sites [154wb] prompted the FBI to issue a warning to American businesses in October. In December, the FBI issued another warning of an "increase in hacker activity specifically targeting U.S. systems associated with e-commerce."

Yet in spite of these indicators, IW thinkers say a cyberwar is years away.

"Clearly, the eventuality of such an attack is present. That's what motivated [the Clinton] administration to move forward with a national plan," says Tritak. "But I don't think anyone has the cybercapability today to launch an attack that would cripple the nation's infrastructure [155in]. [The presidential directive] predicts such a scenario is still years away."

<http://edition.cnn.com/2001/TECH/computing/01/24/information.warfare.idg/index.html?iref=allsearch>

50. November 22, 2000

U.S. Army kick-starts cyberwar machine

IDG) -- The U.S. military has a new mission: Be ready to launch a cyberattack against potential adversaries, some of whom are stockpiling cyberweapons.

Such an attack would likely involve launching massive distributed denial-of-service assaults [156in], unleashing crippling computer viruses or Trojans, and jamming the enemy's computer systems through electronic radio-frequency interference [157cm]

An order from the National Command Authority - backed by President Clinton and Secretary of Defense William Cohen - recently instructed the military to gear up to wage cyberwar.

The ability of the U.S. to conduct such warfare "doesn't exist today," according to a top Army official speaking at a conference in Arlington, Va., last week.

"We see three emerging threats: ballistic missiles, cyberwarfare and space control," said Lt. Gen. Edward Anderson, deputy commander in chief at U.S. Space Command, which was recently assigned the task of creating a cyberattack strategy.

"Cyberwarfare is what we might think of as attacks against digital ones and zeros."

Anderson spoke about the Space Command's cyberwarfare responsibilities at the National Strategies and Capabilities for a Changing World conference. The event was organized by the Institute for Foreign Policy Analysis, Tufts University's Fletcher School of Law and Diplomacy and the U.S. Army. The conference attracted military top brass and international diplomats.

Anderson told attendees that the U.S. Space Command, the agency in charge of satellite communications, has begun to craft a computer network attack strategy. This strategy would detail actions to be followed by the Unified Commanders in Chief (CINC) if the president and the secretary of defense order a cyber strike. The CINCs are senior commanders in the Army, Navy, Air Force and Marines deploying U.S. forces around the world.

The information-warfare strategy will be detailed in a defense plan called "OPLAN 3600" that Anderson said will require "unprecedented cooperation with commercial enterprises and other organizations."

There's no set deadline for completing OPLAN 3600, Anderson told *Network World*. But he noted that other countries, including Russia, Israel and China, are further along in building their information-warfare capabilities.

Anderson said the U.S. may end up with a new type of weaponry for launching massive distributed denial-of-service attacks and computer viruses. "The Chinese recently indicated they are already moving along with this," he added.

In addition to the possibility of cybercombat between nations, the military acknowledges that terrorists without the backing of any country can potentially use cyberweapons to **disrupt U.S. telecommunications or banking systems that are largely electronic.** [158cm]

That's one reason the U.S. Space Command is joining with the FBI to build an information-warfare strategy.

"This requires a close relationship between military and law enforcement," said Michael Vatis, an FBI official who also spoke at the conference. He noted that the FBI will have to help determine if any cyberattack suffered by U.S. military or business entities calls for a military or law enforcement response.

"The Internet is ubiquitous. It allows attacks from anywhere in the world. Attackers can loop in from many different Internet providers," said Vatis, who noted that a cyberattack can include espionage using computer networks [159cm]

"It could start across the street but appear to be coming from China. And something that might look like a hacker attack could be the beginning of cyberwarfare," he added.

Vatis said the growing bullets-and-guns conflict in the Middle East between Israel and the Palestinians, with Islamic supporters elsewhere, is being accompanied by cyberattacks from each side against the other. It's serious enough, he said, that the FBI issued an alert about it to the U.S. Space Command, giving U.S. forces warning that the action on the cyber front could affect them, too.

<http://edition.cnn.com/2000/TECH/computing/11/22/cyberwar.machine.idg/index.html?iref=allsearch>

51. November 2, 2000

Mideast fighting spills onto the Internet

JEROUSALEM(CNN) -- The violence pitting Arabs and Jews in the Middle East has spilled from the physical into the virtual world, as combatants on both sides lay siege to the Internet sites of one another.

Mickey Buzaghlo began cyber warfare from his bedroom a few weeks ago. Upset by what he saw on Arab Web sites that attacked Israel, the 21-year-old Israeli and some friends broke into the Web site of Hezbollah, the Lebanese fundamental Islamic guerillas, replacing their content with the Israeli flag and the star of David [160wb]

"We, the Israeli hackers, need to show the right pictures and we will not give a chance, for example, to a Hezbollah site that will show propaganda [161wb] against Israel," he said. "So this is the reason why I decided to attack a couple of Hezbollah sites."

Pro-Arab hackers struck back and within days. Israeli government Web sites like the Ministry of Foreign Affairs, the Defense Forces and the Knesset were attacked and brought down for as long as two days. [162in]

"I would say it's vandalism, not war, because it is an effort by some people to prevent others from reading our material," said Ori Noi of the Israeli Foreign Ministry. "We don't pretend to be objective. We just want to bring the view of the government, the Ministry of Foreign Affairs. This is like burning books. This is like censorship. [163wa] "

In Ramallah in the West Bank, near the scene of fierce clashes between Palestinians and Israelis on the ground, Palnet, the major Palestinian service provider, has had to defend its clients against pro-Israeli hackers.

"The attacks have been initiated after a response after major attacks that were carried out on pro-Palestinian and pro-Islamic Web sites around the country, and this is where it ignited some people's feelings that they should do something against it," said Maan Bseiso, the CEO of Palnet.

In the heart of Israel's version of Silicon Valley lies Netvision, the biggest Internet service provider in one of the world's most connected countries. The Israeli government is one of its customers.

Both Netvision and Palnet say they are strongly opposed to hacking, regardless of the perpetrator.

Netvision hires counter-hackers like 20-year-old Manny, who understands the modus operandi of a hacker.

"Whether it's our hackers trying to knock down a Hezbollah site or Hezbollah trying to knock out the army sites, it's all games, nothing but war games," he said.

In Ramallah, an Internet cafe for young Palestinians is doing a brisk business. Many here are logged onto new Web sites that reflect the daily reality on the streets outside. Some of the sites have been targets of pro-Israeli hackers [164wb].

Despite the cyberwar, some combatants are seeking other methods to get their messages across.

Buzaghlo says he will stop hacking anti-Israeli Web sites but will continue his war of words on his own site. It's not quite a cease-fire, perhaps, but it's not an all-out cyberwar either.

<http://edition.cnn.com/2000/TECH/computing/11/02/mideast.webwar/index.html?iref=allsearch>

52. November 3, 1999

Derailing the vision of a truly digital government

(IDG) -- The gap in pay between federal information technology workers and their private-sector counterparts has been a problem federal IT managers have tried to solve for years - and one that has the potential of derailing the vision of a truly digital government.

That's why it is disconcerting that the Army has waved the white flag in its battle to try to find ways to increase pay for federal IT workers. Giving up on the compensation race seems like a no-brainer. After all, private companies offer Army IT personnel salaries of up to \$80,000 to join their ranks. In addition, the ".com" companies are luring young IT talent with stock options and the promise of striking it rich quick.

But the Army's decision is worrisome, especially when viewed in the context of what the Army wants to be in the 21st century. As Army Vice Chief of Staff Gen. John Keane put it, the IT soldiers are "the linchpin" to fighting cyberwars and to securing U.S. computers from foreign attack. [165in]

Top Army officials believe they can replace money with patriotism: IT grads will join the Army and work for significantly less money in typically less-than-desirable living quarters because they want to serve their country.

Civilian agencies plan to use the same reasoning to attract IT workers to non-DOD work.

Sure, many Americans are willing to give up some money to serve their country. But the reality is that most don't. And that means severely draining the labor pool of qualified candidates.

Even soldiers who chose less pay because of their patriotic duty warn about giving up the compensation battle. In a letter to the editor in this issue, an Army National Guardsman warns, "If we don't pay now, we will pay later".

For sure, this is not an easy problem to solve, especially in light of the strict spending caps. But if government is serious about pursuing a digital future, it cannot afford not to attract and keep talented IT workers.

The cost would be well worth it.

<http://edition.cnn.com/TECH/computing/9911/03/it.dream.deferred.idg/index.html?iref=allsearch>