ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ : ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ – 5ΟΣ ΚΥΚΛΟΣ

Τρομοκρατία, διαδίκτυο και κυβερνοχώρος

Νέα βήματα, νέες δράσεις

Αβδελίδης Στυλιανός ΜΘ:2009001

Πέμπτη, 3 Νοεμβρίου 2011

Επιβλέπουσα καθηγήτρια: Μπόση Μαρία

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ ΤΜΗΜΑ : ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ – 5ος ΚΥΚΛΟΣ

Τρομοκρατία, διαδίκτυο και κυβερνοχώρος

Νέα βήματα, νέες δράσεις

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Αβδελίδη Στυλιανού

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την _____

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Μαρία Μπόση	Αριστοτέλης Τζιαμπίρης	Ανδρέας Λιαρόπουλος
Καθηγητής Πα.Πει.	Καθηγητής Πα.Πει.	Καθηγητής Πα.Πει.

Αθήνα, Τρίτη, 10 Απριλίου 2012

(Υπογραφή)

.....

Αβδελίδης Στυλιανός

Διπλωματούχος Διεθνών και Ευρωπαϊκών Σπουδών ΠΑ.ΠΕΙ.

Ευχαριστήριο σημείωμα

Θα ήθελα να ευχαριστήσω την κα. Μαρία Μπόση για την πολύτιμη βοήθεια της στην δημιουργία αυτού του πονήματος, καθώς και τον κο. Ανδρέα Λιαρόπουλο για τις δημιουργικές ιδέες που μου έδωσε μέσα από τις διαλέξεις του. Σας ευχαριστώ πολύ.

Πίνακας περιεχομένων

Εισαγωγή

Η ανατολή του 21ου αιώνα, βρίσκει την τρομοκρατία να αποτελεί αντικείμενο σχολιασμού από διαφόρους επιστημονικούς κλάδους, για το οποίο έχουν γραφτεί χιλιάδες τόμοι βιβλίων, άρθρων και μελετών. Η ερμηνεία του φαινομένου της τρομοκρατίας, μπορεί να εμπίπτει κατά κύριο λόγο, σε πολιτικούς όρους αλλά ευρύτερες αναλύσεις έχουν δείξει ότι διαθέτει πολυάριθμες πτυχές, οι οποίες μπορεί να εμπίπτουν σε πολλές κατηγορίες επιστημονικής ανάλυσης, όπως η οικονομική προσέγγιση, η ηθική, η επιστήμη των διεθνών σχέσεων και της πολιτικής κτλ.

Η εποχή της ραγδαίας τεχνολογικής εξέλιξης δεν θα μπορούσε να αφήσει την τρομοκρατία ανεπηρέαστη. Η εποχή της πληροφόρησης (information), έδωσε περαιτέρω ώθηση στην ήδη συνεχή ροή εξέλιξης του φαινομένου. Η λεγόμενη **ηλεκτρονική τρομοκρατία,** ή **κυβερνοτρομοκρατία,** αποτελεί ένα νέο είδος τρομοκρατικής επίθεσης. Αφορά την επίθεση που λαμβάνει χώρα στο άυλο τοπίο του κυβερνοχώρου, όπου η ροή των πληροφοριών στιγμιαία εξελίσσεται διαμέσου του παγκόσμιου δικτύου. Ο κυβερνοχώρος, σύμφωνα με τον Winn Schwartau[1], είναι μία αχανής πραγματικότητα, ένα ηλεκτρονικό τοπίο όπου τα δεδομένα κινούνται με ταχύτητα μεγαλύτερη από αυτή του φωτός. Μία ακόμη ερμηνεία του κυβερνοχώρου, έρχεται από την Υπηρεσία Προστασίας των Συστημάτων Πληροφόρησης των ΗΠΑ[2], ορίζοντας το ως το ηλεκτρονικό περιβάλλον που δημιουργείται ως άθροισμα των πόρων τηλεπικοινωνίας παγκοσμίως. Ο κυβερνοχώρος, θεωρείται ως η εικονική Πέμπτη διάσταση, που δεν χαρακτηρίζεται από γεωγραφικά, εθνικά ή χρονικά όρια, ιδιοκτησίες και νόμους.

Στο παρόν πόνημα, γίνεται μία προσπάθεια, προκειμένου να αναλυθεί το φαινόμενο του νέου είδους της τρομοκρατίας. Η προσέγγιση του νέου είδους της τρομοκρατίας, μου έδωσε την δυνατότητα να κατανοήσω το λόγο για τον οποίο η κυβερνότρομοκρατία, δεν αφορά μόνο την πολιτική ζωή μίας χώρας, αλλά επεκτείνεται και σε επίπεδο διεθνούς πολιτικής. Η κατανόηση του φαινομένου,

1 Schwartau, Winn Terminal Compromise: computer terrorism: when privacy and freedom are the victims: a novel.

2 Marchetti, Victor; John D. Marks (1974). The CIA and the Cult of Intelligence.

προϋποθέτει χρησιμοποίηση όρων από άλλες επιστήμες, όπως η γεωπολιτική επιστήμη, η οικονομία, το δίκαιο, κ.α.

Στο πρώτο μέρος της εργασίας αυτής επιχειρείται μία μελέτη του φαινομένου της τρομοκρατίας σε θεωρητικό επίπεδο. Η ερμηνευτική προσέγγιση της τρομοκρατίας, σε γενικό πλαίσιο, θα μας δώσει εφόδια προκειμένου να αναλυθεί το νέο εξελιγμένο είδος της τρομοκρατίας. Είναι αναγκαίο να δοθεί σε πρώτο επίπεδο, η ιστορική βάση του φαινομένου της τρομοκρατίας, για να οριστεί το φαινόμενο της τρομοκρατίας. Επιπλέον θα επιχειρήσουμε να προσδιορίσουμε το φαινόμενο αυτό με επιστημονικές προσεγγίσεις, πέραν της πολιτικής, προκειμένου να ερευνήσουμε της ευρύτερες πτυχές της. Μέσα από αυτή την ανάλυση, θα προσπαθήσουμε να ορίσουμε τα κίνητρα των δρώντων των τρομοκρατικών επιθέσεων, καθώς και τα μέσα που αυτοί χρησιμοποιούν για να πετύχουν τους σκοπούς τους.

Στη συνέχεια της εργασίας, το ενδιαφέρον στρέφεται στην επίλυση του γρίφου σχετικά με την προέλευση της τρομοκρατίας του κυβερνοχώρου. Χρησιμοποιώντας όρους, όπως κυβερνό-έγκλημα (cyber-crime) και κυβερνό-επίθεση (cyber-attack), προσπαθούμε να λύσουμε το πάζλ που δημιουργείται σχετικά με την προέλευση του φαινομένου. Ταυτόχρονα, το πολιτικό υπόβαθρο του νέου είδους της τρομοκρατίας και βαθμός της απειλής που φέρει για την διεθνή ασφάλεια, ερευνάται διαδραστικά μέσω της επιστήμης των διεθνών σχέσεων και της γεωπολιτικής ανάλυσης.

Η οικονομική διάσταση του φαινομένου μας απασχολεί σε αυτό το κομμάτι, τόσο σε επίπεδο χρηματοδότησης των τρομοκρατικών επιθέσεων μέσω του κυβερνοχώρου αλλά και σε επίπεδο επιπτώσεων που μπορεί να έχει μια τρομοκρατική επίθεση μέσω των ηλεκτρονικών υπολογιστών και συστημάτων. Εξερευνώντας την σχέση της κυβερνητικής τρομοκρατίας και της οικονομίας ανάγουμε συμπεράσματα, σχετικά με την επίπτωση που έχει αυτή στον τομέα της οικονομίας μίας χώρας, καθώς και σε διεθνές πλαίσιο, και το πώς επηρεάζει τις σχέσεις αλληλεξάρτησης και οικονομικού ανταγωνισμού μεταξύ των ισχυρών κρατών του διεθνούς συστήματος. Η εργασία μας κλείνει, με την αναφορά σχετικά με την καταπολέμηση του φαινομένου αυτού από διεθνούς φορείς, όπως οι ΗΠΑ και η ΕΕ.

Κεφάλαιο 1 Μελετώντας το ζήτημα της τρομοκρατίας

1.1 Οι ρίζες του φαινομένου της τρομοκρατίας

Ερευνώντας το πολύ σοβαρό ζήτημα της τρομοκρατίας που απασχολεί την υφήλιο τα τελευταία χρόνια γίνεται αντιληπτό ότι για να κατανοήσουμε τη βαθύτερη αιτία του φαινομένου θα πρέπει πρώτα να προσδιορίσουμε την έννοια του κράτους-πολιτείας. Μία πολύ σημαντική παρατήρηση έγινε από τον Αριστοτέλη[3], στο έργο του *Πολιτικά*, όπου αναφέρει ότι το κράτος, η πολιτεία αλλιώς, συνίσταται από μία σειρά κανόνων δικαίου με στόχο την προστασία των δικαιωμάτων του κοινού, δηλαδή των πολιτών που την απαρτίζουν.

Επιπροσθέτως, δε, αναφέρει τα αίτια που οδηγούν τις πολιτείες σε παρεκβάσεις δημιουργώντας έτσι καταστάσεις που προκαλούν δυσαρέσκεια στο λαό, με αποτέλεσμα να δίνουν κίνητρα και αφορμές για συγκρούσεις με το κράτος. Τα αίτια[4] αυτά μπορεί να είναι:

1) Η **ανισότητα**, όταν αυτή στηρίζεται όχι στην πραγματική αξία αλλά σε εξωτερικά κριτήρια,όπως είναι ο πλούτος.

2) Η **παραβίαση των νόμων**, που μπορεί να ξεκινήσει από μικρά και ασήμαντα ζητήματα και να καταλήξει στην κατάργηση της έννομης τάξης και του πολιτεύματος, και ακολούθως να πλήξει τα δικαιώματα του κάθε πολίτη. Για παράδειγμα, η άνοδος δικτατορικών κυβερνήσεων, εύνοια της ολιγαρχίας και κάθε καταπάτηση των νόμων του Συντάγματος.

Σε παρόμοιο μήκος κύματος, υπήρξαν οι Ασσασίνοι, μία ακόμη ομάδα που έδειξε διακριτά χαρακτηριστικά τρομοκρατικής δράσης, όπως την ξέρουμε σήμερα. Αποτελούσαν μία αποσχισμένη φατρία της μουσουλμανικής ομάδας των Σηιτών, η

[3] Αριστοτέλης, *Πολιτικά*.(παρ. 1252α)
[4] Αριστοτέλης, *Πολιτικά*.(παρ. 1252β)

οποία υιοθέτησε την τακτική δολοφονίας των εχθρικών ηγετών επειδή η λατρεία τους δεν επέτρεπε την ανοιχτή σύγκρουση.

Παρόλο που οι Ζηλωτές και οι Ασσασίνοι, ενήργησαν αιώνες πριν, η δράση και οι μεθοδεύσεις τους θεωρείται ότι επαναλαμβάνεται και σήμερα. Μπορούν να θεωρηθούν, αρχικά πρωτεργάτες της σύγχρονης μορφής της τρομοκρατίας, σε θέματα όπως κίνητρα, οργάνωση, επιλογή στόχων και σκοπών. Ακόμη παρά το γεγονός ότι οι ενέργειες και των δύο στέφθηκαν, εν τέλει με πλήρη αποτυχία, έχουν μείνει στην ιστορία για τον υψηλό βαθμό ψυχολογικής βίας που άσκησαν.

Μία συγκροτημένη ερμηνευτική βάση σχετικά με το φαινόμενο της τρομοκρατίας, θα γίνει το έτος 1648 με την συνθήκη της Βεστφαλίας, που σηματοδοτεί τα όρια και τις αρμοδιότητες του έθνους-κράτους, την κεντρική αρχή την οποία αντιμάχεται η τρομοκρατία. Η λατινική λέξη «terror» που σημαίνει «τρόμος» υποδήλωνε τον τρόμο, το αίσθημα του πανικού και της απειλής μίας εχθρική εισβολή. Η ευρύτερη χρήση του όρου, με σύγχρονη πολιτική ερμηνεία, έγινε κατά την Γαλλική Επανάσταση, από το τάγμα των Ιακωβίνων[5]. Η εποχή αυτή σηματοδότησε την πρώτη χρήση των όρων «τρομοκράτης» και «τρομοκρατία». Το 1785, λίγο πριν την Γαλλική επανάσταση, ο όρος «τρομοκρατία» χρησιμοποιείται από τον Ροβεσπιέρο ως αναφορά στην Εποχή του Τρόμου (Reign of Terror), η οποία προήλθε από την διακυβέρνηση της Γαλλίας. Οι πράκτορες της επιτροπής Δημόσιας Ασφάλειας και του Διεθνούς Συνεδρίου που επέβαλλαν πρακτικές άσκησης «τρόμου» επονομάστηκαν ως τρομοκράτες[6].

Ο όρος «τρομοκρατία», καθιερώθηκε ήδη από τον 19^{ο} αιώνα και υποδήλωνε μία κρατική μορφή κυριαρχίας η οποία χρησιμοποιούσε παράνομα καταπιεστικούς κανόνες για εκφοβισμό, με σκοπό την επιβολή και τη διατήρηση της εξουσίας (Hoffman, 1998[7], σελ. 218, έπεται βλ. επίσης και Laquer, W., 1998[8]).

---

5 Βλέπε Hoffman, Bruce "Inside Terrorism" Columbia University Press 1998 ISBN 0-231-11468-0. σελ. 132.

6 Βλέπε " Laqueur Walter, A History of Terrorism'', Transaction Publishers, 2000.

7 Βλέπε Hoffman, Bruce "Inside Terrorism" Columbia University Press 1998 ISBN 0-231-11468-0. σελ. 167. Βλέπε Review in the New York Times Inside Terrorism

8 Βλέπε Laquer, W Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind, Woodrow Wilson Center Press, 1998

Κατά την διάρκεια αυτού του αιώνα, δημιουργήθηκε ένα αυξανόμενο ρεύμα εθνικισμού σε ολόκληρο τον κόσμο, το οποίο όριζε τον συνδυασμό του έθνους-κράτους και της πολιτικής κοινωνίας. Ενόσω τα κράτη ξεκινούσαν να δίνουν έμφαση σε εθνικές ταυτότητες, οι λαοί οι οποίοι είχαν κατακτηθεί ή αποικιοποιηθεί, όπως οι ζηλωτές και οι Εβραίοι, είχαν να επιλέξουν ανάμεσα στην αφομοίωση και την πάλη. Ο επόμενος αιώνας βρίσκει τον εθνικισμό, όπως και τον κομμουνισμό, με μεγαλύτερη ιδεολογική βάση.

Τον αιώνα αυτό, δραστηριοποιείται επίσης μία τρομοκρατική ομάδα, η οποία εξυπηρετεί ως μοντέλο ανάλυσης για μελλοντικές τρομοκρατικές επιθέσεις, η ρωσική Narodnya Volya (η θέληση των ανθρώπων). Η βασική τους διαφορά σε σχέση με την σύγχρονη τρομοκρατία, εντοπίζεται στην επιθυμία τους να ακυρώσουν επιθέσεις, προκειμένου να προστατεύσουν την σωματική ακεραιότητα ανθρώπων που ίσως βρεθούν εν μέσω επίθεσης. Πέρα από αυτό, διαπιστώνουμε, χαρακτηριστικά της τρομοκρατίας που υπάρχουν μέχρι και σήμερα, όπως επιθέσεις σε χρόνο απρόβλεπτο και απρογραμμάτιστο με δυσκολία εντοπισμού.

Στο τέλος αυτού του αιώνα, δίνεται μία ιδιαίτερη σημασία στον όρο «τρομοκρατία» και εκλαμβάνεται ως μία ειδική μορφή βίας, η οποία χρησιμοποιείται από πολιτικές ομάδες που επιδιώκουν την αλλαγή του συστήματος. Έτσι λοιπόν, ο όρος «τρομοκρατία» αποκτά διττή σημασία που συνεχίζει να ισχύει σήμερα (βλ. Alex Peter Schmid 2005, σελ.199)[9]. Μετά από κάθε τρομοκρατική πράξη υπάρχει μία επαναστατική οργάνωση, η οποία όχι μόνο αναλαμβάνει την ευθύνη αλλά και με προκήρυξη της σπεύδει να ομολογήσει την ενέργεια της αυτή.

Η χρήση βίας είναι επακόλουθο, όταν οι κοινωνικό-οικονομικές συνθήκες μεταβάλλονται έτσι ώστε μπορούν να δημιουργήσουν συνθήκες αστάθειας, που έχουν ως επακόλουθο την κοινωνική ανισότητα. Εκείνη, σηματοδοτεί, ανάμεσα σε άλλες ενέργειες, μία σειρά επαναστατικών ενεργειών συγκεκριμένων κοινωνικών ομάδων που νιώθουν ότι αδικούνται και έχουν μια καχυποψία απέναντι στο πολιτικό σύστημα

9 Βλέπε Schmid, ΣΕΛ. Alex, A. J Longman. *Political terrorism: a new guide to actors, authors, concepts, data bases, theories, & literature*.(2005)

του κράτους. Επίσης, σύμφωνα με έρευνες[10], η τρομοκρατία δεν είναι παράγωγο μόνο της περιθωριοποίησης ή της θρησκείας, καθώς υπήρχε και το φαινόμενο της αναρχίας. Οι αναρχικοί ήταν πολύ ενεργοί κατά τα τέλη του 19ου αιώνα με αρχές του 20ου αιώνα.

Αναρχικοί (1890-1910) Οι Ρώσοι αναρχικοί επεδίωκαν την ανατροπή του Ρώσου τσάρου Αλέξανδρου Β' με τη δολοφονία του την οποία πραγματοποίησαν το 1881. Πίστευαν ότι ο θάνατος του τσάρου καθώς και των άλλων βασιλιάδων και ευγενών στην Ευρώπη, θα επιφέρει πτώση των κυβερνητικών μηχανισμών. Για το σκοπό αυτό, οι αναρχικοί εισήγαγαν ένα νέο πιο εξελιγμένο είδος τρομοκρατίας, την **ατομική τρομοκρατία.** Η **ατομική τρομοκρατία**[11] αφορά την επιλεκτική χρήση τρόμου λόγω του ότι οι στόχοι είχαν επιλεγεί με βάση την θέση τους στον κυβερνητικό μηχανισμό. Οι τρομοκρατικές ενέργειες, πραγματοποιούνται με γνώμονα το κτύπημα της κρατικής εξουσίας αλλά με προϋπόθεση να μην κινδυνεύσουν αθώοι, κάτι που δεν συμβαίνει σήμερα. Οι δύο πιο γνωστές ενέργειες από τους αναρχικούς, μεταξύ άλλων, ήταν οι δολοφονίες του Προέδρου Mc Kinley (1901)[12] και του αρχιδούκα Φερδινάνδο (1914)[13].

Η Ιρλανδική Επανάσταση (1919-1921). Ο Ιρλανδικός πόλεμος του 1919 έφερε στο προσκήνιο τρεις έννοιες σχετικά με την ανάπτυξη της τρομοκρατίας

1. Επιλεκτική τρομοκρατία
2. Πρόκληση φόβου
3. cell operations-επιχειρήσεις απελευθέρωσης «συντρόφων»

---

10 Βλέπε Daniel Guerin, *Anarchism: From Theory to Practice*(New York: Monthly Review Press, 1970).

11 Βλέπε David C. Rapoport, ''The Four Waves of Modern Terrorism,'' in Audrey Kurth Cronin and James M. Ludes, Attacking Terrorism: Elements of a Grand Strategy (Washington,D.C.: Georgetown University Press, 2004), 46.

12 http://library.buffalo.edu/libraries/units/hsl/resources/guides/mck271.pdf The Official Report on the Case of President McKinley

13 Στις 28 Ιουνίου 1914, ο αρχιδούκας Franz Ferdinand της Αυστρίας, διάδοχος του αυστροουγγρικού θρόνου, και η σύζυγος του, Σοφία, δούκισσα του Hohenberg βρέθηκαν νεκροί από πυροβολισμούς στο Σαράγεβο, με δράστες μία ομάδα Σέρβοβόσνιων δολοφόνων υπό την εποπτεία του Danilo Ilić. Ο πολιτικός σκοπός της δολοφονίας ήταν να αποδυναμώσει την αυστροουγγρική αυτοκρατορία, σε ότι έχει να κάνει με τις σλαβικές επαρχίες στο νότο, με στόχο αυτές να ενωθούν με την «Γιουγκοσλαβία».

Ο σκοπός του πολέμου ήταν να κερδίσει την ανεξαρτησία της Ιρλανδίας από την Αγγλία. Με ηγέτη τον Michael Collins, η χρήση πράξεων βίας απευθυνόταν σε εκπροσώπους του αγγλικού κράτους (αστυνομία, στρατός, κυβερνητικούς αξιωματούχους, κ.α.) σε μία προσπάθεια να εντείνουν τις διαδικασίες για την αποχώρηση αυτών από τις θέσεις τους[14]. Ωστόσο, έχει μεγάλη σημασία να τονίσουμε μία σημαντική αναφορά σε σχέση με την Ιρλανδική Επανάσταση. Η Ιρλανδική Επανάσταση αποτελεί μία έκφραση εθνικιστικού χαρακτήρα από ομάδες, τις οποίες, η βρετανική κυβέρνηση δεν θεωρούσε τρομοκρατικές. Εν αντιθέσει, με τους αναρχικούς, που μάχονται για τις ιδέες τους, οι ομάδες αυτές μάχονται για την χώρα τους και παρουσιάζονται ως συμβατικοί στρατιώτες πατριωτισμού, παρόλο που πιθανόν να χρησιμοποιούν μεθόδους και τακτικές αναρχισμού[15].

Η τρομοκρατία εισήλθε σε μία νέα φάση ανάπτυξης στα τέλη της δεκαετίας του 1960. Εκείνη την εποχή η τρομοκρατία αποτέλεσε κεντρικό θέμα της παγκόσμιας κοινής γνώμης με έμφαση στη Μέση Ανατολή. Με τον πόλεμο του 1967, όπου το Ισραήλ κέρδισε επί της Ιορδανίας, της Αιγύπτου και της Συρίας, έχοντας κάτω από τον έλεγχο τους τα Υψίπεδα του Γκόλαν (Συρία), τμήμα της Ιερουσαλήμ, τη λωρίδα της Γάζας και τη Χερσόνησο του Σινά (Αίγυπτος), η χρήση βίας ως μέσο άσκησης εξωτερικής πολιτικής ήρθε στο προσκήνιο, με στόχο να καταδείξει την προσπάθεια των ισχυρών κρατών να αυξήσουν την επιρροή τους, καταλύοντας διεθνείς κανόνες και ανθρώπινα δικαιώματα[16].

Τρομοκρατία, Μέση Ανατολή και Ισλαμισμός: Τα τελευταία είκοσι χρόνια του εικοστού αιώνα ολοκληρώθηκε ο κύκλος που ξεκίνησε δεκαπέντε αιώνες πριν, με την έξαρση εθνικοαπελευθερωτικών κινημάτων στη Μέση Ανατολή. Ειδικότερα, έχουμε την Hizbullah και την Hamas, οι οποίες μάχονταν εναντίον του ισραηλινού κράτους, με την πρώτη να δραστηριοποιείται στο Λίβανο και το δεύτερο στην Παλαιστίνη. Εν

14 Ο Michael Collins ήταν η κινητήριος δύναμη πίσω από το κίνημα ανεξαρτησίας. Η ευφυΐα του και η οργανωτική του ικανότητα ήταν ασυναγώνιστη. Δημιούργησε ένα αποτελεσματικό δίκτυο κατασκοπείας ανάμεσα σε μέλη της μητροπολιτικής αστυνομίας του Δουβλίνου (DMP) "G division" και άλλους κλάδους της βρετανικής διοίκησης. Δημιούργησαν «Την Ομάδα», που αποτελείτο από άτομα με μόνη τους υποχρέωση να θανατώνουν τα άτομα της "G division".

15 Βλέπε Moloney, Ed (2002). A Secret History of the IRA. Penguin Books. σελ. 246.

16 Βλέπε *Endgame: Resistance*, by Derrick Jensen, Seven Stories Press, 2006

συντομία να αναφέρουμε ότι η Hizbullah αποτέλεσε την δεκαετία του 1980 πολιτοφυλακή με σημαντικό σημείο της πορείας της, την συμμετοχή στον εμφύλιο πόλεμο του Λιβάνου[17]. Ακολούθως η Hamas, μετά τη συμφωνία του Όσλο το 1993 η οποία έλαβε πρωτοβουλίες για σύναψη ειρήνης μεταξύ Ισραήλ και Παλαιστινίων, κλιμάκωσε τις επιθέσεις τρομοκρατικής βίας, με επιθέσεις αυτοκτονίας[18].

Ο Huntington (1996)[19], συγγραφέας της θεωρίας περί σύγκρουσης πολιτισμών, αναφέρει την διαμάχη του Ισλαμικού κόσμου και της Δύσης, προχωρώντας πέρα από την θρησκευτική συνιστώσα της τρομοκρατίας. Το μίσος εκείνων, δεν θεωρείται πλέον μόνο θρησκευτικό, αλλά και προερχόμενο από πολιτιστικές, γεωπολιτικές και στρατηγικές διαφορές (Mirskii 2003, 64)[20] . Πράγματι, υπάρχει η άποψη σχετικά με τη σύγκρουση μεταξύ του Ισλάμ και της Δύσης, άποψη που βρίσκει όλο και μεγαλύτερο κοινό στη Μέση Ανατολή, θεωρώντας ότι οι δυτικές αξίες θεωρούνται ξένες και απειλητικές (Kibble 2002)[21].

Η δεκαετία του 1980 σηματοδότησε την τρομοκρατία που είχε σαν στόχο τα αμερικανικά συμφέροντα σε όλο τον κόσμο. Η δεκαετία του 1990 προσέθεσε στην τρομοκρατία, γενοκτονίες και υψηλής επικινδυνότητας επιχειρήσεις αυτοκτονίας[22]. Μεταξύ του 1993 και του 2001, σημειώθηκαν επτά τρομοκρατικές επιχειρήσεις ενάντια στις ΗΠΑ, με κύριο στόχο την υλική καταστροφή και την ανατροπή του

17 On Hizbullah's evolution βλέπε Judith Palmer Harik, Hezbollah: The Changing Face of Terrorism (London: I.B.Tauris, 2004), Κεφ. 3; Nizar A. Hamzeh, 'Lebanon's Hizbullah: From Islamic Revolution to Parliamentary Accommodation', Third World Quarterly, Τομ. 14, No. 2 (1993).

18 Βλέπε Jeroen Gunning, 'Peace with Hamas? The Transforming Potential of Political Participation', International Affairs, Τομ. 80, No. 2 (2004), σελ. 245–7.

19 Βλέπε Huntington, S. 1996. *The clash of civilizations and the remaking of world order*. New York: Simon& Schuster Inc

20 Βλέπε Mirskii, G. 2003. Political Islam and Western society. *Russian Social Science Review* 44:63–78

21 Βλέπε Kibble, D. 2002. The attacks of 9/11: Evidence of a clash of religions? *Parameters* 32:34–45

22 Ο Κόφι Αννάν, γενικός γραμματέας των Ηνωμένων Εθνών, όρισε την τρομοκρατία το Μάρτιο του 2005 ως κάθε πράξη, που στοχεύει στο να προκαλέσει θάνατο ή σοβαρές σωματικές βλάβες σε πολίτες και αμάχους, για λόγου εκφοβισμού.

πολιτικού σκηνικού. Ο παρακάτω πίνακας αναφέρει τα κυριότερα περιστατικά της δεκαετίας και των αριθμό των θυμάτων που ανέκυψαν:

Χρονολογία	Περιστατικά	Αριθμός Θυμάτων
1993	Επίθεση στο Παγκόσμιο Κέντρο Εμπορίου στη Νέα Υόρκη (World Trade Centre)[23]	6
1996	Επίθεση στους Πύργους Khobar στην Σαουδική Αραβία[24]	58
1997	Τρομοκρατικά πυρά ενάντια στο ναό Hatshepsut στην Αίγυπτο[25]	224

23 http://www.usfa.fema.gov/downloads/pdf/publications/tr-076.pdf Σύμφωνα με αναφορές του πυροσβεστικού τμήματος της Νέας Υόρκης, στις 26 Φεβρουαρίου 1993, εξερράγη εκρηκτικός μηχανισμός στο Παγκόσμιο Κέντρο Εμπορίου στη Νέα Υόρκη, σκορπώντας τον θάνατο σε έξι άτομα και τραυματίζοντας 1.042. Εκτιμάται ότι περίπου 25.000 άτομα εκκένωσαν τους δύο πύργους κατά τον βομβαρδισμό. Ο εκρηκτικός μηχανισμός, ο οποίος περιεχόταν σε όχημα που στάθμευε στο γκαράζ του Κέντρου, έθεσε το σύστημα ισχύος εκτός λειτουργίας. Το αρχικό σχέδιο των τρομοκρατών ήταν να εκπέσει ο νότιος πύργος στο βόρειο προκειμένου να κατεδαφιστούν. Την ευθύνη για την επίθεση αυτή ανέλαβαν στελέχη της ισλαμικής τρομοκρατίας, και συγκεκριμένα του Απελευθερωτικού Στρατού.

24 http://www.rewardsforjustice.net/english/index.cfm?page=kt Στις 25 Ιουνίου 1996, μέλη της τρομοκρατικής οργάνωσης Hezbollah στη Σαουδική Αραβία, εξαπέλυσαν επίθεση με στόχο τους Πύργους Khobar, κοντά σε συγκρότημα κατοικιών στο Dhahran. Την περίοδο εκείνη το συγκρότημα αυτό φιλοξενούσε στρατιωτικό προσωπικό των ΗΠΑ. Κατά τη διάρκεια της πορείας ενός οχήματος που περιείχε πλαστικά εκρηκτικά, οι τρομοκράτες τα πυροδότησαν καταστρέφοντας το πλησίον κτίριο. Η επίθεη σκότωσε 19 στρατιώτες, και τραυμάτισε 372 άλλους διαφορετικών εθνοτήτων. Στις 21 Ιουνίου 2001, ένας ομοσπονδιακός δικαστής στην Αλεξάνδρεια της Βιρτζίνια κατέδειξε 14 τρομοκράτες ανάμεσα σε αυτούς τους Ahmad al-Mughassil, Ali el-Hoorie, Ibrahim al-Yacoub, Abdelkarim al-Nasser και πολλούς άλλους.

25 http://www.nytimes.com/1997/11/18/world/70-die-in-attack-at-egypt temple.html?pagewanted=all&src=pm Στις 18 Νοεμβρίου 1997, έλαβε χώρα η μεγαλύτερη τρομοκρατική επίθεση κατά της κυβέρνησης της Αιγύπτου από Ισλαμιστές τρομοκράτες, στα πλαίσια της εκστρατείας τους για την κατάρριψη της Αιγυπτιακής κυβέρνησης που διήρκησε πέντε χρόνια. Οι

2000	Βομβαρδισμοί αμερικανικών πρεσβειών στην Υεμένη.	17
2001	Επίθεση στους Δίδυμους Πύργους του Παγκόσμιου Κέντρο Εμπορίου στη Νέα Υόρκη[26]	χιλιάδες

Το κυριότερο ενδιαφέρον για ένα τρομοκράτη είναι να πείσει τον, κατά περίπτωση εχθρό του για το ότι διαθέτει περισσότερη ισχύ, έτσι ώστε να καταφέρει την μεταλλαγή της συμπεριφοράς του[27]. Η στρατηγική αυτή της τριβής είναι σχεδιασμένη για να επιτύχει αυτό το σκοπό. Όσο μεγαλύτερο είναι το κόστος για ένα τρομοκράτη, τόσο μεγαλύτερη είναι η πιθανότητα να προκαλέσει μεταβολή συμπεριφορών[28].

1.2. Ερμηνευτική προσέγγιση του όρου

Όπως αναφέρθηκε, η τρομοκρατία, ετυμολογικά σχετίζεται με τους όρους *terror* and *terrorisme, που υιοθετήθηκαν κατά τον 18ο αιώνα, στη περίοδο της Γαλλικής Επανάστασης, και κατόπιν έγιναν χρησιμοποιήθηκαν από τη σύγχρονη πολιτική σκηνή των τελευταίων χρόνων*[29]. Ο ελληνικός όρος τρομοκρατία, μπορεί να σημάνει την πολιτική που ασκείται μέσω απειλής ή χρήσης βίας απέναντι σε θύματα που

τρομοκράτες άνοιξαν πυρ εναντίον μίας ομάδων τουριστών που είχε επισκεφτεί τον αρχαίο αιγυπτιακό ναό της Hatshepsut, σκορπώντας τον θάνατο σε 70 άτομα. Η αστυνομία παρενέβη, με αποτέλεσμα να ακολουθήσει μία σειρά από πυροβολισμούς μεταξύ αυτής και των τρομοκρατών, όπου οι τελευταίοι κατέληξαν νεκροί

26 The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Cosimo, Inc. July 30, 2010

27 Βλέπε Per Baltzer Overgaard, "The Scale of Terrorist Attacks as a Signal of Resources," *Journal of Conflict Resolution*, τομ. 38, No. 3 (September 1994), σελ. 452–478; and Harvey E. Lapan and Todd Sandler, "Terrorism and Signaling," *European Journal of Political Economy*, τομ. 9, No. 3 (August 1993), σελ. 383–398

28 Βλέπε J. Maynard Smith, "The Theory of Games and Evolution in Animal Conflicts," *Journal of Theoretical Biology*, τομ. 47 (1974), σελ. 209–211; John J. Mearsheimer, *Conventional Deterrence* (Ithaca,

29 Βλέπε Λοβέρδου, Α. *Για την τρομοκρατία και το πολιτικό έγκλημα,* 1987, σελ. 71.

αποτελούν τους στόχους αυτής της πολιτικής[30]. Οι άμεσοι στόχοι της πολιτικής επιλέγονται τυχαία (ευκαιριακοί στόχοι) ή επιλεκτικά (αντιπροσωπευτικοί ή συμβολικοί στόχοι), και αποτελούν μέσα εκπομπής μηνυμάτων. Μία γενική άποψη, είναι ότι η τακτική, της χρήσης ή της απειλής χρήσης βίας μέσω της τρομοκρατίας είχε ως ζητούμενο την εξασφάλιση της απαραίτητης δημοσιότητας, όπως αναφέρει ο Schmidt (1988) με το παρακάτω σχήμα[31].

Μία ακόμη ερμηνεία, μπορεί να βρεθεί στο άρθρο 22 του Αμερικανικού Κώδικα[32], ο οποίος την ερμηνεύει ως «μία πράξη ή ένα σύνολο πράξεων πολιτικά υποκινούμενων, οι οποίες διαπράττονται με ένα τρόπο ενάντια στην εθνική ή διεθνή νομολογία, με στόχο άμαχους πληθυσμούς. Ειδικοί στην επιστήμη της τρομοκρατίας, όπως οι Michael Nacht[33] και Steven Weber[34], υπογραμμίζουν ότι η πράξη γίνεται με στόχο την δημιουργία μία κατάστασης φόβου ή πανικού σε αποδέκτες διαφορετικούς από τα εν τέλει θύματα. Η ερμηνεία μίας πράξης ως τρομοκρατική, εξαρτάται από την ηθική, νομική και συμπεριφορική σκοπιά από την οποία την εξετάζουμε. Αν εστιάζουμε στην πράξη μέσω ηθικών και νομικών κριτηρίων, τότε η αξία του ερμηνευτή αφορά τον σκοπό παρά την πράξη καθαυτή. Εάν όμως η δράση αυτή αναλύεται υπό το πρίσμα της συμπεριφοράς, τότε εξετάζουμε την πράξη ανάλογα με την αντίδραση που αυτή προκαλεί.

30 Βλέπε Schmidt, A. and A. Jogman (2005) *Political Terrorism*, Piscataway, NJ: Transaction Publishers

31 Βλέπε Schmidt, A. (1988) *Political Terrorism: A new guide to actors, authors, concepts, databases, theories and literature*, Amsterdam: North-Holland Publishing Company.

32 Βλέπε U.S Code Title 22.

33 Βλέπε "Michael Nacht - Assistant Secretary of Defense for Global Strategic Affairs - WhoRunsGov.com/ The Washington Post

34 Βλέπε Weber S, "Cooperation and Discord in U.S."- Soviet Arms Control (Princeton Press, 1991)

Το υπουργείο εξωτερικών των Ηνωμένων Πολιτειών, ανέφερε ότι διεθνής δράσης και εμβέλειας τρομοκράτες σκόρπισαν τον θάνατο σε 405 άτομα ένα χρόνο πριν το τρομοκρατικό χτύπημα στη Νέα Υόρκη (2000). Η 11η Σεπτεμβρίου 2001, βρίσκει το κράτος των ΗΠΑ, να δέχεται το ισχυρότερο τρομοκρατικό χτύπημα στην ιστορία της με επιπτώσεις σε οικονομικό, πολιτικό, κοινωνικό και ανθρωπιστικό επίπεδο. Οι επιθέσεις ενάντια στους Δίδυμους Πύργους του παγκόσμιου εμπορίου και του αμερικανικού Πενταγώνου, μέσω αεροσκαφών μέτρησαν θύματα της τάξεως των 6000 ατόμων. Παρά το μέγεθος της απώλειας, μελέτες υποστηρίζουν ότι θύματα τρομοκρατικών πράξεων είναι συγκριτικά μικρότερα σε αριθμό από περιστατικά τα οποία, σχετίζονται με την ευρύτερη εγκληματικότητα στις ΗΠΑ. Για ποιο λόγο όμως εστιάζουμε στα θύματα της τρομοκρατίας;

Αρχικά θα πρέπει να αναφέρουμε, τον ψυχολογικό αντίκτυπο της τρομοκρατίας. Δεν είναι δύσκολο να αντιληφθούμε τον απόλυτο τρόμο που προκάλεσαν οι μαζικές τρομοκρατικές επιθέσεις κατά την αρχή του 21ου αιώνα, αφού τα Μέσα Ενημέρωσης (εθνικά και διεθνή) έπαιξαν καταλυτικό ρόλο στη διαμόρφωση της κοινής γνώμης. Μέσω της μαζικής παρουσίας των Μέσων Ενημέρωσης ανακαλύπτουμε τρία διαφορετικά επίπεδα δράσης[35]

1. Τον πραγματικό κόσμο (τι ακριβώς συμβαίνει;)

2. Το συμβολικό (την εικόνα του πραγματικού κόσμου όπως παρουσιάζεται μέσα από τα ΜΜΕ)

3. Το αντικειμενικό επίπεδο (ο κόσμος όπως ερμηνεύεται από τον λαό, τα πιστεύω του που δημιουργούνται μέσω ενός συνδυασμού άμεσων εμπειριών με πραγματικά πρόσωπα και γεγονότα καθώς και το πώς προβάλλονται από τα Μέσα).

Η καταλυτική παρουσία των Μέσων ενημέρωσης δημιουργεί αναμφίβολα ένα ψυχολογικό αντίκτυπο στον κόσμο αφήνοντας σε δεύτερη μοίρα τα ιδεολογικά και πολιτικά κίνητρα του κάθε δρώντα.

Κάποιος, ίσως θεωρήσει ότι το πιο δύσκολο κομμάτι στην αντιμετώπιση τους φαινομένου είναι η ερμηνεία αυτού. Η λέξη «τρομοκρατία», έχει χρησιμοποιηθεί για να περιγράψει μία ποικιλία από βίαιες πράξεις, από ενδοκρατικές φιλονικίες έως βία

35 Βλέπε David L. Paletz and Alex ΣΕΛ. Schmid, Terrorism and the Media. How Researcher, Terrorists, Government, Press, Public, Victims View and Use the Media Newbury Park: Sage Publications 1992) σελ.33.

συμμοριών και προσχεδιασμένη ανθρωποκτονία. Υπάρχει μία εισήγηση του Υπουργείου Εξωτερικών των ΗΠΑ[36], σχετικά με την πολιτικά υποκινούμενη άσκηση βίας με στόχο την επιρροή μίας μερίδα ατόμων. Μέσω αυτής μπορούμε να διακρίνουμε τρία κριτήρια που διαφοροποιούν την τρομοκρατία από άλλες πράξεις βίας.

Σε πρώτη φάση η τρομοκρατία, σε ορισμένες περιπτώσεις μπορεί να θεωρηθεί ως καταλυτικό μέσο πολιτικής στρατηγικής. Ενώ δεν υπάρχουν μη πολιτικές εκφάνσεις της τρομοκρατίας (όπως ψυχοπαθολογική τρομοκρατία), το πολιτικό κίνητρο είναι πάντοτε παρόν και προβάλλεται τόσο από τους ίδιους τους τρομοκράτες όσο και από αναλυτές[37]. Οι σκοποί των επιθέσεων στην Νέα Υόρκη και την Ουάσινγκτον, για παράδειγμα, αφορούν την μεταβολή της κυβερνητικής πολιτικής των ΗΠΑ για τη Μέση Ανατολή.

Δεύτερον, η τρομοκρατική βία έχει σαν στόχο πολυάριθμα θύματα αμάχων πολιτών ή ομάδων που δεν είναι προετοιμασμένοι να αμυνθούν ακόμη και μέλη στρατιωτικών ομάδων που δέχονται επιθέσεις σε καιρό ειρήνης. Η Τρομοκρατία, μέσω της χρήσης βίας ενάντια σε ένα θύμα, επιζητεί να καταναγκάσει και να πιέσει τους άλλους[38]. Ο άμεσος στόχος αποτελεί απλώς το εξιλαστήριο θύμα, μέσω του οποίου θέλει να στείλει ένα καλά σχεδιασμένο μήνυμα σε ένα ευρύτερο κοινό. Ακόμη ο Chaliand (2007)[39], υπογράμμισε ότι η τρομοκρατία βασίστηκε στην πρόκληση υψηλού αισθήματος κινδύνου και ανησυχίας σε μία ομάδα ατόμων, πιθανόν διαφορετικής από τα θύματα. Η τρομοκρατία μπορεί να εκφραστεί, επομένως, μέσω της δημιουργίας ενός αισθήματος φόβου πέρα από το άμεσο θύμα (Jones & Fong, 1994)[40].

---

36 Βλέπε "Patterns of Global Terrorism" http://www.state.gov/s/ct/rls/pgtrpt/

37 Βλέπε Buijs, F.J. (2001) 'Political Violence, Threat and Challenge' in *The Netherlands' Journal of Social Science*, Τομ. 37, No. 1, σελ. 7-23.

38 Βλέπε Jeffrey Ian Ross. Controlling State Crime: Toward an Integrated Structural Model. In: J.I. Ross (Ed.). Controlling State Crime. An Introduction. New York, Garland Publ. Co., 1995.

39 Βλέπε Chaliand, Gerard. The History of Terrorism: From Antiquity to al Qaeda. Berkeley: University of California Press, 2007. σελ.56

40 Βλέπε Jones, F., & Fong, Y. (1994). Military psychiatry and terrorism. In Department of the Army, Textbook of military medicine (σελ.. 264–269). Washington, D.C.: Department of the Army.

Ο Τέιλορ (1988), προχώρησε σε μεγαλύτερο ερευνητικό βάθος για την ερμηνεία του φαινομένου. Η συζήτηση επεξεργάστηκε τρεις οπτικές που χρησιμοποιούν οι άνθρωποι για να καθορίσουν εάν μία πράξη είναι τρομοκρατική ή όχι. Η παρουσίαση αυτών των προοπτικών υπογράμμισε το ότι διαφορετικοί άνθρωποι, μπορούν να ερμηνεύσουν διαφορετικά μία πράξη ανάλογα με την προοπτική. Σε πρώτη φάση, τα άτομα εξετάζουν την τρομοκρατία ως θέμα νομικό. Με αυτή την άποψη, μία πράξη θεωρείται τρομοκρατική μόνον εάν είναι ενάντια στις διατάξεις του δικαίου, τόσο εθνικού, όσο και διεθνούς. Οι κυβερνήσεις, ίσως χρησιμοποιήσουν αυτήν την οπτική για να ερμηνεύσουν την τρομοκρατία, ωστόσο, ο καθορισμός για εάν μία πράξη θεωρείται τρομοκρατική κάτω από αυτή τη σκοπιά, εξαρτάται με το ποια κυβέρνηση προσπαθεί να ερμηνεύσει την πράξη αυτή.

Μία δεύτερη προσέγγιση του Τέιλορ, αφορά την ηθική φύση, με την τρομοκρατία να θεωρείται μία πράξη μόνο σε περίπτωση που δεν έχει ηθική αιτιολογία. Ορισμένες ομάδες είναι πρόθυμες να διαπράξουν παράνομη πολιτικά υποκινούμενη βία αλλά με την πίστη ότι είναι απαραίτητη και ηθικά σωστή. Η στρατηγική, όμως των τρομοκρατών, υποδηλώνει ακόμη την σχετική αδυναμία τους και την ανικανότητα τους να ασκήσουν βία με παραδοσιακά μέσα. Η πολιτεία, με τη σειρά της είναι φυσικό να εκμεταλλευτεί αυτή την αδυναμία για να από-πολιτικοποιήσει την βία των μικρών εξτρεμιστικών ομάδων και να σχεδιάσει το προφίλ του τρομοκράτη παρά να ασκήσει πολιτική βία (White, 2002)[41].

Μερικές φορές, κυβερνήσεις μπορούν να χρησιμοποιήσουν αυτή την οπτική. Για παράδειγμα, υπάρχουν πολλές συζητήσεις μετά τα γεγονότα της Νέας Υόρκης (11 Σεπτεμβρίου 2001) και της Ουάσινγκτον, σχετικά με τον ιερό πόλεμο (τζιχάντ) ο οποίος έχει διεξαχθεί από άτομα που προέρχονται από την Μέση Ανατολή και την κεντρική Ασία, για να νικήσει το κακό που επικρατεί στον κόσμο, σύμφωνα με το Ισλάμ. Πολιτικά υποκινούμενη βία ενάντια σε αμάχους μπορεί να δικαιολογηθεί στο όνομα του ιερού πολέμου[42]. Φωτεινό παράδειγμα, αυτών των προσπαθειών είναι η ενορχήστρωση των επιθέσεων αυτών, από τον Οσάμα Μπιν Λάντεν, ως μαχητών της αδικίας των ΗΠΑ κατά της Μέσης Ανατολής. Νομικά, η χρήση των ηθικών

41 Βλέπε White, J. R. (2002). Terrorism: An introduction, 3rd ed. Stamford, CN: Wadsworth-Thomson Learning σελ. 269-271

42 Βλέπε Al-Khattar, Aref M. Religion and Terrorism: An Interfaith Perspective. Westport, CT: Praeger, 2003.

κριτηρίων μπορεί να οδηγήσει στην δημιουργία περισσότερων από μία, οπτικών γωνιών σχετικά με την ίδια πράξη, εξαρτώμενοι από την μάζα των ατόμων που επιχειρούν να των ερμηνεύσουν.

Η Τρίτη προσέγγιση του Taylor[43], αφορά την συμπεριφοριστική ιδιότητα της τρομοκρατίας. Υπό το πρίσμα της συμπεριφοράς, η τρομοκρατία ορίζεται, καθαρά από τις συμπεριφορές που εμπλέκονται, ανεξάρτητα με τους νόμους και την ηθική όσων την ορίζουν. Παρά το γεγονός αυτό, δεν πρέπει, όταν εξετάζουμε το θέμα της τρομοκρατίας με βάση συμπεριφορές, να αγνοούμε την επίδραση των κοινωνικών και πολιτιστικών αξιών που διέπουν τα άτομα που διενεργούν τις τρομοκρατικές πράξεις. Πράγματι, το γεγονός ότι ορισμένες κυβερνήσεις θεωρούν την τρομοκρατία ως «ανήθικη» αποτελούν κομμάτια του πάζλ που συνθέτει τον ορισμό του φαινόμενου. Η άποψη όμως είναι, ότι δεν υπάρχει καθολική άποψη από μέρους των κυβερνήσεων πότε μία πράξη θεωρείται ως παράνομη.

Η χρήση ενός νομικού ή ηθικού μοντέλου ίσως φέρει στο προσκήνιο νέες σημαντικές μεταβλητές που επηρεάζουν την ανάπτυξη τρομοκρατικών ομάδων και πράξεων. Οι δύο αυτές οπτικές, επίσης ελαχιστοποιούν την πιθανότητα, σχετικά με το ότι διαφορετικά άτομα έχουν διαφορετικούς κανόνες δικαίου και ηθικούς κώδικες. Η υιοθέτηση αυτών των προοπτικών, ίσως οδηγήσει σε μερική κατανόηση των επιθέσεων και ενός έντονου ενδιαφέροντος στα μέσα δράσης παρά στην δράση αυτή καθαυτή. Παρόλαυτα, η χρήση ενός συμπεριφοριστικού μοντέλου ίσως οδηγήσει στην επανεκτίμηση των κυβερνήσεων για το εάν οι πράξεις αυτές αποτελούν τρομοκρατική βία, άσχετα με το εάν είναι ή όχι ηθικές.

1.3. Η μεταλλασσόμενη φύση της τρομοκρατίας

Ορισμός

Πως θα μπορούσαν οι παραδοσιακές νόρμες της τρομοκρατίας να μεταβληθούν για να προσαρμοστούν στα νέα φαινόμενα, όπως οι επιθέσεις μέσω του κυβερνοχώρου; Μία απάντηση σε αυτό το ερώτημα μπορεί να δοθεί από ένα γενικό ορισμό της τρομοκρατίας, που έχει δοθεί από τον Thomas Perry Thornton: "μια συμβολική

43 Βλέπε Taylor & Francis (2010), "Terrorism and Political Violence". Routledge, τομ. 23.

πράξη που είναι σχεδιασμένη να επηρεάσει πολιτική συμπεριφορά με υπεράνω ηθικής μέσα, όπως η χρήση ή απειλή χρήσης βίας"[44].

1.3.1 Συμβολική βία

Η τρομοκρατία, από αυτούς που την ασκούν, είναι το όπλο του αδύναμου ενάντια στον ισχυρό. Ο τρόμος χρησιμοποιείται για να ξεπεράσει εμφανώς ανυπέρβλητες διαφορές που εντοπίζονται μεταξύ των τρομοκρατών και των στόχων των επιθέσεων, οι οποίοι κατά κύριο λόγο, ανήκουν στην πολιτική σφαίρα. Ο Thornton, υποστηρίζει ακόμη ότι «η σχετικά υψηλή προσαρμοστικότητα της τρομοκρατίας προκύπτει από τη συμβολική φύση της. Εάν ο τρομοκράτης κατανοεί ότι επιζητεί έναν υψηλό βαθμό επίδειξης και την ευκαιρία να περάσει ένα ισχυρό μήνυμα προς την κοινωνία, θα επιτεθεί ενάντια σε στόχους με μεγάλη συμβολική σημασία[45]. Ενώ ο Thornton, ενδιαφέρεται πρωταρχικά στην σχέση της τρομοκρατίας με την ανταρσία, δεν παραλείπει να εστιάσει στο ότι, η αξία της επίθεσης ενάντια σε συμβολικούς στόχους είναι εφαρμόσιμη και στην τρομοκρατία. Ακόμη αν ο στόχος ενός τρομοκράτη είναι, η τελική κατάρρευση του κυβερνητικού μηχανισμού, τότε εκείνος πρέπει να επιχειρήσει να οργανώσει μία αποτελεσματική επιχείρηση ανταρσίας.

Ο Thornton, επιπλέον αναφέρει ότι οι σημαντικότεροι συμβολικοί στόχοι για ένα τρομοκράτη είναι εκείνοι που αναφέρονται στην κανονιστική δομή που διέπει το υποστηρικτικό πλαίσιο της κοινωνίας[46]. Εάν οι συμβολικοί στόχοι παύσουν να υφίστανται, τότε η ανταρσία έχει επιτύχει να προκαλέσει αποξένωση μεταξύ των ατόμων από την κοινωνία που προηγουμένως ένιωθαν ασφαλείς και προστατευμένοι. Στην εποχή της πληροφόρησης την οποία διανύουμε, μερικές από τις κανονιστικές δομές, μπορεί να αποτελούνται και από υψηλής τεχνολογίας δίκτυα που επιτρέπουν στα άτομα να επικοινωνούν, να έχουν πρόσβαση σε λογαριασμούς χρημάτων και να εργάζονται. Για το λόγο αυτό, είναι οι ιδανικοί στόχοι για την άσκηση συμβολικής βίας.

---

44 Βλέπε Thomas Perry Thornton, "Terror as a weapon of Political Agitation," in Internal War: Problems and Ασελ.roaches, ed. Harry Eckstein (New York Free Press of Glencoe, 1964), 73

45 Βλέπε Thornton, 77.

46 Βλέπε Thornton,77

Η πρόθεση ενός τρομοκράτη δύναται να χρησιμοποιηθεί για να εκτιμήσει την «συμβολική» φύση του επιλεγόμενου στόχου. Ο σκοπός οδηγεί στον συμβολισμό. Μία προσεκτική μελέτη επάνω στην πρόθεση αυτή του τρομοκράτη, βοηθά για να διαφοροποιηθεί μεταξύ του απλού εγκληματία, που ήδη υπάρχει τόσο σε πραγματικό πλαίσιο, όσο και στο πλαίσιο του κυβερνοχώρου. Ο Philip Karber υπογραμμίζει την διάκριση αυτή[47]:

Η συμβολική φύση της τρομοκρατίας παρέχει δύο μεγάλης σημασίας διακρίσεις μεταξύ της τρομοκρατίας και της επανάστασης και μεταξύ της τρομοκρατίας και άλλων μορφών βίας[48]. Εάν ο σκοπός της βίας είναι η απόκτηση χρήσιμων αντικειμένων (χρήματα, όπλα, κ.α.) ή η άρνηση αυτών των πόρων σε έναν εχθρό, η πράξη αυτή εμπίπτει στον όρο του εγκλήματος, όπως ληστεία, δολοφονία εκ προμελέτης, κ.α. εάν από την άλλη ο σκοπός μας είναι η συμβολική έκφραση, τότε έχουμε να κάνουμε με την τρομοκρατία (Thornton). Αυτό υπογραμμίζει την διάκριση μεταξύ τρομοκρατίας και επανάστασης, όπου η συμβολική βία χρησιμοποιείται όχι μόνο για λόγος κατάρριψης ενός πολιτικού συστήματος, αλλά ως μέσο για να τραβήξει την προσοχή και να *αποδυναμώσει* οικονομικά συστήματα και συστήματα ασφαλείας μέσω επιθέσεων στα δίκτυα.

1.3.2 Επιρροή σε πολιτική συμπεριφορά

Το δεύτερο στοιχείο στον ορισμό που δίνει ο Thornton, είναι το ότι ο τρόμος και η πρόκληση αυτού είναι μία πράξη σχεδιασμένη να επηρεάσει πολιτικές συμπεριφορές. Το μέρος αυτό του ορισμού εστιάζει σε άλλες κατηγοριοποιήσεις της τρομοκρατίας, όπως εγκληματική ή παθολογική τρομοκρατία. Ενώ δεν υπάρχει γενικώς αποδεκτός ορισμός για την τρομοκρατία στην πολιτική επιστήμη, η τρομοκρατία μπορεί να προσεγγιστεί ερμηνευτικά με όρους πολιτικούς. Σύμφωνα με αυτούς, η τρομοκρατία αφορά την εναλλαγή των δράσεων είτε μεταξύ του κατεστημένου διαφόρων ομάδων (εκδικητική τρομοκρατία) είτε μεταξύ του συνόλου του πληθυσμού (καθεστωτική ή πολιτειακή τρομοκρατία)[49]. Η σύσταση νέων

47 Βλέπε Philip, A. Karber, *Terrorism as a social protest, 1971.*

48 Βλέπε Philip, A. Karber, *Urban Terrorism: Baseline Data and a Conceptual Framework,* Social Science Quarterly 52, (December, 1971).

49Βλέπε Alex ΣΕΛ. Schmidt, Violence as Communication, (Beverly Hills: Sage, 1982), 60.

τεχνολογιών σε ότι αφορά την πληροφόρηση και την χρήση αυτής για εχθροπραξίες, θα επηρεάσει τον σχεδιασμό κάθε τύπου της τρομοκρατίας αλλά όχι την πρόθεση του τρομοκράτη να επηρεάσει πολιτικές συμπεριφορές.

1.3.3 Ιδιότητες

Κατά τον Schmidt εντοπίζει πέντε στοιχεία που χαρακτηρίζουν μία τρομοκρατική ενέργεια:

1) Το **όπλο δράσης:** οι τρομοκράτες έχουν μία μακρά ιστορία στην χρήση «συμβατικών» όπλων όπως μαχαίρια, περίστροφα και εκρηκτικά για να δράσουν (φόνους, δολοφονίες, βομβαρδισμούς, πλήγματα σε μεταφορές, κ.α.). Αυτά τα όπλα λαμβάνουν νέες διαστάσεις στο μυαλό των θυμάτων και του κοινού-δέκτη.

2) Η **Πράξη:** ενώ η χρήση χημικών και άλλων όπλων και η καταστροφή κτιρίων αποτελούν κοινοτοπίες στην ενδοκρατική σύγκρουση, η τοποθέτηση εκρηκτικών μηχανισμών υψηλού κινδύνου σε μέσα μεταφοράς και η καταστροφή μίας πρεσβείας ή άλλου κυβερνητικού κτιρίου, έγκειται στην σφαίρα του μη αποδεκτού, σε ότι έχει να κάνει με εγκληματική συμπεριφορά. Ενώ ένας κυβερνοτρομοκράτης, δεν έχει ακόμη δεχτεί κάποιο είδος τιμωρίας, η πρώτη πράξη εξ ορισμού θα είναι πέρα από τα όρια του φυσιολογικού. Τουλάχιστον θα είναι μοναδική.

3) Ο **τόπος και ο χρόνος:** το τρίτο στοιχείο της ιδιότητας είναι ο τόπος και ο χρόνος της επίθεσης. Στην τρομοκρατία, δεν υπάρχει «πολεμική διακήρυξη» μεταξύ δύο κρατικών μονάδων που προετοιμάζει τον πληθυσμό για μία ενδεχόμενη σύρραξη μεταξύ ενός κράτους και ενός εχθρού. Για το λόγο αυτό, μία τρομοκρατική επίθεση είναι συνήθως «κεραυνός εν αιθρία», που είναι σχεδιασμένο να δημιουργεί τρόμο στο κοινό το οποίο στοχεύει εξαιτίας του απροσδόκητου χαρακτήρα του. Όπως ο Schmid δηλώνει:

> **«Το πεδίο δράσης ενός τρομοκράτη είναι επίσης ακαθόριστο. Δεν υπάρχουν μέτωπα, δεν υπάρχει πεδίο μάχης. Η αιφνίδια έξαρση βίας**

μπορεί να συμβεί σε κάθε οικείο χώρο. Η διαφορά όμως μεταξύ έξαρσης βίας σε ένα οικείο χώρο και σε ευρύτερο κρατικό επίπεδο, έγκειται στην εκδήλωση του φόβου. Κανένας δεν μπορεί να είναι σίγουρος για τον κίνδυνο που μπορεί να αντιμετωπίσει το επόμενο δευτερόλεπτο. Η σκέψη ότι μπορεί να υπάρξει βίαιη επίθεση με άγνωστης ταυτότητας θύματα είναι συνεχώς στο μυαλό του πληθυσμού»[50].

Η ικανότητα του να πραγματοποιηθεί μία επίθεση παντού και ανά πάσα στιγμή είναι ένα στοιχείο το οποίο θα αποτελέσει σημαντικό παράγοντα στην εποχή της πληροφόρησης. Εάν οι τρομοκράτες, επιθυμούν, για παράδειγμα να επιτεθούν σε δίκτυα-κλειδιά του κρατικού μηχανισμού, θα είναι ικανοί να πλήξουν είτε μέρη αυτού είτε ολόκληρο τον μηχανισμό. Η μη ύπαρξη μετώπων, όπως προαναφέραμε, είναι πλέον μία πραγματικότητα στον κυβερνοχώρο όπου δεν υπάρχουν σύνορα. Χρησιμοποιώντας μεθόδους επίθεσης μέσω του κυβερνοχώρου, οι τρομοκράτες μπορούν να πλήξουν οποιοδήποτε στόχο ακόμη κι αν βρίσκεται στο άλλο άκρο του πλανήτη.

4) **Μυστική φύση:** η ιδιότητα αυτή αφορά τόσο την ανταρσία όσο και την τρομοκρατία καθαυτή. Είναι φυσικό ένα σώμα τρομοκρατών και ακολούθως μία τρομοκρατική οργάνωση, να θέλουν να κρατήσουν μυστική την ταυτότητα τους για τις επιχειρήσεις τους. Η αυγή της εποχής της πληροφόρησης παρουσιάζει νέες μεθόδους επικοινωνίας για μία τρομοκρατική οργάνωση. Αντίστροφα, η εποχή της πληροφόρησης προτείνει μία σειρά από εργαλεία στις αντιτρομοκρατικές υπηρεσίες για χρήση ενάντια στους τρομοκράτες.

5) **Παραβίαση των κανόνων συμπεριφοράς:** με την απουσία ενός «πραγματικού» πεδίου μάχης, υπάρχει και η απουσία οποιουδήποτε νόμου ή γενικότερου συστήματος τήρησης του δικαίου, σχετικά με την πολεμική προσπάθεια. Ο τρομοκράτης, ωστόσο, δεν έγκειται σε αυτή την ανάλυση. Το θύμα δεν είναι ο αληθινός δράστης, είναι μόνο το αντικείμενο για να

50 Βλέπε Schmidt, Political Terrorism, 108.

ενεργοποιήσει μία τέτοια σχέση[51]. Τα θύματα στον κυβερνοχώρο, δεν θα μπορέσουν ποτέ να δουν το πρόσωπο του θύτη, ούτε πιθανόν να έχουν οποιαδήποτε σχέση με τους φορείς των επιθέσεων σε πραγματικό χρόνο. Η οποιαδήποτε δραστηριότητα τοποθετείται αποκλειστικά στον κυβερνοχώρο.

Συνοψίζοντας, η αδυναμία του να καθορίσουμε την ταυτότητα της απειλής ή να προτείνουμε λύση χρησιμοποιώντας φυσιολογικές διαδικασίες συντελεί στην δημιουργία τρόμου. Ο Thornton, υπογραμμίζει «ότι η γνώση και η κατανόηση της πηγής του κινδύνου παρέχει στο θύμα ένα πλαίσιο στο οποίο μπορεί να μελετήσει την φύση του, σχετίζοντας το με προηγούμενη εμπειρία, και ακολούθως λαμβάνει μέτρα για να το μετριάσει»[52]. Εάν η αιτία του κινδύνου, είναι άγνωστη και απρόβλεπτη, μία κατάσταση ανησυχίας, χαρακτηριζόμενη από «τον φόβο του αγνώστου» θα επικρατήσει. Εάν η απειλή είναι μεγάλη, το αποτέλεσμα είναι μία κατάσταση φόβου και απόγνωσης με την πεποίθηση της συνεχόμενης απειλής. Όσο η εμπιστοσύνη στην δράση των υπολογιστικών συστημάτων στην καθημερινή δραστηριότητα των ανθρώπων αυξάνεται, τόσο το επίπεδο της αναστάτωσης και της αποδιοργάνωσης θα αυξάνεται.

1.3.4. Άσκηση ή απειλή βίας

Ένα τελικό στοιχείο που εισάγει ο Thornton στον ορισμό του για την τρομοκρατία, αφορά την χρήση ή την απειλή χρήσης βίας. Το στοιχείο αυτό, απαιτεί μεγαλύτερη προσοχή επειδή η ικανότητα να απειλεί κάποιος ή να χρησιμοποιεί σωματική βία στον κυβερνοχώρο είναι ανύπαρκτη. Ο Thornton λέει ότι «ένα μη βίαιο πρόγραμμα δύσκολα μπορεί να θεωρηθεί τρομοκρατία»[53]. Δυστυχώς, οι ποικίλοι ορισμοί που δίνονται για την βία είναι τόσοι όσοι και οι ορισμοί που δίνονται για την τρομοκρατία γενικότερα. Ένα σημαντικό στοιχείο όλων αυτών των ορισμών θεωρεί ότι η βία αφορά την

51 Βλέπε Schmidt, Political Terrorism, 109
52 Βλέπε Thornton, 75.

53 Βλέπε Thornton, 76

πρόκληση φυσικής βλάβης σε ένα άτομο ή αντικείμενο. Ένα παράδειγμα είναι ο ορισμός που δίνει ο Paul Wilkinson:

> **Η βία μπορεί να οριστεί ως η παράνομη χρήση ή η απειλούμενη χρήση εξαναγκασμού με αποτέλεσμα, ή με επιδιωκόμενο αποτέλεσμα τον τραυματισμό, τον θάνατο ή τον εκφοβισμό των ανθρώπων ή ακόμη και την καταστροφή η κλοπή της περιουσίας τους.** [54]

Όσο η τρομοκρατία προχωρά στην εποχή της πληροφόρησης, ο ορισμός της βίας πρέπει να περιέχει και «κυβερνό-βία». Ενώ η καταστροφή των δεδομένων δεν είναι μία φυσική πράξη, και δεν θέτει την ανθρώπινη ζωή σε άμεσο κίνδυνο, πρέπει να θεωρηθεί εξίσου τρομοκρατική. Εάν ο στόχος ενός τρομοκράτη που εργάζεται μέσω του κυβερνοχώρου, είναι να δημιουργήσει τρόμο, η καλύτερη πορεία δράσης ίσως είναι η προσφυγή σε μία φυσική πράξη βίας, ή μία επίθεση σε συστήματα υπολογιστών που θα θέσει ανθρώπινες ζωές σε κίνδυνο, όπως συστήματα εναέριας κυκλοφορίας. Εάν οι κυβερνότρομοκράτες, δεν είναι ικανοί να δημιουργήσουν μία αίσθηση φυσικού κινδύνου στον κόσμο, δεν θα είναι ικανοί να δημιουργήσουν αίσθημα τρόμου. Φυσικά θα πρέπει να καλύψουν και άλλους σκοπούς της τρομοκρατίας.

1.3.5 Σκοποί

Ο Thornton[55] απευθύνει πολλαπλούς σκοπούς στην μελέτη του για την ιδιότητα του τρόμου ως όπλο. Ο πρώτος σκοπός είναι η δημιουργία ηθικού μέσα στην τρομοκρατική οργάνωση. Ο δεύτερος σκοπός είναι η ενημέρωση, όπου η οργάνωση θα ανακοινώνει την ύπαρξη της, το μέρος δράσης και τα ενδιαφέροντα της. Έτσι ξεφεύγει από τα όρια του συμβολικού. Οι τρομοκράτες χρησιμοποίησαν αυτού του είδους προπαγάνδας, με στόχο να προκαλέσουν την αντίδραση της πολιτικής σκηνής αλλά και της κοινής γνώμης για τις πράξεις τους. Για παράδειγμα, ο βομβαρδισμός

54 Βλέπε Paul Wilkinson, Terrorism and the Liberal State (New York: New York UP, 1986), 24.
55 Βλέπε Thornton, 85

του ομοσπονδιακού κτιρίου Murrah Federal[56] στην Οκλαχόμα είναι παράδειγμα του πόσο ένας συμβολικός στόχος μπορεί να προκαλέσει θέματα πέρα από την πράξη καθαυτή. Η συμβολική φύση της επίθεσης έστρεψε την προσοχή του έθνους καθώς επίσης ανάγκασε πολλές νομικές υπηρεσίες να επανεξετάσουν τις αποφάσεις τους.

Όταν υπάρχει προσπάθεια αναγκαστικής κατάργησης της κυβέρνησης από ομάδες που χρησιμοποιούν βία, τότε σύμφωνα με τον Thornton, ένας άλλος στόχος γίνεται ζωτικός για ένα τρομοκράτη:

> **Ο αποπροσανατολισμός είναι ο κατεξοχήν στόχος ενός τρομοκράτη, αφαιρώντας τα θεμέλια της τάξης στην οποία οι στόχοι δραστηριοποιούνται καθημερινά. Η στρατηγική κάθε ομάδας που προχωρά σε πράξεις βίας είναι η δικαιολογία ότι με αυτό το τρόπο, η ηγεσία του κάθε κράτους θα πάψει να αποπροσανατολίζει το λαό.**
> **Η επίδειξη είναι, ωστόσο, μόνο μία πλευρά της διαδικασίας αποπροσανατολισμού. Σε δεύτερο επίπεδο, ο στόχος είναι η απομόνωση του ατόμου από το κοινωνικό πλαίσιο. Ο υπέρτατος στόχος της διαδικασίας επιβολής τρόμου, σύμφωνα με την Hannah Arendt, είναι η απομόνωση του ατόμου, σύμφωνα με την οποία έχει μόνο τον εαυτό για να βασιστεί και δεν μπορεί να αντλήσει δύναμη από τα συνηθισμένα κοινωνικά στηρίγματα.** [57]

Εάν η εποχή της τεχνολογίας συνεχίζει να δημιουργεί μία κοινωνία που εξαρτάται από τους υπολογιστές για την επικοινωνία και την δραστηριότητα, κάθε παρέμβαση σε τέτοιου είδους διαύλους επικοινωνίας, θα είναι κρίσιμη για την δημιουργία αποπροσανατολισμού. Μία κυβέρνηση πρέπει να εξασφαλίσει ότι αυτά τα συστήματα στα οποία βασίζεται για την διατήρηση της τάξης και του ελέγχου, διαθέτουν σημαντικούς αμυντικούς μηχανισμούς ενάντια σε επιθέσεις τρομοκρατών και ανταρτών.

Εν τέλει, ένας από τους σκοπούς μίας τρομοκρατικής ομάδας μπορεί να είναι η πρόκληση απάντησης μετά το γεγονός. Συχνά, μία τρομοκρατική οργάνωση θα

56 Βλέπε Oklahoma Today. 9:02 am, April 19, 1995: The Official Record of the Oklahoma City Bombing. Oklahoma City: Oklahoma Today, 2005

57 "Thinking Out Loud", in Lingua Franca, fall 1999. (review, Politics, Philosophy, Terror: Essays on the Thought of Hannah Arendt)

πραγματοποιήσει μία βίαιη επίθεση με την ελπίδα ότι η κυβέρνηση ενός κράτους θα ανταποκριθεί άμεσα[58]. Για το λόγο αυτό, η κυβέρνηση πρέπει να φροντίσει να μην παίξει το παιχνίδι των τρομοκρατικών οργανώσεων. Στην κατά της τρομοκρατίας», πολλές φορές λαμβάνονται που θα επηρεάζουν όχι μόνο τον τρομοκράτη αλλά και το κοινωνικό σύνολο[59].

1.4 Είδη τρομοκρατίας

Η κατηγοριοποίηση των τρομοκρατικών οργανώσεων είναι μία αρκετά περίπλοκη υπόθεση. Η ανάλυση μέσα από την οποία θα διαχωριστεί η τρομοκρατία σε διαφορετικά είδη, είναι δυνατό να γίνει σε διαφορετικά πλαίσια, όπως της πολιτικής, κατά κύριο λόγο, της επικοινωνίας και προπαγάνδας, του εγκλήματος, κ.α. (Schmid and Jogman, 2005)[60]. Σύμφωνα, λοιπόν με εκείνα μπορούμε να εντοπίσουμε δέκα περίπου βάσεις ταξινόμησης της τρομοκρατίας, όπως φαίνεται παρακάτω:

1. Δρώντες
2. Θύματα
3. Αίτια
4. Περιβάλλον δράσης
5. Μέσα δράσης
6. Πολιτικός προσανατολισμός
7. Κίνητρα
8. Σκοποί
9. Απαιτήσεις
10. Στόχοι

είναι μία πράξη που εκτελείται από συγκεκριμένα υποκείμενα. Οι αυτουργοί της τρομοκρατίας, μπορεί να δρουν είτε σε ατομικό επίπεδο (ατομική τρομοκρατία) είτε

58 Βλέπε Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: University of Pennsylvania Press, 2004)

59 Βλέπε James Mitchell, "Identifying Potential Terrorist Targets" a study in the use of convergence. G2 Whitepaper on terrorism, copyright 2006, G2. Counterterrorism Conference, June 2006, Washington D.C.

60 Βλέπε Schmidt A. and A. Jongman (2005) *Political Terrorism, Piscataway,* NJ: Transaction Publishers.

ομαδικό (οργανώσεις). Σε δεύτερο επίπεδο, έχουμε τον πολιτικό προσανατολισμό, με αναφορές στα κίνητρα και τις καταβολές των δρώντων. Εν συνεχεία εξετάζουμε τις σκοπούς δράσης, που δεν είναι άλλου από την επιβολή του φόβου, και τέλος το γεωγραφικό περιβάλλον δράσης[61].

Αναλύοντας την τρομοκρατία σε επίπεδο δρώντων, δεν μπορούμε να μην εστιάσουμε στην γεωγραφική προέλευση του τρομοκράτη. Ο Waugh (1982)[62], εξετάζοντας το στοιχείο αυτό εισήγαγε τρεις κατηγορίες τρομοκρατίας:

1) Την εξαπλωμένη τρομοκρατία (spill-over terrorism, η οποία αποτελεί την χρήση βίας ενάντια σε αλλογενή άτομα και ιδιοκτησίες
2) Την εσωτερική τρομοκρατία, που έγκειται στις εθνικότητες των τρομοκρατών και των θυμάτων, με ομάδες αυτόχθονες στο κράτος το οποίο εχθρεύονται
3) Την εξωτερική τρομοκρατία, που σχετίζεται με την τοποθέτηση των τρομοκρατών ή των στόχων εκτός της επικράτειας του στόχου, εναντίον του οποίου επιθυμούν να δράσουν.

Η γεωγραφική κατηγοριοποίηση της τρομοκρατίας συστήνει μία σειρά από είδη όπως: **διεθνής τρομοκρατία, εγχώρια τρομοκρατία, διεθνική τρομοκρατία** και **παγκόσμια τρομοκρατία**. Ο Jenkins[63], υποστηρίζει ότι οι τρομοκρατικές ενέργειες που λαμβάνουν χώρα σε ξένα εδάφη, με στόχο την εξόντωση θυμάτων που σχετίζονται με το ξένο κράτος (διπλωμάτες, αξιωματούχους και απεσταλμένους για ειδικές αποστολές) κατατάσσονται στο χώρο της **διεθνούς τρομοκρατίας**. Από την άλλη κάθε ενέργεια που πραγματοποιείται από γηγενείς τρομοκράτες στα εδάφη τους, θεωρείται ως εγχώρια τρομοκρατία[64].

61 Βλέπε Schmidt A. and A. Jongman (1988) *Political Terrorism. A new guide to actors, authors, concepts, databases, theories and literature,* Amsterdam: North-Holland Publishing Company

62 Βλέπε Waugh, W.L. Jr. (1982) *International terrorism :how actions respond to terrorists,* Salisbury, N.C.: Documentary Publications

63 Βλέπε Jenkins, ΣΕΛ. *Images of Terror: What We Can and Can't Know About Terrorism.* New York: Aldine de Gruyter, 2003.
64 Βλέπε http://www.tkb.org/Methodologies.jsp

Αξίζει να αναφέρουμε επίσης μία ειδοποιό διαφορά μεταξύ **διεθνούς** και **διεθνικής** τρομοκρατίας. Ο Reinares (2005)[65], υπογραμμίζει ότι η δεύτερη περικλείει την πρώτη, αλλά όχι το αντίστροφο. Σύμφωνα με εκείνον, η **διεθνική** τρομοκρατία δρα διαμέσου των κρατών και αφορά άτομα δύο ή περισσότερων εθνικοτήτων, ενώ η **διεθνής** έχει να κάνει με την αλλαγή των δομικών στοιχείων και την ανακατανομή της ισχύος στο παγκόσμιο πολιτικό σύστημα. Τέλος η παγκόσμια τρομοκρατία, αφορά πέρα από την κατάργηση των γεωγραφικών συνόρων, πολιτικές και οικονομικές δραστηριότητες, όπως παγκοσμιοποίηση και τεχνολογική ανάπτυξη παρέχοντας τους δρώντες των τρομοκρατικών επιθέσεων με νέα μέσα και όργανα επιβολής[66].

Η εξερεύνηση των σκοπών και των κινήτρων δράσης, αποτελεί βασικός παρονομαστής στη μελέτη του φαινομένου της τρομοκρατίας, όπως αναφέρθηκε σε προηγούμενο κεφάλαιο. Ο Boyer Bell (1975)[67], παρουσιάζει μία συνολική κατηγοριοποίηση των τρομοκρατικών δραστηριοτήτων με βάση: α) την προσπάθεια των τρομοκρατών να πλήξουν τις οργανωτικές δομές ενός κράτους, την εσωτερική πειθαρχία και την αμεσότητα επιβολής δικαιοσύνης σε άτομα που διαπράττουν παράνομες ενέργειες, β) την αλληλεγγύη για τις πράξεις τους από τους απλούς πολίτες, γ) την υιοθέτηση λειτουργικών στρατηγικών για τις μελλοντικές δραστηριότητες τους, δ) την χειραγώγηση για τη δημιουργία ευκαιριακών καταστάσεων προκειμένου να ικανοποιηθούν τα αιτήματα τους, και ε) την συμβολική ιδιότητα των δραστηριοτήτων τους (βλέπε 1.3.1).

Η ανάλυση με βάση τα κίνητρα των επιθέσεων, αποτέλεσε αντικείμενο μελέτης των Hoffman (1999)[68] και Vasikenko[69] (2004) έχοντας ως στόχο την θέσπιση νέων κατηγοριών τρομοκρατίας. Συγκεκριμένα, ο πρώτος εισήγαγε τέσσερις βασικές

65 Βλέπε Reinares, F. (2005) 'Conceptualising International Terrorism', ARI, no. 82.

66 Βλέπε Speer, D.L. (2000) *Terrorist Motivations and Unconventional Weapons,* in ΣΕΛ.R. Lavoy et al.(eds). *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons,* Ithaca: Cornell University Press.

67 Βλέπε *Boyer Bell, J. (1975) Transnational Terror, Stanford, CA: Hoover Institution*

68 Βλέπε Hoffman, Bruce: *Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations.* Santa Monica, CA: RAND, 2003.

69 Βλέπε Vasilenko, V.I. (2004) *Terrorism as a challenge for national and international law: security vs liberty?,* Berlin: Springer.

κατηγορίες τρομοκρατών: 1) τους εθνικιστές τρομοκράτες, 2) τους τρομοκράτες ωθούμενους από ιδεολογικές προσεγγίσεις της αριστεράς, 3) τους ακροδεξιούς τρομοκράτες και 4) εκείνους που προχωρούν σε τρομοκρατικές ενέργειες με βάση το θρησκευτικό φρόνημα. Ο δεύτερος ακολουθεί μία παρόμοια διάκριση, αλλά εντοπίζει πέντε βασικές κατηγορίες:

1. **Πολιτική τρομοκρατία**: αποσκοπεί στον αγώνα για ανακατανομή της ισχύος
2. **Αυτονομιστική τρομοκρατία**: στοχεύει στην παραβίαση της εδαφικής ακεραιότητας μίας χώρας
3. **Εθνικιστική τρομοκρατία**: απομόνωση των άλλων εθνικοτήτων και εθνοτικών ομάδων από όλες τις σφαίρες επιρροής (πολιτική, κοινωνική, οικονομική, κ.α.)
4. **Θρησκευτική τρομοκρατία**: αναγνώριση του ηγετικού ρόλου της θρησκείας την οποία κάθε άτομο-ομάδα ακολουθεί και κατάπαυση άλλων θρησκευτικών φρονημάτων
5. **Εγκληματική τρομοκρατία**: έμφαση στο κέρδος, την καταστολή και την εξάλειψη άλλων αντιπάλων για την ικανοποίηση συγκεκριμένων σκοπών.

Μετά από αυτή την σύντομη αναφορά στα είδη της τρομοκρατίας, είναι φρόνιμο να εστιάσουμε στην ισλαμική τρομοκρατία, που έχει δραστηριοποιηθεί περισσότερο από κάθε άλλη σε διεθνές επίπεδο. Η καταγραφή σειράς γεγονότων, σε ευρωπαϊκό επίπεδο, μας δίνει μία πιο συγκεκριμένη εικόνα σχετικά με το κάθε είδος τρομοκρατίας.

1.4.1 Ισλαμική τρομοκρατία

i. Ιστορικό επιθέσεων

Το τρομοκρατικό χτύπημα των Διδύμων Πύργων του Παγκόσμιου Εμπορίου στη Νέα Υόρκη, σηματοδότησε την δημιουργία ενός ντόμινου εξελίξεων στην διεθνή πολιτική σκηνή με την επάνοδο του ισλαμικού φονταμενταλισμού και την εκπλήρωση αυτού μέσω τρομοκρατικών επιθέσεων[70]. Η διεθνής ασφάλεια δέχτηκε ένα ισχυρότατο πλήγμα και η μέχρι πρότινος μοναδική υπερδύναμη στον πλανήτη είχε κυριολεκτικά επέλθει σε ένα ψυχολογικό τέλμα. Η ισλαμική τρομοκρατία, παρά την μακρόχρονη δραστηριότητα[71] της, δεν θα μπορούσε να μην αποτελεί σημαντικό κομμάτι της διεθνούς τρομοκρατίας την τελευταία δεκαετία.

Πρόσφατες αναφορές[72] της Ευρωπαϊκής Ένωσης, δείχνουν ότι η γηραιά ήπειρος αποτέλεσε και αποτελεί αποδέκτη του ισλαμικού φονταμενταλισμού. Το 2008, καταγράφηκε μία επίθεση όπου ένας Βρετανός, ακολουθώντας τις πρακτικές της ισλαμικής τρομοκρατικής δράσης, τοποθέτησε εκρηκτικό μηχανισμό σε ένα εστιατόριο στην νοτιοδυτική ακτή της Αγγλίας. Ο μηχανισμός αποτελούσε δείγμα ερασιτεχνισμού από μέρους του δράστη, ο οποίος είχε μυηθεί στον ισλαμισμό. Τον Οκτώβρη του ίδιου έτους ομολόγησε την ενοχή του για σχεδιασμό και πράξη τρομοκρατικής επίθεσης, και καταδικάστηκε σε ισόβια κάθειρξη[73].

Με αφορμή αυτό το περιστατικό, μπορούμε να ανατρέξουμε στον αριθμό των συλλήψεων που πραγματοποιήθηκαν την ίδια χρονιά για υπόπτους τρομοκρατικών επιθέσεων σε χώρες-μέλη της Ευρωπαϊκής Ένωσης. Η πλειονότητα των επιθέσεων τα τελευταία χρόνια σε ευρωπαϊκό επίπεδο, εντοπίζεται στην Γαλλία[74] και την Ισπανία.

---

70 Rabasa Angel, *The Muslim world after 9/11*. Project Air Force. RAND Corporation 2004.

71 http://www.nytimes.com/2005/07/27/opinion/27iht-edpabst.html Blond Phillip and Pabst Adrian, The roots of Islamic terrorism. New York Times, July 28, 2005.

72 Europol, *The European Union (EU) Terrorism Situation and Trend Report (TE-SAT) 2008*

73 http://news.bbc.co.uk/2/hi/uk_news/england/devon/7434548.stm Ο Nicky Reilly, με το ψευδώνυμο Abdulaziz Rashid Saeed-Alim, αντιμετώπισε κατηγορίες για συνεργεία στην βομβιστική επίθεση του εστιατορίου Giraffe στη πόλη Exeter.

74 http://news.bbc.co.uk/2/hi/europe/8303658.stm Ο32χρονος άνδρας αλγερινής καταγωγής εργάζεται στην Ευρωπαϊκή Οργάνωση Πυρηνικών Ερευνών (CERN), το κύριο κέντρο της Ευρώπης μελετών

Άλλες χώρες που ανέφεραν τρομοκρατικές επιθέσεις είναι το Βέλγιο, η Δανία, η Αγγλία και η Γερμανία. Η καταγωγή των δραστών ήταν κυρίως από χώρες της Βόρειας Αφρικής, όπως Αλγερία, Μαρόκο, και φυσικά από γηγενείς των ευρωπαϊκών κρατών, όπως Βέλγιο και από χώρες της ανατολής (Τουρκία, Πακιστάν).

Η κυριότερη κατηγορία ήταν βασισμένη απλά σε ενδεχόμενη εμπλοκή σε τρομοκρατική επίθεση σε ότι αφορά την ισλαμική τρομοκρατία. Μελετώντας έναν αριθμό τρομοκρατικών επιθέσεων μπορούμε να εξάγουμε το συμπέρασμα ότι, οι ύποπτοι είναι μέλη τρομοκρατικών οργανώσεων, όπως Αλ Κάιντα[75]. Ωστόσο, υπήρξε και ένας μεγάλος αριθμός υπόπτων που δεν ανήκε σε κάποια γνωστή ισλαμική τρομοκρατική οργάνωση αλλά ακολουθούσε την ισλαμική ιδεολογία στον σχεδιασμό και την εκτέλεση των δράσεων. Με την πάροδο των χρόνων, ωστόσο, έχει παρατηρηθεί ότι οι νεότερες γενιές Ισλαμιστών που έχουν μετακινηθεί κυρίως στην ευρωπαϊκή επικράτεια, εστιάζουν σε μεγάλο βαθμό στη διδασκαλία του Ισλάμ, μη αποδεχόμενη την κουλτούρα της χώρας που κατοικούν[76]. Το γεγονός αυτό φανερώνει μία πολιτική διάσταση που έχει δοθεί στο Ισλάμ.

Η περισσότερο γνωστή ιδεολογία, είναι η επονομαζόμενη από την Αλ Κάιντα, ως «Τζιχάντ[77]». Επιπλέον υπήρχαν κατηγορίες που αφορούσαν την χρηματοδότηση των τρομοκρατικών επιθέσεων, σε επίπεδο σχεδιασμού, εκτέλεσης και προπαγάνδας. Από το 2005, χιλιάδες άτομα συνελήφθησαν στη Γαλλία με την κατηγορία ότι

πυρηνικής φυσικής, ήταν ένας από τους δύο αδελφούς που κρατούνται στην Βιέννη αντιμετωπίζοντας την κατηγορία ότι είχε σε επαφή με άτομα που συνδέονται με την Αλ Κάιντα του Ισλαμικού Μαγκρέμπ και τις σχεδιαζόμενες επιθέσεις. BBC news

75 Al-Qaeda in the Islamic Maghreb (AQIM)

76 Brent F. Nelsen *Religion and European Unity: Toward a Cultural Theory of Integration.* Prepared for delivery at The Annual Meeting of the American Political Science Association, Chicago I11, 30 August- 2 September 2007.

77 Ο όρος «Τζιχάντ» ή «Ιερός Πόλεμος» χρησιμοποιείται για να περιγράψει την θρησκευτική υποχρέωση των Μουσουλμάνων να μεταδώσουν την διδασκαλία του Ισλάμ μέσω της σύγκλισης πολεμικών συγκρούσεων. Το «Τζιχάντ» θεωρεί ότι οτιδήποτε αφορά την διάδοση της πίστης μέσω συγκρούσεων, ως «ιερό πόλεμο». Το Ισλάμ διακρίνει τέσσερις κατηγορίες, σύμφωνα με τις οποίες υπάρχουν τέσσερις τρόποι διάδοσης της πίστης, με τον **λόγο,** την **καρδιά,** το **χέρι** και το **σπαθί.** Ο πρώτος και ο τρίτος τρόπος αφορούν την εξάπλωση της πίστης μέσω προπαγάνδας για το τι είναι το «σωστό» και πως θα διορθωθεί το λάθος στις πράξεις των ατόμων. Ο δεύτερος αφορά την κάθαρση του πνεύματος ενάντια στη μάχη με το κακό. Ο τέταρτος και πιο δημοφιλής πλέον τρόπος είναι η πολεμική σύρραξη ενάντια σε όσους εχθρεύονται το Ισλάμ και σε όσους είναι άπιστοι. (πηγή Britannica Encyclopedia)

δημιούργησαν δίκτυα στήριξης στο Ιράκ, με την αποστολή εθελοντών. Πρόσφατες μελέτες ωστόσο δείχνουν ότι περισσότερο «δημοφιλής» προορισμός για συμμετοχή σε ένοπλη επίθεση είναι το Αφγανιστάν.

Το 50% των ατόμων που συνελήφθησαν τα τελευταία χρόνια, με την κατηγορία για συμμετοχή σε τρομοκρατικές επιθέσεις, κυμαίνονταν ηλικιακά από 31 έως 40 ετών. Τα άτομα αυτά, συνδέονταν κυρίως με την εκπαίδευση για λήψη τρομοκρατικής δράσης, αλλά και χρηματοδότησης αυτών. Οι νεαρότεροι από αυτούς, σχετίζονταν με την στρατολόγηση και την προπαγάνδα.

ii. Δραστηριότητες

Ανάμεσα στον ραγδαία αυξανόμενο πληθυσμό κατά τη δεκαετία του 2000 στην Ευρώπη, εντοπίζουμε μία μεγάλη μερίδα μεταναστών από τις χώρες που έχουν ως κύριο θρήσκευμα τον ισλαμισμό, είναι ιδιαίτερα εκτεθειμένες στην στρατολόγηση και στην ριζοσπαστικοποίηση. Για ορισμένο χρόνο, υπήρξαν ενδείξεις για την ύπαρξη συνδέσμων μεταξύ υποστηρικτών του «Τζιχάντ» στο Ηνωμένο Βασίλειο και των ομολόγων τους στο Πακιστάν.

Πληροφορίες από τις χώρες-μέλη της Ένωσης, αποκαλύπτουν ότι ο ρόλος των τζαμιών στην στρατολόγηση και ριζοσπαστικοποίηση των Ισλαμιστών τρομοκρατών είναι φθίνουσα. Αυτό, σε μεγάλο μέρος συνέβη εξαιτίας, του γεγονότος ότι οι μουσουλμανικές κοινότητες έχουν γίνει περισσότερο μάχιμες και πρόθυμες να αντιμετωπίσουν τον εξτρεμισμό[78]. Παρά το γεγονός ότι, κάποια από αυτά, χρησιμοποιούνται για ιδεολογική αφομοίωση, η στρατολόγηση, γίνεται σε μεγάλο βαθμό υπόγεια, με ελάχιστη προπαγάνδα από μέρους των τζαμιών. Οι κυριότεροι δρώντες της ισλαμικής τρομοκρατίας είναι, ακτιβιστές, με τη έννοια ότι δρουν πέρα από τα όρια που ορίζει το τζαμί[79]. Για το λόγο αυτό είναι σκόπιμο να διαχωρίσουμε

78 Anspaha Katrine, The Integration of Islam in Europe: Preventing the radicalization of Muslim diasporas and counterterrorism policy. Riga, Latvia 2008, 25 -27 September

79 Olesen Thomas, "*Social Movement Theory and Radical Islamic Activism".* Islamist as a. social movement. Centre for Studies in Islamism and Radicalization (CIR). Department of Political Science Aarhus University, Denmark, May 2009

την διαφορά της στρατολόγησης και της ριζοσπαστικοποίησης αναφορικά με την ισλαμική τρομοκρατία(βλέπε πίνακα)[80].

Στρατολόγηση (Recruitment)	Ριζοσπαστικοποίηση (Radicalization)
• Αφορά την διαδικασία σύμφωνα με την οποία τα άτομα γίνονται μέρος ενός συνόλου για να μοιραστούν τις σκέψεις και τους σκοπούς με τους υπολοίπους • Είναι απόφαση εθελοντικού χαρακτήρα • Μπορεί να επιτευχθεί μέσω προσκείμενων σε αυτών ατόμων ή οργανισμών.	• Αφορά την υιοθέτηση βίαιων στρατηγικών με στόχο την επίτευξη πολιτικών σκοπών • Έπεται του σταδίου της στρατολόγησης • Συμβαίνει κυρίως μέσα σε οργανισμούς.

Οι φυλακές και άλλα μέρη, στα οποία τα άτομα μπορεί να είναι ευάλωτοι, και στερούνται προσανατολισμού ή εμπειρίας σε προσωπική κρίση συνεχίζουν να αποτελούν πηγή ανησυχίας για ριζοσπαστικοποίηση.

Υπάρχουν εμφανείς διαφορές ανά κράτος μέσα στην Ευρωπαϊκή Ένωση, σχετικά με την επιστράτευση σχετικά με την Ισλαμική τρομοκρατία. Το διαδίκτυο, παίζει ένα σημαντικό ρόλο στην κατήχηση των νέων τρομοκρατών, Προσφέρει την πιθανότητα της διάδοσης μίας προπαγάνδας ανά συγκεκριμένο είδος κοινού. Παρά το γεγονός αυτό, το Διαδίκτυο δεν μπορεί να αντικαταστήσει την προσωπική συναναστροφή μεταξύ ενδεχόμενους νεοσύλλεκτους και στρατολόγους. Για παράδειγμα, η Αλ Κάιντα χρησιμοποιεί το διαδίκτυο, για:

1. Οικονομική ενίσχυση μέσω προπαγάνδας για την εξυπηρέτηση ενός κοινού σκοπού.

80 Olesen Thomas, *"Social Movement Theory and Radical Islamic Activism": Islamist as a social movement, sel 9.*

2. Την εκπαίδευση και την καθοδήγηση σε υποψήφιους τρομοκράτες
3. Επιχειρησιακά σχέδια επίθεσης μέσω ηλεκτρονικών συστημάτων και πληροφόρηση για πιθανούς στόχους[81]

Παρακάτω θα δούμε αναλυτικά την χρήση του Διαδικτύου για τρομοκρατικούς σκοπούς.

iii. Προπαγάνδα

Οι τρομοκράτες μπορούν να προωθήσουν την «ατζέντα» των θεμάτων τους μέσω των μέσων, και κατά κύριο λόγο μέσω του Ιντερνέτ, με μεγάλη ευκολία. Γεγονότα σε περιοχές, όπως η Μέση Ανατολή, το Πακιστάν και το Αφγανιστάν αποτελούν αντικείμενο εκμετάλλευσης από προπαγανδιστές που ακολουθούν την ιδεολογία του Τζιχάντ, με στόχο να προβάλλουν μία αφήγηση σχετικά με ένα υποτιθέμενο πόλεμο κατά του Ισλάμ. Αυτοί και άλλοι παράγοντες, συντελούν στο γεγονός ότι, ένας αυξανόμενος αριθμός ανθρώπων παρασύρονται από ένα, παγκόσμιας εμβέλειας, μήνυμα, το οποίο δημιουργείται από τους αποστολείς που θεωρούνται ως οι ηγέτες της Αλ Καιντα και κατά συνέπεια στρατολογείται από τρομοκρατικές οργανώσεις. Πέρα από αυτό, ο μεγάλος αριθμός ανθρώπων οι οποίοι εκφράζουν εξτρεμιστικές απόψεις, είναι αποτέλεσμα συνεχών προσπαθειών που έγιναν από τις αρχές που εμπλέκονται για την καλύτερη κατανόηση της φύσης της απειλής και την λήψη ορθής καταλυτικής δράσης, εκθέτοντας το πρόβλημα.

Η ιδεολογία της Αλ Κάιντα συνδέεται με την αποκλειστική σύνδεση των Μουσουλμάνων από την κοινωνία στην Ευρώπη, σε συγκρούσεις που λαμβάνουν χώρα στη Μέση Ανατολή , το Αφγανιστάν, το Πακιστάν , το Ιράκ, την Αλγερία και τη Σομαλία. Οι ιδεολόγοι από την διοίκηση της Αλ Κάιντα παίρνουν προβάδισμα από την ριζοσπαστική προπαγάνδα μέσω του Ιντερνέτ. Ο βαθμός, στον οποίο τέτοιο υλικό μπορεί να προκαλέσει έναν άνθρωπο να προχωρήσει σε τέτοιες πράξεις βίας είναι σπάνια διακριτός, αλλά αναμφίβολα αποτελεί αντικείμενο για διερεύνηση.

Ένα παράδειγμα μπορούμε να εντοπίσουμε στην Αυστρία το 2008, όπου δύο άτομα αντιμετώπισαν κατηγορίες από το δικαστήριο της Βιέννης, για εξάπλωση

81 Hoffman Bruce, T*he Use of Internet by Islamic Extremists.* House Parliamentary Select Committee on Intelligence. May 2006.

μηνυμάτων με περιεχόμενο προπαγανδιστικό στο Διαδίκτυο, με την ονομασία Global Media Islamic Front (GIMF)[82]. Καταδικάστηκαν κατά την πρώτη συνεδρία, για την μετάφραση στα Γερμανικά μηνυμάτων προπαγάνδας από μέρους των Ισλαμικών Οργανώσεων και για την δημοσίευση μηνύματος μέσω βίντεο, προσπαθώντας να εξαναγκάσουν τις κυβερνήσεις της Αυστρίας και της Γερμανίας να υποχωρήσουν από το Αφγανιστάν. Οι δύο κατήγοροι καταδικάστηκαν σε τέσσερα χρόνια φυλάκιση και 22 μήνες αντίστοιχα[83].

iv. Υλικοτεχνική υποστήριξη

Παρόλο που ορισμένα κράτη μέλη της Ένωσης θεωρούν την απειλή της ισλαμικής τρομοκρατίας χαμηλής επικινδυνότητας, πολλοί αναφέρουν δραστηριότητες σχετικά με, την υλικοτεχνική υποδομή των οργανώσεων. Οι τρομοκρατικοί πυρήνες στην Ισπανία, για παράδειγμα, έχουν διευκολύνει την είσοδο στην χώρα Ισλαμικών τρομοκρατικών οργανώσεων , είτε μέσω της παροχής ψευδών κρατικών εγγράφων (διαβατήρια, ταυτότητες, άδειες εισόδου και παραμονής, συμβάσεις εργασίας), είτε με την χρηματοδότηση και την εξασφάλιση καταφυγίων.

Στην Αυστρία, πολλές έρευνες βασίστηκαν στην υποψία για χρηματοδότηση ισλαμικών τρομοκρατικών οργανώσεων το 2008. Οι περισσότερες υποθέσεις ενεργοποιήθηκαν ως απάντηση στις κοινοποιήσεις που έγιναν από οικονομικά ινστιτούτα. Οι έρευνες έδωσαν βάση σε φυσικά και νομικά πρόσωπα. Οι ύποπτοι αποτελούνταν και από άτομα με καταγωγή από τη Βόρεια Αμερική, τα οποία φέρονται να έχουν συγκεντρώσει χρήματα για τρομοκρατικές οργανώσεις μέσω εγκλημάτων ιδιοκτησίας. Υπάρχουν ενδείξεις ότι, οι άνθρωποι αυτοί είναι μέρη ενός Ευρωπαϊκού δικτύου[84].

82 Global Islamic Media Front: Αποτελεί φορέα της ευρωπαϊκής προπαγάνδας της Αλ Κάιντα και άλλων ριζοσπαστικών ισλαμικών οργανισμών. Ο φορέας αυτός δημιουργήθηκε από Ισλαμιστές που ζουν στην Ευρώπη ιδιαίτερα στην Αυστρία και τη Γερμανία, πιθανόν ως απάντηση στην εισβολή των Αμερικανών στο Ιράκ το 2003. (πηγή http://globaljihad.net/view_page.asp?id=1752)

83 Γερμανική ομοσπονδιακή αστυνομία συνέλαβε δύο άνδρες την Τρίτη, Νοέμβριος 25,για τη λειτουργία μια ριζοσπαστική ισλαμική ιστοσελίδα και είναι πιθανό να αντιμετωπίσει κατηγορίες για υποστήριξη της τρομοκρατίας, των εισαγγελέων (πηγή http://www.dw-world.de/dw/article/0,,3821556,00.html)

84 TE SAT Report 2009, Europol, Austria

Στη Σουηδία[85], οι κάτοικοι που ακολουθούν το Ισλάμ, καθώς και τα δίκτυα που έχουν δημιουργήσει για την εξάπλωση της βίας, έχουν ιδρυθεί όχι μόνο για την επιθετική δράση εναντίον των στόχων , αλλά κυρίως για να χρησιμοποιήσουν την χώρα ως βάση για την υλικοτεχνική τους υποστήριξη για δραστηριότητες σε άλλες χώρες. Το ίδιο συμβαίνει και σε άλλες χώρες, όπως η Σλοβενία. Στην Σλοβενία, αναφορές έχουν δείξει ότι η χώρα μπορεί να χρησιμοποιηθεί ως ζώνη διέλευσης για να επιτρέψει στους τρομοκράτες να φτάσουν με μεγαλύτερη ταχύτητα στους στόχους τους. Μία άλλη περίπτωση, στο Ηνωμένο Βασίλειο, υπάρχουν-πέρα από άτομα που αναλαμβάνουν να πραγματοποιήσουν τις επιθέσεις εντός ή εκτός της χώρας- και άλλοι που παραμένουν σε ετοιμότητα για να δώσουν την υποστήριξη τους σε τρομοκράτες μέσω της διάθεσης των κεφαλαίων, υλικοτεχνικής ενίσχυσης και εκπαίδευσης[86]. Τα είδη της εκπαίδευσης ποικίλουν σε επίπεδο πρακτικών γνώσεων που απαιτούνται για να πραγματοποιήσουν τρομοκρατικές επιθέσεις, καθώς και την προώθηση εξτρεμιστικού υλικού.

Εκτός όμως από τις δραστηριότητες, μέσα στην Ευρωπαϊκή Ένωση, παρατηρήθηκαν πρόσφατα και τρομοκρατικές επιθέσεις από Ισλαμιστές πέρα από την ευρωπαϊκή περιφέρεια με θύματα όμως Ευρωπαίους πολίτες. Εξελίξεις και γεγονότα σε σχέση με την ισλαμική τρομοκρατική δράση, μπορεί να παρατηρηθούν σε χώρες της Βόρειας Αφρικής, όπου η AQIM, η οποία μετά την σύμπραξη με την ηγεσία της Αλ Κάιντα διέπραξαν υψηλής κλίμακας τρομοκρατικές επιθέσεις αυτοκτονίας στο λαό της Αλγερίας και σε κεφαλαιούχους της Αλγερίας στα τέλη του 2007[87]. Τον επόμενο χρόνο, οι επιθέσεις πολλαπλασιάστηκαν. Μερικές από αυτές, κατέληξαν με ένα μεγάλο αριθμό θυμάτων, όπως εκείνη τον Αύγουστο του 2008, όταν ένας «καμικάζι» σκόρπισε το θάνατο σε 43 άτομα και τραυμάτισε γύρω στα 38, μπροστά από μία στρατιωτική σχολή.

---

85 TE SAT Report 2009, Europol, Sweden

86 Hoffman Bruce, *The Use of Internet by Islamic Extremists*, σελ. 13.

87 The Al-Qaeda Organization in the Islamic Maghreb': The Evolving Terrorist Presence in North Africa", Inquiry and Analysis, Middle East Media Research Institute, 03-07-2007.

Σε ότι αφορά την Ασία και κυρίως την Μέση Ανατολή, υπάρχουν ενδείξεις ότι η επιρροή της Αλ Κάιντα στην Μεσοποταμία (η οποία αποτελεί την Ισλαμική Κοινότητα του Ιράκ), έχει περιοριστεί γεωγραφικά με τους αλλογενείς μαχητές να έχουν αποχωρήσει από την χώρα. Άτομα, που είναι μέλη της Αλ Κάιντα, έχουν στραφεί σε νέους στόχους όπως το Πακιστάν και το Αφγανιστάν, που θα δούμε παρακάτω.

Στο **Αφγανιστάν**, οι Ταλιμπάν, έφεραν την ευθύνη για έναν μεγάλο αριθμό επιθέσεων στην ενδοχώρα. Αρχικά σχετίζονταν με επιθέσεις σε στόχους υψηλού κύρους, όπως το ξενοδοχείο Serena[88], στις 14 Ιανουαρίου το 2008 και μία επίθεση αυτοκτονίας εναντίον της πρεσβείας της Δανίας στην Καμπούλ. Δεν υπάρχουν ασφαλείς αποδείξεις σχετικά με, τον αριθμό των επιθέσεων αυτοκτονίας στο Αφγανιστάν για το 2008. Όμως, ο αριθμός των επιθέσεων αυτού του είδους τα δύο προηγούμενα χρόνια εκτιμώνται ότι έφτασαν τις 145. Ένας αριθμός από αυτές τις επιθέσεις έχει πραγματοποιηθεί από ξένους μαχητές, στις οποίες έχει συμμετάσχει τουλάχιστον ένας Γερμανός.

Μαζί με το Αφγανιστάν, το Πακιστάν, παραμένει το κεντρικό σύνορο στη μάχη ενάντια στην Αλ Κάιντα και την ηγεσία της, καθώς και σε κινήματα που συμμερίζονται την ιδεολογία της, όπως οι Ταλιμπάν και η Ισλαμική Ένωση «Τζιχάντ». Υπάρχει σοβαρή υποψία, ότι τουλάχιστον το τμήμα της ηγεσίας της Αλ Κάιντα, τοποθετείται στις φυλετικές περιοχές και προσελκύει νέα σώματα από ξένους εθελοντές, όπως άτομα από την Ευρωπαϊκή Ένωση, στην περιοχή.

Στις 20 Σεπτεμβρίου του 2008, σημειώθηκε μία επίθεση εναντίον του ξενοδοχείου Marriott στο Ισλαμαμπάντ, η οποία μπορεί να θεωρηθεί ως ένα τεράστιο πλήγμα για τις πακιστανικές αρχές. Το ξενοδοχείο αυτό, είχε προηγουμένως γίνει στόχος τρομοκρατών «καμικάζι», χωρίς να έχουν ληφθεί τα απαραίτητα μέτρα ασφαλείας, προκειμένου να εμποδίσουν την μεταγενέστερη επίθεση στην πρεσβεία της Δανίας στο Πακιστάν, που κόστισε τη ζωή σε 60 άτομα. Τέλος, υπήρχαν και άλλες επιθέσεις εναντίον δυτικών, όπως την

88 Carnage in Kabul hotel, BBC News. (πηγή http://news.bbc.co.uk/2/hi/south_asia/7188196.stm)

βομβιστική επίθεση σε δημοφιλές εστιατόριο της πρωτεύουσας και εναντίον της πρεσβείας της Δανίας[89].

Κεφάλαιο 2 Η έννοια της κυβερνητικής ισχύος

Εισαγωγή

Το 2001, οι Ηνωμένες Πολιτείες Αμερικής, βίωσαν την μεγαλύτερη τρομοκρατική επίθεση στην ιστορία, τα αποτελέσματα της οποίας, επηρέασαν καταλυτικά το διεθνές πολιτικό σκηνικό. Το γεγονός αυτό, προκάλεσε πολλούς κυβερνητικούς μηχανισμούς, ανά την υφήλιο, να αναθεωρήσουν τις πρακτικές προστασίας και ασφάλειας τους. Επιπλέον, έδωσε μία εικόνα σχετικά με τις νέες μεθόδους, που ίσως υιοθετήσουν οι τρομοκράτες για να επιτύχουν τους στόχους τους. Οι επιθέσεις αυτές είχαν ως στόχο, να προκαλέσουν ζημιά είτε σε οικονομικό επίπεδο, είτε σε επίπεδο απώλειας της ανθρώπινης ζωής. Εν μέσω αυτών των αλλαγών, προκύπτει η λεγόμενη ηλεκτρονική τρομοκρατία ή τρομοκρατία του κυβερνοχώρου, που μπορεί να οριστεί ως πολιτικά υποκινούμενες επιθέσεις διαμέσου του κυβερνοχώρου[90]. Η απειλή αυτών των επιθέσεων ενισχύει πλέον την ανάγκη για περισσότερους ειδικούς σε θέματα υπολογιστών προκειμένου να αυξήσουν το επίπεδο ασφάλειας αυτών.

Η δεκαετία του 1970 σηματοδοτεί την δημιουργία του διαδικτύου που έμελλε να αποτελέσει μέσο ελέγχου δραστηριοτήτων πολιτικής και άλλης φύσεως. Το Διαδίκτυο, ή Internet, όπως αποκαλείται σήμερα, ήταν περισσότερο κεντρικό, περιοριζόμενο κυρίως στις αμερικανικές δραστηριότητες[91]. Ο Ψυχρός Πόλεμος και ο φόβος της Σοβιετικής Ένωσης έφερε την αποκέντρωση του Διαδικτύου. Η επόμενη

89 Six killed, 24 injured in blast near Danish Embassy". Associated Press of Pakistan. 2008-06-02. (πηγή http://www.ασελ..com.pk/en_/index.php?option=com_content&task=view&id=40082&Itemid=1)

90 Βλέπε Dorothy Denning, "A View of Cyberterrorism Five Years Later," 2007, σελ.. 2–3, http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf

91 Βλέπε Greg Goth, "Terror on the Internet: A Complex Issue, and Getting Harder," IEEE Computer Society, March 2008,www2.computer.org/portal/web/csdl/doi/10.1109/MDSO.2008.11.

δεκαετία, βρίσκει το Ιντερνέτ να είναι ανοιχτό στους ιδιωτικούς και δημόσιους χρήστες. Αυτό σήμαινε ότι ο καθένας με πρόσβαση σε αυτό, θα μπορούσαν να αποσπάσουν πληροφορίες από ολόκληρο τον κόσμο, όπου υπήρχε δυνατότητα σύνδεσης. Αυτό φυσικά δεν θα μπορούσε να στερήσει την δυνατότητα, ένας τρομοκράτης να χρησιμοποιήσει την ευελιξία που προσφέρει το Διαδίκτυο, με σκοπό να διαδώσει την βία και τον φόβο, μέσα από τον σχεδιασμό και την εκτέλεση τρομοκρατικών επιθέσεων.

Ο Weimann (2006)[92] υποστηρίζει ότι το Διαδίκτυο χαρακτηρίζεται αρχικά από ευκολία πρόσβασης σε ένα τεράστιο όγκο πληροφοριών με ελάχιστη ή μηδαμινή λογοκρισία, καθώς και κυβερνητικού ελέγχου γενικότερα. Η ταχύτητα διάδοσης των πληροφοριών, εξαπλώνεται σε ένα τεράστιο αριθμό ατόμων, διατηρώντας παράλληλα την ανωνυμία στην επικοινωνία μεταξύ αυτών. Η είσοδος και παραμονή εντός του ηλεκτρονικού δικτύου πραγματοποιείται με ελάχιστο κόστος, μέσα σε ένα περιβάλλον, δίνοντας την ευχέρεια συνδυασμού κειμένων, γραφικών, ηχητικών εκπομπών, καθώς και την προμήθεια κάθε είδους ηλεκτρονικού υλικού (ταινιών, βιβλίων, λογισμικών και έντυπου υλικού γενικότερα). Τέλος η ικανότητα έκθεσης στα μέσα μαζικής ενημέρωσης, καθιστά το διαδίκτυο ανεξάντλητη πηγή ιστοριών και ρεπορτάζ.

Ο Jaeger[93], μελετώντας το φαινόμενο της κυβερνότρομοκρατίας, αναφέρθηκε αρχικά σε ένα αριθμό συμβάντων στον κυβερνοχώρο. Το Νοέμβριο του 1999, ένας άνδρας από την Φλόριντα των Ηνωμένων Πολιτειών, κατηγορήθηκε ενώπιον του Ομοσπονδιακού Δικαστηρίου, για εκβιασμό και σεξουαλική παρενόχληση μέσω του Διαδικτύου, στην τιμωρία του οποίου συμμετείχε και το FBI (FBI, 1999). Δύο χρόνια αργότερα ένας νεαρός καναδικής καταγωγής, γνωστός ως «Mafia Boy», αντιμετώπισε πολλαπλές κατηγορίες υψηλής κλίμακας, σχετικά με την υπεξαίρεση χρημάτων από ιστοσελίδες που αφορούν το ηλεκτρονικό εμπόριο, όπως Google,

92 Βλέπε Gabriel Weimann. (2006). *Terror on the Internet. The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press, 309 σελ..

93 Βλέπε Jaeger, Carl "The Internet Encyclopedia", Southern Oregon University.

Yahoo, κ.α. Το δικαστήριο των κήρυξε ένοχο για 56 πράξεις ηλεκτρονικής απάτης για τις οποίες ο δράστης δεν έδειξε την παραμικρή μεταμέλεια (Raines, 2001) [94].

Ο υπ' αριθμόν ένα δράστης που κατηγορείται για απάτες μέσω του διαδικτύου, είναι ο λεγόμενος Kevin Mitnick, ο επονομαζόμενος ως «Κόνδορας» στα αρχεία του FBI, κατόρθωσε να «σπάσει τους κωδικούς πιστωτικών καρτών και να αντιγράψει αρχεία λογισμικών για υπολογιστές, αξίας δισεκατομμυρίων δολαρίων. Ο δράστης εξέτισε ποινή 5 χρόνων Randolph, 2006[95]). Το Ερευνητικό Κέντρο Τρομοκρατίας σχετικά με την πληροφόρηση, έδωσε αναφορά για 50 περίπου συμβάντα κατά την δεκαετία του 1980, που έχουν να κάνουν με παράνομη είσοδο σε ιστοτόπους, εγκλήματα κυβερνοχώρου και άρνηση εξυπηρέτησης μέσω του ηλεκτρονικού εμπορίου. Οι στόχοι αυτών μπορεί να είναι η NASA, το υπουργείο άμυνας των Ηνωμένων Πολιτειών, ο Λευκός Οίκος, αμερικανικές βάσεις, κ.α.

Οι πολίτες κάθε κράτους, κατανοούν ότι η βία μέσω του κυβερνοχώρου, επιδρά άμεσα σε αυτούς. Μία μελέτη που έγινε το Δεκέμβριο του 2001[96], έδειξε ότι το 75% του αμερικανικού πληθυσμού εκφράζει την ανησυχία του σχετικά με την κλοπή και την παράνομη χρήση προσωπικών πληροφοριών τους. Η χρήση αυτή μπορεί να αποσκοπεί σε κακόβουλους σχεδιασμούς και επίθεση εναντίον έργων υποδομής, όπως τηλεφωνικά δίκτυα και μονάδες παραγωγής ενέργειας.

2.1 Η σημασία της κυβερνητικής ισχύος (cyber power)

Η έννοια της ισχύος, αποτελεί ένα ευρύτατα διαδεδομένο όρο στις διεθνείς σχέσεις που χρησιμοποιείται για να περιγράψει την συμπεριφορά των κρατών στο διεθνές περιβάλλον. Ένας τέτοιος όμως όρος με τόσο μεγάλη χρησιμότητα, αλλά με δυσκολία απόδοσης ασφαλούς και ολοκληρωμένης ερμηνείας, δεν παύει να διατηρεί το ιδιαίτερο περιεχόμενο του. Όπως ακριβώς και πολλοί άλλοι όροι, η ισχύς είναι όρος σχετικός και άρρηκτα συνδεδεμένος με πλαίσιο στο οποίο χρησιμοποιείται, ανάλογα με τα συμφέροντα και τις αξίες των ανθρώπων που την χρησιμοποιούν. Ένας κοινός

94 Portraits: 9/11/01: The Collected "Portraits of Grief" from the New York Times

95 Βλέπε Kevin Mitnick and William L. Simon, Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, 2011.

96 Fafinski, S. (2009) Computer Misuse: Response, regulation and the law Cullompton: Willan

τόπος για να ξεκινήσουμε την ανάλυση μας, είναι να περιγράψουμε την ισχύ, ως «την ικανότητα να πραγματοποιούμε δράσεις», αλλά πιο συγκεκριμένα και κινούμενοι σε πολιτικό πλαίσιο, μπορούμε να ορίσουμε την ισχύ «**ως το όργανο επιρροής άλλων ατόμων για να διασφαλίσουν τα επιδιωκόμενα αποτελέσματα**». Φυσικά οι όροι ισχύς» και «επιρροή» χρησιμοποιούνται εναλλάξ, προκαλώντας περαιτέρω παρερμηνείες.

Ένας από τους σκοπούς για τους οποίους κάποιος μπορεί να χρησιμοποιήσει το όρο ισχύ είναι για να καταδείξει την ικανότητα ενός ατόμου ή ομάδας Α να επιβληθεί σε ένα άτομο ή μία ομάδα Β, καθώς και να εξετάσει το εύρος των ευκαιριών που ανοίγονται σε αυτόν. Σύμφωνα με τον Max Weber[97], η ισχύς περικλείει σε πρώτη φάση την κατοχή της ικανότητας επιβολής της θέλησης του ενός υποκειμένου δράσης απέναντι στο άλλο, συνοδευόμενο πάντα από τα μέσα υλοποίησης της δράσης. Για παράδειγμα, οι Ηνωμένες Πολιτείες Αμερικής, μπορεί να θελήσουν ανά πάσα στιγμή να επέμβουν στρατιωτικά εναντίον οποιουδήποτε απειλεί την ισορροπία στο διεθνές σύστημα, έχουν επίσης και τα απαραίτητα μέσα για να προχωρήσουν στην πραγματοποίηση της επέμβασης. Η παρατήρηση αυτή, μας βοηθά να κατανοήσουμε το ότι η άσκηση της ισχύος, προαπαιτεί την ύπαρξη ενός υποκειμένου και την θέληση αυτού μέσα σε μία πολιτική ή κοινωνική θέση[98], καθώς όμως και την αναφορά στο πλαίσιο δράσης, δηλαδή σε ποια θέματα εστιάζουν. Επιπλέον η έννοια της ισχύος αφορά και την αντίσταση στην επιβολή της θέλησης ενός υποκειμένου. Η ικανότητα αντίστασης στην πρωτοβουλία δράσης, προκαλεί την έκλυση της υπάρχουσας ισχύος, που σε αντίθετη περίπτωση δεν θα υπάρξει.

Κάτι που πρέπει να αναφέρουμε ακόμη, είναι ότι η εκδήλωση της ύπαρξης ή μη της ισχύος, εξαρτάται και από τα αποτελέσματα που θα προκύψουν μέσω αυτής. Εάν όμως εστιάσουμε αποκλειστικά στα αποτελέσματα, χωρίς να εξετάσουμε την ίδια την φύση αυτής, τότε δεν μπορούμε να κάνουμε ασφαλείς εκτιμήσεις για το περιεχόμενο της, όπως το τι προκάλεσε την ενδεχόμενη αντίσταση. Για το λόγο αυτό το πλαίσιο δράσης αποτελεί βασικό στοιχείο στη μελέτη μας.

97 Βλέπε Max Weber, 1947, σελ. 152

98 Βλέπε Jack Nagel, The descriptive Analysis of Power, (New Haven, Yale University Press, 1975), σελ.14

Η εξέλιξη της σύγχρονης κοινωνικής επιστήμης, προσπαθεί να δώσει νέες ερμηνείες στον όρο ισχύς, δίνοντας έμφαση, σε πρώτο επίπεδο, στην συμπεριφορά που προκύπτει από την κατοχή ισχύος, στην διάσταση που αφορά στην ατζέντα θεμάτων που αναφέρονται, και τέλος στην πραγματοποίηση των προτιμήσεων των άλλων ατόμων ή ομάδων. Μία ακόμη διάκριση μπορεί να πραγματοποιηθεί σχετικά με το φάσμα στο οποίο γίνεται η άσκηση μίας συμπεριφοράς, εξετάζοντας την ισχύ με όρους, όπως πειθώ και θέλγητρα. Η πρώτη αφορά την λεγόμενη «σκληρή» ισχύ και η δεύτερη αφορά την λεγόμενη ήπια. Το φάσμα της ήπιας και της σκληρής ισχύος, μπορεί να περιγραφεί από το παρακάτω σχήμα[99]

Σκληρή Ισχύς Ήπια Ισχύς

Διαταγή> Εξαναγκασμός Απειλή Πληρωμή Κύρωση Πλαίσιο Πειθώ Έλξη <Συνεργασία

Για παράδειγμα μπορούμε να αναφέρουμε την σχέση ισχύος μεταξύ ενός οργάνου άσκησης της δικαιοσύνης και ενός κατηγορούμενου για αδίκημα, στο αμερικανικό σύστημα δικαιοσύνης. Σε πρώτη φάση έχουμε την επιβολή κυρώσεως (φυλάκιση) για το αδίκημα που διέπραξε ο κατηγορούμενος. Σε δεύτερη φάση έχουμε την εξέταση του ιστορικού δράσης του κατηγορουμένου (μητρώο, κ.α.) με στόχο την ελάφρυνση της ποινής και την δυνατότητα έκδοσης αναστολής της ποινής και τέλος υπάρχει ειδική καθοδήγηση από ειδικούς επιστήμονες, προκειμένου να διορθωθούν στάσεις και συμπεριφορές του κατηγορουμένου που θα διευκολύνουν την επανένταξη του στην κοινωνία. Η τελευταία φάση αποτελεί παράδειγμα χρήσης της ήπιας ισχύος, η οποία όμως, όπως αναφέραμε εξαρτάται από την ικανότητα πειθούς και την εμπιστοσύνη που απαιτείται.

Επιστρέφοντας στην πολιτική ανάλυση του όρου, κατανοούμε ότι υπάρχουν χώρες που κινούνται σε μεγάλο βαθμό με κανόνες σκληρής ισχύος, όπως οι Ηνωμένες Πολιτείες, που βρίσκονται να μοιράζονται την διεθνή πολιτική σκηνή με νέους κρατικούς δρώντες, αντιμετωπίζοντας προβλήματα στο να ελέγξουν το εύρος δράσης στο πλαίσιο του κυβερνοχώρου. Ο κυβερνοχώρος, δεν μπορεί να αντικαταστήσει την

99 Βλέπε J.S. Nye, Soft Power: The means to Success in World Politics,(New York, Public Affairs Press, 2004)

γεωγραφική έκταση ενός κράτους ούτε να καταργήσει την εδαφική κυριαρχία του, αλλά η διάδοση της ισχύος στον κυβερνοχώρο θα συνεχίζει να υπάρχει

.

2.2 Ερμηνεία του όρου Κυβερνητική ισχύς (cyber power)

Η ισχύς που σχετίζεται με πληροφοριακούς φορείς δεν είναι καινούρια έννοια, η ισχύς μέσω του κυβερνοχώρου, όμως είναι. Υπάρχουν πολλοί ορισμοί του κυβερνοχώρου, αλλά όπως αναφέρθηκε είναι το πλαίσιο στο οποίο λαμβάνουν χώρα δραστηριότητες μέσω πολυμέσων και ηλεκτρονικών υπολογιστών διαμέσου αλληλένδετων συστημάτων, για εκμετάλλευση της πληροφορίας. Η ισχύς εξαρτάται από το πλαίσιο, όπως είπαμε και η κυβερνητική ισχύς αφορά τα πεδία δράσης του κυβερνοχώρου.

Κάποιες φορές ίσως μας διαφεύγει πόσο πρόσφατη είναι η έννοια του κυβερνοχώρου. Το 1969, το Υπουργείο Άμυνας των ΗΠΑ, ξεκίνησε μία μικρής κλίμακας σύνδεση μεταξύ υπολογιστών με την ονομασία APRANET, και το 1972, οι κωδικοί για ανταλλαγή πληροφοριών (TCP/IP) δημιουργήθηκαν για να συγκροτήσουν ένα δίκτυο ψηφιακής πληροφόρησης[100]. Η εισαγωγή των διευθύνσεων που δίνουν πρόσβαση στον κυβερνοχώρο, δημιουργήθηκαν το 1983. Το διαδίκτυο, με την σημερινή του μορφή δημιουργήθηκε το 1989, ταυτόχρονα με την εισαγωγή της διεθνώς αναγνωρισμένης μηχανής αναζήτησης, της Google που δημιουργήθηκε το 1998. Η δεκαετία του 1990, βρίσκει τις επιχειρήσεις να χρησιμοποιούν το νέο αυτό μέσο, για να ενισχύσουν την παραγωγική διαδικασία, καθώς και να συντονίσουν την προμήθεια προϊόντων μέσω ενός παγκόσμιου δικτύου κατανομής. Μία σημαντική χρονιά είναι επίσης το 1998, όπου η αμερικανική κυβέρνηση να σχεδιάζει σημαντικά σχέδια υλοποίησης πολιτικών και στρατηγικών για την εθνική ασφάλεια. Οι χρήστες του Ιντερνέτ, κατά το πρώτο μέρος της δεκαετίας του 1990, έφτασαν τα δύο δισεκατομμύρια[101]. Πρακτικά οι κυβερνήσεις και οι περιφερειακές αρχές παίζουν ένα σημαντικό ρόλο αλλά το πλαίσιο δράσης σημειώνει υπερβολική διασπορά ισχύος[5].

100 Franklin Kramer, "Cyberpower and National Security," in Kramer, αναφ., 12

101 Βλέπε Stuart H. Starr, "Toward a Preliminary Theory of Cyber power," in Kramer et al., eds, αναφ., σελ.52

Ο κυβερνοχώρος μπορεί να θεωρηθεί, ως ένα πεδίο πολύπλευρων δράσεων, αλλά μία πρώτη εκτίμηση οδηγεί στην αντίληψη ότι είναι ένα μοναδικό υβριδικό σύστημα από φυσικές και εικονικές ιδιότητες[102]. Τα φυσικά στρώματα των υποδομών ακολουθούν τους οικονομικούς κανόνες των αντίπαλων πόρων και των αυξανόμενων οριακών κοστών, και τους πολιτικούς κανόνες του ελέγχου και της κυρίαρχης δικαιοδοσίας[103]. Επιθέσεις μέσω του εικονικού στρώματος του κυβερνοχώρου, όπου το κόστος είναι χαμηλότερο, ενάντια στο πραγματικό μέρος του κυβερνοχώρου μπορεί να έχει συνέπειες σε τοπικό και διεθνές επίπεδο.

Η ισχύς που δίνει ο κυβερνοχώρος, μπορεί να οριστεί με όρους που αφορούν την δημιουργία, τον έλεγχο και την επικοινωνία μέσω ηλεκτρονικών υπολογιστών σε κρατικές δομές, δίκτυα, λογισμικά προγράμματα, ανθρώπινο δυναμικό. Με βάση την συμπεριφορική άποψη, η κυβερνητική ισχύς, είναι η ικανότητα απόκτησης επιθυμητών αποτελεσμάτων μέσω της χρήσης ηλεκτρονικά συνδεδεμένων επικοινωνιακών φορέων και οργάνων ισχύος[104]. Η κυβερνητική ισχύς χρησιμοποιείται για να παράγει επιθυμητά αποτελέσματα, μέσα στο κυβερνοχώρο, ή να χρησιμοποιήσει τα ήδη υπάρχοντα μέσα για να αποδώσει τα επιθυμητά αποτελέσματα σε πλαίσια εκτός αυτού.

Για να κατανοήσουμε την σημασία της κυβερνητικής ισχύος, μπορούμε να αντλήσουμε παραδείγματα από άλλα είδη ισχύος, που μας έχουν δοθεί μέσα από την παγκόσμια ιστορία. Η ναυτική ισχύς, ο οποίος σύμφωνα με την γεωπολιτική ανάλυση, έχει δοθεί από τον Alfred Mahan[105], αφορά μεν την νίκη επί του πεδίου των ωκεανών μέσω των πλοίων, αλλά και την ικανότητα ανάπτυξης του θαλάσσιου εμπορίου και την δυνατότητα εκπλήρωσης στρατηγικών βλέψεων μεταξύ των κρατών. Η ναυτική ισχύς, προσαρμόστηκε σε νέα δεδομένα που προέκυψαν μέσα από την ανάπτυξη της τεχνολογίας, όπως χρήση βομβαρδιστικών πλοίων μικρής και μεγάλης κλίμακας, αεροπλανοφόρων, κ.α. Οι πολιτικές εξελίξεις, κυρίως κατά τον Β'

102 Βλέπε Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World, Oxford, Oxford University Press, 2006.

103 Βλέπε Martin Libicky, Cyber deterrence and Cyber war, Santa Monica, RAND, 2009. σελ.12. The internet can be βλέπε in multiple layers. Βλέπε Marjory Blumental and David D. Clark, "The Future of the Internet and Cyber Power," in Kramer, et al eds., Cyber Power and National Security.

104Βλέπε Kuehl, in Kramer, αναφ. above, σελ. 38

105 Mahan, Alfred Thayer. The Influence of Sea Power upon History, 1660–1783 (1890)

Παγκόσμιο πόλεμο, οδήγησαν την εξέταση των ευκαιριών που δίνονται από το γεωπολιτικό περιβάλλον, εστιάζοντας σε νέες στρατηγικές, όπως η αεροπορική στρατηγική. Αντιλαμβανόμενοι τις ευκαιρίες που δίνονται μέσω αέρος, έστρεψαν το ενδιαφέρον τους προς τα εκεί, αναλογιζόμενοι την δυνατότητα που προσφέρει να προκαλεί ακαριαία χτυπήματα σε νευραλγικά σημεία των αντιπάλων.

Φτάνοντας στο θέμα της κυβερνητικής ισχύος, κατανοούμε την ευελιξία και την ευρύτητα των μέσων που προσφέρονται μέσω του κυβερνοχώρου, αφού εκείνος είναι περισσότερο εύπλαστος από κάθε άλλο πλαίσιο ανάπτυξης ισχύος. Τα γεωγραφικά όρια που δίνονται από χερσαία και υδάτινα περιβάλλονται, δύσκολα μεταβάλλονται. Αντίθετα, ο κυβερνοχώρος μπορεί να ελεγχθεί και να μεταβληθεί με το πάτημα ενός κουμπιού[106]. Συν τοις άλλοις το κόστος κίνησης και δραστηριότητας είναι ελάχιστο, σε αντίθεση με το φυσικό περιβάλλον.

Η ασφάλεια ακόμη, του κυβερνοχώρου παραμένει σε χαμηλά επίπεδα, η οποία μπορεί να γίνει αντικείμενο εκμετάλλευσης από μικρά κράτη και μη Κυβερνητικούς Οργανισμούς[107]. Σε αντίθεση με άλλα είδη ισχύος, όπως ναυτική και αεροπορική ισχύς, η κυβερνητική ισχύς, μοιράζεται χαρακτηριστικά με την φυσική ισχύ: τον αριθμό των δρώντων, τη εύκολη πρόσβαση και την ευκαιρία για απόκρυψη στοιχείων. Ένα κράτος, το οποίο είναι υπερδύναμη εδαφικά και πολιτικά, δεν σημαίνει ότι διαθέτει ίσες δυνατότητες στον κυβερνοχώρο. Εάν οι στρατιωτικές και οικονομικές δραστηριότητες, εμπλέκονται άμεσα με συστήματα του κυβερνοχώρου, οι οποιαδήποτε αδυναμίες μπορεί να αξιοποιηθούν άμεσα από μη Κυβερνητικούς παράγοντες[108].

Ο βαθμός της σύγκρουσης μέσα στο κυβερνοχώρο είναι διαφορετικός απ' ότι στο γεωγραφικό χώρο. Οι ισχυρές δυνάμεις μπορεί να κατέχουν το πλεονέκτημα στην χρήση μεγάλης κλίμακας ισχύος, οι αποδέκτες- υπερασπιστές όμως, έχουν πλήρη επίγνωση του περιβάλλοντος με τις δυνατότητες και τις αδυναμίες τους. Η

106 Βλέπε Gregory J Ratrray, "An environmental Ασελ.roach to Understanding Cyber Power," in Kramer et al, eds. Cyber power and National Security, σελ.253-374

107 Jordan, T. (1999a) Cyberpower: The Culture and Politics of Cyberspace and the Internet, London: Routledge

108 Kollock, ΣΕΛ. and Smith, M. (eds) (1998) Communities in Cyberspace, London: Routledge

κινητικότητα και οι πόροι έχουν μεγάλο κόστος. Στο εικονικό περιβάλλον, που προωθείται μέσω του κυβερνοχώρου , οι δρώντες διατηρούν την ανωνυμία τους, η απόσταση μεταξύ αυτών μηδενίζεται και η οποιαδήποτε επίθεση έχει μηδαμινό κόστος. Η επίθεση έχει μεγαλύτερο πλεονέκτημα από την άμυνα. Ο γεωγραφικά ισχυρότερος κρατικός δρώντας δεν μπορεί να αφοπλίσει ή να εξαλείψει τον εχθρό με την ίδια ευκολία. Η πολυπλοκότητα, η προσαρμοστικότητα και η γρήγορη επαναφορά των μέσων στον κυβερνοχώρο, είναι χαρακτηριστικά των επιθέσεων που πραγματοποιούνται μέσω του κυβερνοχώρου.

Η κυβερνητική ισχύς μπορεί να διαχωριστεί σε, α) **εσωτερική ισχύς του κυβερνοχώρου** και β) **εξωτερική ισχύς του κυβερνοχώρου**. Ο διαχωρισμός αυτός, μπορεί να συσχετιστεί με την ναυτική ισχύ που αφορά την πολεμική ισχύ και εκείνη που περικλείει οικονομικές και άλλες δραστηριότητες (εμπόριο, κ.α.). Η διάκριση αυτή περιλαμβάνεται στον παρακάτω πίνακα.

Πίνακας 1

Φυσικές και Εικονικές διαστάσεις και στόχοι της κυβερνητικής ισχύος

	Εξωτερικό πλαίσιο	**Εσωτερικό πλαίσιο**
Όργανα Πληροφόρησης	Σκληρή ισχύς: επιθέσεις μέσω άρνησης υπηρεσιών Ήπια ισχύς: δημιουργία κανόνων και δεδομένων	Σκληρή ισχύς: επίθεση σε συστήματα SCADA Ήπια ισχύς: διπλωματική καμπάνια για επιρροή κοινής γνώμης
Φυσικά μέσα	Σκληρή ισχύς: κυβερνητικοί έλεγχοι σε επιχειρήσεις Ήπια ισχύς: υποδομή για την διευκόλυνση προπαγάνδας ακτιβιστών.	Ήπια ισχύς: εκρηκτικοί μηχανισμοί και αποκοπή τηλεπικοινωνιών Σκληρή ισχύς: διαμαρτυρίες κατ' όνομα.

Όπως περιγράφει ο πίνακας 1, στο εσωτερικό πλαίσιο του κυβερνοχώρου, τα όργανα της πληροφορίας συνηθίζουν να παράγουν ήπια ισχύ μέσω πειθούς και έλξης. Για παράδειγμα, η ελεύθερη δίχως περιορισμούς διανομή λογισμικού υλικού, από προγραμματιστές αποτελεί δείγμα άσκησης ήπιας ισχύος.

Οι πόροι του κυβερνοχώρου, μπορούν ακόμη να παράγουν και σκληρή ισχύ μέσα σε αυτόν. Για παράδειγμα, κρατικοί ή μη κρατικοί δρώντες μπορούν να οργανώσουν μία επίθεση μέσω άρνησης εκπλήρωσης υπηρεσιών χρησιμοποιώντας «πειρατικά δίκτυα» με χιλιάδες υπολογιστές οι οποίοι πλημμυρίζουν μία εταιρεία ή το διαδικτυακό σύστημα μίας χώρας και αναστέλλουν την λειτουργία τους. Όπως θα δούμε παρακάτω, τα «πειρατικά δίκτυα», και η οργάνωση αυτών μπορεί να είναι αρκετά πολυέξοδη και χρονοβόρα.

Επιπλέον, η πληροφορία μέσω του κυβερνοχώρου, μπορεί να ταξιδέψει μέσω αυτού, για να δημιουργήσει ήπια ισχύ με το να προσελκύει πολίτες από άλλα κράτη. Μία διπλωματική καμπάνια, μέσω του διαδικτύου, είναι μία τέτοια περίπτωση. Όμως τέτοιου είδους πληροφόρηση, μπορεί να αποτελέσει πηγή σκληρής ισχύος η οποία είναι σε θέση να προκαλέσει φυσικές καταστροφές στο αντίπαλο κράτος ή μη κυβερνητικό οργανισμό. Για παράδειγμα, πολλές βιομηχανίες, επιτηρούνται μέσω συστημάτων **SCADA** (Supervisory Control and Data Acquisition)[109]. Ακόμη επικίνδυνο λογισμικό πρόγραμμα, μπορεί να προσβάλλει οποιαδήποτε δραστηριότητα, με πραγματικά καταστροφικά αποτελέσματα. Εάν ένας hacker, προσβάλλει το σύστημα ηλεκτροδότησης μίας ισχυρής χώρας, όπως οι ΗΠΑ ή η Γερμανία, μπορεί να προκαλέσει ανάλογες καταστροφές με εκείνες ενός εκρηκτικού μηχανισμού.

Γενικότερα ο πίνακας υποστηρίζει ότι φυσικά μέσα μπορούν να προκαλέσουν τόσο σκληρή όσο και ήπια ισχύ ενάντια στο διαδίκτυο. Το στρώμα της πληροφόρησης από τον κυβερνοχώρο, έγκειται σε μία φυσική υποδομή η οποία είναι εκτεθειμένη σε κινδύνους, άμεσης στρατιωτικής επίθεσης ή σαμποτάζ είτε από κυβερνήσεις είτε από τρομοκράτες ή εγκληματίες. Τα δίκτυα των υπολογιστών είναι δυνατό να καταστραφούν εάν τα καλώδια σύνδεσης ή οι κεντρικοί υπολογιστές υποστούν φθορές. Σε ότι αφορά, το πεδίο της ήπιας ισχύος, μη κυβερνητικοί οργανισμοί μπορούν να οργανώσουν προπαγάνδες ενάντια σε κυβερνήσεις και επιχειρήσεις, προσβάλλοντας την εικόνα τους στο διαδίκτυο. Για να κατανοήσουμε καλύτερα, την έννοια της ισχύος στον κυβερνοχώρο, είναι χρήσιμος ο επόμενος πίνακας.

109 Βλέπε Martin C. Libicki, Cyberdeterrence and Cyberwarfare (Santa Monica: RAND, 2009), xiii. Βλέπε ακόμη William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, D.C.: National Academies Press, 2009).

Πίνακας 2

Τα τρία πρόσωπα στο πλαίσιο του κυβερνοχώρου

1ο πρόσωπο: εξαναγκασμός του δρώντα Α έναντι στον Β, ακόμη κι αν ο Β έχει διαφορετική επιθυμία **Σκληρή Ισχύς:** άρνηση εξυπηρέτησης επιθέσεων, εισαγωγή επιζήμιου λογισμικού **Ήπια Ισχύς:** εκστρατεία πληροφόρησης με σκοπό να μεταβάλλει τις αρχικές προτιμήσεις των hacker, στρατολόγηση νέων μελών τρομοκρατικών οργανώσεων
2ο πρόσωπο: Έλεγχος ατζέντας: ο Α αποκλείει επιλογές του Β με το να αποκλείει αντίστοιχες στρατηγικές του. **Σκληρή Ισχύς:** τείχη προστασίας(firewall), άσκηση πίεσης **Ήπια Ισχύς:** εξετάζει τα όρια διανομής λογισμικών προγραμμάτων.
3ο πρόσωπο: ο Α διαμορφώνει προτιμήσεις του Β με στόχο να αποκλείσει συγκεκριμένες μελλοντικές στρατηγικές. **Σκληρή Ισχύς:** μη νομιμοποίηση ιδεών **Ήπια Ισχύς:** πληροφόρηση για δημιουργία προτιμήσεων, ανάπτυξη κανόνων μεταστροφής (π.χ. παιδική πορνογραφία).

Το πρώτο πρόσωπο της ισχύος, αφορά την ικανότητα ενός δρώντα να επιβάλλει σε άλλους να πράξουν αντίθετα με αυτό που επιθυμούν. Παραδείγματα που σχετίζονται με την σκληρή ισχύ, περιλαμβάνουν την σύλληψη υπόπτων που επιχειρούν να στείλουν τα μηνύματα τους μέσω του κυβερνοχώρου. Σε ότι αφορά την ήπια ισχύ, ένα άτομο ή ένας οργανισμός μπορεί να πείσει τους άλλους να αλλάξουν την συμπεριφορά τους. Η κυβέρνηση της Κίνας για παράδειγμα, κάποιες φορές για να κινητοποιήσει Κινέζους φοιτητές, ενάντια στην Ιαπωνία, όταν αξιωματούχοι

εξέφρασαν απόψεις που προσέβαλαν τις κινεζικές απόψεις για την σύγκρουση που έλαβε χώρα την δεκαετία του 1930[110].

Το δεύτερο πρόσωπο της ισχύος, είναι η ρύθμιση ατζέντας ενός δρώντα, αποκλείοντας επιλογές και στρατηγικές ενός άλλου δρώντος. Εάν αυτό είναι ενάντια στην θέληση του, τότε είναι δείγμα σκληρής ισχύος, σε αντίθετη περίπτωση είναι δείγμα ήπια ισχύος. Ένα αρκετά πρόσφατο παράδειγμα είναι η επέτειος της Ιρανικής επανάστασης, τον Φεβρουάριο του 2010, όπου η κυβέρνηση έθεσε το διαδίκτυο σε χαμηλή λειτουργία, για να εμποδίσει τους διαμαρτυρόμενους να στείλουν βίντεο διαμαρτυρίας σε δημοφιλείς διαδικτυακούς τόπους (YouTube), όπως είχαν κάνει έξι μήνες πριν[111].

Το τρίτο πρόσωπο της ισχύος, αναφέρεται στην διαμόρφωση προτιμήσεων και στον αποκλεισμό μελλοντικών στρατηγικών. Σε επίπεδο επιβολής της σκληρής ισχύος, αφορά την άρση της νομιμοποίησης κάποιων ιδεολογιών και σε επίπεδο ήπιας ισχύος σχετίζεται με την προσπάθεια να θέλουν να διαμορφώσουν προτιμήσεις[112]. Για παράδειγμα, η Γερμανία και η Γαλλία υποχρεώνουν την παύση των συζητήσεων σχετικά με την ναζιστική ιδεολογία[113]. Οι Ηνωμένες Πολιτείες κάνουν εκστρατεία ενάντια σε εταιρείες που εκδίδουν πιστωτικές κάρτες, προκειμένου να εμποδίσουν την έξαρση τυχερών παιχνιδιών[114].

2.3. Οι δρώντες και οι σχετικοί πόροι ισχύος

Η ροή της ισχύος στο πλαίσιο του κυβερνοχώρου κινείται με υπερβολικά γοργούς ρυθμούς. Εκπροσωπείται από έναν μεγάλο αριθμό δρώντων και από μία σχετική

110 Βλέπε Goldsmith and Wu, σελ. 180

111 Βλέπε http://www.youtube.com/watch?v=JZzMTQClJvo June 26, 2009 campaign and demonstrations in Helsinki,Youtube (June 26, 2009)

112 Βλέπε Max Weber, The Theory of Social and Economic Organization (New York: Oxford UP, 1947), 149

113 Βλέπε Max Weber, The Theory of Social and Economic Organization (New York: Oxford UP, 1947), 152

114 Βλέπε LTC David E. A. Johnson and Steve Pettit, "Principles of the Defense for Cyber Networks," Defense Concepts 4, 2 (Jan 2010), 17.

μείωση των στοιχείων διαφοροποίησης μεταξύ τους. Ένας δράστης, οποιαδήποτε ηλικίας μπορεί να προκαλέσει τεράστιες καταστροφές στα ηλεκτρονικά συστήματα. Οι Ηνωμένες Πολιτείες είναι η πρώτη χώρα παγκοσμίως στην εισβολή των υπολογιστικών συστημάτων την προηγούμενη χρονιά. Όπως αναφέρθηκε παραπάνω, οι τρομοκρατικές οργανώσεις χρησιμοποιούν το διαδίκτυο για να στρατολογήσουν νέα μέλη. Επιπλέον, πολιτικοί και κοινωνικοί ακτιβιστές μπορούν να προσβάλουν δικτυακούς τόπους εταιρειών και κυβερνήσεων. Μία ειδοποιός διαφορά σε ότι αφορά την ισχύ του κυβερνοχώρου, είναι οι διαφορετικοί πόροι που χρησιμοποιούνται και ακόμη το ολοένα και μικρότερο διάστημα μεταξύ κυβερνητικών και μη δρώντων.

Μπορούμε να διακρίνουμε τους δρώντες αυτούς, σε τρεις κατηγορίες: κυβερνήσεις, οργανισμούς με ιδιαίτερης δόμησης δίκτυα και άτομα με τυχαία οργάνωση. Στον πίνακα που ακολουθεί περιγράφονται οι εξής κατηγορίες δρώντων[115].

Πίνακας 3

Σχετικοί πόροι ισχύος των δρώντων στον Κυβερνοχώρο[116]

Α. Κυβερνήσεις 1. ανάπτυξη και υποστήριξη υποδομών, εκπαίδευσης και πνευματικής ιδιοκτησίας 2. νομική και φυσική επιβολή των ατόμων και μεσολαβητών που τίθενται μεταξύ των συνόρων 3. μέγεθος της αγοράς και έλεγχος πρόσβασης, π.χ. Κίνα, Ευρωπαϊκή Ένωση 4. πόροι διαθέσιμοι για επιθέσεις: γραφειοκρατία, προϋπολογισμοί, υπηρεσίες πληροφοριών 5. παροχή δημοσίων αγαθών, π.χ. κανονισμοί για διεξαγωγή εμπορικών συναλλαγών 6. φήμη για νομιμότητα, αγαθοεργία, επάρκεια για την άσκηση ήπιας ισχύος **Κυριότερες αδυναμίες:** υψηλή εξάρτηση από εύκολα προσβαλλόμενα συστήματα, πολιτική σταθερότητα, απώλεια φήμης
Β. Οργανισμοί και υψηλών υποδομών δίκτυα 1. τεράστιοι οικονομικοί πόροι και ανθρώπινο δυναμικό, οικονομίες κλίμακας 2. διεθνική ευελιξία

115 Βλέπε John Markoff, "At Internet Conference, Signs of Agreement Ασελ.ear Between U.S. and Russia," New York Times, April 16, 2010

116 Βλέπε Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

3. έλεγχος κώδικα και παραγωγής προϊόντων 4. Στίγμα και υπόληψη **Κυριότερες αδυναμίες:** νομιμότητα, κλοπή πνευματικής ιδιοκτησίας, προσβολή συστημάτων, απώλεια υπόληψης
Γ. Άτομα και χαμηλής οργάνωσης δίκτυα 1. χαμηλό κόστος επένδυσης εισόδου 2. εικονική ανωνυμία και εύκολη πρόσβαση 3. ασύμμετρη ευπάθεια συγκρινόμενη με κυβερνήσεις και μεγάλους οργανισμούς **Κυριότερες αδυναμίες:** νομική και παράνομη επιβολή από κυβερνήσεις και οργανισμούς

Λόγω του ότι το διαδίκτυο είναι άρρηκτα συνδεδεμένο με τη γεωγραφία και οι κυβερνήσεις είναι κυρίαρχες επί των εδαφών, η τοποθεσία ακόμη έχει θέση ως πόρος ισχύος στο επίπεδο του κυβερνοχώρου. Οι κυβερνήσεις κάνουν προσπάθειες να επιδοτήσουν κρατικές υποδοχές, να ενισχύσουν την εκπαίδευση σε ότι έχει να κάνει με υπολογιστικά συστήματα και να προστατεύσουν την πνευματική ιδιοκτησία που θα ενισχύσει την ανάπτυξη δυνατοτήτων μέσα στα σύνορα[117]. Η παροχή δημοσίων αγαθών, συμπεριλαμβανομένου ενός νομικού και κανονιστικού περιβάλλοντος, μπορεί να εγείρει εμπορική ανάπτυξη των δυνατοτήτων του κυβερνοχώρου. Μία φήμη η οποία μπορεί να ειδωθεί ως καλοήθης και επαρκώς νόμιμη μπορεί να βοηθήσει την ήπια ισχύς ενός κυβερνητικού μηχανισμού με άλλους δρώντες στο πεδίο του κυβερνοχώρου[118].

Εφόσον η αγορά μίας χώρας έχει μεγάλο εύρος, τότε μία κυβέρνηση μπορεί να μεταχειριστεί την ισχύ της εξωτερικά. Τα υψηλά επίπεδα ασφαλείας που έχουν επιβληθεί από την Ευρωπαϊκή Ένωση έχουν τεράστια επίδραση στο διεθνές σύστημα. Όταν εταιρείες όπως η Yahoo έχουν αντιμετωπίσει νομικά θέματα με βάση την δραστηριότητα τους στο διαδίκτυο σε χώρες όπως η Γαλλία, τότε αποφασίζουν να

117 Βλέπε Jonathan Zittrain, The Future of the Internet and How to Stop It (New Haven: Yale UP, 2008).

118 Βλέπε Jack Goldsmith, "Can we stop the global cyber arms race?" Washington Post, February 1, 2010.

συμμορφωθούν με αυτά τα δεδομένα παρά να απέχουν. Εμφανώς υπάρχει μία πληθώρα πόρων ισχύος διαθέσιμων στις κυβερνήσεις , αλλά όχι απαραίτητα σε όλες.

Οι κυβερνήσεις έχουν επίσης, την ικανότητα να πραγματοποιούν επιθετικές επιχειρήσεις μέσω του κυβερνοχώρου[119]. Το πεδίο μάχης είναι ο κυβερνοχώρος. Ωστόσο ο όρος «επίθεση», αναφέρεται σε οτιδήποτε έχει να κάνει με προσπάθειες είτε αφορά επιθέσεις των hacker (καταπάτηση ηλεκτρονικών δικτύων), είτε αφορά την παραμόρφωση δικτυακών τόπων για την πρόκληση φυσικών καταστροφών. Ένας μπορεί να διακρίνει δύο είδη επιθέσεων, εκείνες που έχουν χαμηλό κόστος μέσων των οποίων η εύρεση είναι εύκολα στο διαδίκτυο, και εκείνες που πραγματοποιούνται με εξελιγμένα μέσα (καλλιέργεια ιών, κ.α.), και απαιτούν υψηλή κατάρτιση. Οι κυβερνήσεις μπορούν να πραγματοποιήσουν και τα είδη των επιθέσεων.

Γενικότερα είναι εύκολο να δρομολογηθούν χαμηλής κλίμακας επιθέσεις μέσω του κυβερνοχώρου ενάντια σε στόχους χαμηλής αξίας όπως ηλεκτρονικούς ιστούς. Αλλά περισσότερο μελετημένες επιθέσεις, ενάντια σε υψηλής σημασίας στόχους όπως συστήματα επικοινωνίας και άμυνας, το κόστος των επιθέσεων αυτών μπορεί να είναι μεγαλύτερο, το οποίο μπορεί να περιλαμβάνει την εισβολή και την αποκρυπτογράφηση κωδικών (βλέπε παράρτημα 3). Σε ότι αφορά τους τρομοκράτες, εκείνοι πιθανόν να έχουν αποφασίσει να αφήσουν κατά μέρος τα παραδοσιακά όπλα της δράσης τους και να ψάχνουν νέες μεθόδους[120]. Αυτό σημαίνει, όπως θα δούμε ότι εκείνοι έχουν χρησιμοποιήσει το διαδίκτυο, για την προώθηση των σκοπών τους.

Προσπάθειες από μέρους των κυβερνήσεων, των οργανισμών και των ατόμων δεν είναι νέες, αλλά το χαμηλό κόστος της εισόδου, η ανωνυμία και οι ασυμμετρίες σε ότι έχει να κάνει με την πρόσβαση στα υπολογιστικά συστήματα, έχει ως επακόλουθο, μικροί δρώντες έχουν μεγαλύτερη ικανότητα να ασκήσουν τόσο σκληρή ισχύ όσο ήπια στον κυβερνοχώρο, περισσότερο απ' όσο μπορούν σε πολλαπλά πεδία της διεθνούς πολιτικής. Αλλαγές στην πληροφόρηση είχαν πάντοτε ιδιαίτερη επίπτωση στην άσκηση της ισχύος, αλλά το πλαίσιο του κυβερνοχώρου είναι ένα νέο και εξελισσόμενο περιβάλλον. Τα χαρακτηριστικά του κυβερνοχώρου (βλέπε παράρτημα 4), μειώνουν κάποια διαφοροποιητικά στοιχεία μεταξύ των δρώντων, προβάλλοντας

119 Βλέπε NAS Study

120 Βλέπε John Markoff, "Old Trick Threatens Newest Weapons," *New York Times*, October 27, 2009; and Shane Harris, "The Cyberwar Plan," *National Journal*, November 14, 2009, 18ff.

την μεγάλη ισχύ του και την επιρροή του στην διεθνή πολιτική. Μπορεί ο κυβερνοχώρος να επιδρά καταλυτικά στην πολιτική δραστηριότητα, δίνοντας την ευκαιρία σε μικρότερης ισχύος δρώντες, αλλά δεν αποτελεί μέσο το οποίο θα αλλάξει ολοκληρωτικά την ροή της[121].

Κεφάλαιο 3 Νέα πεδία δράσης- Διαδίκτυο και Κυβερνοχώρος

Εισαγωγή

Η ραγδαία εισχώρηση των τεχνολογιών της πληροφόρησης και της επικοινωνίας στις σύγχρονες εκβιομηχανισμένες κοινωνίες έχει δημιουργήσει νέες ευκαιρίες και κινδύνους για τις κυβερνήσεις και την λεγόμενη «Κοινωνία των Πολιτών»[122]. Η «Κοινωνία των Πολιτών» μπορεί να οριστεί ως «ο χώρος δράσης και οργάνωσης ελεύθερων ατόμων καθώς και το σύνολο των σχετικών δικτύων που έχουν δημιουργηθεί για χάρη της πίστης, της ιδεολογίας και του συμφέροντος που καλύπτουν αυτόν»[123]. Το διαδίκτυο όπως θα δούμε παρακάτω, μπορεί να αποδώσει ένα βαθμό οργανωτικής συνοχής σε αυτές τις ομάδες, πέραν του πολιτικού κατεστημένου. Ωστόσο, αυτές οι ομάδες συχνά αδυνατούν να ενορχηστρώσουν μία εκστρατεία πολιτικής διαμαρτυρίας με το να χρησιμοποιήσουν μόνο τα συμβατικά

121 Βλέπε Richard Clarke "War from Cyberspace," The National Interest on line, October 27, 2009

122 Βλέπε Schuler, Douglas., Shaping the network society: the new role of civil society in cyberspace, Massachusetts Institute of Technology.

123 Βλέπε Walzer, M. , "Towards a Global Civil Society", International Political Currents, Volume 1, Berghan Books, Oxford, 1995, σελ.7

μέσα ενημέρωσης, που φυσιολογικά εκφράζουν τα συμφέροντα των μεγάλων τομέων της κοινωνίας[124].

Η τρομοκρατία θεωρείται, όπως είδαμε ως η χρήση βίας με πολιτικό μήνυμα. Οι σύγχρονοι τρομοκράτες χρησιμοποιούν το διαδίκτυο για να εκφράσουν την ιδεολογία του σε παγκόσμιο επίπεδο και να αποκτήσουν την εύνοια του απλού πολίτη. Οι επιθέσεις στη Νέα Υόρκη και στο Πεντάγωνο το 2001, ήταν απόδειξη των θετικών και των αρνητικών επιπτώσεων της αυξανόμενης χρήσης των τεχνολογιών της πληροφόρησης και της επικοινωνίας. Έρευνες έδειξαν ότι χρησιμοποίησαν υπηρεσίες του διαδικτύου για να συντονίσουν και να πραγματοποιήσουν την εισβολή τους[125].

Η εκμετάλλευση από μέρους των τρομοκρατών των μέσων ενημέρωσης παραμένει ο πιο προσφιλής τρόπος μεταφοράς ενός κλίματος ψυχολογικού εκβιασμού στον πληθυσμό. Η μεταφορά κειμένου και εικόνων σε μία σελίδα του διαδικτύου δίνει περισσότερο έδαφος στις τρομοκρατικές οργανώσεις να επικοινωνήσουν και να οργανώσουν καμπάνιες πολιτικής βίας. Οι τρομοκράτες ευνοούνται από τις γρήγορες και χαμηλού κόστους επικοινωνιακές οδούς που είναι διαθέσιμες σε κάθε άτομα της κοινωνίας. Η κυβερνότρομοκρατία και ο σχεδιασμός ηλεκτρονικών εγκλημάτων αποτελούν απόδειξη της χρήσης των τεχνολογιών της επικοινωνίας για συγκάλυψη δεδομένων. Κάθε τρομοκρατική οργάνωση θα επιχειρήσει να διασκελίσει τον σύνδεσμο μεταξύ της πολιτικής και απολιτικής κοινωνίας στο διαδίκτυο. μόνο όμως σε ημι-αυταρχικές κοινωνίες το διαδίκτυο θα πραγματοποιήσει πραγματική πολιτική αλλαγή.

3.1. Τρομοκρατία και Διαδίκτυο- χρήσεις

Το διαδίκτυο αποτελεί, αν όχι το κύριο, τουλάχιστον ένα από τα πιο σημαντικά και αποτελεσματικά μέσα δραστηριοτήτων του κυβερνοχώρου σε ότι αφορά την τρομοκρατική δράση. Καθώς τα κράτη εξελίσσονται, εξαρτώνται όλο και περισσότερο από υψηλής κλίμακας τεχνολογίες, όπως υπολογιστές, οι οποίοι

124 Βλέπε Gibson, R. & Ward, S., "Reinvigorating Democracy: British Politics and Internet, Ash gate, Alders hot", 2000, σελ.209.

125 Βλέπε Ganor Boaz, von Knop,Katharina, M. Duarte Carlos A(eds). "Hypermedia seduction for terrorist recruiting". IOS Press, 2007, σελ.39

σχετίζονται με στοιχεία που αφορούν εθνικές υποδομές. Εξαιτίας της πολυπλοκότητας και της αλληλεπίδρασης, οι υποδομές αυτές αποτελούν στόχο για τεχνολογικά χτυπήματα. Πολύπλοκα εθνικά συστήματα, παρουσιάζονται ως πιθανοί στόχοι, οι επιθέσεις στα οποία, μπορεί να οδηγήσουν σε καταστροφικά αποτελέσματα. Επιθέσεις μπορεί να πραγματοποιηθούν με τη χρήση υπολογιστών ή εκρηκτικών υλών ή με την παρεμπόδιση διόδων επικοινωνίας, με σκοπό να προκαλέσει ένα κύκλωμα από βλάβες έχοντας τελικό σκοπό την κατάρρευση όλων των συστημάτων ελέγχου μίας σημαντικής κρατικής δομής, όπως ένα αεροδρόμιο.

Το διαδίκτυο, περιέχει πέντε βασικά χαρακτηριστικά, σύμφωνα με τα οποία καθίσταται ως, ιδανικό εργαλείο για τις τρομοκρατικές οργανώσεις[126]. Πρώτον, περιλαμβάνει ταχύτατες επικοινωνίες. Οι άνθρωποι μπορούν να κρατήσουν συζητήσεις σε πραγματικό χρόνο χρησιμοποιώντας υπηρεσίες ηλεκτρονικών μηνυμάτων. Δεύτερον, οδηγίες, πληροφορίες καθώς και χρήματα μπορούν να διακινηθούν μέσω αυτού, με μικρότερο κόστος[127]. Οι τρομοκρατικές οργανώσεις διαθέτουν διπλάσιες δυνατότητες δράσης σε σύγκριση με, κυβερνητικούς οργανισμούς και επιχειρήσεις, σε ότι αφορά τον τομέα της επικοινωνίας και των μέσων πληροφόρησης. Με αυτόν τον τρόπο, ακόμη και μικρές τρομοκρατικές οργανώσεις μπορούν να έχουν μία ισχυρή παρουσία στο διεθνές σύστημα, ανάλογη με εκείνη μεγάλων κυβερνητικών οργανισμών. Ακόμη, η δυνατότητα δημιουργίας λογισμικού βοηθά μικρότερης κατάρτισης χρήστες σε τρομοκρατικές οργανώσεις να χειρίζονται το διαδίκτυο με μεγάλη ευκολία.

Μεγάλης κλίμακας αποσυνδέσεις κατανομής ισχύος, μπορούν να παραλύσουν σημαντικές υποδομές μίας χώρας, όπως προβλήματα σε συχνότητα πτήσεων, διαρροές σε αγωγούς πετρελαίου και φυσικού αερίου, έχουν προκαλέσει μεγάλο ενδιαφέρον από τα μέσα μαζικής ενημέρωσης. Οι τρομοκράτες, μέσω ευρείας και συνεχούς παρατήρησης των εξελίξεων σε κρατικό και διεθνές επίπεδο, όλο και περισσότερο πείθονται ότι οι εθνικές δομές αποτελούν έναν δελεαστικό και ευπαθή

126 Arquilla et al. (1999), "Networks, Netwar, and Information-Age Terrorism" in Terrorism and Counterterrorism: Understanding the new security environment (2004) The McGraw-Hill Companies, σελ. 75

127 Βλέπε παράρτημα 3

στόχο. Για παράδειγμα, οπτικές ίνες [128]επιτρέπουν σε τηλεφωνικές εταιρείες να εξυπηρετούν δεκάδες χιλιάδες συζητήσεις χρησιμοποιώντας μία μόνο γραμμή. Μία δεκαετία πριν, οι συνομιλίες αυτές θα απαιτούσαν ισάριθμα καλώδια σύνδεσης.

Ως αποτέλεσμα έχουμε μεγαλύτερη ευκολία, μεγαλύτερη εξυπηρέτηση και χαμηλό κόστος. Παράλληλα, έχουμε και μία αρνητική εξέλιξη. Το να υπάρξει βλάβη σε ένα απλό καλώδιο επικοινωνίας, είναι δυσάρεστο, το να υπάρχει όμως καταστροφή σε μία οπτική ίνα μπορεί να υπάρξει μία αλυσίδα από καταστροφές. Η πρόοδος μπορεί να αυξήσει την σημασία των κρατικών δομών, αλλά μπορεί να δώσει κίνητρο στους τρομοκράτες για το πρόγραμμα δράσεων.

Ένας τρομοκράτης επιθυμεί να επηρεάσει παγκόσμιες εξελίξεις, όπως την οργάνωση ενός παγκοσμίου τραπεζικού συστήματος[129], ή συναλλαγές μεταξύ τραπεζών θέτοντας τους ως στόχους των επιθέσεων τους. Ένα επιτυχημένο χτύπημα μπορεί, να έχει άμεση επίδραση, αλλά τα περισσότερο σημαντικά χτυπήματα δεν θα προκαλέσουν μόνο απώλειες χρημάτων αλλά μπορούν να προκαλέσουν απώλεια εμπιστοσύνης στα άτομα, και γενικότερα πολιτικές και οικονομικές εξελίξεις τόσο εθνικές όσο και διεθνείς.

Σήμερα πολλές τρομοκρατικές οργανώσεις και κινήματα, έχουν δικούς τους ιστοτόπους στο διαδίκτυο. Χρησιμοποιούν το Ιντερνέτ, για να μεταδώσουν τις σκέψεις τους και τις απόψεις τους, για να στρατολογήσουν νέα μέλη και φυσικά να επικοινωνήσουν μία άλλα μέλη σε άλλες χώρες για την επιτυχή έκβαση των δραστηριοτήτων τους. Τέτοιες οργανώσεις, θεωρούν τις ικανότητες του διαδικτύου ως μέσο άμυνας και ως όπλο μαζικής υπονόμευσης. Μπορούν επίσης να διδάξουν τα

---

128 http://egnatia.ee.auth.gr/~aalexioy/fiber_οσελ.htm Ένα άλλο αρκετά συνηθισμένο καλώδιο στις σύγχρονες καλωδιώσεις είναι η οπτική ίνα. Χρησιμοποιείται, κυρίως, όπου οι αποστάσεις είναι μεγάλες και δεν μπορεί να χρησιμοποιηθεί το καλώδιο συνεστραμένων ζευγών και όπου οι απαιτήσεις σε ρυθμούς μετάδοσης είναι αρκετά αυξημένες. Σκεφτείτε, ότι μπορούμε να χρησιμοποιήσουμε οπτική ίνα για να καλύψουμε απόσταση 5Km και οι ρυθμοί μετάδοσης δεδομένων φθάνουν τα 10 Gbps…

129http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/International/19-Jan-2009/Cyber-attack-on-US-banking-system-more-dangerous-than-911-US-intelligence-official μία επίθεση μέσω κυβερνοχώρου σε τραπεζικά συστήματα των ΗΠΑ μπορεί να είναι δεκάδες φορές πιο ζημιογόνα στην οικονομία μίας χώρας παρά μία υλική καταστροφή. Η οικονομική ζημία θα μπορούσε να είναι 10 φορές μεγαλύτερη από τις οικονομικές; επιπτώσεις του Σεπτεμβρίου 2001.

μέλη για την προετοιμασία πολλαπλών απειλητικών προγραμμάτων και λογισμικών που προκαλούν πολλαπλές καταστροφές.

Λαμβάνοντας υπόψη, τις τάσεις της κυβερνότρομοκρατίας, μπορούμε να συμπεράνουμε ότι η μέρα όπου μερικές τρομοκρατικές οργανώσεις θα υπάρχουν μόνο στον κυβερνοχώρο δεν απέχει πολύ. Οι προσωπικές επαφές θα εκλείψουν και οι τρομοκράτες θα χρησιμοποιούν το Ιντερνέτ για να προετοιμάσουν τις επιθέσεις τους ενάντια σε χώρες με ανεπτυγμένα ηλεκτρονικά δίκτυα. Οι παρεμβάσεις δίνουν βάση σε τραπεζικά και εμπορικά δίκτυα, σε κρατικά δίκτυα, ηλεκτρονικές υπηρεσίες, τηλεφωνικά συστήματα, στο σύστημα υγείας, κ.α. Λίγο πολύ, όλα αυτά τα συστήματα είναι εκτεθειμένα σε υπονομεύσεις και ηλεκτρονικές επιθέσεις. Αναλυτικά αναφέρουμε:

Το διαδίκτυο, μπορεί να χρησιμοποιηθεί για την δημιουργία ομάδων προφίλ. Δημογραφικές έρευνες[130] έχουν δείξει ότι, χρήστες του διαδικτύου επιτρέπουν τρομοκράτες να εστιάζουν σε χρήστες με συμπάθεια απέναντι σε ένα σκοπό ή ένα θέμα, καθώς και να προχωρήσουν σε δωρεές εάν εντοπίσουν χρήστες με το σωστό «προφίλ». Συνήθως, μία ομάδα, η οποία βρίσκεται στην πρώτη γραμμή των εξελίξεων, έχει την ευκαιρία να μεριμνήσει για την παροχή πόρων, συχνά άθελα της. Η χρηματοδότηση, μέσω ηλεκτρονικών μηνυμάτων έχει την δυναμική να ενισχύσει την δημοσιότητα των τρομοκρατών, καθώς και την οικονομική τους ευρωστία[131].

Η έρευνα εφημερίδων και άλλων μέσων τύπου, δίνει την δυνατότητα σε ένα τρομοκράτη να δημιουργήσει ένα προφίλ μέσων, προκειμένου να εκμεταλλευτεί τις όποιες αδυναμίες που μπορεί να έχει ένα σύστημα πληροφοριών. Ένα παράδειγμα, είναι οι σύγχρονες αναφορές σχετικά με, τις προσπάθειες διακίνησης προϊόντων λαθρεμπορίου, μέσα από σημεία ασφαλείας. Μία απλή έρευνα στο διαδίκτυο, μπορεί να προσφέρει στον τρομοκράτη, την ευκαιρία να επιλέξει τον κατάλληλο σημείο επιβίβασης για την επόμενη, ή τις επόμενες επιχειρήσεις του. Πρόσφατες έρευνες[132]

130 Βλέπε Gabriel Weimann, Terror on the Internet, United States Institute of Peace Press (2006)

131 Βλέπε Patrick S. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," unpublished paper, School of Advanced Military Studies, Fort Leavenworth, Kansas, June 2002, σελ. 20.

132 Βλέπε CRS Report for Congress Received through the CRS Web. Computer Attack and Cyber Terrorism 2008

έχουν δείξει ότι οι αμερικανικές υπηρεσίες επιβολής του νόμου, έχουν εντοπίσει κλήσεις με αποδέκτη στελέχη της Αλ Κάιντα, από τηλεκάρτες, κινητά τηλέφωνα, τηλεφωνικούς θαλάμους, και κλήσεις μέσω του Ιντερνέτ. Η έκθεση, των τεχνικών αυτών στο δημόσιο γίγνεσθαι, αναγκάζουν τους τρομοκράτες να αλλάξουν τρόπο προσέγγισης. Η χρήση των προφίλ, από τρομοκράτες βοηθά σε μεγάλο βαθμό την διαδικασία εντολών και ελέγχου των επιχειρήσεων τους. Η υποψία ότι, σε μία ελεύθερη κοινωνία, όπως οι Ηνωμένες Πολιτείες, υπάρχει η δυνατότητα προβολής μίας τεράστιας μάζας πληροφοριών, η οποία μπορεί να μην αφορά τόσο τους απλούς πολίτες, μπορεί να είναι εξαιρετικά αποτελεσματική για τους τρομοκράτες.

Η χρήση του διαδικτύου μπορεί να ελεγχθεί ή να κατευθυνθεί ανάλογα με την διαμόρφωση του κεντρικού χρήστη, με στόχο την δημιουργία ενός ιδεολογικού όπλου. Στο παρελθόν, εάν κάποια έκθεση είχε προσβλητικό περιεχόμενο για την κυβέρνηση του εκάστοτε κράτους, εκείνο θα επιδεχόταν λογοκρισία. Οι κυβερνήσεις, δεν μπορούν να ελέγξουν το Ιντερνέτ στον ίδιο βαθμό, όπως τις εφημερίδες και την τηλεόραση. Ο παγκόσμιος ιστός επιτρέπει την αδιάλειπτη ροή εκδοχών των γεγονότων που αναμεταδίδονται διεθνώς[133]. Το έδαφος αυτό, δίνει μία πρώτης τάξεως ευκαιρίας σε τρομοκρατικές ομάδες με μικρή ή ακόμη και πενιχρή χρηματοδότηση, για να εξηγήσει τις δράσεις τους σε ένα παγκόσμιο επίπεδο, ή να αντισταθμίσει την οποιαδήποτε καταδίκη από μέρους του κυβερνητικών και μη αξιωματούχων, καθώς και του απλού κόσμου. Το διαδίκτυο, μπορεί να αποτελέσει δίοδο αποστολής διαφορετικών μηνυμάτων ανάλογα με το κοινό στο οποίο απευθύνονται.

Ως επακόλουθο των επιθέσεων της 11^{ης} Σεπτεμβρίου 2001, οι λειτουργοί της Αλ Κάιντα χρησιμοποίησαν το Ιντερνέτ, για να κινήσουν μία σειρά μαχών ιδεολογικού και θρησκευτικού χαρακτήρα, σύμφωνα με το γράμμα του νόμου του Ισλάμ. Εκατοντάδες εγκεκριμένοι Μουσουλμάνοι, ανά την υφήλιο, οι οποίοι εξέφρασαν αρνητική άποψη για τις επιθέσεις, θεωρήθηκαν από την Αλ Κάιντα υποκριτές. Η Αλ Κάιντα, δημιούργησε δύο ιστοτόπους στο διαδίκτυο, που συζητούσαν τις επιθέσεις στη Νέα Υόρκη. Εξέφρασε την άποψη ότι έχει καθήκον να διαδώσει τις διδασκαλίες

---

133 http: //www.crime-research.org/news/2002/11/Mess1203.htm: How al Qaeda put Internet to use By Andrew Higgins

του Ισλάμ, δια όπλου. Το αποτέλεσμα ήταν, το ξέσπασμα ενός ιδεολογικού πολέμου μεταξύ ομόθρησκων[134].

Το διαδίκτυο δίνει την απαραίτητη ανωνυμία, προκειμένου να προστατεύσει τις ταυτότητες των τρομοκρατών. Οι τρομοκράτες, έχουν πρόσβαση μέσω του Ιντερνέτ σε συστήματα προκειμένου να καλύψουν την ταυτότητα τους ή να «μεταμφιεστούν». Ηλεκτρονικές υπηρεσίες κρυπτογράφησης, δίνουν την δυνατότητα στους τρομοκράτες να εισβάλλουν σε υπηρεσίες, σπάζοντας κάθε δικλείδα ασφαλείας[135]. Ένα παράδειγμα είναι η ιστοσελίδα mimic.com, όπου πληροφορεί σχετικά με τον τρόπο ροής πληροφοριών πολιτικού περιεχομένου. Λογαριασμοί δικτύων μπορούν να διαγραφούν ή να μεταβληθούν ανάλογα με τις απαιτήσεις. Για παράδειγμα, οι χρήστες του διαδικτύου μπορούν να κάνουν χρήση ηλεκτρονικών υπηρεσιών όπως η AOL (America On Line), ή να δημιουργήσουν λογαριασμούς αποστολής ηλεκτρονικών μηνυμάτων (Yahoo, Google, κ.α.). Ανώνυμες είσοδο σε υπηρεσίες αυτές, είναι πολύ εύκολο να πραγματοποιηθούν, μέσα στο διαδίκτυο. Είναι εφικτό ακόμη, να γίνει η σύνδεση μέσω Internet café, βιβλιοθήκες ή από άλλους πόρους για να εξασφαλιστεί η ανωνυμία των μηνυμάτων τους.

Γενικότερα το Internet, παράγει μία ατμόσφαιρα εικονικού φόβου και εικονική πραγματικότητας. Οι άνθρωποι φοβούνται πράγματα και καταστάσεις που υπάρχουν στη σφαίρα του νοητού στην οποία κινείται το Διαδίκτυο. Η εικονική απειλή των επιθέσεων μέσω ηλεκτρονικών υπολογιστών ανήκει κυρίως στη σφαίρα αυτή. Ο λεγόμενος κυβερνό-φόβος, παράγεται από την υποψία σχετικά με το τι μπορεί να κάνει ένας υπολογιστής (κατάρριψη ιπτάμενων αεροσκαφών, καταστροφή κρατικών δομών, πτώση του χρηματιστηρίου, κ.α.), και πόσο συχνά μπορεί να το κάνει. Αναφορές[136] ίσως οδηγήσουν στο συμπέρασμα, ότι εκατοντάδες ή χιλιάδες άνθρωποι είναι ενεργοί μέσα στο δίκτυο της Αλ Κάιντα, για παράδειγμα, σε καθημερινή βάση, επειδή η ίδια η οργάνωση το προστάζει. Είναι εμφανές, ότι το διαδίκτυο, ενδυναμώνει μικρές ομάδες και τους δίνει την εικόνα του περισσότερο ικανού απ' όσο είναι στην πραγματικότητα. Το γεγονός αυτό πυροδοτεί συνεχή αισθήματα

134 Paul Eedle, "Al-Qaeda Takes Fight for 'Hearts and Minds' to the Web," Jane's Intelligence Review, August 2002, rpt. in CNO/IO Newsletter, 5-11 August 2002.

135 http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p4 What advantages does the Internet offer terrorists? By John Arquilla

136 Mark Hosenball, "Islamic Cyberterror," *Newsweek*, 20 May 2002

φόβου σε κρατικούς ή μη φορείς αλλά και σε απλούς πολίτες. Το διεθνές ηλεκτρονικό δίκτυο, επιτρέπει την ενίσχυση των συνεπειών των πράξεων τους με συνεχή μηνύματα και απειλές κατευθείαν εναντίον της πλειοψηφίας του πληθυσμού, ακόμη και εάν η τρομοκρατική οργάνωση είναι ανίκανη για δράση. Ως αποτέλεσμα, το Ιντερνέτ, επιτρέπει σε ένα άτομο ή σε μία ομάδα να μεγιστοποιεί την παρουσία του και τη σημασία του, παρουσιαζόμενο πιο απειλητικό απ' ότι είναι.

Το διαδίκτυο, μπορεί να χρησιμοποιηθεί για την εξάπλωση της πληροφορίας, απειλητικών μηνυμάτων, ή τρομακτικών εικόνων από πρόσφατες ενέργειες (μία από αυτές είναι δολοφονία του δημοσιογράφου Daniel Pearl από τους Πακιστανούς). Πρακτικά, φαίνεται ότι οι επιθέσεις αυτές είναι επαρκώς προσχεδιασμένες και ελεγχόμενες. Τα μηνύματα είναι, συνήθως μονομερή, και αντικατοπτρίζουν ένα συγκεκριμένο πολιτικό κλίμα[137]. Υπάρχει συχνά, μικρή πιθανότητα να ελεγχθεί το γεγονός για το εάν αντιπροσωπεύει την πραγματικότητα ή απλά είναι μία χαμηλού επιπέδου απειλή. Το διαδίκτυο, μπορεί να είναι μέσο εξάπλωσης πληροφοριών και λαθεμένων αναφορών τις οποίες πολλοί άνθρωποι, μετά από προσεκτική μελέτη μπορούν να κατανοήσουν το περιεχόμενο τους[138].

Πρόσφατα, η αραβική τηλεόραση και συγκεκριμένα ο σταθμός Al Jazeera, είχαν προβάλλει μαγνητοσκοπημένα, τα μηνύματα του Οσάμα Μπιν Λάντεν και εμφάνισε ένα σημείωμα από τον ίδιο, ό οποίος επαινούσε τις επιθέσεις σε πετρελαιοφόρα στην Υεμένη, και σε αμερικανούς στρατιώτες, κατά τη διάρκεια πολεμικών επιχειρήσεων στο Κουβέιτ[139]. Τα μηνύματα αυτά, συγκεντρώθηκαν και εστάλησαν ηλεκτρονικά σε κάθε γωνιά του πλανήτη. Πολύ πιθανόν, ο ίδιος ο Οσάμα να έχει τραυματιστεί (λόγω της μεγάλης χρονικής διάρκειας μεταξύ των δύο ηλεκτρονικών μηνυμάτων), όμως η εικόνα του μπορεί να υποστεί επεξεργασία μέσα από το ραδιόφωνο και τους υπολογιστές και να φανεί ο ίδιος ως μία εικόνα υγιής και απειλητικός.

Το διαδίκτυο ακόμη, μπορεί να μέσο χρηματοδότησης, ομάδων με μικρό προϋπολογισμό. Η Αλ Κάιντα, αποτελεί μία περίπτωση, όπου με βάση το ιδεολογικό

137 How effective is online terrorist propaganda?: by Eben Kaplan

138 Tom Squitieri, "Cyberspace Full of Terror Targets," USA Today, 5 June 2002.

139 Colin Soloway, Rod Nordland, and Barbie Nadeau, "Hiding (and Βλέπeking) Messages on the Web,"
Newsweek, 17 June 2002, σελ. 8.

υπόβαθρο του Ισλάμ, προχωρά σε φιλανθρωπικές ενέργειες, προκειμένου να μαζευτούν χρήματα για τους τζιχάντ, ενάντια στους θεωρούμενους εχθρούς τους. Οι αναλυτές έχουν διαπιστώσει ότι, η ίδια η Αλ Κάιντα και άλλοι οργανισμοί ανθρωπιστικής βοήθειας χρησιμοποιούσαν τον ίδιο τραπεζικό λογαριασμό, σε διάφορες περιπτώσεις. Αποτέλεσμα, πολλές φιλανθρωπικές ενέργειες της Αλ Κάιντα ανεστάλησαν[140]. Η σουνιτική εξτρεμιστική οργάνωση, για παράδειγμα Hizb al-Tahir χρησιμοποιεί ένα ενοποιημένο δίκτυο από σελίδες του διαδικτύου από την Ευρώπη και την Αφρική, για να ετοιμάσει το έδαφος για την επιστροφή του ισλαμικού χαλιφάτου. Ο ιστότοπος δηλώνει ότι η επιστροφή αυτή πρέπει να γίνει με ειρηνικά μέσα.

Οι υποστηρικτές αυτής της προσπάθειας, παροτρύνονται να ενισχύσουν και οικονομικά, με την παροχή χρημάτων σε αριθμούς λογαριασμών που διακινούνται μέσω πυλών του διαδικτύου. Το χρήμα είναι για τους τρομοκράτες, σύμφωνα με τον Napoleoni (2004)[141], «η γραμμή ζωής για έναν τρομοκράτη, η μηχανή ενός ένοπλου αγώνα . Η αμεσότητα και η διαδραστική φύση της διαδικτυακής επικοινωνίας, ανοίγει πολλαπλούς δρόμους για αυξημένες οικονομικές εισφορές, όπως έχει αποδειχτεί από διάφορους πολιτικούς και κοινωνικούς φορείς». Οι τρομοκράτες αναζητούν χρηματοδότηση, και μέσω ηλεκτρονικών ιστών και μέσω ηλεκτρονικών δομών του διαδικτύου, για να προκαλέσουν κινητοποίηση πόρων με έννομα μέσα.

Αναρίθμητες τρομοκρατικές οργανώσεις ζητούν οικονομική στήριξη άμεσα από χρήστες του διαδικτύου που επισκέπτονται του δικτυακούς τόπους αυτών. Τέτοιου είδους παρακλήσεις ίσως λάβουν την μορφή γενικών δηλώσεων υπογραμμίζοντας την ανάγκη των οργανισμών για χρήματα, οι οποίες εκδηλώνονται είτε με την εντολή για άμεση δωρεά είτε με την παροχή οικονομικών λογαριασμών για την κίνηση κεφαλαίων. Ένας άλλος τρόπος συγκέντρωσης χρημάτων είναι μέσω της δημιουργίας ηλεκτρονικών καταστημάτων και της πώλησης αντικειμένων όπως βιβλία, πολυμέσα, σημαίες, μπλούζες, κ.α. Ως επιβεβαίωση αυτού του σεναρίου, ένας δικτυακός τόπος που συνδεόταν με το Κίνημα Νομικής Κυριαρχίας 32[142], που αποτελεί την πολιτική

140 Colin Soloway, Rod Nordland, and Barbie Nadeau, "Hiding (and Βλέπεking) Messages on the Web," Newsweek, 17 June 2002, σελ. 10.

141 Terrorism and the Economy: How the War on Terror is Bankrupting the World (2010)

142 C. Younger, Ireland's Civil War (Frederick Muller, 1968) σελ. 103

πτέρυγα του IRA, έφερε ένα σύνδεσμο για τον ηλεκτρονικό παροχέα συγγραμμάτων Amazon.com, που ζητούσε από τους επισκέπτες να στηρίξουν τους φυλακισμένους με την αγορά αντικειμένων από το συγκεκριμένο σύνδεσμο. Ο σύνδεσμος αυτός, απομακρύνθηκε από το παροχέα το Νοέμβριο του 2000.

Το Ιντερνέτ ακόμη, διευκολύνει την τρομοκρατική δραστηριότητα με πολλούς τρόπους πέρα από την άμεση εισφορά μέσω ηλεκτρονικών τόπων. Σύμφωνα με τον Rohan Bedi [143], ένα από τους κορυφαίους αντιτρομοκρατικούς ερευνητές, ένας μεγάλος αριθμός σχεδίων ισλαμικής τρομοκρατίας χρηματοδοτούνται μέσω απάτης από πιστωτικές κάρτες (Thomas 2003, 117). [144]Σύμφωνα με ειδικούς, υπάρχουν αδιάσειστες αποδείξεις από φορείς επιβολής του διεθνούς δικαίου, όπως το FBI, ότι οι τρομοκρατικές οργανώσεις χρηματοδοτούν τις δραστηριότητες τους μέσω υπεξαίρεσης χρημάτων από ηλεκτρονικές πληρωμές[145].

Ωστόσο, οι τρομοκρατικές οργανώσεις αποδεδειγμένα, έχουν ιστορικό στην εκμετάλλευση όχι μόνο επιχειρηματικών δραστηριοτήτων, αλλά και φιλανθρωπιών ως υποβόσκον όχημα χρηματοδότησης. Για μία ακόμη φορά οι ισλαμικές τρομοκρατικές οργανώσεις έχουν δώσει δείγματα δραστηριοποίησης σε αυτό τον τομέα. Σε ορισμένες περιπτώσεις, μάλιστα οι τρομοκρατικές οργανώσεις έχουν εγκαταστήσει φιλανθρωπικές δραστηριότητες με φερόμενους ανθρωπιστικούς σκοπούς. Παραδείγματα, μπορούμε να εντοπίσουμε σε οργανώσεις όπως οι Global Relief Fund, κ.α. Οι δραστηριότητες αυτές, έχουν δεχτεί μαζική διαφήμιση από το Διαδίκτυο, συγκεντρώνοντας τεράστιο αριθμό επισκεψιμότητας στο Διαδίκτυο. Οι τρομοκράτες έχουν, με τα χρόνια αναπτύξει ένα τεράστιο δίκτυο οικονομικής αλληλεγγύης για την αύξηση των πόρων τους. Πολλοί από τους οργανισμούς που απαρτίζουν το δίκτυο αυτό, δέχονται τεράστια δημοσιότητα, και όπως ισχυρίζεται ο Todd Hinnen, «είναι σημαντικό να μην δεχόμαστε ως δεδομένο ότι φιλανθρωπικές

143 Rohan Bedi (2004). Money Laundering - Controls and Prevention

144 Thomas T.L. (2003) Al-Qaeda and the Internet: The Danger of "Cyber-planning" www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf Retrieved on 09/04/2007

145 Roth, John, et al. (20 August 2004). "Monograph on Terrorist Financing". National Commission on Terrorist Attacks Upon the United States. σελ. 54–56. http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Ch4.pdf. Retrieved 20 September 2011.

οργανώσεις έχουν τρομοκρατικούς δεσμούς μόνο και μόνο επειδή υποστηρίζουν θρησκευτικές ή ιδεολογικές κοινότητες με τις οποίες πιθανόν να συνδέονται τρομοκρατικές ενέργειες»[146].

Πέρα από την χρήση του Διαδικτύου ως μέσο χρηματοδότησης, μπορούμε να πούμε ότι αποτελεί μηχανισμός ελέγχου και εντολών, κυρίως στρατιωτικής άποψης. Η χρήση αυτή, αφορά την άσκηση εξουσίας και την κατεύθυνση που δίνεται από ένα κατάλληλα διορισμένο εντολέα πάνω σε εκχωρημένους και συνημμένους μηχανισμούς ισχύος για την εκτέλεση μίας αποστολής. Το πλήρωμα, ο εξοπλισμός, η επικοινωνία, οι εγκαταστάσεις και οι διαδικασίες επιτυγχάνουν την εκτέλεση εντολών και έλεγχου με την βοήθεια στον σχεδιασμό, την σκηνοθεσία και την συνεργασία των δυνάμεων και επιχειρήσεων για την επιτυχία μίας αποστολής. Η διαδικασία ελέγχου και εντολών μέσω του Ιντερνέτ δεν εμποδίζεται από την γεωγραφική απόσταση, ή από τη έλλειψη υψηλής ποιότητας επικοινωνιακού εξοπλισμού. Οι τρομοκράτες μπορούν να δώσουν πληροφορίες-κλειδιά μέσω αποστολής ηλεκτρονικών μηνυμάτων (πληροφορίες που μπορούν να χρησιμοποιηθούν ως αντιπερισπασμός) ή ακόμη να στείλουν κρυφά μηνύματα για τα σχέδια και τον συντονισμό των επιθέσεων τους.

Ο μέσος πολίτης, ο αντικυβερνητικός διαμαρτυρόμενος και ο τρομοκράτης έχει πλέον πρόσβαση σε μέσα εντολών και ελέγχου, περιορισμένα φυσικά, για την αποτελεσματικότητα των επιχειρήσεων τους. Επιπλέον, υπάρχουν εργαλεία «σπασίματος» κωδικών διαθέσιμων για τον εντοπισμό σφαλμάτων στην ασφάλεια των συστημάτων και την εκμετάλλευση αυτών[147]. Η επιτυχής πρόσβαση σε ένα διαδικτυακό τόπο, επιτρέπει στον δράστη να ελέγχει κεφάλαια (δυνάμεις και ηλεκτρόνια) που δεν ανήκουν σε εκείνο. Η δυναμική του διαδικτύου για την εντολή και τον έλεγχο μπορεί να βελτιώσει σε μεγάλο βαθμό την ευελιξία ενός οργανισμού αν δεν έχει σωστή καταγραφή πληροφοριών και εγκαταστάσεων ελέγχου, κυρίως για την προπαγάνδα και τις περιοχές εσωτερικού ελέγχου. Εν τέλει, ο έλεγχος μπορεί να επιτευχθεί και μέσω δωματίων ηλεκτρονικής επικοινωνίας (chat rooms). Για παράδειγμα η σελίδα alneda.com, η οποία προσέφερε βοήθεια στην Αλ Κάιντα για στρατηγική καθοδήγηση και φυσικά, ηθική έμπνευση.

146 Statement of Todd M. Hinnen Deputy Assistant Attorney General Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties Committee on the Judiciary United States House of Representatives For a Hearing Entitled "The USA PATRIOT Act" Presented September 22, 2009.

147 Weinberg et al. (2004) "The Challenges of Conceptualizing Terrorism", Terrorism and Political Violence, 16(4), 777 – 794

Ο διεθνής ιστός, επίσης, επιτρέπει τον πλήρη έλεγχο στο περιεχόμενο, και εξαλείφει την ανάγκη του να βασίζεται σε δημοσιογράφους για προβολή. Άτομα που είναι υπέρ ενός σκοπού μπορεί να μυηθούν μέσω εικόνων και μηνυμάτων από τρομοκρατικές οργανώσεις και η προσθήκη ενός βίντεο έχει ενισχύσει αυτή την ικανότητα. Εικόνες και βίντεο είναι εργαλεία ενδυνάμωσης για τους τρομοκράτες. Ακόμη, σύγχρονες εκδόσεις περιηγητών του διαδικτύου, όπως ο Internet Explorer και ο Netscape, υποστηρίζουν λειτουργίες Java[148] οι οποίες επιτρέπουν στους κεντρικούς χρήστες (servers) να γνωρίζουν όποια γλώσσα έχει οριστεί από τον πελάτη υπολογιστή. Ως εκ τούτου, ένα περιηγητής που έχει όρισε την αγγλική γλώσσα ως γλώσσα λειτουργίας, μπορεί να οδηγηθεί σε μία σελίδα στο διαδίκτυο που απευθύνεται σε δυτικούς πληθυσμούς. Αντίθετα ένας περιηγητής που έχει ορίσει την αραβική γλώσσα, θα έχει πρόσβαση σε σελίδες θετικά διακείμενες προς την αραβική ή την ισλαμική κουλτούρα. Η λογική αυτή προωθεί την άποψη για την χρήση του διαδικτύου με σκοπό την στρατολόγηση νέων ταλέντων για τρομοκρατικούς σκοπούς.

Η μαζική μεταφορά και ανταλλαγή δεδομένων μέσω του διαδικτύου, μπορεί να δώσει πληροφορίες σχετικά με την καταλληλότητα των στόχων ενάντια στους οποίους οι τρομοκράτες μπορούν να δράσουν. Μία ιστοσελίδα, με την ονομασία Muslim Hackers Club[149], παρέχει συνδέσμους για αμερικανικές ηλεκτρονικές σελίδες που συνίστανται για να γνωστοποιήσουν ευαίσθητες πληροφορίες όπως κωδικούς ονομάτων και ράδιο-συχνότητες που χρησιμοποιούνται από αμερικανικές μυστικές υπηρεσίες. Η ίδια σελίδα, προσφέρει «σεμινάρια», στην καλλιέργεια ιών, την προσβολή ηλεκτρονικών τειχών προστασίας και απόσπαση μυστικών κωδικών[150]. Πρόσφατοι στόχοι τρομοκρατικών ομάδων είναι οργανισμοί διακίνησης χρημάτων και εγκαταστάσεις ελέγχου της ροής των πληροφοριών μέσω του Διαδικτύου[151]. Για το λόγο αυτό, κάθε πληροφορία μέσω ενός μη ασφαλούς δικτύου, χωρίς κάποιου πρωτοκόλλου ασφαλείας είναι εν δυνάμει καταστροφική. Οι τρομοκράτες έχουν πρόσβαση, όπως και πολλοί Αμερικάνοι, στην απεικόνιση πληροφοριών για πιθανούς

148 www.java.net

149 Βλέπε http://en.wordpress.com/tag/muslim-hackers-club/

150 Mark Hosenball, “Islamic Cyberterror,” Newsweek, 20 May 2002

151 Tom Squitieri, “Cyberspace Full of Terror Targets,” USA Today, 5 June 2002

στόχους, όπως χάρτες, διαγράμματα, και άλλων ζωτικής σημασίας πληροφοριών σε σημαντικές εγκαταστάσεις ή δίκτυα. Πληροφορίες μέσω εικόνων, μπορούν να δώσουν την ευκαιρία στους τρομοκράτες να αποφύγουν κάθε κίνηση καταστολής των ενεργειών τους σε ένα συγκεκριμένο ιστοτόπο.

Σε ότι αφορά την συλλογή πληροφοριών μέσω του Ιντερνέτ, ο γραμματείας του Υπουργείου άμυνας των Ηνωμένων Πολιτειών Donald Rumsfeld, παρατήρησε ένα εγχειρίδιο κατάρτισης σχετικά με την τρομοκρατία μέσω του διαδικτύου, που βρέθηκε στο Αφγανιστάν. Βάσει αυτού δήλωσε ότι, η χρήση δημοσίων πηγών δημόσια και μη δίνοντας βάση σε νόρμες δικαίου, είναι πιθανό να συγκεντρώσει τουλάχιστον 80% των πληροφοριών που απαιτούνται για τον εχθρό.

Από τα προηγούμενα ανάγουμε το συμπέρασμα ότι, το διαδίκτυο αποτελεί μέσο κλοπής και χειραγώγησης της πληροφορίας. Ο Ronald Rick, ο διευθυντής του Εθνικού Κέντρου Προστασίας Κρατικών Υποδομών, θεωρεί την κλοπή πληροφοριών από του τρομοκράτες ως το χειρότερο του εφιάλτη, και ειδικά εάν συνοδεύονται και από φυσική επίθεση. Ο Richard Clark, πρόεδρος του κυβερνητικού συμβουλίου προστασίας κρατικών υποδομών των ΗΠΑ, είπε ότι το πρόβλημα της ηλεκτρονικής ασφάλειας και προστασίας των δεδομένων, έχει αποκτήσει ανάλογες διαστάσεις με τις επιθέσεις της 11 Σεπτεμβρίου όταν ο ιός Nimda[152], εξαπλώθηκε σε εκατομμύρια υπολογιστές σε όλο τον κόσμο, προκαλώντας ζημιές δισεκατομμυρίων δολαρίων. Το 2001, παρατηρήθηκαν πολλαπλές ενέργειες εισβολέων, ενάντια στους υπολογιστές στην Silicon Valley. Έρευνες του FBI[153], εντόπισαν εισβολές σε τηλεπικοινωνιακούς διακόπτες στην Σαουδική Αραβία, Ινδονησία, και Πακιστάν. Ενώ κανείς δεν έχει

152 http://en.wikipedia.org/wiki/Nimda Ο Nimda είναι ένας ιός- σκουλήκι και επιπλέον ένα μολυντικό αρχείων. Εξαπλώνεται ραγδαία, δημιουργώντας οικονομικές καταστροφές. Χιλιάδες χάκερ και προπαγανδιστές του Διαδικτύου επέτρεψαν σε αυτόν να γίνει ο πιο διαδεδομένος ιός μέσα σε 22 λεπτά. Ελευθερώθηκε μία εβδομάδα μετά τα γεγονότα της 11ης Σεπτεμβρίου, γεγονός που οδήγησε τα αμερικανικά μέσα ενημέρωσης στο συμπέρασμα ότι αποτελεί προϊόν της Αλ Κάιντα, κάτι που τελικά αποδείχτηκε αναληθές.

153 Amrutha Gayathri. FBI issues warning: Al Qaeda could be plotting an Independence Day attack on US. International Business Times.

συσχετιστεί ανοιχτά με την Αλ Κάιντα, υπάρχουν σοβαρές υποψίες για την ανάμειξη της.

Η πρακτική της στεγανόγραφιας, που αφορά την αποστολή κρυφών μηνυμάτων, μέσα από γραφικά, είναι ευρέως διαδομένη τέχνη ανάμεσα σε εγκληματίες και τρομοκρατικά στοιχεία. Κρυφές σελίδες ή φράση χωρίς λογική σειρά μπορούν να κωδικοποιηθούν ως οδηγίες για τους λειτουργούς και του υποστηρικτές της Αλ Κάιντα. Η ίδια χρησιμοποιεί ακολουθίες εικόνων και συμβόλων με διαφορές στην αλληλουχία των χρωμάτων. Τα μηνύματα δεν είναι κρυμμένα με εξειδικευμένο τρόπο και είναι δυνατό να είναι προσβάσιμα ανοιχτά στον κάθε χρήστη. Ο παγκόσμιος ιστός ακόμη, είναι ένα ελκυστικό εργαλείο για όσους αναζητούν ένα τρόπο να επιτεθούν στις μεγάλες δυνάμεις της διεθνούς πολιτικής σκηνής. Το γεγονός ότι το διαδίκτυο, είναι ενεργό κάθε στιγμή αφήνει ανοιχτό το δρόμο στα άτομα να επισκέπτονται διάφορους ηλεκτρονικούς τόπους, αλλά δίνει την ευκαιρία στα άτομα για επίπληξη των μεγάλων δυνάμεων δημόσια. Η Αλ Κάιντα, επιτίθεται μέσω του διαδίκτυου, όχι μόνο για να αντισταθμίσει την δυτική δημοσιογραφική δραστηριότητα, αλλά και για να απαριθμήσει όλους εκείνους τους μουσουλμάνους που δεν τάσσονται με την γραμμή που ορίζει το Ισλάμ.

Αξίζει επίσης να αναφέρουμε, ότι το διεθνές δίκτυο είναι τόσο σημαντικό για μία τρομοκρατική οργάνωση, αφού λειτουργεί ως μέσο εκδήλωσης οργής των πολιτών κάθε κράτους ενάντια στην πολιτική σκηνή ενός κράτους. Για παράδειγμα το Κέντρο Ισλαμικών Σπουδών και Έρευνα, αποτελείται από πολλαπλούς τομείς πληροφόρησης, όπως αναφορές για τις εξελίξεις στον πόλεμο του Αφγανιστάν, δημοσιογραφικό υλικό, προκηρύξεις των τζιχάντ, πληροφορίες για τους αιχμαλώτους, κ.α.[154] Πέρα όμως και από την προπαγάνδα που μπορεί να προκληθεί μέσω του διαδικτύου, μπορεί να αποτελέσει το μέσο εκδήλωσης αλληλεγγύης και αδελφότητας ανάμεσα στις ομάδες των ατόμων. Η προώθηση της άποψης, ότι όλοι παλεύουμε κάτω από ένα κοινό σκοπό και ιδεολογία, κινητοποιεί άτομα σε ένα πόλεμο, με ρυθμούς ραγδαίους και αποτελέσματα καταστροφικά.

154 John Schwartz, "Despite 9/11 Warnings, Cyberspace Still at Risk," The Post Standard (Syracuse, N.Y.), 11 September 2002, σελ.. D-10, 11

Συγγραφέας	*Furnell and Warren*[155]	*Cohen*[156]	*Thomas*[157]	*Weinman*[158]
Χρήσεις	Προπαγάνδα και δημοσιότητα, κατανομή πληροφοριών, ευκολία χρηματοδότησης, πρόσβαση σε τηλεπικοινωνίες	Σχεδιασμός τρομοκρατικών επιθέσεων, δημιουργία συνεργατικών σχέσεων μεταξύ τρομοκρατών, πολιτική πράξη	Προπαγάνδα, διαρροή ψευδών πληροφοριών, συλλογή πληροφοριών, κινητοποίηση και στρατολόγηση, κλοπή δεδομένων, οικονομική ενίσχυση, εξέταση ενδεχόμενου κινδύνου.	Ψυχολογικός πόλεμος, δημοσιότητα, στρατολόγηση και κινητοποίηση, σχεδιασμός μέσω επικοινωνίας τρομοκρατικών ομάδων.

Μελετώντας προσεκτικά την χρήση του Διαδικτύου για τρομοκρατικούς σκοπούς είναι φρόνιμο να αναφέρουμε ξεχωριστά την ορολογία που χρησιμοποιείται για να περιγράψει επιθέσεις που έχουν να κάνουν με την ασφάλεια του κυβερνοχώρου. Προκειμένου λοιπόν να αναλύσουμε το φαινόμενο της κυβερνοτρομοκρατίας, αξίζει να σταθούμε σε πρώτο επίπεδο στην έννοια της κυβερνοεπίθεσης ανακαλώντας περιπτώσεις επιθέσεων για να καταδείξουμε το βαθύτερο νόημα της.

155 Furnell and Warren, "Computer Hacking and Cyber-terrorism: The Real Threats in The new Millenium

156 Cohen, "Terrorism and Cyberspace".

157 Thomas, "Al Queda and Internet: The danger of Cyber planning".

158 Weimann G. (2004) www.terror.net How Modern Terrorism Uses The Internet. United States Institute of Peace www.usisελ.org/pubs/specialreports/sr116.pdf Retrieved on 09/04/2007.

3.2 Η έννοια της Κυβερνόεπίθεσης

Υπάρχουν αρκετές αποτελεσματικές επιθέσεις, για την προσβολή συστημάτων ηλεκτρονικών υπολογιστών. Η κυβερνοεπίθεση, ή cyber attack είναι γνωστός ο όρος διεθνώς, είναι η επίθεση που πραγματοποιείται μέσω κακόβουλων κωδικών και λογισμικών προγραμμάτων για την κλοπή ή καταστροφή δεδομένων, καθώς και την προσβολή της αξιοπιστίας αυτών. Υπάρχουν τρία βασικά είδη επιθέσεων ενάντια σε ηλεκτρονικά συστήματα. Η αποτελεσματικότητα, αυτών διαφοροποιείται μέσα στο χρόνο ακολουθώντας τους ραγδαίους ρυθμούς ανάπτυξης της τεχνολογίας. Η κυβερνόεπίθεση αποτελεί την πιο εξελιγμένη μορφή τρομοκρατικής επίθεσης ενάντια σε υπολογιστές. Τα είδη λοιπόν των επιθέσεων αυτών, είναι τα εξής:

- **Η φυσική επίθεση,** η οποία μπορεί να περιγραφεί ως η βίαιη χρήση συμβατικών όπλων ενάντια σε εγκαταστάσεις που αποτελούνται από υπολογιστικά συστήματα, και υψίστης σημασίας κρατικές δομές που προξενούν μείωση της αξιοπιστίας και της απόδοσης τους.
- **Η επίθεση μέσω ηλεκτρομαγνητικής ενέργειας,** δημιουργεί μία ηλεκτρονική επίθεση σε διόδους μεταφοράς της πληροφορίας και δεδομένων, με στόχο την προσβολή της ακεραιότητας αυτών και την δημιουργία σκοπέλων σε ότι έχει να κάνει στην μεταφορά αυτών. Με την εισβολή στις τηλεπικοινωνίες ή την υπερφόρτωση των δικτύων μεταφοράς πληροφοριών αποδεικνύεται ότι η τεχνολογία έχει εισάγει ένα πιο εξελιγμένο είδος επίθεσης που ενεργοποιεί τους τρομοκράτες, κάνοντας τους να σκεφτούν νέους τρόπους τρομοκρατικής δράσης, πιο ευέλικτους και πιο επιζήμιους.
- **Η κυβερνοεπίθεση,** είναι αποτέλεσμα της παγκοσμιοποιημένης δομής που έχει αποκτήσει ο κυβερνοχώρος την τελευταία δεκαετία του 20^{ου} αιώνα και την πρώτη δεκαετία του 21^{ου}. Η κυβερνοεπίθεση, ή αλλιώς επίθεση ενάντια δικτύων υπολογιστών (Computer Network Attack), είναι εκείνη η επίθεση ενάντια σε διαδικασίες εντολών και λογισμικών λειτουργίας ηλεκτρονικών προγραμμάτων. Τα μέσα εκδήλωσης αυτού του είδους της επίθεσης, είναι μία ακολουθία κωδικών που ενεργοποιούν ένα κύμα, κακόβουλων δικτυακών τόπων που μπορούν να διαταράξουν δεδομένα μέσω της εκμετάλλευσης αδυναμιών σε ηλεκτρονικό λογισμικό, ή την ευπάθεια σε ότι αφορά πρακτικές ασφάλειας υπολογιστικών συστημάτων ενός οργανισμού. Πέρα από την αξιοπιστία και την

ακεραιότητα των δεδομένων, οι οποίες προσβάλλονται, σημαντικό πλήγμα είναι πιθανό να δεχτεί και ο βαθμός έγκυρης πληροφόρησης.

Συχνά είναι δύσκολο να κατατάξουμε μία επίθεση στον κυβερνοχώρο ή μία εισβολή ως αποτέλεσμα της δράσης μίας τρομοκρατικής οργάνωσης που έχει ως στόχο την πρόκληση ζημιών , ή ενός κυβερνόεγκληματία που επιθυμεί να υποκλέψει πληροφορίες οικονομικού περιεχομένου. Οι όροι με τους οποίους λειτουργούν οι κυβερνότρομοκράτες, όπως ακριβώς οι τρομοκράτες και οι εξτρεμιστές συχνά βασίζονται στην εκμετάλλευση των ευπαθών χαρακτηριστικών ενός στόχου, θεωρώντας ότι με αυτό τον τρόπο θα αποκτήσουν μεγαλύτερη πρόσβαση για την εκτέλεση μελλοντικών επιθέσεων μέσω του κυβερνοχώρου.

Η εφαρμογή μίας ισχυρότερης πολιτικής ασφαλείας έχει μειώσει τον κίνδυνο, απέναντι σε ορισμένους πιθανούς στόχους, ευάλωτους σε φυσικές επιθέσεις. Επίσης, υπάρχει η άποψη από πολλούς ειδικούς ότι, οι τρομοκράτες πιθανόν, να ενισχύσουν τις γνώσεις πάνω στους υπολογιστές ή να δημιουργήσουν συμμαχίες με κυβερνόεγκληματίες που κατέχουν ένα υψηλό επίπεδο εξειδίκευσης. Επιπλέον, η ολοένα αυξανόμενη δημοτικότητα του Διαδικτύου, καθώς και των αδυναμιών σε θέματα ηλεκτρονικής ασφαλείας, ίσως ενθαρρύνει τους τρομοκράτες να προβούν σε μία επίθεση εναντίον δικτύων υπολογιστών, όπως επίθεση κατά κρατικών δομών ενός κράτους όπως οι ΗΠΑ.

Πρόσφατα, το Ομοσπονδιακό Γραφείο Ερευνών, γνωστό και ως **FBI**[159]**,** ανέφερε ότι οι επιθέσεις μέσω του κυβερνοχώρου που καταλογίζονται σε μέλη τρομοκρατικών οργανώσεων, πραγματοποιούνται με τρόπο επιπόλαιο, χωρίς ιδιαίτερο σχεδιασμό, όπως ιδεολογικό πόλεμο μέσω ηλεκτρονικών μηνυμάτων ή προσβολή δικτυακών τόπων σε επίπεδο ασφάλειας. Έχει ακόμη προβλέψει ότι, οι τρομοκράτες θα σχεδιάσουν τις επιθέσεις τους είτε μόνοι τους είτε θα προσλάβουν ειδικούς (hacker), για τον σκοπό της εκπλήρωσης μεγάλης κλίμακας συμβατικών επιθέσεων μέσω του κυβερνοχώρου. Το διευθυντικό στέλεχος του **FBI**[160]**,** Robert Mueller παρατήρησε ότι οι τρομοκράτες χρησιμοποιούν ευρύτατα το Διαδίκτυο για να επικοινωνούν, να σχεδιάζουν επιθέσεις, να προσηλυτίζουν, να στρατολογούν νέα μέλη, να εκπαιδεύουν

159 Kessler, Ronald (1993). The FBI: Inside the World's Most Powerful Law Enforcement Agency. Pocket Books Publications.

160Βλέπε Theoharis, Athan G. (2004). The FBI and American Democracy: A Brief Critical History. Kansas: University Press.

και να λαμβάνουν λογιστική και οικονομική στήριξη. Η όλη αυτή δραστηριότητα αποτελεί, μία έντονη ανησυχία για το γραφείο μας. Η εγκληματική και τρομοκρατική δράση των επιθέσεων μέσω του κυβερνοχώρου είναι δύο περιπτώσεις οι οποίες είναι δύσκολο να διαχωριστούν.

Διαχωρισμοί μεταξύ των όρων έγκλημα, τρομοκρατία, και πόλεμος τείνουν να καταρρίπτονται όταν γίνεται προσπάθεια να περιγραφεί μία επίθεση κατά των ηλεκτρονικών δικτύων με τρόπο αντίστοιχο με τις επιθέσεις που πραγματοποιούνται στον πραγματικό κόσμο. Για παράδειγμα, εάν ένα κράτος είναι ικανό, μυστικά να στηρίζει οικονομικά μη κυβερνητικούς δρώντες που προχωρούν σε μία ηλεκτρονική επίθεση με τρομοκρατικό υπόβαθρο ή να δημιουργήσουν οικονομική δυσπραγία, η διάκριση των παραπάνω όρων γίνεται δυσκολότερη. Επειδή ένα τέτοιο είδος επίθεσης, είναι πολύπλοκο να οριστούν τα όρια δράσης τους, ένας εισβολέας ίσως προκαλέσει καχυποψία από έναν τρίτο παράγοντα. Κατά αυτόν τον τρόπο, οι δοσοληψίες μεταξύ των τρομοκρατών και των εγκληματιών που χρησιμοποιούν την τεχνολογία των υπολογιστών ίσως προκαλέσουν σύγχυση κατά τον διαχωρισμό μεταξύ κυβερνόεγκλήματος και κυβερνότρομοκρατίας.

Υπάρχει ακόμη η περίπτωση ότι άτομα που παρέχουν αξιοπιστία σε ότι αφορά τα υπολογιστικά συστήματα σε εγκληματίες ή τρομοκράτες, τα οποία όμως δεν είναι γνώστες των πραγματικών κινήτρων και των προθέσεων αυτών που ζήτησαν βοήθεια. Μέχρι στιγμής, παραμένει δύσκολο να ορίσουμε τις πηγές που είναι υπεύθυνες για την πραγματοποίηση των περισσοτέρο επιζήμιων, αλλά και των πιο ραφιναρισμένων που λυμαίνονται το Διαδίκτυο. Σε αυτό προστίθεται και η δυσκολία, του να εντοπιστεί το υποκείμενο των επιθέσεων και των ηλεκτρονικών εισβολών. Τέλος υπάρχει η άποψη ότι, σε αντίθεση με παραδοσιακές εγκληματικές πράξεις, το ενδιαφέρον θα πρέπει να δίνεται περισσότερο στην πράξη, παρά στον αυτουργό της πράξης προκειμένου να γίνουν σωστές προσπάθειες για την αποφυγή καταστροφικών αποτελεσμάτων.

3.2.1 Εσθονία 2007

Την άνοιξη του 2007, τα κυβερνητικά συστήματα υπολογιστών στην Εσθονία βίωσε μία μεγάλης κλίμακας επίθεση που θεωρήθηκε από πολλούς ερευνητές ως

ένδειξη ηλεκτρονικού πολέμου ή κυβερνοτρομοκρατία[161]. Στις 27 Απριλίου , ειδικοί στην Εσθονία θεώρησαν ότι εισήλθαν σε μία νέα μορφή Ψυχρού Πολέμου, ανάλογη με εκείνη που έληξε το 1989. Η φάση αυτή επηρέασε καταλυτικά την κοινή γνώμη, και οδήγησε σε διαμαρτυρίες Ρώσων εθνικιστών και σε επίθεση ενάντια στην Εσθονική Πρεσβεία στη Μόσχα. Το γεγονός αυτό έθεσε σε κίνηση μία σειρά από επιθέσεις άρνησης υπηρεσιών, ενάντια σε εσθονικές εθνικές ιστοσελίδες, μέσα σ' αυτά κυβερνητικές υπηρεσίες καθώς και τα γραφεία του κυβερνόντος κόμματος.

Στις πρώτες μέρες της επίθεσης, οι ηλεκτρονικές σελίδες της κυβέρνησης, οι οποίες είχαν περίπου 1000 επισκέπτες την ημέρα, έφτασαν να δέχονται 2000 επισκέψεις το δευτερόλεπτο. Αυτό προκάλεσε το επαναλαμβανόμενο κλείσιμο κάποιων ιστοσελίδων. Οι επιθέσεις, που εξαπλώθηκαν στους υπολογιστές και στις κεντρικές μονάδες, περιγράφηκαν ως μαζικές, εξαιτίας της υψηλής εξάρτησης της Εσθονίας στην τεχνολογία της πληροφόρησης, αλλά διαθέτουν περιορισμένους πόρους για την προστασία των υποδομών τους. Ειδικοί για την ασφάλεια υποστηρίζουν ότι οι κυβερνό-επιθέσεις ενάντια στην Εσθονία ήταν ασυνήθιστες επειδή η αναλογία του μπαράζ των επιθέσεων ήταν πολύ υψηλή, και η σειρά των επιθέσεων κράτησε εβδομάδες, κι όχι ώρες ή μέρες, που διαρκούν συνήθως τέτοιες επιθέσεις. Εν τέλει, το ΝΑΤΟ και οι Ηνωμένες Πολιτείες έστειλαν ειδικούς ασφαλείας στην Εσθονία για να βοηθήσουν στην αποκατάσταση του συστήματος μετά την επίθεση, να αναλύσουν τις μεθόδους που χρησιμοποιήθηκαν και να επιχειρήσουν να εντοπίσουν την πηγή της επίθεσης. Το γεγονός αυτό, μπορεί να αποτελέσει παράδειγμα για το πώς η τεχνολογία των δικτύων έχει λάβει αρνητική τροχιά και το πόσο έχουν παρεκκλίνει τα όρια μεταξύ του εγκλήματος, της πολεμικής επιχείρησης και της τρομοκρατίας.

Ένα επίμονο ζήτημα κατά τη διάρκεια και μετά την επίθεση είναι η ακριβής ταυτοποίηση του φορέα της επίθεσης, δημιουργώντας ερώτημα είτε εάν υποκινήθηκε από το έθνος, ή ήταν μία ανεξάρτητη επιχείρηση μεταξύ μη συνδεδεμένων ατόμων, ή ακόμη, εάν συγκροτήθηκε από μία ομάδα για να προκαλέσει σύγχυση και φόβο, προκαλώντας ζημία στις υποδομές και στην οικονομία. Η αβεβαιότητα του να μείνει στη σφαίρα της ανωνυμίας, το υποκείμενο της επίθεσης, επίσης επηρεάζει την απόφαση για το ποιος πρέπει να είναι ο στόχος της επίθεσης, και ποια θα πρέπει να είναι η νομική απάντηση ή η στρατιωτική.

161 ^ The Guardian May 17, 2007: Russia accused of unleashing cyberwar to disable Estonia by Ian Traynor

Αρχικά, η ρωσική κυβέρνηση κατηγορήθηκε από τους Εσθονούς για τις επιθέσεις, και υπήρχαν κατηγορίες για διακίνηση πολεμικού υλικού και διενέργεια πολεμικών επιθέσεων. Άλλα ειδικοί υποστήριξαν ότι η ρωσική κυβέρνηση και διεθνείς κυβερνότρομοκράτες που διέθεσαν τα πειρατικά τους δίκτυα διαθέσιμα για άτομα και ομάδες. Παρόλα αυτά όμως παραμένει αδιευκρίνιστο εάν αυτή τη φορά, οι επιθέσεις ενορχηστρώθηκαν από την ρωσική κυβέρνηση ή μέσω ενός «πειρατικού δικτύου». Μετά από έρευνες[162], οι αναλυτές δικτύων συμπέραναν ότι οι επιθέσεις που στόχευαν την Εσθονία δεν ήταν μία μελετημένη επίθεση, αλλά αντίθετα ήταν προϊόν αυθόρμητης οργής από επιτιθέμενους χωρίς καμία οργάνωση.

Τεχνικές πληροφορίες έδειξαν ότι οι πηγές της επίθεσης τοποθετούνταν σε πολλές γωνιές του πλανήτη, παρά σε μικρές τοποθεσίες. Οι αναλυτές που ασχολήθηκαν με την επίθεση αυτή, και εξερεύνησαν τις εσθονικές κυβερνητικές υπηρεσίες, κατέληξαν στο ότι δεν υπήρχε απόπειρα ενάντια σε κρατικές υποδομές, και ούτε υπήρξε θέμα εκβιασμού. Η ανάλυση τους κατέληξε στο συμπέρασμα, ότι δεν υπήρχε ρωσική εμπλοκή στις επιθέσεις κατά της Εσθονίας. Εν τέλει, η έρευνα για το συμβάν συνεχίστηκε, και επίσημοι κυβερνητικοί υπάλληλοι από τις Ηνωμένες Πολιτείες θεωρούν ότι επίθεση αυτή, είναι παράδειγμα για μελλοντική τρομοκρατική επίθεση ενάντια σε ένα έθνος κράτους.

3.3. Η έννοια του κυβερνό-εγκλήματος

Σύμφωνα με την άποψη των Grabosky, Smith και Urbas[163], αναφορικά με τον όρο έγκλημα, καταλήγουν στο συμπέρασμα ότι η «θεμελιώδης αρχή της εγκληματολογίας ορίζει ότι το έγκλημα έγκειται στην ευκαιριακή εκμετάλλευση¨». Ο Grabosky θεωρεί ότι η ανάπτυξη της τεχνολογίας των υπολογιστών και του διαδικτύου έχουν αυξήσει τις ευκαιρίες για τους εγκληματίες να διαπράξουν έγκλημα μέσω του κυβερνοχώρου. Ενώ το γενικότερο πρόβλημα που προκύπτει από το κυβερνοέγκλημα έχει γνωστοποιηθεί μερικώς, υπάρχουν πολλαπλές ερμηνείες σχετικά με τη φύση του κυβερνό-εγκλήματος. Το κυβερνό-έγκλημα, ιστορικά αναφέρεται σε εγκλήματα που συμβαίνουν μέσω δικτύων, κυρίως του Ιντερνέτ, αλλά ο όρος έχει σταδιακά γίνει ένα γενικό συνώνυμο για το ηλεκτρονικό έγκλημα.

162 http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/

163 Βλέπε Russell Smith, Peter Grabosky and Gregor Urbas, *Cyber Criminals on Trial: Prosecutorial and Judicial Responses to Computer Crime*. Cambridge: Cambridge University Press, 2004.

Ένας άλλος συνώνυμος όρος, είναι το **έγκλημα υψηλής τεχνολογίας,** που καθιστά βέβαιο ότι τέτοια εγκλήματα περιλαμβάνουν κάθε χρήση ψηφιακών συσκευών. Δυστυχώς όμως, στην ανάπτυξη περισσότερο λεπτομερών και ακριβών ορολογιών , διαφορετικά κράτη, εθνικοί και υπερεθνικοί οργανισμοί έχουν επέλθει σε σύγχυση σχετικά με την απόδοση επαρκών ορισμών και κατηγοριοποιήσεων. Πράγματι, τα Ηνωμένα Έθνη ισχυρίζονται ότι τα προβλήματα σχετικά με την διεθνή συνεργασία στο πεδίο του ηλεκτρονικού εγκλήματος περιλαμβάνουν την απουσία μίας παγκόσμιας συμφωνίας σχετικά με τις μεθόδους έρευνας του κυβερνόεγκλήματος καθώς και την απουσία συμφωνίας νομικών όρων.

"Ο μοντέρνος κλέφτης μπορεί να κλέψει περισσότερα με έναν υπολογιστή παρά με ένα όπλο. Ο τρομοκράτης του αύριο μπορεί να προκαλέσει μεγαλύτερο κακό με ένα πληκτρολόγιο παρά με μία βόμβα".

– National Research Council, "Computers at Risk", 1991.

Ο παραπάνω ισχυρισμός είναι μία απόδειξη για το ότι ένας εγκληματίας μπορεί να προκαλέσει μεγαλύτερη καταστροφή κάνοντας χρήση των δυνατοτήτων ενός υπολογιστή. Στα πλαίσια λοιπόν της μελέτης μας για την τρομοκρατία του κυβερνοχώρου, είναι φρόνιμο να μελετήσουμε την έννοια του κυβερνοεγκλήματος ξεχωριστά.

Επιχειρώντας να δώσουμε τον ορισμό του κυβερνοεγκλήματος θα μπορούσαμε να καταλήξουμε στο εξής συμπέρασμα[164]:

Το κυβερνό-έγκλημα είναι το έγκλημα που πραγματοποιείται είτε ενάντια στους υπολογιστές είτε μέσω αυτών. Υπάρχει άποψη ότι δεν υπάρχει καθολικά αποδεκτός ορισμός του κυβερνό-εγκλήματος, εφόσον υπάρχει ακόμη το πρόβλημα ορισμού του κυβερνοχώρου, γενικότερα. Παρόλαυτα θεωρείται ότι το κυβερνό-έγκλημα πραγματοποιείται κυρίως μέσα από το διαδίκτυο.

Ωστόσο η έννοια αυτή, καλύπτει και επιθέσεις ενάντια σε υπολογιστές με σκοπό την ελεύθερη προσβολή της διαδικασίας. Επίσης μπορεί να περικλείει την εισβολή για

[164] Βλέπε Easttom C. (2010) *Computer Crime Investigation and the Law*

την δημιουργία παράνομων αντιγράφων ευαίσθητων προσωπικών δεδομένων. Εάν μία τρομοκρατική οργάνωση σχεδιάζει να πραγματοποιήσει μία τέτοια επιχείρηση, τότε μπορεί να μελετηθεί με όρους κυβερνό-εγκλήματος. Υπάρχουν τέσσερις κατηγορίες του όρου αυτού:

1) Κυβερνόεγκλήματα ενάντια σε ανθρώπους
2) Κυβερνοεγκλήματα ενάντια σε ατομικές ιδιοκτησίες
3) Κυβερνοεγκλήματα ενάντια σε οργανισμούς- κυβερνήσεις κρατών.
4) Κυβερνοεγκλήματα ενάντια σε κοινωνικό πλαίσιο

Η πρώτη κατηγορία αφορά εγκλήματα όπως διακίνηση παιδικής και μη πορνογραφίας, παρενόχληση κάθε ατόμου μέσω της χρήσης ενός υπολογιστής. Η διακίνηση, η κατανομή και η δημοσίευση υλικού που δεν εμπίπτει σε ορθές διατάξεις του νόμου αποτελεί ένα από τα πιο δημοφιλή κυβερνοεγκλήματα σήμερα. Το έγκλημα αυτό μπορεί να έχει συνέπειες και σε ψυχολογικό επίπεδο σε νεαρά άτομα εμποδίζοντας την ομαλή ανάπτυξη της προσωπικότητας τους.

Η παρενόχληση, ακόμη και εξεταζόμενη με όρους κυβερνό-εγκλήματος, είναι μία αξιόποινη πράξη. Πολλά είδη παρενόχλησης μπορούν να πραγματοποιηθούν είτε μέσα στον κυβερνοχώρο, είτε μέσω της χρήσης αυτού. Η παρενόχληση μπορεί να είναι είτε σεξουαλική, είτε φυλετική είτε θρησκευτική, κ.α. Το αδίκημα της παρενόχλησης, μας φέρει σε ένα άλλο πλαίσιο, αυτό της παραβίασης του ιδιωτικού βίου του ατόμου. Κανείς δεν επιθυμεί την εισβολή στην εξαιρετικά ευαίσθητη περιοχή του βίου του και κυρίως εάν προέρχεται από το διαδίκτυο.

ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ-ΤΡΟΠΟΙ ΕΚΔΗΛΩΣΗΣ				
Στόχοι	Άτομα	Περιουσία	Οργανισμοί/ Κυβερνήσεις	Κοινωνία
	i. Παρενόχληση μέσω ηλεκτρονικών μηνυμάτων ii. Ηλεκτρονική ενέδρα	i. Βανδαλισμοί πληροφοριών ii.Διάδοση	i. Μη επιτρεπόμενη είσοδος σε υπολογιστικά συστήματα	i. Πορνογραφία (κυρίως παιδική) ii Διακίνηση iii. Οικονομικά

	iii. κατανομή υβριστικού υλικού iv. Ευτελισμός προσώπων v. Μη επιτρεπόμενη είσοδος σε υπολογιστικά συστήματα vi. Μη έντιμη έκθεση vii. Απάτη και κλοπή	ιών iii. Netrespass iv. Μη επιτρεπόμενη είσοδος σε υπολογιστικά συστήματα v. Κλοπή πνευματικής ιδιοκτησίας vi. Κλοπή χρόνου σύνδεσης για το διαδίκτυο.	ii. Κατοχή απόρρητων πληροφοριών iii. Επιθέσεις τρομοκρατών ενάντια σε κυβερνήσεις v. Κατανομή «πειρατικού» λογισμικού	εγκλήματα v. Πώληση παράνομων άρθρων vi.Ηλεκτρονικός τζόγος vii.Πλαστογραφία

Ορισμένα από τα παραπάνω αναφερόμενα αδικήματα αναφέρονται παρακάτω[165]

1. Παρενόχληση μέσω e-mails,

Η παρενόχληση μέσω e-mails, δεν αποτελεί καινούριο είδος επίθεσης. Είναι, προφανώς αρκετά παρεμφερές με την παρενόχληση μέσω αλληλογραφίας. Παρενόχληση μέσω αλληλογραφίας μπορεί να γίνει μεταξύ ζευγαριών με προβληματικές σχέσεις

2. Ηλεκτρονική ενέδρα

[165] Βλέπε McQuade, S. (ed) (2009) *The Encyclopedia of Cybercrime*, Westport, CT: Greenwood Press.

Το λεξικό ορίζει την λέξη «ενέδρα ως «επίμονη και συστηματική παρακολούθηση». Η ηλεκτρονική ενέδρα αφορά την παρακολούθηση κάθε βήματος ανθρώπινου μέσα από το διαδίκτυο με την αποστολή μηνυμάτων (ορισμένες φορές απειλητικών) σε δημοφιλείς ηλεκτρονικούς τόπους, βομβαρδίζοντας το θύμα με μηνύματα.

3. *Ευτελισμός προσώπων μέσω του κυβερνοχώρου*

Είναι μία πράξη εμβολής ενός προσώπου με στόχο να μειώσει την προσωπικότητα του και να προκαλέσει την απώλεια της προσωπικότητας του αφήνοντας τον εκτιθέμενο σε αισθήματα μίσους και ονείδους. Ο ευτελισμός προσώπων μέσω του κυβερνοχώρου δεν είναι διαφορετικός από την συνηθισμένη ηθική βλάβη. Το μόνο που προστίθεται είναι η εμπλοκή ηλεκτρονικών μέσων.

4. *Παράνομη είσοδος σε υπολογιστικά συστήματα*

. Η δραστηριότητα αυτή αναφέρεται ως hacking. Η νομολογία, όμως ορισμένων κρατών όπως η Ινδία δεν επιτρέπει την εναλλαγή αυτών των όρων.

6. *Βανδαλισμοί υπολογιστών*

Ο βανδαλισμός είναι η ελεύθερη καταστροφή ή η ζημιά στην ιδιοκτησία κάποιου άλλου. Έτσι ο βανδαλισμών υπολογιστών αφορά την υλική βλάβη που προξενούνται σε εκείνους από τον καθένα. Οι πράξεις αυτές ίσως λαμβάνουν την μορφή της κλοπής ή της καταστροφής ενός υπολογιστή, μέρος του υπολογιστή ή περιφερειακή ομάδας αυτού.

7. *Εγκλήματα πνευματικής ιδιοκτησίας / Κατανομή πειρατικού λογισμικού*

Η πνευματική ιδιοκτησία αποτελεί σημαντικό ατομικό δικαίωμα. Κάθε παράνομη πράξη όπου καταργείται ο ιδιοκτήτης είναι αδίκημα. Η πιο κοινή μορφή μπορεί να θεωρηθεί η πειρατεία λογισμικού, η κλοπή δικαιώματος ευρεσιτεχνίας, η παραβίαση υπηρεσιών, κ.α.

8. *Διακίνηση*

Η διακίνηση μπορεί να λάβει πολλές μορφές. Μπορεί να είναι διακίνηση ναρκωτικών, λευκής σαρκός, όπλων, κ.α. Οι μορφές αυτές της διακίνησης δεν

υπόκεινται σε νομική επιβολή επειδή έχουν ψευδείς ονομασίες. Για παράδειγμα, διακίνηση ναρκωτικών με το ψευδώνυμο της ζάχαρης.

9. Απάτη

Η ηλεκτρονική απάτη είναι από τις πιο επικερδείς επιχειρήσεις που αναπτύσσονται σήμερα στον κυβερνοχώρο. Μπορεί να λάβει διαφορετικές μορφές. Μερικές από τις περιπτώσεις ηλεκτρονικής απάτης μπορεί να είναι απάτη μέσω πιστωτικών καρτών, αγγελιών, κ.α.

3.3.1 Ορολογία του κυβερνό-εγκλήματος

Στις μέρες μας υπάρχει ένας μεγάλος αριθμός σημασιολογικών όρων έχει χρησιμοποιηθεί για να περιγράψει εγκλήματα μέσω των υπολογιστών. Οι όροι που χρησιμοποιούνται είναι, **έγκλημα μέσω υπολογιστών, διαδικτυακό έγκλημα, ψηφιακό έγκλημα, ηλεκτρονικό έγκλημα , τεχνολογικό έγκλημα και κύβερνο-έγκλημα.** Ο τελευταίος όρος χρησιμοποιείται ευρέως σήμερα, με την έννοια της διάπραξης ενός εγκλήματος, διαμέσου υπολογιστών ή δικτύων, ή οποιασδήποτε ηλεκτρονικής συσκευής. Αυτός είναι ένας αρκετά γενικός όρος που δεν περικλείει μόνο εγκλήματα που χρησιμοποιούν ή στοχεύουν υπολογιστικά συστήματα και δίκτυα, αλλά αφορούν την χρήση μίας ηλεκτρονικής συσκευής ξεχωριστά. Ο Kshetri [166]αναλύει το κυβερνοέγκλημα και τα κίνητρα πίσω από αυτό με όρους **κόστους-οφέλους** για τον κυβερνό-εγκληματία και ορίζει το κυβερνοέγκλημα ως εκείνο που χρησιμοποιεί ένα ηλεκτρονικό δίκτυο κατά την εγκληματική διάπραξη ηλεκτρονικής απάτης, κλοπή ταυτότητας και παρεμβολή σε διαδικτυακές επικοινωνίες. Ωστόσο, ο όρος κυβερνόεγκλημα, αφορά όχι μόνο εγκλήματα ενάντια σε δεδομένα υπολογιστών και συστημάτων, αλλά και παραδοσιακά εγκλήματα όπως υπεξαίρεση χρημάτων και οικειοποίηση απορρήτων πληροφοριών.

3.3.2 Ιεράρχηση σχετικών εννοιών

Ο σκοπός της μελέτης μας πάνω στο επίκαιρο ζήτημα του κυβερνοεγκλήματος, είναι η δημιουργία μίας ιεραρχίας εννοιών που θα διευκολύνει κυβερνητικούς και μη κυβερνητικούς μηχανισμούς στη μάχη ενάντια σε αυτό του είδους έγκλημα. Μερικά

166 Ο Kshetri, Nir, The Global Cybercrime Industry: Economic, Institutional and Strategic. Springer edition.

λοιπόν από τα θετικά αυτής της επιστημονικής μελέτης, είναι η ανταλλαγή πληροφοριών, η ακριβής αναφορά συμβάντων σχετικών με ηλεκτρονικά εγκλήματα και η εναρμονισμένη θεσμοθέτηση νομικών διατάξεων και κανόνων. Εξ ορισμού, λοιπόν μπορούμε να θεωρήσουμε ότι οι υπολογιστές, σε ότι έχει να κάνει με το κυβερνό-έγκλημα μπορεί να είναι:

- **Το εργαλείο:** όταν το άτομο είναι ο κύριος στόχος του κυβερνο-εγκλήματος, ο υπολογιστής μπορεί να θεωρηθεί το εργαλείο παρά ο στόχος. Τα εγκλήματα αυτά, γενικά, δεν απαιτούν τεχνική εξειδίκευση, αφού οι συνέπειες εντοπίζονται στον πραγματικό κόσμο. Οι ανθρώπινες αδυναμίες γίνονται αντικείμενο εκμετάλλευσης. Το υποκείμενο αυτής της πράξης μπορεί να είναι πλέον ικανό να αυξήσει το πεδίο δράσης του και να καλύψει πιο αποτελεσματικά τα ίχνη του
- **Ο στόχος:** οι επιθέσεις που έχουν τα υπολογιστικά συστήματα ως στόχο γίνονται από εγκληματίες με μεγάλο βαθμό εξειδίκευσης. Οι περιπτώσεις αυτές αποτελούν καινούριο στοιχείο ανάλυσης, που όμως η δράση τους αποδεικνύει πόσο ανέτοιμη είναι η κοινωνία σε παγκόσμιο επίπεδο, για την αντιμετώπιση της. Σήμερα, τέτοια εγκλήματα αποτελούν καθημερινό επίπεδο στην ζωή των ατόμων.

Ο παρακάτω πίνακας περιλαμβάνει είδη εγκλημάτων που πραγματοποιούνται είτε ο υπολογιστής αποτελεί τον **στόχο** του εγκληματία είτε το **όργανο** δράσης[167].

Ο υπολογιστής ως **στόχος επίθεσης**	Ο υπολογιστής ως **όργανο επίθεσης**
• Αδικήματα σχετικά με μη νόμιμη πρόσβαση, όπως η παραβίαση κωδικών • Διασπορά επικίνδυνου λογισμικού όπως ιοί • Δημιουργία παράνομων δικτύων παρακολούθησης (botnet)	• παράνομη κατοχή στρατιωτικών μυστικών • Παράνομη χρήση επικοινωνιακών υποδομών με σκοπό εγκληματικές δραστηριότητες

167 Βλέπε Easttom C. (2010) *Computer Crime Investigation and the Law*

• Παράνομη χρήση προσωπικών λογαριασμών ανταλλαγής ηλεκτρονικών μηνυμάτων και εισβολή σε δεδομένα κεντρικών υπολογιστών.	

Η προσπάθεια αυτή σχετικά με την ιεράρχηση έρχεται σε άμεση συνάφεια με το πλαίσιο στο οποίο γίνεται η ανάλυση του όρου κυβερνό-εγκλήματος. Το πλαίσιο μελέτης λοιπόν μπορεί να μας δώσει πληροφορίες σχετικά με τα **κίνητρα,** την **σχέση μεταξύ των εμπλεκομένων** και τον απώτερο **σκοπό.** Οι πληροφορίες αυτές μπορεί να αποτελέσουν σημαντικό εγχειρίδιο στην δράση των κυβερνήσεων και των διεθνών οργανισμών που εργάζονται πάνω στην καταπολέμηση αυτών των εγκλημάτων. Άρα, εστιάζουμε στην ανάλυση μερικών περιπτώσεων εγκλημάτων με την ταυτόχρονη εξέταση χαρακτηριστικών όπως:

- **Ο τύπος του κυβερνόεγκλήματος (ο υπολογιστής είτε ως όργανο είτε ως στόχος)**
- **Το κίνητρο ή ο ρόλος των εμπλεκομένων (αν αφορά ατομική εγκληματική πράξη η πολιτικά υποκινούμενη δράση**
- **Η σχέση μεταξύ των εμπλεκομένων (του αυτουργού και του θύματος), και**
- **Ο σκοπός της δράσης για τον θύτη ή το θύμα της επίθεσης**

3.3.3 Αίτια εκδήλωσης του φαινομένου

Ο Hart στο έργο του "The Concept of Law"[168] υποστηρίζει ότι «τα ανθρώπινα όντα είναι τόσο ευάλωτα και γι' αυτό το δίκαιο πρέπει να τα προστατέψει». Εφαρμόζοντας την άποψη αυτή στην μελέτη του κυβερνοχώρου, συμπεραίνουμε ότι οι υπολογιστές είναι σε μεγάλο βαθμό ευπαθείς και για το λόγο αυτό είναι απαραίτητο ο νόμος να

168 Hart, The Concept of Law Oxford: Oxford University Press: 1961.

τους προστατεύει και να μεριμνά ενάντια στο κυβερνό-έγκλημα. Οι λόγοι μπορεί να είναι:

1. *Ικανότητα αποθήκευσης μαζικής ποσότητας δεδομένων σε σχετικά μικρό χώρο*

Ο υπολογιστής έχει το μοναδικό χαρακτηριστικό αποθήκευσης δεδομένων σε πολύ μικρό χώρο. Αυτό επιτρέπει, αντίστοιχα την απομάκρυνση ή παραγωγή της πληροφορίας είτε με φυσικά είτε με εικονικά μέσα, δημιουργώντας μεγαλύτερη ευελιξία. Η εξέλιξη των υπολογιστών, με την δημιουργία φορητών συσκευών επιτρέπει την μεταφορά των δεδομένων σε κάθε γωνιά του πλανήτη.

2. *Ευκολία πρόσβασης*

Το πρόβλημα που υπάρχει σχετικά με την διαφύλαξη ενός υπολογιστικού συστήματος από παράνομη είσοδο σε αυτό, είναι ότι υπάρχει κάθε πιθανότητα εισβολής όχι μόνο εξαιτίας ανθρώπινου λάθους αλλά λόγω πολύπλοκη τεχνολογίας. Με την δημιουργία σύγχυσης στο σύστημα δεδομένων, υπάρχει η δυνατότητα κλοπής κωδικών, ενισχυμένων φωνογράφων και εικόνων, παραμερίζοντας βιομετρικά συστήματα των δικτύων και απομακρύνοντας κάθε αμυντικό μηχανισμό που πιθανόν διαθέτουν.

3. *Πολυπλοκότητα*

Οι υπολογιστές «τρέχουν» με λειτουργικά συστήματα, τα οποία απαρτίζονται από αναρίθμητους κωδικούς. Το ανθρώπινο μυαλό λειτουργεί με αρκετά ήπιους ρυθμούς και δεν είναι δυνατό να μην αντιμετωπίσουν απώλεια δεδομένων σε κάποια φάση. Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται ενδεχόμενα σφάλματα και εισβάλλουν στο σύστημα.

4. *Απροσεξία και απώλεια δεδομένων*

Η απροσεξία από μέρος του χρήστη είναι πολύ συχνό φαινόμενο. Είναι λοιπόν πολύ πιθανό ότι ενώ προστατεύουμε το σύστημα, από το να υπάρξει οποιαδήποτε απώλεια προσοχής, που παράλληλα μπορεί να δώσει στον εγκληματία την ευκαιρία να κερδίσει πρόσβαση και έλεγχο πάνω στο δίκτυο. Η απώλεια δεδομένων, ακόμη, είναι πολύ κοινότοπο και εμφανές πρόβλημα καθώς όλα τα

δεδομένα καταστρέφονται σταδιακά. Περαιτέρω περισυλλογή δεδομένων πέρα από το τοπικό επίπεδο δημιουργεί παράλυση στο σύστημα εγκληματικής έρευνας.

3.3 .4 Προφίλ Εγκληματιών του κυβερνοχώρου[169]

Οι εγκληματίες του κυβερνοχώρου προέρχονται από διάφορες κοινωνικές κατηγορίες. Η διάκριση μπορεί να δικαιολογηθεί στην βάση του αντικειμένου που έχουν στο μυαλό τους. Κατηγορίες εγκληματιών μπορεί να είναι

1. *Παιδιά και έφηβοι ηλικίας 6-18 ετών*

Ένας απλός λόγος για αυτό τον τύπο της προβληματικής συμπεριφοράς σε ότι έχει να κάνει με τα παιδιά είναι το ανεξάντλητο ενδιαφέρον να γνωρίσουν και να εξερευνήσουν τα πάντα. Άλλος γνωστός λόγος είναι η επιθυμία να αποδείξουν ότι είναι ξεχωριστοί ανάμεσα σε άλλα συνομήλικα και μεγαλύτερα παιδιά. Επίσης, οι λόγοι μπορεί να είναι και ψυχολογικοί.

2. *Οργανωμένοι hacker*

Τα είδη αυτά των hacker οργανώνονται συνήθως για να εκπληρώσουν ένα συγκεκριμένο σκοπό. Ο λόγος μπορεί να είναι η άσκηση πολιτικής βίας, φονταμενταλισμού, κ.α. Οι Πακιστανοί θεωρούνται ως οι καλύτερου hacker στον κόσμο. Γνωρίζοντας την μακρόχρονη σύγκρουση Ινδίας-Πακιστάν, οι Πακιστανοί επιτίθενται ενάντια στην Ινδική κυβέρνηση με σκοπό την εκπλήρωση πολιτικών στόχων. Ακόμη η *NASA* όπως και η *Microsoft* σε επίπεδο ιστοσελίδων είναι συχνοί στόχοι ενάντια σε επιθέσεις hacker.

3. Επαγγελματίες hacker

169 Βλέπε Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online,* Routledge, London

Η δραστηριότητα τους έχει ως κύριο στόχο την απόσπαση χρημάτων. Αυτό το είδος των hacker προσλαμβάνονται για να εισβάλλουν στα site αντιπάλων για να αποσπάσουν αξιόπιστες και πολύτιμές πληροφορίες. Επιπλέον προσλαμβάνονται να δημιουργήσουν υποδομές ασφαλείας για τα συστήματα του εργοδότη τους για να αποφευχθούν αντίπαλες εισβολές.

4. *Άνεργοι και απολυμένοι*

Η ομάδα αυτή περιλαμβάνει άτομα που έχουν χάσει τις δουλειές τους είτε είναι δυσαρεστημένοι με τον εργοδότη τους. Για να εκδικηθούν εισβάλλουν στο σύστημα του εργοδότη για να προξενήσουν ζημιές.

3.3.5 Πρόληψη ενάντια στο κυβερνόεγκλημα

Η πρόληψη είναι η καλύτερη θεραπεία. Είναι προτιμότερο να λαμβάνουμε ειδικές επιφυλάξεις ενόσω χειριζόμαστε το δίκτυο. Ο Saileshkumar Zarkar[170], τεχνικός σύμβουλος και υπεύθυνος ασφαλείας δικτύων της ινδικής αστυνομίας σε θέματα ηλεκτρονικής προστασίας, προτείνει πέντε όρους για την ηλεκτρονική προστασία:

i. Προφύλαξη
ii. Πρόληψη
iii. Προστασία
iv. *Διαφύλαξη*
v. *Επιμονή*

Ακόμη ο χρήστης των ηλεκτρονικών δικτύων πρέπει να λαμβάνει υπόψη τα εξής:

1. Την πρόληψη κατά της ηλεκτρονικής ενέδρας με την απόκρυψη πληροφοριών που αφορούν το άτομο προσωπικά. Αυτό είναι θετικό όσο η απόκρυψη της ταυτότητας σε ξένους σε δημόσιο χώρο.

170 Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.

2. Πάντοτε να αποφεύγει να στέλνει φωτογραφικό υλικό σε ξένους και «δικτυακούς φίλους», γιατί μπορεί να προκύψει κίνδυνος παράνομης χρήσης αυτού.

3. Πάντοτε να χρησιμοποιούν την τελευταία ανανεωμένη έκδοση λογισμικού προστασίας ενάντια σε επιθέσεις ιών.

4. Πάντοτε να κρατούν εξωτερικό αρχείο με ευαίσθητες πληροφορίες σε περίπτωση απώλειας αυτών από επιθέσεις ιών

5. Να επιτηρείται η χρήση του διαδικτύου από τα παιδιά με σκοπό να μην υπάρξει κίνδυνος παρενόχλησης ή εκφοβισμού των παιδιών

6. Είναι καλύτερο το να χρησιμοποιείται ένα πρόγραμμα ασφάλειας που θα ελέγχει τις πρόσφατες εργασίες μέσω υπολογιστών

7. Οι ιδιοκτήτες των διαδικτυακών τόπων πρέπει να επιτηρούν την διακίνηση πληροφοριών και να είναι σε ετοιμότητα να υπερνικήσουν κάθε παράνομη δραστηριότητα

8. Η χρήση τειχών προστασίας μπορεί να είναι ευνοϊκή.

9. Οι δικτυακές κεφαλές που «τρέχουν» δημόσιας χρήσης ιστοσελίδες πρέπει να είναι φυσικά προστατευμένες σε ένα εσωτερικό δίκτυο συνεργασίας.

3.4 Κυβερνότρομοκρατία- ερμηνευτική πρόσεγγιση

Ο ορισμός του φαινομένου της κυβερνότρομοκρατίας είναι μία εξαιρετικά πολύπλοκη διαδικασία. Σε αρχικό στάδιο θα μπορούσαμε να κατατάξουμε το φαινόμενο στο ευρύτερο φάσμα της τρομοκρατίας, διαχωρίζοντας το όργανο δράσης αυτού. Με άλλα λόγια, η απλή ερμηνεία του όρου, έγκειται στο ότι **κυβερνοτρομοκρατία είναι η τρομοκρατική πράξη μέσω της χρήσης υπολογιστών. Σ**το πλαίσιο αυτό θα μπορούσαμε να αναφέρουμε ότι η παράνομη εισβολή σε αρχεία της CIA ή του FBI με στόχο τον εξαναγκασμό της αμερικανικής κυβέρνησης και του απλού λαού, θα μπορούσε να θεωρηθεί παράδειγμα της κυβερνητικής τρομοκρατίας. Μία άλλη περίπτωση είναι εκείνη που αφορά τον τομέα της υγείας είναι η απόσπαση ηλεκτρονικών αρχείων από τις βάσεις δεδομένων των νοσοκομειακών μονάδων και η αλλαγή του ιστορικού υγείας των ασθενών, η οποία θα μπορούσε να αποβεί θανατηφόρα για εκείνους, λόγω της λαθεμένης διάγνωσης και

παροχής φαρμακευτικής αγωγής. Το 2003, ο Coleman[171], αναφερόμενος σε θέματα ηλεκτρονικού εμπορίου, υποστήριζε ότι «εάν το διαδίκτυο τεθεί εκτός λειτουργίας θα υπάρξει μία μαζική σύγχυση στις συναλλαγές κόστους 6 δισεκατομμυρίων δολαρίων.

Γενικότερα, υπάρχει μία διχογνωμία σχετικά με τον ορισμό του φαινομένου της κυβερνοτρομοκρατίας. Η μία άποψη ερευνά το φαινόμενο με βάση την μέθοδο της αιτίας-αποτελέσματος και η άλλη είναι εκείνη που την ερευνά στηριζόμενη στην διαδικτυακή της δράση. Σε ότι αφορά την πρώτη άποψη, εκείνη της αιτίας-αποτελέσματος, η τρομοκρατία του κυβερνοχώρου υπάρχει όταν επιθέσεις μέσω των ηλεκτρονικών υπολογιστών καταλήγουν σε μία κατάσταση όπου ο φόβος παράγεται, όπως και σε μία παραδοσιακή τρομοκρατική πράξη. Απεναντίας σε μία προσπάθεια οι τρομοκράτες να πλήξουν μέσω του διαδικτύου άτομα ή οργανισμούς έχουν στόχο να προξενήσουν οικονομική δυσπραγία. Ο σκοπός της επίθεσης μέσω του κυβερνοχώρου περιλαμβάνει τέσσερις κατηγορίες: την απώλεια της ακεραιότητας, της απώλεια της διαθεσιμότητας, την ανυπαρξία του απορρήτου και την φυσική καταστροφή.

Η χρήση του Διαδικτύου καθώς και άλλων συσκευών τηλεπικοινωνίας είναι συνεχώς αυξανόμενη. Η ασφάλεια των συνόρων και των ατόμων οδηγεί τους τρομοκράτες και τους εξτρεμιστές να χρησιμοποιούν το Ιντερνέτ για να πλήξουν ισχυρά κράτη τους διεθνούς συστήματος, κυρίως τις Ηνωμένες Πολιτείες. Εξαιτίας των αδυναμιών σε ότι έχει να κάνει με την ασφάλεια στην χρήση του Διαδικτύου και των υπολογιστών, αυτό θα μπορούσε να δώσει την ευκαιρία στους τρομοκράτες να ενισχύσουν τις γνώσεις τους στα υπολογιστικά συστήματα, καθώς και να συμπράξουν με εγκληματικές οργανώσεις.

Σύμφωνα με τους Rollins και Wilson (2007)[172], έχουν γίνει αναφορές που καταδεικνύουν την ολοένα συχνότερη συνεργασία μεταξύ των τρομοκρατών και των εξτρεμιστών με τους εγκληματίες του κυβερνοχώρου για την διεθνή διακίνηση χρήματος καθώς και για λαθρεμπόριο όπλων και ναρκωτικών ουσιών. Οι σύνδεσμοι αυτοί με τους hackers και τους ηλεκτρονικούς εγκληματίες αποτελούν παραδείγματα που που αποκαλύπτουν την επιθυμία των τρομοκρατών να εξευγενίσουν τις

171 Coleman, Keivin "Cyber Terrorism www.directionsmasελ.com/article.php?article.id=432 , Oct. 10, 2003

172 Rollins, J. & Wilson, C. CRS Report for Congress. Terrorist Capabilities for Cyberattack: Overview and Policy Issues, January 22, 2007.

ικανότητες τους στην χρήση των ηλεκτρονικών υπολογιστών, και να σφυρηλατήσουν σχέσεις μέσω της συνεργατικής διακίνησης ναρκωτικών που καταλήγουν στην παροχή υψηλής ποιότητας προγραμματιστών για τις επιχειρήσεις τους. Φωτεινό παράδειγμα αυτής της δράσης είναι η βομβιστική επίθεση που έλαβε χώρα τον Ιούλιο του 2005 στο Λονδίνο, που είχε ως στόχο τον μητροπολιτικό σιδηρόδρομο, η οποία δείχνει το πόσο εξελιγμένο μπορεί να είναι το δίκτυο πληροφόρησης των τρομοκρατών.

Η διαφοροποίηση μεταξύ ενός τρομοκράτη του κυβερνοχώρου και ενός hacker, δεν είναι πάντοτε εύκολο να ειδωθεί. Το πρόβλημα είναι, ότι παρά το γεγονός ότι τρομοκράτες εστιάζουν στα τρωτά σημεία των στόχων τους για μελλοντικές επιθέσεις, οι κυβερνο-εγκληματίες ακολουθούν την ίδια τακτική με τη διαφορά ότι αποσκοπούν στο οικονομικό όφελος μέσα από την πληροφόρηση. Είναι θετικό το ότι το FBI έχει αναφέρει ότι οι ηλεκτρονικές επιθέσεις από τους τρομοκράτες έχουν κατά κανόνα περιοριστεί στον βομβαρδισμό μέσω ηλεκτρονικών μηνυμάτων και στην παραμόρφωση των ιστοσελίδων. Ωστόσο, εξαιτίας της αυξανόμενης γνώσης αυτών, η ικανότητα επίθεσης στα ηλεκτρονικά δίκτυα κατέχει υψηλή βαθμίδα κινδύνου. Το FBI πιθανόν, προβλέπει την πρόσληψη από μέρους των τρομοκρατών, ειδικών σε θέματα ηλεκτρονικών υπολογιστών με στόχο την αντικατάσταση συμβατικών επιθέσεων με αυτές στον κυβερνοχώρο. Επιπλέον, σύμφωνα με τον Muller[173] (2007), ο οποίος είναι διοικητικό στέλεχος του FBI, παρατηρήθηκε ότι οι τρομοκράτες χρησιμοποιούν ευρέως το Διαδίκτυο για να επικοινωνήσουν, να σχεδιάσουν επιθέσεις, να προσηλυτίσουν, να επιστρατεύσουν μέσα για τους σκοπούς του, καθώς και να αποκτήσουν λογιστική και οικονομική βοήθεια. Η δραστηριότητα αυτή αποτελεί μείζον ζήτημα για το FBI.

Το 2005, έχουν σημειώθει επιθέσεις κατά της ασφάλειας των ηλεκτρονικών υπολογιστών έχουν αυξηθεί κατά 50%, με κυριότερους στόχους τις βιομηχανίες και τις κυβερνητικές οργανώσεις στις ΗΠΑ. Εφόσον το κυβερνο-έγκλημα έχει γίνει μία αρκετά συχνή δραστηριότητα, η δυσκολία διαφοροποίησης μεταξύ αυτού και της τρομοκρατίας έχει γίνει μεγαλύτερη. Οι Ηνωμένες Πολιτείες έχουν κάνει βήματα για την επιβολή δικαίου εναντίον αυτού του είδους των επιθέσεων (βλέπε κεφ. 4). Όπως

173 Βλέπε Graff, Garrett. "Robert Mueller: Remaking the FBI", Washingtonian, August 1, 2008.

δείχνουν πρόσφατα στοιχεία, οι επιθέσεις μέσω των υπολογιστών θα γίνουν αναρίθμητες, γρηγορότερες και περισσότερο εξελιγμένες.

Η ταχύτητα με την οποία το ηλεκτρονικό έγκλημα εξελίσσεται είναι ραγδαία. Έχουν σημειωθεί χιλιάδες περιστατικά επιθέσεων μέσω του κυβερνοχώρου, όπως επιθέσεις μέσω ιών, ηλεκτρονικές απάτες, επιθέσεις spoofing, κ.α. Φυσικά τα παραπάνω δεν συγκρίνονται με την απειλή της κυβερνοτρομοκρατίας. Αξίζει να αναφέρουμε το περιστατικό κατά το οποίο ένας έφηβος, κατόρθωσε να υποκλέψει τους κωδικούς σε συστήματα ελέγχου στο φράγμα που βρίσκεται στο Salt River της Αριζόνα, όπου θα μπορούσε να εξαπολύσει τόνους νερού σκορπώντας τον θάνατο σε χιλιάδες κατοίκους.

Ένας πιο ολοκληρωμένος ορισμός σχετικά με το φαινόμενο της κυβερνότρομοκρατίας είναι, ο εξής:

Κυβερνότρομοκρατία είναι η έμμεση χρήση παρεμβατικών δραστηριοτήτων, ή απειλών, στο κυβερνοχώρο με την πρόθεση να επιτευχθούν ευρύτεροι κοινωνικοί, ιδεολογικοί, θρησκευτικοί, πολιτικοί και άλλοι σκοποί. Επίσης εξ ορισμού, καλύπτει και την πρόθεση να προκαλέσει φόβο και ανασφάλεια σε άτομα πολιτικής, οικονομικής και κοινωνικής σφαίρας.

Άρα λοιπόν μπορούμε να κατανοήσουμε το γεγονός κατά το οποίο, η κύβερνοτρομοκρατία έχει εξελιχθεί με ταχύτατους ρυθμούς κατάτην τελευταία δεκαετία. Για το λόγο αυτό είναι σκόπιμο να αναφέρουμε μία σειρά από χαρακτηριστικά Σε πρώτο επίπεδο έχουμε το χαμηλό κόστος των δραστηριοτήτων. Σε αντίθεση με τα κανονικά όπλα και οπλικά συστήματα, η ανάπτυξη των τεχνικών που βασίζονται στην πληροφορική δεν απαιτεί μεγάλα χρηματικά ποσά ή κρατικές επιχορηγήσεις. Το μόνο που είναι απαραίτητο, είναι η πολύ καλή γνώση για την διαχείριση των ηλεκτρονικών υπολογιστών και των δικτύων ανταλλαγής πληροφοριών. Θα μπορούσαμε να πούμε ακόμη ότι ένας «ηλεκτρονικός» στρατιώτης μισθοφόρος μπορεί να είναι περισσότερο επικίνδυνος από έναν άλλο ο οποίος το μόνο που γνωρίζει είναι σκοποβολή.

Σε δεύτερη φάση έχουμε τα μη διακριτά σύνορα των κρατών. Τα παραδοσιακά σύνορα μεταξύ κρατών ή τα γνωστά όρια μεταξύ Δημοσίων και ιδιωτικών συμφερόντων ή ακόμη και οι διαφορές μεταξύ στρατιωτικών ή εγκληματικών

συμπεριφορών εμπλεκόμενα με τα συστήματα των δικτύων, που δύσκολα μπορούν ν' αναγνωριστούν. Επιπλέον έχουμε την παρουσία νέων τεχνικών που βασίζονται κυρίως στην τεχνική της παραπλάνησης, σημαντικό στοιχείο κάθε μορφής τρομοκρατίας. .

Οι hackers, όπως έγινε λόγος παραπάνω ηλικιακά κυμαίνονται μεταξύ 16 και 30 ετών. Η ηλικία αυτή φανερώνει την αυξημένη ενασχόληση τους με τους υπολογιστές και την ευφυΐα που αυτοί δείχνουν κατά τη χρήση τους. Βέβαια υπάρχουν και μεγαλύτεροι σε ηλικία χρήστες, όπου εργάζονται ή έχουν εργαστεί σε εταιρείες ηλεκτρονικών υπολογιστών ή στις ένοπλες δυνάμεις, όπου είχαν την ευκαιρία ν' ασχοληθούν ουσιαστικά με την ανάπτυξη και την εξέλιξη των υπολογιστών, όπως και προγραμμάτων για υπολογιστές. Οι λόγοι που ίσως ωθήσουν αυτούς τους νέους ανθρώπους να πειραματίζονται με τα δίκτυα είναι συνήθως η απλή προσωπική ευχαρίστηση, η διασκέδαση ακόμη και η περιέργεια. Πέρα όμως από την προσωπική ικανοποίηση, υπάρχουν και άτομα τα οποία είναι περισσότερο πολιτικοποιημένα, που ασχολούνται με καίρια ζητήματα, όπως η εξωτερική πολιτική, η οικονομική πορεία μίας χώρας ή ακόμη και κοινωνικά ζητήματα όπως η εγκληματικότητα, η ανεργία, η καταστροφή του περιβάλλοντος, κ.α. Ίσως κάποιοι θεωρήσουν ότι μέσω αυτού του τρόπου εκδήλωσης βίας, επιθυμούν να δείξουν την διαμαρτυρία τους απέναντι στην πολιτική ζωή ενός ή περισσοτέρων κρατών.

Οι ειδικοί του αμερικανικού Πενταγώνου [174]πιστεύουν ότι αυτή η ειδική κατηγορία των hackers[175] είναι πιθανόν να εγείρει το ενδιαφέρον από τρομοκρατικές οργανώσεις. Στο πλαίσιο αυτό, υπάρχει η άποψη ότι τρομοκρατικές οργανώσεις, ίσως θελήσουν να εκμεταλλευτούν τις ικανότητες τους και την ιδεολογία τους προκειμένου να τους μετατρέψουν σε «στρατιώτες» με την πρόφαση ότι συμμερίζονται την ιδεολογία τους, και για αυτό το λόγο θέλουν να τους εντάξουν προκειμένου να έχουν

174 Βλέπε Katie Hafner & John Markoff (1991). Cyberpunk: Outlaws and Hackers on the Computer Frontier. Simon & Schuster.

175 Οι χάκερ «μαύρου καπέλου» εισβάλουν σε συστήματα υπολογιστών παράνομα για να προκαλέσουν ζημία ή καταστροφή δεδομένων, όπως εισβολή σε συστήματα τραπεζών για υπεξαίρεση χρημάτων.(πηγή Techopedia.com)

μεγαλύτερη ελευθερία δράσης . Φυσικά χρησιμοποιούν και οικονομικά κίνητρα για να επιτύχουν τους σκοπούς τους, ή, ακόμη, για την επέμβαση στα δίκτυα πληροφορικής κρατών που βρίσκονται σε αντιπαράθεση.

Η εξέλιξη της ηλεκτρονικής τρομοκρατίας αποτελεί πλέον μια ολοκληρωμένη συνιστώσα του σύγχρονου πλαισίου ασφάλειας, έχοντας ήδη παρουσιάσει δείγματα που ξεκινούν από τη διείσδυση σε χρηματιστηριακές δραστηριότητες και καταλήγουν σε υποδομές πυραυλικής άμυνας. Η ανατροπή της λογικής του συμβατικού πολέμου είναι πλέον γεγονός, ενώ κανένα στοιχείο πια δεν θα πρέπει να θεωρείται απόλυτα ασφαλές. (πίνακας 4)

Πίνακας 4

	Φυσικός Στόχος	**Ψηφιακός Στόχος**
Φυσικό μέσο	*Παραδοσιακή τρομοκρατία (π.χ. Βομβαρδισμοί στην Οκλαχόμα)*	*Π.χ. Επιθέσεις της τρομοκρατικής οργάνωσης IRA στο Λονδίνο, 1992.*
Ψηφιακό μέσο	*π.χ. η εισβολή σε ένα δίκτυο ελέγχου εναέριας κυκλοφορίας μπορεί να προκαλέσει πτώση των αεροσκαφών*	*Είσοδος σε συστήματα που καθορίζουν τις οικονομικές συναλλαγές με σκοπό να πλήξουν εθνικές οικονομίες.*

3.4.1 Όργανα δράσης κυβερνοτρομοκρατίας

Τα όπλα δραστηριότητας των κυβερνότρομοκρατών δεν είναι σχεδιασμένα να σκοτώνουν άτομα ή να προξενούν ζημιές σε υλικά αντικείμενα. Απεναντίας, υπάρχουν αποκλειστικά για να παραποιήσουν ή να καταστρέψουν ηλεκτρονικά αρχεία. Τα όπλα και οι στόχοι είναι τα ηλεκτρόνια που κινούνται στον κυβερνοχώρο. Παρόλο που ο άνθρωπος είναι το υποκείμενο των δράσεων, παραμένει ο πιο αδύναμος κρίκος στο σύστημα. Ορισμένα από τα όργανα που επιδρούν στα δίκτυα είναι:

1. **Ιοί:** ένα από τα περισσότερο αποδοτικά μέσα των κυβερνότρομοκρατών είναι η καλλιέργεια ιών. Οι ιοί είναι προγράμματα που σχεδιάζονται για να εκπληρώσουν πράξεις που δεν είναι στην πρόθεση του δράστη. Οι πράξεις αυτές αφορούν την απώλεια ή μεταβολή ευαίσθητων δεδομένων με κακόβουλο ή μη μέσο. Ένας ιός, ονομάζεται έτσι επειδή παρασιτεί σε ένα

άλλο οργανισμό και εξαπλώνεται χωρίς κάποια συγκεκριμένη δράση. Ένας από τους πιο διαδεδομένους ιούς ήταν το 1992, ο ιός Michelangelo, ο οποίος πήρε το όνομα του από τον γνωστό καλλιτέχνη, επειδή εμφανίστηκε στις 6 Μαρτίου, ημέρα των γενεθλίων του γνωστού ζωγράφου.

2. **Άλογα Trojan:** ο δεύτερος τύπος όπλου είναι τα **Άλογα Trojan.** Είναι ένα πρόγραμμα το οποίο, δεν έχει καταστροφική δράση αρχικά, αλλά απελευθερώνει ένα δεύτερο πρόγραμμα το οποίο εκπληρώνει εργασίες ενάντια σε εντολές λειτουργών του συστήματος. Το πρόγραμμα αυτό, μπορεί να χρησιμοποιηθεί για την εγκατάσταση ενός άλλου προγράμματος που συλλέγει κωδικούς εισόδου από νόμιμους χρήστες και τους αποθηκεύει για μελλοντική χρήση. Οι κυβερνότρομοκράτες χρησιμοποιούν αυτό το μέσο, για να αποσπάσουν πληροφορίες, εισβάλλοντας σε ένα σύστημα, υιοθετώντας ψεύτικα προφίλ για να αποφύγουν οποιαδήποτε μηχανισμό άμυνας.
3. **«Σκουλήκια»:** Τα «σκουλήκια» είναι προγράμματα που αναπτύσσονται για να ταξιδεύουν μέσω συστημάτων και να εκτελούν εργασίες όπως, διαγραφή εργασιών και συλλογή δεδομένων. Μπορεί να είναι αποτελεσματικά εάν προγραμματιστούν αλλά μπορεί να έχουν καταστροφικά αποτελέσματα. Ένας ιός εισβάλλει σε ένα πρόγραμμα, ένας ιός-σκουλήκι, εκτείνεται σε όλο το σύστημα ανεξάρτητα. Έχει ακόμη, την δυνατότητα να αντιγράφει τον εαυτό του, ενώ συνεχίζει να εξαπλώνεται στο δίκτυο. Ένα παράδειγμα είναι ο ιός σκουλήκι Stuxnet[176].
4. **Όπλα ηλεκτρομαγνητικών παλμών** (EMP Weapons): αποτελούν υψίστης ποιότητας όπλα, τα οποία μπορούν να καταστρέψουν δίκτυα και συστήματα υπολογιστών μέσω ηλεκτρομαγνητικών παλμών[177]**.** Η ικανότητα πρόκλησης ενός συνεχούς ηλεκτρομαγνητικού παλμού μπορεί να προκαλέσει ανάλογη καταστροφή, σε οποιοδήποτε σύστημα βρίσκεται στην ακτίνα δράση αυτών των όπλων, με ένα όπλο μαζικής καταστροφής. Τα όπλα αυτά δεν αφήνουν ίχνη όπως τα παραδοσιακά και ο εντοπισμός αυτών είναι εξαιρετικά δύσκολο και είναι ικανά να καταστρέψουν ολόκληρα κτίρια μέσα σε λίγα λεπτά .

176 Ο stuxnet είναι ιός σκουλήκι που είχε ως στόχο την επίθεση σε πυρηνικές εγκαταστάσεις του Ιράκ το 2010.

177 James, W. Rawles, "High Technology Terrorism" Defense Electronics, January 1990, 74.

Παραδείγματα τέτοιων όπλων είναι τα HERF (High Energy Radio Frequency) και το EMPT (Electromagnetic Pulse Transformer)[178].

3.4.2 Πότε μία Κυβερνόεπίθεση μπορεί να θεωρηθεί ως Κυβερνότρομοκρατία?

Κάποιοι παρατηρητές θεωρούν ότι ο όρος «Κυβερνοτρομοκρατία» δεν είναι κατάλληλος. Αυτό μπορεί να συμβεί επειδή μία ραγδαία εξαπλωμένη επίθεση μέσω του κυβερνοχώρου, ίσως προκαλέσει απλά, ενοχλήσεις και όχι τρόμο, όπως ένας εκρηκτικός μηχανισμός ή άλλα χημικά βιολογικά ή πυρηνικά όπλα. Ωστόσο, υπάρχει η άποψη ότι τα αποτελέσματα μίας ευρείας επίθεσης ενάντια στα ηλεκτρονικά δίκτυα, μπορεί να είναι απρόβλεπτα και ίσως προκαλέσουν οικονομικές καταστροφές, τρόμο, θνησιμότητα και για το λόγο αυτό μπορεί να θεωρηθεί τρομοκρατική. Υπάρχουν τουλάχιστον δύο βασικές απόψεις, σύμφωνα με τις οποίες μία κυβερνόεπίθεση μπορεί να θεωρηθεί ως τρομοκρατική:

- Η άποψη σχετικά με τα **αποτελέσματα** της επίθεσης, τα οποία μπορούν να θεωρηθούν τρομοκρατικά. Η κυβερνοτρομοκρατία, υπάρχει όταν επιθέσεις μέσω υπολογιστών καταλήγουν σε αποτελέσματα τα οποία προξενούν διαταραχές και είναι δυνατό να γεννήσουν φόβο ανάλογο με εκείνο που μπορεί να προκαλέσει μία παραδοσιακή τρομοκρατική επίθεση, ακόμη κι αν οι δράστες είναι κατά βάση, εγκληματίες.

- Η δεύτερη άποψη που προκύπτει είναι η **πρόθεση** των κυβερνότρομοκρατών να προχωρήσουν σε επιθέσεις εναντίον ηλεκτρονικών δικτύων γίνονται με σκοπό να εξαναγκάσουν και να τρομοκρατήσουν τον κυβερνητικό μηχανισμό ενός κράτους, με πολιτικά κίνητρα για την πρόκληση ζημίας ή οικονομικής καταστροφής.

3.4.3 Οι κρατικές υποδομές ως στόχοι της κυβερνοεπίθεσης

178 Schwartau, 171-189

Ένας επιτραπέζιος υπολογιστής ή μία οποιαδήποτε χειροκίνητη ηλεκτρονική συσκευή, είναι το μέσο με το οποίο ο καθένας μπορεί να έχει πρόσβαση στο διαδίκτυο, ταυτόχρονα όμως μπορεί να γίνει και το όργανο εκδήλωσης μίας κυβερνόεπίθεσης. Παρόλαυτα, μία οργανωμένη επίθεση για να καταστεί επιτυχής, θα πρέπει τα υποκείμενα της επίθεσης να εξασφαλίσουν ότι το δίκτυο καθαυτό, θα πρέπει να παραμείνει λίγο πολύ ανέπαφο, εκτός εάν θεωρούν ότι τα προσδοκώμενα κέρδη από το «κλείσιμο του διαδικτύου» θα ξεκινήσει διαδικασίες που θα καταλήξουν στην συνοδευόμενη απώλεια της επικοινωνίας[179]. Μία οργανωμένη επίθεση, μπορεί να είναι αποτελεσματική εάν κατευθύνεται ενάντια σε μέρος του συνόλου των κρατικών υποδομών σε ένα κράτος, και εάν υπάρχει σωστός συγχρονισμός μπορεί η επίθεση μέσω του κυβερνοχώρου να ενισχύσει οποιαδήποτε συμβατική επίθεση με όπλα μαζικής καταστροφής.

Μία τέτοια επίθεση, είναι βέβαιο ότι έχει ως κύριο στόχο την οικονομική ισχύ ενός κράτους. Η άποψη αυτή, υιοθετείται και από υπεύθυνους ασφαλείας του υπουργείου εξωτερικών των Ηνωμένων Πολιτειών[180], οι οποίοι θεωρούν ότι οι ζημιές και η απώλεια ανθρώπινων ζωών δεν είναι παρά, παράπλευρες απώλειες. Επιπροσθέτως, μία επίθεση μέσω του κυβερνοχώρου, μπορεί να έχει μεγαλύτερη αποτελεσματικότητα, εάν γίνει παράλληλα με μία φυσική επίθεση. Ένα παράδειγμα, θα μπορούσε να είναι η απόπειρα πρόκλησης βλάβης κέντρου βοήθειας, όπως τα συστήματα υγείας ενός κράτους παράλληλα με την πυροδότηση εκρηκτικών μηχανισμών. Αυτό το παράδειγμα μπορεί να έρθει σε αντίθεση με μία ευρεία συντονισμένη κυβερνόεπίθεση, χωρίς την συνοδεία μίας φυσικής επίθεσης, η οποία τεχνικά θα είναι εξαιρετικά δύσκολο να σχεδιαστεί και πιθανόν να μην αποδώσει τα αναμενόμενα αποτελέσματα. Επειδή μία τέτοια επίθεση, δεν μπορεί να προκαλέσει φυσικές καταστροφές και απώλεια ανθρώπινης ζωής, αυτό ίσως εξηγήσει την δυσκολία στην εύρεση αποδείξεων για το εάν επιθέσεις μέσω κυβερνοχώρου είναι αποτέλεσμα διεργασιών τρομοκρατικών οργανώσεων[181].

179 Βλέπε Andress, Jason. Winterfeld, Steve. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.

180 Βλέπε Ross J. Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems,*

181 Βλέπε Carr, Jeffrey. (2010). *Inside Cyber Warfare: Μασελ.ing the Cyber Underworld*. O'Reilly

Όμως, άλλοι ερευνητές υποστηρίζουν ότι, λόγω του ότι οι κρατικές υποδομές αλληλεξαρτώνται, και για το λόγο αυτό επιθέσεις ενάντια σε ένα τομέα μπορεί να επηρεάσουν ταυτόχρονα και άλλους τομείς και κατ' επέκταση μακροπρόθεσμες συνέπειες στην οικονομία. Οι ίδιοι παρατηρητές, ισχυρίζονται ότι η αλ Κάιντα και άλλες τρομοκρατικές οργανώσεις ακολουθούν πλέον τους ρυθμούς της τεχνολογίας και υπάρχει πλέον μία ευρύτερη εξυγίανση στις επιθέσεις αυτών και πλέον γνωρίζουν ότι κάθε επίθεση μέσω του κυβερνοχώρου μπορεί να δώσει ισχυρά πλήγματα στην αμερικανική οικονομία.

Η δημοσιότητα θα μπορούσε να είναι ένας από τους πρωταρχικούς στόχους για μία τρομοκρατική επίθεση. Εκτεταμένη κάλυψη έχει γίνει στην αδυναμία των αμερικανικών κρατικών δομών που αφορούν την πληροφόρηση και την πιθανή καταστροφή που μπορεί να προκληθεί από μία επίθεση μέσω κυβερνοχώρου. Αυτό ίσως οδηγήσει τους τρομοκράτες στην άποψη ότι, ακόμη και μία οριακά επιτυχημένη επίθεση τέτοιου είδους ενάντια σε μία υπερδύναμη όπως είναι οι ΗΠΑ, ίσως συγκεντρώσει αυξημένη δημοσιότητα[182]. Επίσης υπάρχει η άποψη ότι, μία τέτοια επίθεση, από μία τρομοκρατική οργάνωση μπορεί να προκαλέσει ανησυχία στο ευρύτερο κοινό, ανεξαρτήτως αποτελέσματος, όπου μπορεί να οδηγήσει σε αυξανόμενες υποχωρήσεις επενδύσεων και πωλήσεις των μετοχών.

Για να κατανοήσουμε τον βαθμό με τον οποίο, επιθέσεις ενάντια σε υποδομές, επηρεάζουν την κοινή γνώμη, είναι χρήσιμο να ανατρέξουμε στην περίοδο αμέσως μετά τον δεύτερο Παγκόσμιο Πόλεμο, σε μία έρευνα που επιμελήθηκαν οι Ηνωμένες Πολιτείες. Η έρευνα αυτή εξέταζε την συχνότητα με την οποία οι ΗΠΑ και η Μεγάλη Βρετανία πυροδοτούσαν εκρηκτικούς μηχανισμούς ενάντια στην Γερμανία, προσπαθώντας να καταστρέψουν τις υποδομές τους προσπαθώντας να δώσουν ένα ισχυρό πλήγμα στην οικονομία τους, να καταλύσουν την βιομηχανική της βάση και να μειώσουν την θέληση του πληθυσμού να συνεχίσει τον πόλεμο. Θεωρητικοί που συμμετείχαν σε αυτή την έρευνα πρόβλεψαν ότι μία τέτοια προσπάθεια θα προκαλούσε παράλυση ή εξάλειψη του στόχου. Η έρευνα, ωστόσο έδειξε ότι οι βιομηχανικές κοινωνίες είναι εντυπωσιακά ανθεκτικές. Η βιομηχανική παραγωγή είχε αυξηθεί για δύο χρόνια, κατά τη διάρκεια των βομβαρδισμών. Το παράδειγμα αυτό, μας δείχνει ότι μία οικονομικά ισχυρή χώρα, και ακόμη

182 The Media and Terrorism: A Reassessment Paul Wilkinson. Terrorism and Political Violence, Τομ.9, No.2 (Summer 1997), σελ..51–64 Published by Frank Cass, London

περισσότερο μία χώρα που βασίζεται σε βιομηχανική δραστηριότητα είναι δυνατό να επιβιώσει ευκολότερα από μία επίθεση μέσω του κυβερνοχώρου.

Έχει δοθεί ακόμη ιδιαίτερη σημασία στην μελέτη των κυβερνοεπιθέσεων, είτε αυτές προέρχονται από τρομοκράτες, είτε από τρομοκρατικές οργανώσεις. Αναλογιζόμενοι την ευαισθησία που μπορεί να έχουν οι κρατικές υποδομές του αμερικανικού κράτους απέναντι σε κυβερνοεπιθέσεις, όπως το εθνικό σύστημα ηλεκτροδότησης, εκπρόσωποι του αμερικανικού Πενταγώνου, όπως ο Kenneth Bacon, υποστηρίζουν ότι το «φάντασμα» των επιθέσεων αυτών, σε συστήματα όπως τηλεπικοινωνίες, εγκαταστάσεις πετρελαίου και φυσικού αερίου, στρατιωτικές βάσεις, συστήματα υδροδότησης και κυρίως το σύστημα υγείας[183]. Ο βαθμός στον οποίο, οι υποδομές αυτές εξαρτώνται από τα συστήματα πληροφόρησης δεν έχει ακόμη ξεκαθαριστεί. Τα συστήματα πληροφόρησης συνδέονται με αυτής της υψίστης σημασίας υποδομές, αποτελούν τους κύριους στόχους για τρομοκράτες, έθνη-κράτη, και ηλεκτρονικούς εγκληματίες στην εποχή της ασύμμετρης πολεμικής ετοιμότητας. Μερικά παραδείγματα:

- **Συστήματα τραπεζών και οικονομικοί οργανισμοί** έχουν μία ευαισθησία απέναντι σε επιθέσεις εξαιτίας της εξάρτησης τους από τα δίκτυα. Ωστόσο, ο τομέας αυτός διατηρεί ιδιωτικά και εσωτερικά δίκτυα με πολύ περιορισμένη εξωτερική πρόσβαση, διατηρώντας ένα επίπεδο προστασίας από εξωτερικές επιθέσεις.

- **Συστήματα τηλεπικοινωνιών** είναι εκτεθειμένα σε επιθέσεις που σχετίζονται με την λειτουργία των λογισμικών προγραμμάτων από εσωτερικούς λειτουργούς που είναι γνώστες των τεχνικών λεπτομερειών των συστημάτων αυτών. Αυτό αφορά και υπηρεσίες υγείας και αστυνομίας.

- **Συστήματα ηλεκτροδότησης** που διαθέτουν αισθητήρες για τον έλεγχο της δραστηριότητας του δικτύου σε έκτακτες περιπτώσεις φυσικών καταστροφών. Τα όργανα αυτά, είναι ευπαθή σε οποιαδήποτε είδους ηλεκτρονική εκμετάλλευση, έχοντας ως αποτέλεσμα διακοπές ρεύματος

[183] Kenneth Bacon, Refuges International.

και υπερφορτώσεις ισχύος που δημιουργούν καταστροφές σε κάθε είδους ηλεκτρονική συσκεύη.

- **Η υδροδότηση** και ο έλεγχος των επιπέδων ύδατος ελέγχονται από αισθητήρες και τηλεχειριστές. Η φυσική προστασία, μαζί με υψηλή αίσθηση κινδύνου, πρέπει να τηρηθεί κατά τη διάρκεια της πιθανής σύγκρουσης.

- **Εγκαταστάσεις πετρελαίου και φυσικού αερίου** χρησιμοποιούν ευρέως το Σύστημα Επιτήρησης και Απόκτησης Πληροφοριών (SCADA), το οποίο όμως είναι δεκτικό σε κάθε επίθεση κυβερνοχώρου με την τάση να επηρεάζει πολυάριθμους οικονομικούς τομείς, όπως μεταφορές.

Οι κακόβουλοι χρήστες του διαδικτύου, αποτελούν την μεγαλύτερη απειλή σε κρατικές υποδομές ζωτικής σημασίας για την σταθερότητα και την ανάπτυξη ενός κράτους. Διαθέτουν επίσης καταρτισμένη γνώση σε συστήματα και αυξημένη πρόσβαση η οποία μπορεί να είναι αρκετά επιζήμια. Η τραγωδία της 11^{ης} Σεπτεμβρίου, έδειξε ότι οι τρομοκράτες είναι πιθανό να βρίσκονται στο εσωτερικό πυρήνα του αμερικανικού κράτους, αποκτώντας εξειδικευμένες γνώσεις με φονικές τάσεις.

i. Επιθέσεις παραμόρφωσης δικτυακών τόπων και σχετικών δραστηριοτήτων

Μία επίθεση παραμόρφωσης δικτυακών τόμων, είναι εκείνες που διενεργούνται με σκοπό να μεταβάλλουν την οπτική ενός ηλεκτρονικού τόπου ή μιας ιστοσελίδας. Ο σκοπός αυτών που επιχειρούν αυτού του είδους την μεταβολή, είναι να αντικαταστήσουν τον ιστοτόπο με ένα δικό τους για να προβάλλουν απόψεις υπέρ της τρομοκρατίας και κατά της αμερικανικής πολιτικής. Η πιο σημαντική εξ αυτών είναι οι παραμορφώσεις δικτύων είναι οι «σημασιολογικές επιθέσεις»[184]. Οι επιθέσεις αυτές περιλαμβάνουν την αλλαγή του περιεχομένου μίας ιστοσελίδας με ευφυή τρόπο, διαδίδοντας ψευδείς πληροφορίες. Μία τέτοια επίθεση σε σελίδες ειδήσεων και κυβερνητικών δραστηριοτήτων αποτελεί ένα σημαντικό ηλεκτρονικό προπύργιο στον πόλεμο μεταξύ τρομοκρατών και κυβέρνησης, το οποίο έχει έρεισμα στον αμερικανικό πληθυσμό. Πιθανοί στόχοι μπορούν να είναι σελίδες της

184 http://www.answers.com/topic/semantic-attack Η χρήση λανθασμένων πληροφοριών με στόχο να πλήξουν την αξιοπιστία των στόχων του και των πόρων αυτών ή να προκαλέσουν άμεση ή έμμεση ζημιά. Παραδείγματα περιλαμβάνουν το «λίβελλο» για λόγους προπαγάνδας και λαϊκισμού

κυβέρνησης καθώς και της στρατιωτικής εξουσίας, και σελίδες παροχής πληροφοριών.

ii. Επιθέσεις σε ηλεκτρονικές σελίδες ευρετηρίων

Τα υπολογιστικά συστήματα που συνδέονται με το διαδίκτυο, επικοινωνούν μεταξύ τους χρησιμοποιώντας διευθύνσεις **IP (Internet Protocol) .** Οι ηλεκτρονικές σελίδες ευρετηρίων, οι οποίες αποτελούν έναν ψηφιακό «χρυσό οδηγό», που παρέχει πληροφορίες για το όνομα ενός ηλεκτρονικού ιστού και την διεύθυνση αυτού. Για παράδειγμα όταν ένας χρήστης θελήσει να συνδεθεί με τη δημοφιλή ηλεκτρονική σελίδα του CNN, ο κεντρικός υπολογιστής του δικτύου (server) αναζητά την αριθμητική διεύθυνση στο διαδίκτυο για να καταστήσει επιτυχή την πρόσβαση. Σε περίπτωση που ο κεντρικός υπολογιστής, δώσει μία λάθος αριθμητική διεύθυνση τότε η σύνδεση δεν θα πραγματοποιηθεί επιτυχώς. Ακόμη χειρότερο είναι η σύνδεση αυτή να μην κινήσει την προσοχή του χρήστη. Το αποτέλεσμα μπορεί να είναι η εικόνα που θα δοθεί στον χρήστη, ο οποίος ίσως νομίσει ότι βρίσκεται στην σελίδα που επιθυμεί ενώ ταυτόχρονα θα είναι σε σελίδα του δράστη.

Το σύστημα της ιεραρχίας των κεντρικών υπολογιστών στο διαδίκτυο είναι προκαθορισμένο. Εκείνοι διατηρούν την θέση τους μέσα στις ζώνες δραστηριότητας τους, υπακούοντας σε επίσημους κανόνες και επικοινωνούν με άλλους κεντρικούς υπολογιστές για πληροφορίες σχετικά με τις κινητές ζώνες. Στην κορυφή της ιεραρχίας αυτής υπάρχουν αντίστοιχα επικεφαλείς υπολογιστές που δίνουν την επίσημη εντολή για την γεωγραφική ζώνη στην οποία οι κεντρικοί υπολογιστές (servers) λειτουργούν. Ιστορικά, επιτυχημένες επιθέσεις σε κεντρικούς υπολογιστές, έχουν πραγματοποιηθεί κυρίως σε τοπικό επίπεδο ή επίπεδο ζώνης, δημιουργώντας σύγχυση στις επιλεγόμενες ιστοσελίδες, με στόχο την απώλεια σημαντικών δεδομένων.

iii. Επιθέσεις άρνησης εκπλήρωσης εντολών

Οι επιθέσεις αυτές αφορούν στόχους υψηλής σημασίας, κυρίως σε ότι έχει να κάνει στην πολιτική και οικονομική ζωή ενός κράτους, όπως οι Ηνωμένες Πολιτείες. Οι λεγόμενοι hacker, συχνά εξαπολύουν επιθέσεις ενάντια σε μία συστοιχία από στόχους αλλά ο κίνδυνος εντοπίζεται σε μία ενορχηστρωμένη

επίθεση σε σημαντικούς εθνικούς πόρους όπως τηλεπικοινωνίες, τραπεζικό σύστημα και ασφάλεια. Οι επιθέσεις αυτές σε συστήματα τηλεπικοινωνιών, μπορούν να αποβούν μοιραίες, ειδικότερα σε περιόδους κρίσεις. Για παράδειγμα, κατά τη διάρκεια των τρομοκρατικών επιθέσεων στην Νέα Υόρκη, το 2001, τα τηλεφωνικά δίκτυα υπερφορτώθηκαν, το διαδίκτυο και τα συστήματα επικοινωνίας που έγκεινται σε αυτό, ήταν η μόνη δίοδος πληροφόρησης για εκατομμύρια ανθρώπους. Πιθανοί λοιπόν στόχοι, μπορεί να είναι ιστοσελίδες επικοινωνίας και αποστολής ηλεκτρονικών μηνυμάτων.

Ο κύριος λόγος για την ευπάθεια των υπολογιστικών συστημάτων ενάντια σε τέτοιου είδους επιθέσεις είναι η ελλιπής παρουσία πόρων προστασίας, υπολογιστών και δικτύων, όπως προγράμματα αποθήκευσης εργασιών και προστασίας από εισβολείς. Οι επιθέσεις αυτές, κρύβουν ακόμη μία πρόκληση, η οποία έγκειται σε μία συνεχή επιτήρηση και εξερεύνηση πόρων. Οι επιθέσεις αυτές, συνήθως πραγματοποιούνται από αθώα συστήματα[185] τα οποία έχουν οικειοποιηθεί οι τρομοκράτες. Η διενέργεια αυτών των επιθέσεων αποτελεί ένα συνεχές πρόβλημα για τις υπηρεσίες που ασχολούνται με την επιβολή δικαιοσύνης, λόγω της δυσκολίας εύρεσης των υποκειμένων δράσης. Επιπλέον, οι επιθέσεις αυτές κινούνται ενάντια σε ευαίσθητα δίκτυα, σημαντικά για την εθνική ασφάλεια. Μερικές φορές, ακόμη κι αν εντοπιστούν οι αυτουργοί, η διεθνής νομολογία που αφορά την έκδοση των κατηγορουμένων για έγκλημα ίσως αντιμετωπίσει δυσκολία στην εκφορά αυτών ενώπιων της δικαιοσύνης.

iv. Επιθέσεις μέσω ηλεκτρονικών μηνυμάτων

Τα μηνύματα που αποστέλλονται μέσω του διαδικτύου, αποτελούν τα τελευταία χρόνια την πιο φημισμένη μορφή επικοινωνίας, λόγω της αυξημένης ταχύτητας και ευελιξίας αυτών. Οι ιδιότητες αυτές δεν θα μπορούσαν να περάσουν απαρατήρητες από τρομοκράτες, με εκείνους να μετατρέπουν την μορφή αυτή της επικοινωνίας σε ιδανικό μέσω επικοινωνίας μεταξύ τους.

185 Πολλές σελίδες στο διαδίκτυο επιτρέπουν την «ελεύθερη» και απλά απόκτηση των Trojan. Το χαρακτηριστικό αυτό είναι εξαιρετικά ενδιαφέρον σε ερασιτέχνες hacker, που αρέσκονται στο να πειράζουν τους φίλους τους. Αυτό που δεν γνωρίζουν είναι ότι μέσω αυτών, αποκτούν τον πλήρη έλεγχο στους κεντρικούς υπολογιστές που τους χρησιμοποιούν ενάντια σ τα θύματα τους.

Για παράδειγμα μπορεί να σταλεί ένα ηλεκτρονικό μήνυμα, το οποίο έχει υποστεί πλαστογραφία, που παρουσιάζεται ότι έχει σταλεί από έναν κεντρικό υπολογιστή, ενώ δεν είναι. Η πλαστογραφία αυτή είναι πολύ εύκολο να επιτευχθεί. Το περισσότερο γνωστό πρωτόκολλο εκπομπής ηλεκτρονικών μηνυμάτων είναι το SMPT (Simple Mail Transfer Protocol). [186]Ενα μήνυμα μπορεί να μεταδοθεί μέσω υπολογιστών που υπάγονται σε αυτό το πρωτόκολλο, το καθένα από τα οποία το φέρει πιο κοντά στο στόχο του, πριν την επιτυχή παράδοση του. Το πρωτόκολλο όμως αυτό, δεν φέρει πιστοποίηση, κι έτσι ένας κακόβουλος χρήστης ίσως συνδεθεί με έναν υπολογιστή του, και επιδώσει εντολές εκπομπής μηνυμάτων με τυχαίο αποστολέα και παραλήπτη.

Τα μηνύματα αυτά μπορούν να εντοπιστούν με μία προσεκτική παρατήρηση της επικεφαλίδας του μηνύματος, η οποία περιέχει, μεταξύ άλλων, μία λίστα από υπολογιστές (servers), που διαχειρίζονται το μήνυμα αυτό και των αριθμό επαναλήψεων της αποστολής τους. Για παράδειγμα, εάν δεν εμφανιστεί ο σωστός υπολογιστής που είναι αρμόδιος για την αποστολή του μηνύματος, τότε η νομιμότητα του μηνύματος αμφισβητείται. Σε πολλές περιπτώσεις, τα μηνύματα αυτά , μπορούν συχνά να εντοπιστούν και να απορριφθούν από φίλτρα προστασίας που έχουν τοποθετηθεί στους υπολογιστές-παραλήπτες των μηνυμάτων.

Ο αποστολέας και ο παραλήπτης ενός ηλεκτρονικού μηνύματος, μπορεί να βρίσκεται σε οποιοδήποτε μέρος του πλανήτη και να στείλει μηνύματα ανά πάσα στιγμή. Ταυτόχρονα το διαδίκτυο, και οι υπηρεσίες που προσφέρει είναι κατά πλειοψηφία, δωρεάν και το εύρος ζώνης είναι απεριόριστο. Για παράδειγμα, η τρομοκρατική οργάνωση Hamas, χρησιμοποιεί το διαδίκτυο, πολλά χρόνια για να πραγματοποιεί αποστολή αρχείων και μηνυμάτων με κωδικούς προστασίας, σε μέλξη σχετικά με τις επιθέσεις τους, περιλαμβάνοντας χάρτες, φωτογραφίες, οδηγίες και τεχνικές λεπτομέρειες των επιθέσεων τους[187].

186 Βλέπε Johnson, K (2000). Internet Email Protocols: A Developer's Guide. Addison-Wesley Professional

187 Col. (R) Sami Barak, "Between Violence and e-jihad: Middle Eastern Terror Organizations in the Information Age," in Lars Nicander and Magnus Ransdorp, Terrorism in The Information Age-New Frontiers? (Stockholm, Swedish National Defence College, 2004). Ο επικεφαλής της Χαμάς Abd-al-Rahman Zaydan καταδικάστηκε το 1995, με βάση τα δεδομένα που κατείχε στον υπολογιστή του, που περιλάμβαναν μία βάση δεδομένων που συνέδεε ομάδες δράσεων της με τους τρομοκράτες στο Ισραήλ, την Ιορδανία και τη Γερμανία.

Με την πάροδο των χρόνων, οι τρομοκράτες και οι λειτουργοί της πληροφόρησης έχουν επιστρατεύσει όλους τους τρόπους μεθόδων επικοινωνίας. Η πρόσβαση στο διαδίκτυο μπορεί να πραγματοποιηθεί με πολλαπλούς τρόπους, περιλαμβάνοντας τους πιο εμπορικές μεθόδους και μερικές συνακόλουθες:

Α. Υψηλό εύρος ζώνης, αμεσότητα συνδέσεων: από τις διαθέσιμες αποδείξεις, ένας μικρός αριθμός τρομοκρατών έχουν συνδέσεις υψηλού εύρους με άμεση σύνδεση στο Ιντερνέτ, με στόχο να συγκαλύψουν συστήματα επικοινωνιών.

Β. Τηλεφωνικές υπηρεσίες: σε ένα μεγάλο μέρος της δράσης τους οι τρομοκράτες βασίζονται σε τηλεφωνικές υπηρεσίες είτε χρησιμοποιώντας γραμμές σταθερού δικτύου είτε μέσω γραμμών κινητής τηλεφωνίας. Πρακτικά ένας τρομοκράτης μπορεί να συνδεθεί μέσω των γραμμών αυτών, και να στείλει μηνύματα από κάθε γωνιά του πλανήτη χωρίς να υπάρχει κίνδυνος εντοπισμού.

Γ. Εισβολή σε μη γνωστούς κεντρικούς υπολογιστές (servers): η εισβολή σε έναν άγνωστης προέλευσης κεντρικό υπολογιστή και μετατρέποντας τον ως φορέα αποστολής ηλεκτρονικών μηνυμάτων, αποτελεί μία πιθανή τεχνική επιθέσεων των κυβερνότρομοκρατών. Η δραστηριότητα όμως αυτή, αποτελεί μονάχα πρακτική των τρομοκρατών παρά μία μέθοδος που μπορεί να χρησιμοποιηθεί συστηματικά. Σε μεγάλο βαθμό, οι τρομοκράτες μπορούν να ειδωθούν ως ιδιοφυΐες στα υπολογιστικά συστήματα αλλά δεν σημαίνει ότι έχουν μεγάλο βαθμό εξέλιξης σε ότι έχει να κάνει στην ηλεκτρονική παρανομία.

Δ. Επιθέσεις μέσω ασύρματου διαδικτύου και άλλων δικτύων: η πρόσβαση σε ασύρματο Internet (Wi-Fi), έχει κινήσει νέες δράσεις σε ότι έχει να κάνει με την κυβερνοτρομοκρατία. Η πρόσβαση αυτή, είναι διαθέσιμη σε μία μεγάλη κλίμακα δημοσίων μερών, όπως καφετέριες, αεροδρόμια, κ.α. τέτοιες τοποθεσίες, έχουν όλα τα πλεονεκτήματα όπως μεγάλο εύρος ζώνης και εύκολη μεταφορά αρχείων. Η ανώνυμη πρόσβαση, η οποία μπορεί να είναι ωριαία ή ημερήσια είναι άμεση και μεταφέρει σε μηδενικό χρόνο τον τρομοκράτη σε κάθε ηλεκτρονική υπηρεσία.

Μεγάλη σημασία, για τους τρομοκράτες έχει η λειτουργική ασφάλεια, και μπορεί να επιτευχθεί με αρκετούς τρόπους. Πρώτον, ο πολλαπλασιασμός των λογαριασμών με ψευδώνυμα και ο τεράστιος αριθμός των κεντρικών υπολογιστών (servers), σε όλο τον κόσμο κάνει την διαφύλαξη των προσωπικών δεδομένων

εύκολη. Την τελευταία δεκαετία, έχει γίνει γνωστό ότι, πολλές τρομοκρατικές οργανώσεις έχουν συστήσει κεντρικές μονάδες υπολογιστών (servers), σε πολλές χώρες ως εμπορική κάλυψη.

v. Κρυπτογράφηση

Μία αυξανόμενη ηλεκτρονική τάση, στις μέρες μας, είναι η συνεχής χρήση της κρυπτογράφησης δεδομένων, της στενογραφίας[188] από τρομοκράτες και μέλη οργανωμένων συνδικάτων εγκλήματος. Η αυστηρή κρυπτογράφηση θεωρείται ο καλύτερος φίλος του τρομοκράτη ή του εγκληματία. Ενδεικτικά παραδείγματα είναι εκείνα του Οσάμα Μπιν Λάντεν[189], του Ramsey Yousef[190], του συνδικάτου Cali[191] και των γερμανικών συνδικάτων. Η τεχνολογική πρόοδος που εξελίσσεται σε ραγδαίους ρυθμούς προκαλεί εμπόδια στην παγκόσμια πληροφόρηση. Για δεκαετίες, εξειδικευμένοι χρήστες του διαδικτύου που ασχολείται με την αποκωδικοποίηση (code-breaking), χρησιμοποιούν τελευταίας τεχνολογίας υπολογιστές που κάθε φορά ελαχιστοποιούν τον χρόνο δράσης. Κατά ένα μεγάλο κομμάτι της σύγχρονης ιστορίας, η κρυπτογράφηση, έχει περιοριστεί σε κυβερνητικούς και στρατιωτικούς μηχανισμούς. Μπορούμε να παρατηρήσουμε δύο στάδια σχετικά με την κρυπτογράφηση, που συνάδουν με την γενικότερη ροή της τεχνολογικής εξέλιξης:

- **Την αναλογική εποχή,** όπου τα συστήματα κρυπτογράφησης είναι χρονοβόρα και με μεγάλο κόστος
- **Την ψηφιακή εποχή** όπου η ποικιλία των υπολογιστικών συστημάτων αυξάνεται και είναι ικανά να εκπληρώσουν πολύπλοκους στόχους.

---

188 Η στεγανογραφία, αφορά την απόκρυψη των δεδομένων σε ένα άλλο αντικείμενο. Μπορεί να χρησιμοποιηθεί για να κρύψει κείμενα λέξεων και αρχεία ήχου.

189 Ο εγκέφαλος της επιχείρησης πίσω από την επίθεση του Σεπτεμβρίου 2001 στην Νέα Υόρκη, φέρεται να έχει χρησιμοποιήσει στεγανογραφία για να εξασφαλίσει την αδιαφάνεια των διαύλων επικοινωνίας που χρησιμοποιούσε.

190 Ήταν πίσω από τον βομβαρδισμό του Παγκόσμιου
Εμπορικού Κέντρου το 1993 και ενός αεροσκάφους που ανήκε στην πολεμική αεροπορία των Φιλιππίνων το 1995.

191 Το συνδικάτο αυτό φέρεται να χρησιμοποιεί εξελιγμένη αποκρυπτογράφηση για να συγκαλύψει τις τηλεφωνικές της επικοινωνίες μέσω συσκευών παραποίησης φωνής και εικόνας.

Η «ψηφιακή επανάσταση» [192], φέρει νέα μέσα μεταφοράς δεδομένων, ήχου και πληροφοριών, περισσότερο ισχυρά και ταχύτερα. Η σωστή λειτουργία αυτών εξαρτάται από μία σειρά εντολών (αλγόριθμος). Οι απαιτήσεις ενός χρήστη αυξάνονται επίσης. Οι χρήστες όμως, επιζητούν ταυτόχρονα υψηλά επίπεδα ασφάλειας μέσω της κρυπτογράφησης, συμπεριλαμβανόμενων και των τρομοκρατών, κάνοντας, παράλληλα, τις προσπάθειες των υπηρεσιών ασφαλείας και επιβολής νόμου για εύρεση αυτών μία δύσκολη υπόθεση. Ο κόσμος μας δεν αποτελείται από μικρό αριθμό επικοινωνιών κρυπτογράφησης, γεγονός που ευνοεί κάθε παράνομη δράση. Οι δύο ερωτήσεις που μένουν είναι οι εξής: πρώτον, αν εν τέλει οι κρυπτογραφημένες επικοινωνίες μπορούν να εντοπιστούν, και δεύτερον αν είναι δυνατή η αποκρυπτογράφηση με τρόπο έγκαιρο και όσο το δυνατό μικρότερο κόστος. Αρχικά η εύρεση συστημάτων επικοινωνίας τέτοιου τύπου και η αποκρυπτογράφηση αυτών, μπορεί να αποβεί εξαιρετικά πολύπλοκη[193]. Από την άλλη η αναζήτηση αυτή μπορεί να διευκολυνθεί εάν εντοπίσουμε την πηγή των δεδομένων, μέσω της ατόπης απαγωγής. Για παράδειγμα, ο εντοπισμός όλων των υπολογιστών που χρησιμοποιήθηκαν από την Αλ Κάιντα στο Πακιστάν, το 2004, έκανε πιθανό το να εξετάζονται οι σκληροί δίσκοι των υπολογιστών.

Η απάντηση στο δεύτερο ερώτημα είναι ακόμη πιο προβληματική. Η ραγδαία εξαπλωμένη διαθεσιμότητα των ισχυρών ψηφιακών επεξεργαστών και οι πολυσχιδείς ακολουθίες εντολών, αποτελούν σκοπέλους για την επιτυχία αποκρυπτογράφησης. Ακόμη κι αν η πρόσβαση είναι τεχνικά εφικτή, οι πόροι που απαιτούνται σχετικά με τον χρόνο και το ανθρώπινο δυναμικό μπορεί να είναι σημαντικοί. Για τις υπηρεσίες πληροφοριών η χρήση εποχή της απεριόριστης πρόσβασης έχει έλθει στο τέλος της. Κάποιες λιγότερο γνωστές περιπτώσεις εγκληματιών που χρησιμοποιούσαν τεχνολογίες κρυπτογράφησης είναι:

- .Η υπόθεση Aum Shinri Kyo[194]

192 Virginia Heffernan (New York Times) - The Digital Revolution

193 Είναι δύσκολο να υπάρξουν σωστές εκτιμήσεις σχετικά με τον ακριβή όγκο των ψηφιακών δεδομένων στο διαδίκτυο σήμερα, αλλά γίνονται σωστά βήματα προς αυτή την κατεύθυνση.

194 Στις 20 Μαρτίου 1995, η Λατρεία της Υψηλής Αληθείας, πέρασε δηλητηριώδη αέριο sarin στον υπόγειο σιδηρόδρομο στο Τόκιο σκορπώντας τον θάνατο σε 12 άτομα και τραυμάτισε 6000. Υπήρχε η άποψη ότι το κίνημα αυτό επιθυμούσε να αναπτύξει πυρηνική ικανότητα και να πραγματοποιήσει μαζικές επιχειρήσεις αυτοκτονίας. Τα αρχεία αυτού του κινήματος, έχουν αποθηκευτεί σε

- Η υπόθεση των βολιβιανών τρομοκρατών[195]
- Η υπόθεση του James Dalton Bell[196]
- Η υπόθεση Kevin Poulson[197]

Κεφάλαιο 4 Πολιτικές προστασίας ενάντια στην τρομοκρατία του 21ου αιώνα

4.1 Εισαγωγή

Στην προσπάθεια να οργανωθούν συστήματα ασφάλειας ενάντια σε επιθέσεις μέσω του κυβερνοχώρου, είναι αναγκαίο να υπάρχει ένα στάδιο **προορατικής** δράσης και ένα στάδιο **αντιδραστικής** δράσης. Η πρώτη αναφέρεται κυρίως στην εγκατάσταση εμποδίων και μπλοκ ενάντια σε προσπάθειες τρομοκρατών για εκπλήρωση επιθέσεων ενάντια σε συστήματα υποδομών της πληροφόρησης. Αυτό μπορεί να επιτευχθεί μέσω της εφαρμογής ενός μοντέλου πολυεπίπεδης προστασίας, δηλαδή, το μοντέλο των προστατευτικών δεσμών που περιλαμβάνουν:

- **Την φυσική προστασία (**άρνηση της φυσικής πρόσβασης)

κρυπτογραφημένη μορφή. Οι αρχές στάθηκαν ικανές να αποκρυπτογραφήσουν τις πληροφορίες αφού κατόρθωσαν να βρουν τους κωδικούς σε μία δισκέττα που βρέθηκε σε φυλάκια τους. Οι στόχοι τους ήταν μαζική θανάτωση πληθυσμών σε Ιαπωνία και ΗΠΑ.

195 Το 1997, μία βολιβιανή τρομοκρατική οργάνωση δολοφόνησε 4 αξιωματικούς του αμερικανικού στρατού. Μία επιδρομή στις κρυψώνες των τρομοκρατών έφερε στο φως πληροφορίες χρησιμοποιώντας συμμετρική κρυπτογράφηση. Μία πολύωρη επίθεση ωμής βίας κατέληξε στην αποκρυπτογράφηση των πληροφοριών και έπειτα οδήγησε στην σύλληψη των τρομοκρατών

196 Ο James Bell, σκηνοθέτησε μία βεντέτα ενάντια στην Υπηρεσία Εσωτερικών εσόδων των ΗΠΑ. Οι δραστηριότητες του περιλάμβαναν τον εκφοβισμό αξιωματούχων, αποδίδοντας αμοιβές σε όσους σκότωσαν επιλεκτικά κυβερνητικούς υπάλληλους και μόλυναν με αέριο μία έκταση έξω από τα γραφεία της υπηρεσίας αυτής σε πολλές πολιτείες των ΗΠΑ. Μετά την σύλληψη του, οι ερευνητές κατόρθωσαν να αποκρυπτογραφήσουν μηνύματα που παρέλαβαν μόνο και μόνο επειδή, κοινοποίησε τον κωδικό εισόδου σε γραπτό μήνυμα.

197 Ο Kevin Poulson ήταν ένας ευφυής hacker, που εισέβαλε σε ραδιοφωνικές εκπομπές και διέρηξε γραφεία τηλεφωνικών κέντρων για να εντοπίσει στο τηλεφωνικό δίκτυο ποιος τηλεφωνικός αριθμός είναι συνδεδεμένος και να συνδέσει τις δικές του τηλεφωνικές συσκευές. Εκείνος είχε κρυπτογραφήσει όλα τα δεδομένα που απέκτησε μέσω των τηλεφωνικών υποκλοπών. Όταν συνελήφθη από τις αρμόδιες αμερικανικές αρχές, αποκαλύφθηκε ότι είχε στην κατοχή του 10.000 σελίδες με αποδείξεις.

- **Την τεχνική προστασία** (για παράδειγμα, συστήματα εντοπισμού για πρόληψη επιθέσεων)
- **Ανθρώπινοι πόροι (**ορθή επιλογή προσωπικού και παροχή επαρκών συνθηκών εργασίας)
- **Οργανωτική σφαίρα (**μέτρα και δραστηριότητες, αξιοποίηση ικανοτήτων και πόρων)
- **Η νομική σφαίρα** (νόμοι, οδηγίες, σχέδια και άλλες ρυθμίσεις που νομιμοποιούν και μια συγκεκριμένη πράξη και τα αποτελέσματα αυτής).

Σε επίπεδο **αντιδραστικής** δράσης έχουμε την εφαρμογή μέτρων που θα επιτρέψουν στα συστήματα επικοινωνιών και πληροφόρησης να επαναφέρουν τις βασικές τους λειτουργίες μετά από μία επίθεση (υψηλό επίπεδο ακεραιότητας, τήρηση του απορρήτου, και άλλα ποιοτικά χαρακτηριστικά). Μία γρήγορη και απλή απάντηση στην επίθεση ενάντια σε συστήματα επικοινωνιών και πληροφόρησης περιλαμβάνει τα εξής:

- **Προστασία της ζωής και της ασφάλειας των ατόμων**
- **Εντοπισμός της καταστροφής**
- **Εκτίμηση του μεγέθους της ζημίας**
- **Εύρεση των αιτίων της**
- **Διόρθωση των σφαλμάτων**
- **Ανανέωση της πολιτικής προστασίας**

Η **προορατική** δράση μπορεί να προσφέρει μεγαλύτερη προστασία των κρατικών υποδομών που αφορούν την επικοινωνία και την πληροφόρηση. Με την προσέγγιση αυτή, οι επιπτώσεις για τον στόχο μίας επίθεσης μπορεί να είναι λιγότερο σοβαρές και είναι ευκολότερο να εντοπιστεί ο υπεύθυνος για αυτές. Η προορατική δράση για την ασφάλεια των συστημάτων και της επικοινωνίας είναι πιο απαιτητική διαδικασία αφού προδιαθέτει συνεχείς δραστηριότητες και απαιτεί σημαντικούς οικονομικούς πόρους. Ο αριθμός των υποκειμένων για την μετρίαση και κατάπαυση των επιθέσεων είναι σε κάθε περίπτωση μεγαλύτερος.

Η υιοθέτηση εθνικών πολιτικών προστασίας για την ασφάλεια του κυβερνοχώρου θα εξαλείψει ή θα μειώσει σημαντικά την ευπάθεια σε επιθέσεις μέσω του κυβερνοχώρου και θα ελαχιστοποιήσει την ζημιά δίνοντας χρόνο για γρήγορη

επαναφορά με την παροχή κατευθυντήριων γραμμών για την ασφάλεια του κυβερνοχώρου. Επίσης, μεγάλη σημασία έχει η σύμπραξη ιδιωτικού και δημοσίου φορέα για την αντιμετωπίση οποιασδήποτε κυβερνό-απειλής. Η συνεργασία φορέων ιδιωτικής και δημόσιας σφαίρας προϋποθέτει την ύπαρξη αμοιβαίου αισθήματος συνεργασίας και ανταλλαγής πληροφοριών που αφορούν τα ευαίσθητα σημεία των συστημάτων υπολογιστών. Ο ιδιωτικός φορέας χρειάζεται να έχει πληροφόρηση από τον ιδιωτικό για τους ενδεχόμενους κινδύνους που απορρέουν από ενδεχόμενη επίθεση καθώς και στοιχεία από προηγούμενες επιθέσεις που χρειάζεται για να προστατευτεί τόσο ώστε να αποφύγει ανεπιθύμητη δημοσιότητα και διαρροή ευαίσθητων δεδομένων.

Οι διαδικασίες ερευνών και δοκιμών είναι υψίστης σημασίας για να ανακαλύψουμε τις αδυναμίες ενός συστήματος. Είναι απαραίτητο να επενδυθεί μεγαλύτερη ποσότητα οικονομικών πόρων για την ανάπτυξη λογισμικού προστασίας, λειτουργικών συστημάτων και απόκρυψη αλγορίθμων. Σε εθνικό επίπεδο, ακόμη, είναι σημαντικό, οι δημόσιοι λειτουργοί να λαμβάνουν επαρκή μέτρα προστασίας απορρήτων πληροφοριών, καθώς και να θεσπίσουν κανονιστικές διατάξεις που θα φέρουν οποιαδήποτε λαθραία επίθεση ενώπιον του νόμου.

Ωστόσο, λόγω του ότι ακόμη και η πιο σθεναρή πολιτική **προορατικής** δράσης δεν μπορεί να εξασφαλίσει απόλυτη προστασία, είναι αναγκαίο κάποιος να έχει διαθέσιμους όλους τους πόρους που είναι διαθέσιμοι για απάντηση σε ενδεχόμενη επίθεση. Τα σημεία-κλειδιά αυτών των μέτρων προστασίας αφορούν τον εύρυθμο εκμηδενισμό και την απομόνωση μίας επίθεσης και την επαναφορά του συστήματος στην προτεραία κατάσταση. Οι πολιτικές επαναφοράς στην σύγχρονη εποχή περιλαμβάνει την δημιουργία εφεδρικών εγγράφων στα οποία καταγράφονται σημαντικές πληροφορίες, καθώς και εφαρμογή λύσεων για προβλήματα προστασίας με την ομαδοποίηση αντιγράφων ασφαλείας για λογισμικό και μη. Τέλος ένα κατάλληλο σύστημα προστασίας ενάντια σε κυβερνοεπιθέσεις, σε εθνικό επίπεδο, θα βοηθήσει τις ανακριτικές και άλλες αρχές επιβολής του δικαίου να βρουν την οποιαδήποτε σύνδεση μεταξύ συγκεκριμένων ατόμων και συμβάντων, με τον συνδυασμό πολιτικών προστασίας με διαθέσιμες πληροφορίες, στο σωστό χρόνο.

4.2 Ο κυβερνητικός μηχανισμός ενάντια στη καταπολέμηση της τρομοκρατίας του κυβερνοχώρου

Το νέο αυτό είδος της τρομοκρατίας, προκύπτει σε μία εποχή όπου η τεχνολογική πρόοδος εξελίσσεται με ταχύτατους ρυθμούς. Η μαζικότητα των πληροφοριών και των δεδομένων στον κυβερνοχώρο, εμποδίζει την εύρεση της ταυτότητας των υπευθύνων κάθε επίθεσης, οδηγώντας επίσης και σε λαθεμένες εκτιμήσεις και εικασίες. Ένα μέρος του προβλήματος είναι η αδυναμία των κυβερνήσεων να αντιδράσουν καταλυτικά σε αυτό το επικίνδυνο, για τη δημόσια ασφάλεια, φαινόμενο. Η αμερικανική κυβέρνηση έχει επιχειρήσει να συστήσει μηχανισμούς ενάντια στην έξαρση της κυβερνοτρομοκρατίας και γενικότερα της ηλεκτρονικής εγκληματικότητας. Σε μία προσπάθεια να θέσει σε ετοιμότητα μηχανισμούς ασφαλείας ενάντια της κυβερνητικής τρομοκρατίας, έχει προχωρήσει στην θέσπιση Εθνικής στρατηγικής για την Ασφάλεια του Κυβερνοχώρου. Οι τρεις στόχοι της στρατηγικής αυτής είναι:

1. Να προλαμβάνει τις κυβερνο-επιθέσεις εις βάρος θεμελιακών κρατικών υποδομών της χώρας
2. Να ελαχιστοποιεί τις εθνικές αδυναμίες έναντι των επιθέσεων αυτών
3. Να ελαχιστοποιεί τη βλάβη και το χρόνο αποκατάστασης από κυβερνο-επιθέσεις όταν αυτές συμβαίνουν.

Για την αποτελεσματικότητα της στρατηγικής αυτής, είναι αναγκαία η ενεργός συμμετοχή όλων των χρηστών του διαδικτύου, ακόμη και μέσω των χρηστών και των κυβερνητικών υπηρεσιών. Εξαιτίας της πολύπλοκης φύσης και δραστηριότητας αυτών των επιθέσεων, απαιτείται μια συνδυασμένη προσπάθεια των διεθνών, ομοσπονδιακών και τοπικών δυνάμεων απονομής δικαιοσύνης, για να συγκροτηθεί ένας αποτελεσματικός παράγοντας ασφάλειας ενάντια στην κυβερνητική τρομοκρατία .

4.3 Πρωτοβουλίες των ΗΠΑ

Ένας μεγάλος αριθμός ομοσπονδιακών υπηρεσιών και τμημάτων προστασίας έχουν ως αρμοδιότητα να επιβάλλουν την ασφάλεια του κυβερνοχώρου, μέσω της εγκατάστασης μίας σειράς προγραμμάτων. Υπάρχει η άποψη ότι η ευθύνη αυτών των υπηρεσιών είναι να αναγνωρίζουν την ασφάλεια του κυβερνοχώρου ως εθνική

προτεραιότητα. Οι προσπάθειες αυτές μπορούν ακόμη να συσχετιστούν με έλλειψη συνεκτικής στρατηγικής για την κατανόηση της πραγματικής απειλής ενάντια στην κυβερνητική ασφάλεια, καθώς και την κατανομή ρόλων και ευθυνών μεταξύ των υπευθύνων[198].

Το Υπουργείο Εθνικής Προστασίας[199] (Department of Homeland Security): ειδικοί του υπουργείου Εθνικής Προστασίας ανησυχούν ότι η γενικότερη σύσταση του υπουργείου έχει καθυστερήσει σημαντικές προσπάθειες για την ασφάλεια του κυβερνοχώρου. Υπάρχει η άποψη ότι σε μία χρονική στιγμή όπου οι τρομοκράτες, έχουν αναπτύξει αυξημένη ευκολία στην χρήση υπολογιστών, κερδίζοντας ταυτόχρονα εξειδίκευση, το ομοσπονδιακό γραφείου του Υπουργείου δεν έχει αναπτύξει συγκροτημένο πρόγραμμα δράσης για την ασφάλεια του κυβερνοχώρου. Πρόσφατα, το Υπουργείο συμμετείχε και χρηματοδότησε μία προσπάθεια για να εκτιμήσει την ικανότητα των Ηνωμένων Πολιτειών, των διεθνών δρώντων και του ιδιωτικού τομέα να αναγνωρίσουν, να εμποδίσουν και να απαντήσουν σε μία μεγάλης κλίμακας κυβερνοεπίθεση.

Το αποτέλεσμα αυτής της ανάλυσης, ήταν οκτώ προτάσεις σχετικά με την βελτίωση της ετοιμότητας του αμερικανικού έθνους ενάντια σε επιθέσεις μέσω του κυβερνοχώρου και απάντησης σε αυτές. Οι προτάσεις αυτές είναι: α) η Συνεργασία μεταξύ υπηρεσιών, β) το μακροπρόθεσμο και λεπτομερειακό σχέδιο, γ) η εκτίμηση των κινδύνων και των ευθυνών, δ) το γενικό πρόγραμμα δραστηριότητας, ε) η συνεργασία μεταξύ φορέων δημοσίου και ιδιωτικού δικαίου, στ) το κοινό πλαίσιο για την προσβασιμότητα στην πληροφόρηση, ζ) Επικοινωνιακή στρατηγική και Δημόσιες Σχέσεις, και η) βελτίωση της διαδικασίας και των τεχνολογικών δομών[200].

Υπουργείο Άμυνας (Department of Defense): Το 2005, το Υπουργείο Άμυνας των ΗΠΑ, έθεσε σε εφαρμογή προγράμματα όπως το «Πρόγραμμα Προστασίας Κρατικών

198 GAO, Information Security; Emerging Cybersecurity Issues Threaten Federal Information Systems, reports 05-231, May 2005

199 Το Υπουργείο Εθνικής Προστασίας των Ηνωμένων Πολιτειών δημιουργήθηκε για να προστατέψει την αμερικανική ενδοχώρα και τον λαό. Προωθεί τον μοναδικό δίαυλο για το τεράστιο εθνικό δίκτυο των θεσμών και των οργανισμών στις προσπάθειες τους να προστατέψουν τις Ηνωμένες Πολιτείες. Είναι υπεύθυνο, επίσης και για ζητήματα που αφορούν την τρομοκρατία του κυβερνοχώρου.

200 DHS, DHS Releases Cyber Storm Public Exercise Report, September 13, 2006 [http://www.dhs.gov/xnews/releases/pr_1158341221370.shtm].

Υποδομών» (DOD) για να ρυθμίσει την συνεργασία ιδιωτικού και δημοσίου φορέα με στόχο την προστασία και την δημιουργία μηχανισμών άμυνας ενάντια σε επιθέσεις που έχουν στόχο τις κρατικές υποδομές ενός κράτους, και φυσικά τρομοκρατικές επιθέσεις μέσω του κυβερνοχώρου[201]. Η δυναμική αυτού του προγράμματος είναι ικανή τόσο για επιθετικούς όσο και αμυντικούς σκοπούς[202].

FBI (Federal Bureau Intelligence): Το πρόγραμμα προστασίας των υπολογιστικών συστημάτων παρέχει υποστήριξη και καθοδήγηση για την καταπολέμηση των επιθέσεων ενάντια σε υπολογιστικά συστήματα. Η **CIA** (Central Intelligence Agency), έχει προχωρήσει σε σχέδια δράσης για να εκτιμήσει απειλές ενάντια σε συστήματα υπολογιστών από ξένες κυβερνήσεις, εγκληματικές και τρομοκρατικές οργανώσεις και άτομα εισβολείς. Μία από αυτές τις πρακτικές είναι και ο «Σιωπηλός Ορίζοντας»[203] του 2005, σχετικά με την αντίδραση σε επιθέσεις μέσω του κυβερνοχώρου και του διαδικτύου. Όλα όμως τα προγράμματα προστασίας, έχουν χρονικό πλαίσιο πέντε χρόνια αργότερα. Ο βασικός στόχος αυτών των προγραμμάτων είναι το πώς θα δεχόταν ο κυβερνοχώρος μία επίθεση ανάλογης βαρύτητας όπως εκείνη της 11ης Σεπτεμβρίου στη Νέα Υόρκη[204].

Interpol: Σε διεθνές επίπεδο, η Ιντερπόλ έχει παίξει καταλυτικό ρόλο στην μάχη κατά της κυβερνητικής τρομοκρατίας. Λειτουργεί ως σύνδεσμος μεταξύ των δυνάμεων τήρησης της τάξης 178 των κρατών μελών που απαρτίζουν την οργάνωση. Οι χώρες μέλη της, παρέχουν πληροφορίες σχετικά με καταζητούμενους, περιουσιακά στοιχεία και πιθανούς στόχους επιθέσεων. Επιπλέον επιδοτεί ομάδες εργασίας σε πολλά εγκληματολογικά θέματα, ανάμεσα σε αυτά την ηλεκτρονική εγκληματικότητα και τρομοκρατία. Διαθέτει μία βάση δεδομένων που περιέχει πάνω από 300.000 φακέλους εγκληματιών.

Σε ότι αφορά την κυβερνητική τρομοκρατία, η Ιντερπόλ, προσπαθεί να διευκολύνει την ροή των δεδομένων μεταξύ των χωρών μελών, διενεργώντας επιχειρησιακή

201 Το Πρόγραμμα Προστασίας Κρατικών Υποδομών (DOD), αποτελείται από δικτυακούς φορείς με σκοπό να επιτηρεί και να υποστηρίζει στρατιωτικές δυνάμεις και επιχειρήσεις παγκοσμίως.

202 John Lasker. "U.S. Military's Elite Hacker Crew," Wired News, April 18, 2005.

203 Ted Bridis "'Silent Horizon' war games wrap up for the CIA". Associated Press

204 Ted Bridis, " 'Silent Horizon' war games wrap up for the CIA," USA Today, May 26, 2005.

ανάλυση πληροφοριών, επιδοτώντας την εκπαίδευση σε θέματα κυβερνητικής τρομοκρατίας και παρέχοντας υλικό κατασκοπείας σε όλα τα μέλη.

Ένα ακόμη μέτρο που λαμβάνεται σε διεθνές επίπεδο για την καταπολέμηση της κυβερνητικής τρομοκρατίας είναι η μορφοποίηση κοινών ομάδων εργασίας. Οι κοινές ομάδες εργασίας είναι πλέον σε θέση να αυξήσουν την ανταλλαγή πληροφοριών μεταξύ χωρών, να ενισχύσουν την συνεργασία στις έρευνες, να διευκολύνουν την υπογραφή συνθηκών αμοιβαίας νομικής αρωγής και έχουν κατορθώσει να υπογράψουν αρκετές άλλες σημαντικές συνθήκες κατά της τρομοκρατίας.

4.4 Πολύπλευρες προσεγγίσεις για την αντιμετώπιση κυβερνό-απειλών

Όλες οι χώρες πρέπει να εργαστούν μαζί για την δημιουργία μίας ενιαίας πολιτικής προστασίας ενάντια σε επιθέσεις που μπορεί να πλήξουν κρατικές υποδομές και κεφάλαια, εκτιμώντας παράλληλα τις κυβερνό-απειλές. Κοινές υπερεθνικές πλατφόρμες εργασίας πρέπει να επιτευχθούν. Οι πρωταρχικοί στόχοι διεθνών συμφωνιών είναι:

- Κατανόηση του τι μπορεί να οριστεί ως εχθρική πράξη, αρχικά, που μπορούν να τραβήξουν τις γραμμές μεταξύ της επίθεσης και της ενόχλησης (για παράδειγμα, την χρήση των ιστοσελίδων)
- Ορισμός των πράξεων που απαιτούνται για μία νομική απάντηση, ακόμη κι αν ένας στόχος μπορεί να εντοπιστεί πριν η νομολογία τεθεί σε ισχύ, και ακόμη σε τι συνθήκες μπορεί να γίνει αυτό.
- Την δημιουργία γλωσσικών όρων με στόχο να μελετήσουν τεχνικά προβλήματα και περιορισμούς. Συγκεκριμένα οι όροι αυτοί πρέπει να διευκολύνουν την θέσπιση πολιτικής που δεν απαιτεί σιγουριά για την ταυτότητα ή ακόμη την φύση της επίθεσης.
- Συμφωνία συνεργασίας, μέσα σε επιτρεπτά όρια για την απόδοση κατηγορίας για επιθέσεις, και κατά συνέπεια ενδεχόμενη νομική πρωτοβουλία, για να μην υπάρξει υποβιβασμός των εθνικών συμφερόντων μίας χώρας που ίσως αποτελέσει πιθανό στόχο επιθέσεων

Πολλές χώρες έχουν ήδη, δώσει πολύ εξειδικευμένους ορισμούς και νομικές διατάξεις αναφορικά με τα ηλεκτρονικά εγκλήματα. Οι διατάξεις αυτές μπορούν να βοηθήσουν στον εντοπισμό, την εκδίωξη και την καταδίκη των εμπλεκομένων. Επίσης βοηθούν στο να δοθεί μία κοινώς αποδεκτή ερμηνεία σε διεθνές επίπεδο για τα εγκλήματα αυτά, αφήνοντας ανοιχτό για πιο συγκροτημένες διεθνείς πολιτικές.

Σε ότι αφορά την θεμελίωση διεθνών συμβάσεων και συμφωνιών, είναι χρήσιμο να εξετάσουμε υπάρχοντα πρότυπα διεθνής συνεργασίας σχετικά με τις ανησυχίες για θέματα ασφάλειας. Η εγγύηση για την θέσπιση νορμών προστασίας από κάθε είδους εγκληματικές επιθέσεις, συχνά είναι πρωτοβουλία ισχυρότερων οικονομικά δυνάμεων και υιοθετούνται, στη συνέχεια από μικρότερα κράτη, επειδή τα πρώτα διαθέτουν σιγουριά για τεχνική υποστήριξη και βοήθεια. Σε τέτοια μοντέλα συνεργασίας, η πληροφόρηση γίνεται σε διεθνικό επίπεδο χωρίς να παραβιάζεται η κυριαρχία κανενός έθνους και χωρίς να καταπατείται καμία μορφή δικαίου.

4.5 Πρωτοβουλία της Ευρωπαϊκής Ένωσης

Οι προσπάθειες καταπολέμησης του αναδυόμενου είδους της διεθνούς τρομοκρατικής δραστηριότητας από την Ευρωπαϊκή Ένωση, ξεκίνησαν κατά τα τέλη του έτους 2003 και στις αρχές του 2004. Η αφορμή για την κίνηση αυτή ήταν η τρομοκρατική επίθεση στην Μαδρίτη, το Μάρτιο του 2004, η οποία έθεσε τις βάσεις για ευρύτερη εφαρμογή τη πολιτικής ασφαλείας στην Ευρωπαϊκή ένωση κατά τη διάρκεια του πολέμου ενάντια στην τρομοκρατία[205]. Η άποψη, όμως που εκφράζεται εκ μέρους της Ευρωπαϊκής ένωσης είναι αρκετά διαφοροποιημένη από εκείνη των Ηνωμένων Πολιτειών. Η τρομοκρατία δεν είναι μία απειλή που θα αντιμετωπιστεί με καθαρά στρατιωτικά μέσα, αλλά με μία σειρά μέτρων και πολιτικών

4.5.1 Κύρια θέση της ΕΕ

Ο βασικός στόχος στην μάχη ενάντια στην τρομοκρατία είναι να δημιουργήσει μία τάξη για τους κατοίκους της, για να εξασφαλιστεί η ομαλή βιωσιμότητα, μέσα σε κλίμα ειρήνης και ασφάλειας. Για την επίτευξη αυτού του σκοπού, θα πρέπει το επίπεδο ασφάλειας μέσα στην ευρωπαϊκή κοινότητα να λειτουργεί, συγχρόνως με την

205 Muslims in Europe: Promoting Integration and Countering Extremism. Congressional Research Service

προώθηση σταθερότητας και ευημερίας με άλλες χώρες. Η πολιτική αυτή υποδηλώνει την διάθεση της ευρωπαϊκής κοινότητας να δημιουργήσει ένα πνεύμα συνεργασίας, να μειώσει ή και να εξαλείψει οποιοδήποτε ενδεχόμενο τρομοκρατικών απειλών και επιθέσεων ενάντια τόσο στους πολίτες αυτής, όσο στις υπηρεσίες και στα παραγωγικά συστήματα αυτών. Επιπλέον ενδιαφέρεται για την εκκίνηση μηχανισμών (αξιοπιστία, έγκαιρη ειδοποίηση, συστήματα συναγερμού και διαδικασίες αυστηρού ελέγχου) για την πιο ευέλικτη και εύρυθμη δράση ενάντια σε δυσμενείς συνθήκες που θα προκύψουν από οποιαδήποτε επίθεση. Η δράση πρέπει να ληφθεί ενάντια στις βαθύτερες αιτίες της μη ασφάλειας και τους παράγοντες που ευνοούν την έξαρση της τρομοκρατίας. Τα βήματα που έχουν γίνει για την ενίσχυση της ασφάλειας πρέπει να γίνουν χωρίς προκατάληψη σε ατομικά δικαιώματα και ελευθερίες και με την εύνοια και την ανεκτικότητα της κοινωνίας να παραμένουν σε υψηλά επίπεδα. Ταυτόχρονα οι δράσεις της Ευρωπαϊκής Κοινότητας στοχεύουν στο να ενδυναμώσουν την διακυβέρνηση, συμπεριλαμβανόμενου και του δικαίου, και να συμβάλλουν στην ανάπτυξη υγιών θεσμικών πλαισίων της Ένωσης με τρίτες χώρες.

Συνοπτικά η τρομοκρατία:

- Εκμεταλλεύεται τα τεκταινόμενα αυτής της εποχής για περισσότερα ανοιχτά σύνορα και ενοποιημένες οικονομίες
- Υποσκάπτει την κοινωνική ανοχή
- Φέρει προκλήσεις στους κεντρικούς σκοπούς της Ευρωπαϊκής Ένωσης με την προώθηση μίας ελεύθερης διακίνησης ανθρώπων, αγαθών, υπηρεσιών και κεφαλαίων, και
- Φανερώνει την εσωτερική σύνδεση μεταξύ ενδοκρατικής και διεθνικής ασφάλειας

Η πρόκληση έγκειται στο να εκμεταλλευτούν τα πλεονεκτήματα της ελεύθερης διακίνησης, ενώ ελαχιστοποιούν τις απειλές ασφαλείας και να ελέγξουν τον πόλεμο ενάντια στην τρομοκρατία με ένα ευρύτερο πλαίσιο δράσης. Η ασφάλεια ανάμεσα στα κράτη της Ένωσης δεν μπορεί να επιτευχθεί μόνο με την δημιουργία ενός εσωτερικού σχεδίου δράσης. Η προσέγγιση της Ε.Ε. προσδοκά στο να ενδυναμώσει την εθνική ασφάλεια με ένα συνεργαζόμενο και πολύπλευρο τρόπο, και να προωθήσει σταθερότητα και ασφάλεια πέρα από τα σύνορα, αποφεύγοντας

παράλληλα την σύσταση νέων διαχωριστικών γραμμών, κυρίως με τις γείτονες χώρες.

Πολυάριθμες ευρωπαϊκές πολιτικές συνεισφέρουν στην μάχη ενάντια στην τρομοκρατία, αλλά δεν έχουν συγκροτήσει ή αναπτύξει συγκεκριμένα προγράμματα δράσης για τον περιορισμό της τρομοκρατίας. Πολλοί από τους μηχανισμούς και τις δραστηριότητες που είναι απαραίτητες για να αντιπαλέψουν την τρομοκρατία, είναι ίδιες με εκείνες που χρειάζονται για να καταπολεμήσουν άλλες μορφές οργανωμένου εγκλήματος. Δυναμική πολιτική, νόμοι και συνεργατική γραφειοκρατία βοηθούν στην μάχη ενάντια σε οργανωμένες εγκληματικές ομάδες, όπως οι τρομοκράτες. Η χρηματοδότηση των δράσεων εγκληματικών και τρομοκρατικών ομάδων μπορεί να αντιμετωπιστεί με αποδοτικά μέτρα κατά τους "ξεπλύματος μαύρου χρήματος (money laundering)". Μηχανισμοί απαραίτητοι για να προστατέψουν τις υποδομές επικοινωνίας ενάντια σε τρομοκρατικές επιθέσεις είναι ίδιοι με εκείνους που συγκροτούνται για την προστασία ενάντια σε άλλες εγκληματικές δράσεις μέσω του κυβερνοχώρου.

Ο μηχανισμός της πολιτικής προστασίας της Ευρωπαϊκής Κοινότητας αφορά την ενεργοποίηση ενάντια σε φυσικές καταστροφές αλλά και ανθρώπινες καταστροφές όπως τρομοκρατικές επιθέσεις. Αποτελεσματικός έλεγχος των συνόρων αποτελεί μία άμυνα ενάντια στην διακίνηση ναρκωτικών και παράνομων εμπορευμάτων. Η μάχη ενάντια στην τρομοκρατία αφορά μία πληθώρα παικτών και οργάνων, τόσο σε εθνικό επίπεδο όσο και σε ευρωπαϊκό. Η Ένωση προτίθεται να ενισχύσει την εσωτερική της δράση προκειμένου να ρυθμίσει επιζήμια θέματα που αφορούν την ασφάλεια.

4.5.2 Ασφάλεια συνόρων

Η ασφάλεια των συνόρων αποτελεί ένα από τα σημαντικότερα στοιχεία στην μάχη ενάντια στην τρομοκρατία, τόσο σε επίπεδο Ένωσης όσο και σε διεθνές. Ένα από τα πρωταρχικά όπλα στην προσπάθεια αυτή, είναι η δημιουργία μίας ενοποιημένης πολιτικής ασφαλείας. Η πολιτική αυτή, αποτελείται από μία μεγάλη ποικιλία μέτρων που αφορούν τον έλεγχο των συνόρων, την προστασία σημαντικών ατομικών εγγράφων, όπως ταυτότητα και φυσικά των συστημάτων

επικοινωνίας. Ο παρακάτω πίνακας, περιγράφει την προσπάθεια της ΕΕ, σχετικά με την ασφάλεια των συνόρων

Έλεγχος συνόρων	Η συγκρότηση από μέρους της ΕΕ, μίας υπηρεσίας αρμόδιας για την προστασία των εξωτερικών συνόρων, καθώς και την εφαρμογή των όρων την συνθήκης Σένγκεν με στόχο να εγκαθιδρύσουν ένα καθεστώς ελέγχου και ασφάλειας των διεθνών συνόρων. Οι προσπάθειες αυτές θα ενισχύονται και από το ευρωπαϊκό δικαιακό σύστημα προκειμένου να τηρηθεί οποιαδήποτε νομολογία και να παταχθεί κάθε εγκληματική ή τρομοκρατική δράση.
Ασφάλεια εγγράφων	Η κοινότητα έχει προτείνει μία προσέγγιση που αφορά την ασφάλεια σημαντικών εγγράφων του κάθε ατόμου (ταυτότητα, διαβατήριο). Η χρήση των **βιομετρικών ελέγχων*** συστήνει την ασφάλεια εγγραφών διακίνησης με την εναρμόνιση και την δημιουργία νομικών πολιτικών.
Συστήματα πληροφόρησης	Η κοινότητα προτείνει την δημιουργία διαύλων επικοινωνίας με στόχο την ενδυνάμωση της εθνικής ασφάλειας, καθώς και την καταπολέμηση τρομοκρατικών και άλλων εγκληματικών δράσεων. Οι δράστες πιθανόν να χρησιμοποιούν τα προσωπικά αρχεία των πολιτών για να δημιουργήσουν λίστες με πιθανούς στόχους επιθέσεων.

4.5.3 Νομικά πλαίσια

Ο στόχος της ΕΕ, είναι να θέσει σε εφαρμογή, για πρώτη φορά νομικά πλαίσια που θα δίνουν στα κράτη μέλη την δυνατότητα να δημιουργήσουν μία κοινή τάξη δικαίου. Η προσπάθεια αυτή, αφορά την εγκαθίδρυση νομικών νορμών και την αποδοχή κοινών οδών άσκησης του δικαίου, μέσα από συνεργασία των αρχών του κάθε κράτους.

Η χρονολογία του 2002, αποτελεί σημαντική χρονική στιγμή για την Ένωση. Υπήρξε μία σειρά αποφάσεων σχετικά με την καταπολέμηση της τρομοκρατίας, με κεντρικά στοιχεία την διατήρηση των δικαιωμάτων της ασφάλειας, της ελευθερίας και της δικαιοσύνης στη μάχη ενάντια στην τρομοκρατία. Το **Ευρωπαϊκό Σύμφωνο Σύλληψης** των τρομοκρατών, υποχρεώνει εκείνους να συλλαμβάνονται από τις αρχές του εκάστοτε κράτους, και να παραδίδονται άμεσα ενώπιον της δικαιοσύνης. Η ευρωπαϊκή Ένωση, έχει αναπτύξει ταυτόχρονα με την θέσπιση πολιτικών προστασίας, έντονη δράση στην δημιουργία οργανώσεων για την καταπολέμηση της

τρομοκρατίας. Οι δύο κυριότερες οργανώσεις είναι η Europol και η Eurojust, οι οποίες δραστηριοποιούνται στην επιβολή νόμου, την επικοινωνιακή εξάπλωση και την δημιουργία νέων οργάνων, λειτουργώντας υπό το αίσθημα της συνεργασίας.

Europol[206]	Παίζει κεντρικό ρόλο στην μάχη ενάντια στην τρομοκρατία, μετά τις επιθέσεις στις ΗΠΑ το Σεπτέμβρη του 2001. Η Μονάδα Καταπολέμησης του Εγκλήματος της Europol έχει λάβει ιδιαίτερη δράση για την καταπολέμηση της τρομοκρατίας, περιλαμβάνοντας την περισυλλογή και την ανάλυση πληροφοριών για την πρόληψη ενάντια σε τρομοκρατικές απειλές ενάντια κρατών μελών της Ένωσης.
Eurojust[207]	Ιδρύθηκε ως ανεξάρτητο σώμα από νομικά πρόσωπα κρατών-μελών της Ένωσης, που στοχεύει στην δημιουργία σχέσεων συνεργασίας μεταξύ ερευνητών και νομικών για να αντιμετωπίσουν σοβαρά εγκλήματα διεθνούς φύσεως, όπως τρομοκρατία. Τα κράτη μέλη υποχρεούνται να δημιουργήσουν μία εθνική απάντηση για θέματα τρομοκρατίας προκειμένου να ενισχύσουν την προσπάθεια καταπολέμησης της.

4.5.4 Τρομοκρατία και οικονομία

Οι τρομοκράτες χρειάζονται μια σειρά από οικονομικούς πόρους, προκειμένου να προχωρήσουν στην δράση τους. Ένας κεντρικός παράγοντας στην λειτουργικότητα των επιθέσεων τους είναι η ικανότητα διακίνησης χρήματος μέσα στο παγκόσμιο οικονομικό σύστημα. Λαμβάνοντας υπόψη αυτό, οι στόχοι της Ευρωπαϊκής Ένωσης, είναι να καταστήσουν αδύνατη την απόκτηση και την χρήση οικονομικών πόρων για τις δραστηριότητες τους. Συγκεκριμένα, έχουν ληφθεί μία σειρά από μέτρα νομικής και λειτουργικής φύσεως, για την καταπολέμηση της προσπάθειας χρηματοδότησης της τρομοκρατίας. Η Ευρωπαϊκή Ένωση έχει κινητοποιηθεί με γοργούς ρυθμούς, συνεργαζόμενο με το Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών, δίνοντας εντολή να «παγώσουν» κεφάλαια και εισοδήματα ανθρώπων και οργανώσεων που είναι ύποπτοι για κάθε είδος τρομοκρατικής δράσης. Για την καλύτερη οργάνωση των προσπαθειών αυτών της Ένωσης, η Ευρωπαϊκή Επιτροπή μαζί με τον ευρωπαϊκό

206Βλέπε http://books.google.gr/books?id=cVDR3TLF2aEC&pg=PA197&lpg=PA197&dq=Europol+vs+Terrorism&source=bl&ots=gYnTCzUwzh&sig=xelRKNNGl06Y8OeRXyYDDu0Xovo&hl=el&ei=R86yTraKJayP4gTF45zoAw&sa=X&oi=book_result&ct=result&resnum=4&ved=0CDAQ6AEwAzgK

207 Βλέπε http://europa.eu/agencies/pol_agencies/eurojust/index_el.htm

τραπεζικό τομέα έχει δημιουργήσει μία ηλεκτρονική βάση δεδομένων με στοιχεία ατόμων που αποτελούν πιθανούς στόχους κάθε είδους τρομοκρατικής δράσης. Περαιτέρω μέτρα για την παρεμπόδιση κάθε προσπάθειας χρηματοδότησης τρομοκρατικών επιθέσεων, καθώς και την διαφοροποίηση της τρομοκρατίας με οποιαδήποτε εγκληματική δράση, θα μπορούσαν να είναι:

- Εποπτεία λογαριασμών ατόμων που ανήκουν σε μη κυβερνητικούς οργανισμούς, οι οποίοι έχουν φιλανθρωπική δράση, με σκοπό να αποκαλύψουν οποιαδήποτε συναλλαγή μεταξύ τρομοκρατών που χρησιμοποιούν το κάλυμμα της ανθρωπιστικής δράσης.
- Μέτρα για την παρακολούθηση οποιοδήποτε κινήσεων σε τραπεζικούς λογαριασμούς. Οι κινήσεις αυτές, μπορούν να αφορούν είτε κρατήσεις είτε προσθήκη τόκων. Ο στόχος για την παρακολούθηση αυτών των κινήσεων, είναι να πληροφορεί τις αρμόδιες αρχές κάθε κράτους-μέλους της ΕΕ για να αποφευχθεί οποιαδήποτε προσπάθεια χρηματοδότησης ή ξεπλύματος μαύρου χρήματος.

Η χρηματοδότηση των τρομοκρατικών πράξεων, ωστόσο, δεν μπορεί να εξεταστεί μεμονωμένα. Υπάρχει αδιάσειστη απόδειξη για την ύπαρξη άρρηκτων δεσμών μεταξύ της τρομοκρατίας και του οργανωμένου εγκλήματος. Είναι απαραίτητο να κατανοηθούν αυτοί οι δεσμοί για να δημιουργηθούν κατάλληλες πολιτικές ασφαλείας.

4.5.5 Προστασία των Κρατικών Υποδομών

Με την ραγδαία ανάπτυξη ενός αυξανόμενου δικτυακού κόσμου , η προστασία των κρατικών υποδομών που αφορούν την πληροφόρηση είναι ένα καίριο ζήτημα, ακόμη περισσότερο στις μέρες μας. Όπως αναφέρθηκε παραπάνω, Η επίδραση πιθανών τρομοκρατικών επιθέσεων στις υποδομές αυτές, μπορεί να έχει καταστροφικά αποτελέσματα σε όλους τους οικονομικούς τομείς, όπως η ενέργεια, οι τηλεπικοινωνίες, οι μεταφορές και τα συστήματα ηλεκτροδότησης και υδροδότησης. Η Ευρωπαϊκή Ένωση έχει αναπτύξει μία πολυμερή προσέγγιση, ενισχύοντας τα νομικά πλαίσια, αναπτύσσοντας συνεχώς πολιτικές ενάντια στο κυβερνό-έγκλημα και βελτιώνοντας τους μηχανισμούς πρόληψης επιθέσεων.

Οι αγορές του ηλεκτρισμού και της διακίνησης πετρελαίου και φυσικού αερίου είναι εξαιρετικά ευάλωτες στον ανταγωνισμό με τον ίδιο τρόπο όπου είναι οι υπηρεσίες επικοινωνίας. Η ενέργεια θεωρείται ένα εξαιρετικά ποιοτικό αγαθό, του οποίου η ασφάλεια παροχής, πρέπει να αποτελεί πολιτική προτεραιότητα. Πυρηνικές εγκαταστάσεις είναι, ακόμη ένα παράδειγμα υποδομής που απαιτεί υψηλό επίπεδο ασφάλειας.

Διαμέσου δικτύων που πιθανόν να ορίζονται από ιδιωτικό φορέα, τα κράτη-μέλη της Ένωσης, καθιστούν βιώσιμη την επιτήρηση της οικονομικής συμπεριφοράς του. Στις μέρες μας η ασφάλεια και η προστασία των δικτύων παροχής ενέργειας, συνοδεύεται και από ισχύοντες εθνικούς κανόνες και διατάξεις. Εξαιτίας της αυξανόμενης αλληλεξάρτησης των αγορών ενέργειας κάθε κράτους μέλους, η νομική προσφορά της Επιτροπής για την ασφάλεια των υποδομών θα πρέπει να ενισχυθεί ουσιαστικά.

4.5.6. Δράση ΕΕ σε επίπεδο Διεθνών Σχέσεων

Η Ευρωπαϊκή Επιτροπή θεωρεί ότι ο πρωταρχικός στόχος της Ένωσης σε εξωτερικά πλαίσια για τη μάχη ενάντια της τρομοκρατίας και της τρομοκρατίας του κυβερνοχώρου, κατ' επέκταση, είναι η προώθηση ενός πλαισίου εφαρμογής διεθνών νορμών και νομικών διατάξεων. Αυτό μπορεί να καταστεί δυνατό, μέσω πολιτικού διαλόγου και τεχνικής υποστήριξης, καθώς και συνεργασίας περιφερειακών και διεθνών οργανισμών. Αυτό προαπαιτεί την χρήση κάθε πολιτικής εξωτερικής δράσης σε ένα ολιστικό και συνεχόμενο τρόπο, ταυτόχρονα με την πλήρη άλλων εξωτερικών πολιτικών σκοπών.

Η μάχη ενάντια στην τρομοκρατία συνεχίζει να είναι ένα σημαντικό στοιχείο στις **σχέσεις της Ευρωπαϊκής Ένωσης με τρίτες χώρες.** Η Ευρωπαϊκή Επιτροπή διαθέτει ένα αρκετά αναλυτικό αρχείο στην απόδοση τεχνικής προστασίας (π.χ. εθιμικό δίκαιο και πρακτικές, μεταναστευτικοί νόμοι και πολιτικές, οικονομικό δίκαιο, κ.α.). Μέσω αυτού, η Επιτροπή έχει ορίσει έναν αριθμό συγκεκριμένων προγραμμάτων κατάπαυσης των τρομοκρατικών δράσεων , αρχικά στην Ινδονησία και στις Φιλιππίνες, όπου έχουν ξεκινήσει προγράμματα για την καταπολέμηση χρηματοδότησης της τρομοκρατίας και συνοριακού ελέγχου.

Η συνεργασία με την σύμπραξη συμφωνιών της ΕΕ με τρίτες χώρες προωθούν πολύτιμα πλαίσια για στρατηγικές που μπορούν να βοηθήσουν στην εύρεση των

βαθύτερων ριζών του προβλήματος της ανασφάλειας και φυσικά της τρομοκρατίας. Το πρόγραμμα συνεργασίας **Cotonu**[208]**,** αποτελεί φωτεινό παράδειγμα για την σύλληψη ενός πλαισίου το οποίο πέρα από την ενίσχυση της ασφάλειας και της σταθερότητας, βοηθά επιπλέον στην μείωση της φτώχειας, του σεβασμού των ανθρωπίνων δικαιωμάτων και την οικοδόμηση ειρηνικών σχέσεων με τρίτες χώρες δίνοντας ευκαιρίες πολιτικού διαλόγου.

Η ΕΕ θεωρεί αναγκαία την ουσιαστική επαφή με τρίτες χώρες, ειδικά με εκείνες που δίνουν σημαντικό αγώνα εναντίον τρομοκρατικών επιθέσεων. Η ανάγκη βοήθειας σε τρίτες χώρες για περιορισμό τρομοκρατικών τάσεων παραμένει μέγιστη. Είναι επίσης, αναγκαία και η τεχνική προστασία από μέρους της Ένωσης προκειμένου να καταπολεμηθεί οποιαδήποτε σύγκρουση από εθνοτικές ομάδες και να μην υπάρξει κίνδυνος δημιουργίας αποτυχημένων πολιτειών (failed states[209]). Η όλη προσπάθεια θα γίνει πράξη μέσω διμερών διαλόγων με τρίτες χώρες, οι οποίοι θα περιλαμβάνουν θέματα σχετικά με ρατσισμό, ξενοφοβία και άλλα προβλήματα εθνικού περιεχομένου που θα μπορούσαν να δημιουργήσουν τριβές στις σχέσεις αυτών με την ΕΕ.

4.5.7. Προστασία ατομικών δικαιωμάτων και ελευθεριών για την καταπολέμηση του ρατσισμού

Η Ευρωπαϊκή Ένωση ιδρύθηκε υπό τις αρχές της ελευθερίας, της δημοκρατίας, του σεβασμού των θεμελιωδών δικαιωμάτων και ελευθεριών και του δικαίου. Το δικαίωμα στην ισότητα ενώπιον του νόμου και η προστασία όλων των ανθρώπων από οποιονδήποτε διαχωρισμό, μαζί με τον σεβασμό και την προώθηση των δικαιωμάτων των μειονοτικών πληθυσμών, είναι απαραίτητη για την ομαλή λειτουργία των δημοκρατικών κοινωνιών. Θα πρέπει λοιπόν, να καταστήσουμε βέβαιο ότι ευπαθείς μειονοτικές ομάδες μέσα στην Ένωση θα τυχαίνουν προστασίας και σεβασμού των ανθρωπίνων δικαιωμάτων τους, μέσα στα πλαίσια εφαρμογής πολιτικών για την καταπολέμηση της τρομοκρατίας.

208 Βλέπε http://www.acp-eu-trade.org/index.php?loc=faq/ACP-Secretariat-FAQ.php

209 Δεν υπάρχει καθολικά αποδεκτός ορισμός σχετικά με το ζήτημα των αποτυχημένων πολιτειών (failed states. Μία άποψη που επικρατεί είναι ότι οι αποτυχημένες πολιτείες είναι ο όρος που χρησιμοποιείται για κράτη που δεν διαθέτουν τους απαραίτητους μηχανισμούς ανάπτυξης. Πηγή: http://www.gsdrc.org/go/fragile-states/κεφ.-1--understanding-fragile-states/definitions-and-typologies-of-fragile-states

Μετά τις επιθέσεις τις 11ης Σεπτεμβρίου 2001, υπήρξε έντονη δραστηριότητα από μέρους της Ένωσης για να εξετάσουν την δραστηριότητα των ισλαμικών κοινοτήτων και άλλων μειονοτικών ομάδων και τον λόγο για τον οποίο αντιμετωπίζουν τέτοια εχθρότητα. Αναφορές λοιπόν επιτροπών της Ένωσης[210] σχετικά με την ξενοφοβία ενάντια σε ισλαμικές ομάδες, αποτέλεσαν σημαντικό στοιχείο στην δημιουργία μηχανισμών καταπολέμησης τρομοκρατικών δράσεων, κατανοώντας την σημασία των ανθρωπίνων δικαιωμάτων, της κοινωνικής συνοχής και της δυνατότητας πρόσβασης σε κοινοτικές υπηρεσίες. Τέλος, έχει γίνει μία προσπάθεια της Ένωσης για να αποφευχθεί οποιαδήποτε προκατάληψη που θα οδηγήσει σε φλεγόμενα μέτωπα με τις μειονοτικές ομάδες κάθε εθνικότητας.

Επίλογος

Η τρομοκρατία του κυβερνοχώρου σήμερα και αύριο

Η Ιστορία δείχνει ότι οι πολιτικές και στρατιωτικές συγκρούσεις συνοδεύονται, ολοένα και περισσότερο από επιθέσεις μέσω του κυβερνοχώρου. Οι επιθέσεις αυτές, κλιμακώνονται σε ένταση και επίπεδο συνεργασίας. Οι δημιουργοί πολιτικών προστασίας πρέπει να αναγνωρίσουν την ανάγκη για συνεργασία και συνοχή ανάμεσα σε μία ευρεία ποικιλία δρώντων, όπως άλλα κράτη και ιδιωτικούς φορείς.

Η ανάγκη για ταχεία αντίδραση θα συνεχίσει να υπερισχύει την ικανότητα για εντοπισμό και τιμωρία. Όλες οι κυβερνήσεις πρέπει να εργαστούν για μία ενιαία πολιτική απάντησης για την πρόληψη επιθέσεων σε κάθε είδους υποδομές. Οι κυβερνήσεις, ακόμη, δεν θα είναι ικανές να επιτύχουν αυτό τον στόχο χωρίς τον ιδιωτικό τομέα. Είναι απαραίτητο για δημόσιους και ιδιωτικούς φορείς να συνεχίσουν την βελτίωση και την διεύρυνση των μηχανισμών ανταλλαγής πληροφοριών, συνεργασίας και των προαπαιτούμενων μέσων για ενισχυμένη προστασία εσωτερικά και εξωτερικά των κυβερνητικών μηχανισμών.

Μόνο με τον συνδυασμό των δυναμικών τόσο του ιδιωτικού, όσο και του δημόσιου φορέα σε θέματα όπως η έγκαιρη προειδοποίηση, η προώθηση των καλύτερων πρακτικών και η συμφωνία σχετικά με πολιτικές προστασίας για

210 Eurobarometer 47.1 “Racism and Xenophobia in Europe”

πληροφορίες, θα καταστεί βέβαιη η αλλαγή στην τάση για την ασφάλεια των μηχανισμών του κυβερνοχώρου[211].

Τα τρομακτικά γεγονότα της 11ης Σεπτεμβρίου έχουν πραγματικά αλλάξει τον κόσμο όπως τον γνωρίζουμε. Η τρομοκρατία επιτέθηκε ενάντια στην ελευθερία εκείνη την ημέρα. Και, όσο προχωρούμε, πρέπει να θυμηθούμε ότι το Διαδίκτυο και οι τεχνολογίες πληροφόρησης είναι εργαλεία ελευθερίας τον 21ο αιώνα. Θα πρέπει να γίνουν προσεκτικές κινήσεις για την προστασία αυτών, καθώς και της ελευθερίας που αντιπροσωπεύουν. Η υπεράσπιση του δικαιώματος της ελευθερίας δεν απαιτεί τίποτα λιγότερο.

Τα τελευταία εννέα χρόνια, η απειλή του αναδυόμενου αυτού είδους είναι τεράστια, καθώς επίσημα δεν έχει καταγραφεί οποιοδήποτε συμβάν σε σχέση με την τρομοκρατία του κυβερνοχώρου. Το αμερικανικό ηλεκτρονικό δίκτυο άμυνας και ασφάλειας έχει απομονωθεί σε σχέση με τον υπόλοιπο κυβερνοχώρο. Οι υπολογιστές που δεν ανήκουν σε κρατικό δρώντα αλλά σε ιδιώτη, είναι περισσότερο ευπαθείς στις επιθέσεις μέσω του κυβερνοχώρου. Οι περισσότερες από αυτές δεν έχουν καμία πολιτική σκοπιμότητα, οι οποίες όμως δίνουν το έρεισμα σε τρομοκρατικές οργανώσεις.

Το ζήτημα λοιπόν είναι ότι οι επιθέσεις αυτές, προξενούν μεγάλη σύγχυση σε κρατικούς δρώντες, λόγω του ότι: πρώτον, σύμφωνα με την Denning[212], οι τρομοκρατικές και άλλες επιθέσεις μέσω δικτύων και υπολογιστών είναι πολύ δημοφιλής και ραγδαία εξελισσόμενοι, συμβαδίζοντας με την ίδια την τεχνολογική εξέλιξη. Η χρήση των υπολογιστών στις μέρες μας, κυρίως από νέους, κάνει την σημασία και το περιεχόμενο αυτών των επιθέσεων πιο ελκυστικό. Δεύτερον, η μαζική επίδραση των μέσων ενημέρωσης, αποτυγχάνει να ορίσει τις πτυχές είτε της κοινής επίθεσης είτε της τρομοκρατικής πράξης του κυβερνοχώρου, δημιουργώντας άγνοια κινδύνου κυρίως στην μερίδα των νέων και μυθοπλασίες σχετικά με την πραγματική φύση του σε άλλες κατηγορίες του κοινού. Εάν, για παράδειγμα, ένας νέος εισβάλλει

211 Cyber-Security: Private-Sector Efforts Addressing Cyber Threats, Testimony of Dave McCurdy, President, Electronic Industries Alliance, Executive Director, Internet Security Alliance; Before the Subcommittee on Commerce, Trade, and Consumer Protection House Energy and Commerce Committee

212 Dorothy Denning, "A View of Cyberterrorism Five Years Later," 2007, σελ.. 10

στα αρχεία του Αμερικανικού Πενταγώνου, τότε η ανασφάλεια σχετικά με το τι μπορεί να κάνει μία τρομοκρατική οργάνωση, που είναι εκπαιδευμένη με μεγαλύτερο οικονομικό επίπεδο, είναι τεράστια.

Τρίτον, η άγνοια του κινδύνου, όπως αναφέρθηκε, μπορεί να γίνει όργανο οικονομικής εκμετάλλευσης από ιδιωτικές εταιρείες, οι οποίες θα επιχειρήσουν να δημιουργήσουν ένα δίκτυο προστασίας, για να δημιουργήσουν εμπορικά μονοπώλια, αλλά και να δώσουν την εντύπωση ότι η απειλή σε κρατικό επίπεδο είναι ασύμμετρη και ότι εκείνοι αποτελούν καινοτόμους αρωγούς για την ασφάλεια του κράτους. Επιπλέον, η πολιτική εξουσία, σκόπιμα μπορεί να χρησιμοποιήσει την ενδεχόμενη αυτή απειλή, προκειμένου να προβάλλουν τα ζητήματα της δικής τους ατζέντας και να θελήσουν να κερδίσουν την εμπιστοσύνη του κοινού ότι εκείνοι θα καταπολεμήσουν την απειλή αυτή, για να κερδίσουν την εύνοια του λαού σε ενδεχόμενες εκλογικές αναμετρήσεις.

Ο Vernon[213] υποστηρίζει, ότι η Αλ Κάιντα έχει δείξει ένα ιδιαίτερο ενδιαφέρον για την τεχνολογία, παραπέμποντας στα λεγόμενα του Οσάμα Μπιν Λάντεν, μετά τις επιθέσεις της 11ης Σεπτεμβρίου 2001. Ο ίδιος, είχε δηλώσει ότι μία μεγάλη ομάδα επιστημόνων είναι έτοιμη να διαθέσει τις γνώσεις της για την οργάνωση, περιλαμβάνοντας και τους υπολογιστές. Αυτό είναι ένα παράδειγμα σχετικά με το κατά πόσο, μία υψηλού επιπέδου τρομοκρατική οργάνωση χρησιμοποιεί την τεχνοκρατική εξέλιξη προκειμένου να αυξήσει την ευελιξία, την αποτελεσματικότητα και το εύρος των επιθέσεων της. Οι νέες γενιές τρομοκρατών, μεγαλώνουν σε ένα κόσμο, στον οποίο υπάρχει μία ψηφιακή ομπρέλα, επιτρέποντας τους να χρησιμοποιούν τον υπολογιστή ως μέσο επίθεσης με μεγαλύτερη ταχύτητα και ελεύθερη πρόσβαση. Για παράδειγμα, μέλη από μία τρομοκρατική οργάνωση, μπορούν να τοποθετήσουν εκρηκτικό μηχανισμό σε ένα τρένο και ταυτόχρονα να χρησιμοποιήσουν τον κυβερνοχώρο ως μεγεθυντικό φακό της επίθεσης του, προξενώντας αναταραχή σε παγκόσμιο επίπεδο, μέσα σε μόλις λίγα λεπτά.

Συνοψίζοντας, είναι αναγκαίο να υπογραμμίσουμε ότι η τρομοκρατία εξελίσσεται, όπως και η δραστηριότητα του ανθρώπου με αλματώδη βήματα. Η τρομοκρατική ύπερεξαπλωση, διαμέσου του κυβερνοχώρου και των τμημάτων που τον απαρτίζουν,

213 Βλέπε Kelley, Tina (14 February 2002), "Vernon Walters, Ex-Envoy And Deputy C.I.A. Chief, 85", *New York Times*

δημιουργεί μία σειρά από αλυσιδωτές αντιδράσεις σε κοινωνικό, πολιτικό και οικονομικό πλαίσιο. Η ανασφάλεια για το τι μπορεί να ξημερώσει η επόμενη μέρα στην υφήλιο, εντείνεται σε βαθμό ψυχολογικής φθοράς.

Η χωρητικότητα του ανθρώπινου μυαλού είναι ανυπέρβλητη. Είναι αδύνατο να εξαλειφθεί το κυβερνόέγκλημα από τον κυβερνοχώρο ολοκληρωτικά. Είναι αρκετά δυνατό όμως να υπάρξει επαρκής έλεγχος. Η ιστορία είναι ο μάρτυρας για το ότι δεν υπάρχει νομική πρωτοβουλία που θα επιτύχει την ολοκληρωτική απαλλαγή του κόσμου από το έγκλημα. Το μόνο πιθανό δείγμα είναι η ενημέρωση του κόσμου για τα δικαιώματα και τις υποχρεώσεις τους. Αναμφίβολα η απειλή του κυβερνοεγκλήματος είναι τεράστια, το μόνο που μπορούμε να κάνουμε είναι να θέσουμε περιορισμούς έτσι ώστε να μετριαστεί η εξάπλωση του.

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα 1: Τυπολογία τρομοκρατίας

Α. Τυπολογία

Η παραδοσιακή τρομοκρατία είναι αρκετά σημαντική για να κατανοήσουμε την δυναμική της κυβερνότρομοκρατίας που αποτελεί το αντικείμενο της εργασίας μας. Οι τακτικές και τεχνικές του πολέμου της πληροφόρησης, σε ότι έχει να κάνει με την κυβερνότρομοκρατία και την αντιτρομοκρατική δραστηριότητα συνοψίζονται στην παρακάτω τυπολογία για να καταδείξει το πόσο η τρομοκρατία και η απάντηση σε αυτή μπορεί να αλλάξει στο μέλλον.

1. **Από την παραδοσιακή τρομοκρατία στον Κυβερνό-τρόμο**

Παραδοσιακή τρομοκρατία	**Τεχνο-τρομοκρατία**	**Κυβερνοτρομοκρατία**
Οι στόχοι υπάρχουν σε «πραγματικό» τόπο • Αεροπορικές γραμμές • Κτίρια • Υψηλής δημοτικότητας	Οι στόχοι υπάρχουν σε «πραγματική» απόσταση μεταξύ του κυβερνοχώρου και του πραγματικού: • Ηλεκτρικά δίκτυα	Οι στόχοι υπάρχουν αποκλειστικά στον κυβερνοχώρο με επιπτώσεις φυσικού χώρου: • Τηλεπικοινωνίες

άτομα • Χαμηλής δημοτικότητας άτομα	• Συστήματα υπολογιστών • Τηλεπικοινωνίες	• Συστήματα υπολογιστών • Συστήματα ελέγχου
Δημιουργία πραγματικής απειλής	Δημιουργία πραγματικής και εικονικής απειλής	Δημιουργία πραγματικής και εικονικής απειλής
Όπλα: • Εκρηκτικά • Μαζικής καταστροφής	Όπλα: • Εκρηκτικά Μαζικής καταστροφής	Όπλα: • Κακόβουλο λογισμικό • Όπλα διαχείρισης και καταστροφής δεδομένων
Τεχνικές: • Βομβαρδισμοί • Απαγωγές • Δολοφονίες	Τεχνικές: • Βομβαρδισμοί • Φυσική καταστροφή μερών των συστημάτων	Τεχνικές: • «εικονική» καταστροφή των στόχων στον κυβερνοχώρο • Απενεργοποίηση των λογισμικών του συστήματος • Υπέρβαση συστημάτων ελέγχου
Μέγεθος ομάδων: • Μεγάλο: πολλαπλές επιπτώσεις • Μικρό: λίγες επιπτώσεις	Μέγεθος ομάδων: • Μεγάλο: πολλαπλές επιπτώσεις • Μικρό: λίγες επιπτώσεις	Μέγεθος ομάδων: • Μεγάλο: πολλαπλές επιπτώσεις • Μικρό: μεγάλες επιπτώσεις
Μεγάλη ποσότητα απαιτούμενου χρήματος για μεγάλες επιχειρήσεις	Αρκετή ποσότητα απαιτούμενου χρήματος για μεγάλες επιχειρήσεις	Μικρή ποσότητα απαιτούμενου χρήματος για μεγάλες επιχειρήσεις
Υψηλός φυσικός κίνδυνος για τρομοκράτες	Μερικός φυσικός κίνδυνος για τρομοκράτες	Χαμηλός φυσικός κίνδυνος για τρομοκράτες
Σημασία της κρατικής βοήθειας: • Με χρήματα • Με εξοπλισμό • Με εκπαίδευση	Σημασία της κρατικής βοήθειας: • Με χρήματα • Με εξοπλισμό • Με εκπαίδευση	Σημασία της κρατικής βοήθειας: • Με πληροφόρηση

• Με πληροφόρηση • Με συστήματα μεταφορών	• Με πληροφόρηση • Με συστήματα μεταφορών	
Ο ρόλος των μέσων: κρίσιμος	Ο ρόλος των μέσων: κρίσιμος	Ο ρόλος των μέσων: μέτριος
Η νομολογία είναι ξεκάθαρη	Η νομολογία είναι ξεκάθαρη	Η νομολογία είναι αμφισβητήσιμη
Οι απαιτήσεις πληροφόρησης είναι χαμηλές	Οι απαιτήσεις πληροφόρησης είναι μέτριες	Οι απαιτήσεις πληροφόρησης είναι υψηλές
Οι επικοινωνίες είναι ζωτικής σημασίας για την επιτυχία	Οι επικοινωνίες είναι ζωτικής σημασίας για την επιτυχία	Οι επικοινωνίες είναι ζωτικής σημασίας για την επιτυχία
Η ενδεχόμενη διατάραξη είναι μέτρια: • Πολύπλοκες οι συντονισμένες επιχειρήσεις	Η ενδεχόμενη διατάραξη είναι μεγάλη: • Δύσκολες οι συντονισμένες επιχειρήσεις	Η ενδεχόμενη διατάραξη είναι αρκετά χαμηλή: • Σημαντικά εύκολες οι συντονισμένες επιχειρήσεις
Είδη τρομοκρατικών ομάδων: • Εθνικιστικές-Αυτονομιστικές-Αλυτρωτικές • Μονοθεματικές • Ιδεολογικές • Κυβερνητικές • Θρησκευτικές	Είδη τρομοκρατικών ομάδων: • Εθνικιστικές-Αυτονομιστικές-Αλυτρωτικές • Μονοθεματικές • Ιδεολογικές • Κυβερνητικές • Θρησκευτικές	Είδη τρομοκρατικών ομάδων: • Εθνικιστικές-Αυτονομιστικές-Αλυτρωτικές • Μονοθεματικές • Ιδεολογικές • Κυβερνητικές • Θρησκευτικές
Η φυσική παρουσία απαραίτητη για μία επιτυχή επιχείρηση	Η φυσική παρουσία απαραίτητη για μία επιτυχή επιχείρηση	Η φυσική παρουσία ΔΕΝ απαραίτητη για μία επιτυχή επιχείρηση
Η επίθεση έχει συγκεκριμένα αποτελέσματα	Η επίθεση έχει απρόβλεπτα αποτελέσματα	Η επίθεση έχει και συνήθη και μη προβλεπόμενα αποτελέσματα

2. **Η τεχνοτρομοκρατία είναι το ενδιάμεσο στάδιο μεταξύ τρομοκρατίας και τρομοκρατίας του κυβερνοχώρου. Ο τεχνό-τρομοκράτης κατανοεί την πολυπλοκότητα και τη σημασία των δικτύων υψηλής τεχνολογίας. Σε αντίθεση με τον κυβερνότρομοκράτη, ο τέχνοτρομοκράτης θα στοχεύσει και θα επιτεθεί ενάντια εκείνων των συστημάτων που υπάρχουν στο πραγματικό χώρο, για να προκαλέσουν σύγχυση στο κυβερνοχώρο. Άρα ό στόχος είναι ο υπολογιστής κι όχι το σύστημα γενικότερα. Ο**

τεχνοτρομοκράτες θα χρησιμοποιήσει «συμβατικά όπλα» όπως βόμβες για να πλήξει ή να καταστρέψει τα συστήματα που ελέγχουν τον κυβερνοχώρο[214].

Παράρτημα 2

Πληροφόρηση αποτελεί το κάθε δεδομένο, συμβάν ή οδηγία σε κάθε μέσο και μορφή

Παγκόσμια Υποδομή Πληροφοριών (GII): Είναι παγκόσμια διασύνδεση των διαύλων επικοινωνίας, όπως δίκτυα, υπολογιστές, βάσεις δεδομένων που διαθέτουν μαζικές πληροφορίες στους χρήστες. Οι υποδομές του παγκοσμίου συστήματος πληροφοριών προμηθεύει επίσης εξοπλισμό, όπως κάμερες, σαρωτές (scanner), συστήματα αποθήκευσης δεδομένων, περιφερειακά (οθόνες, δορυφόρους κ.α).

Προστασία Δεδομένων: Οι διαδικασίες πληροφόρησης απαιτούν ένα αυξημένο επίπεδο προστασίας με στόχο να διατηρηθεί η διαθεσιμότητα, η ακεραιότητα και αυθεντικότητα και να αποφευχθεί κάθε είδους κατάχρηση.

Επιχειρήσεις πληροφόρησης: είναι οι δραστηριότητες με στόχο να αποκτηθούν πληροφορίες για τους αντιπάλους προστατεύοντας παράλληλα τα οικεία συστήματα πληροφόρησης.

[214] CRS Report for Congress - Computer Attack and Cyber Terrorism

Σύστημα πληροφόρησης: Κάθε υποδομή, οργανισμό, ομάδα ατόμων που συλλέγουν, επεξεργάζεται, αποθηκεύει, μεταφέρει και παρουσιάζει μία σειρά δεδομένων-πληροφοριών

Πολεμικές επιχειρήσεις πληροφόρησης: Διαδικασίες συλλογής, μεταφοράς και επεξεργασίας δεδομένων, εν καιρώ κρίσης, με σκοπό την εκπλήρωση ή την προώθηση συγκεκριμένων αποστολών ενάντια σε αντίπαλες δυνάμεις. (παραπομπή σε 2.3)

Παράρτημα 3 Ορολογία σχετικά με το κυβερνόεγκλημα

Vulnerability scanner (Ερευνητής σφαλμάτων)

Ερευνητής σφαλμάτων είναι ο τύπος ανιχνευτή που χρησιμοποιείται από παροχείς ασφαλείας με στόχο να εντοπίσουν αδυναμίες ασφαλείας σε ένα σύστημα υπολογιστών. Η συσκευή αυτή μπορεί να χρησιμοποιηθεί από απλούς χρήστες, ή ακόμη από διαχειριστές για λόγους ασφαλείας, ή ακόμη μπορεί να χρησιμοποιηθεί από χάκερ με στόχο να εξασφαλίσουν παράνομη πρόσβαση σε υπολογιστικά συστήματα. (Πηγή : Techopedia.com)

Password cracking («Σπάσιμο κωδικών»)

Είναι μία μέθοδος ανάκτησης κωδικών από κινούμενα δεδομένα ή δεδομένα αποθηκευμένα στον υπολογιστή. Η μέθοδος αυτή, μπορεί να βοηθήσει ένα νόμιμο χρήστη ανακτήσετε έναν παλαιότερο κωδικό πρόσβασης. Οι διαχειριστές συστήματος μπορούν να χρησιμοποιούν αυτή τη μέθοδο, ως μια προληπτική τακτική, για να τροποποιηθεί αυξημένη ασφάλεια. Μη εξουσιοδοτημένοι χρήστες τη χρησιμοποιούν για να αποκτήσουν παράνομη πρόσβαση. (Πηγή: ehow.com)

Spoofing attack (Επίθεση πλαστογράφησης)

Μια επίθεση πλαστογράφησης περιλαμβάνει ένα πρόγραμμα, σύστημα, ή μία ιστοσελίδα που έχει μεταμφιεστεί επιτυχώς σε ένα άλλο πρόγραμμα μέσα από την παραποίηση στοιχείων και ως εκ τούτου θεωρείται ως ένα αξιόπιστο σύστημα του χρήστη ή κάποιο άλλο πρόγραμμα. του παρόντος είναι συνήθως για να ξεγελάσουν , τα συστήματα, ή τους χρήστες ώστε να αποκαλύπτουν εμπιστευτικές πληροφορίες, όπως ονόματα χρηστών και κωδικούς πρόσβασης. (Πηγή: Techopedia.com)

Social engineering (επίθεση κοινωνικής μηχανικής)

Η επίθεση μέσω κοινωνικής μηχανικής αφορά την δεύτερη φάση εισβολής ενός Hacker σε ένα σύστημα, όπου εκείνος χρησιμοποιεί σελίδες κοινωνικής δικτύωσης με στόχο την πρόσβαση στο δίκτυο. Η επίθεση αυτή, μπορεί να πραγματοποιηθεί είτε μέσω εκφοβισμού, είτε μέσω διαπραγματεύσεων μέσω των οποίων θα εξασφαλιστούν τα απαραίτητα δεδομένα. (Πηγή: Techopedia.com)

Παράρτημα 4 Χαρακτηριστικά κυβερνοχώρου

Κατηγορίες	**Χαρακτηριστικά**	**Αναφορές-πηγές**
Εικονική πραγματικότητα	Ύπαρξη ενός διαφορετικού επιπέδου ζωής και δραστηριότητας	Wertheim, 1999[215]; Kollock, 1999[216]
	Πραγματικότητα του εικονικού κόσμου	Wertheim, 1999; Hang, 2000

215 Βλέπε Wertheim, M. (1999). The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet. Sydney: Doubleday. MA: Harvard University Press

216 Βλέπε Smith, M., Kollock, ΣΕΛ.(1999). Communities in cyberspace. New York: Routledge. MA: Harvard University Press

Αλληλεπίδραση	Κοινωνική δικτύωση και ψυχαγωγία	Wertheim, 1999
	Κοινωνία κοινών ενδιαφερόντων και δραστηριοτήτων	Wertheim, 1999
	Ισότητα δημοσίου χώρου	Wertheim, 1999; (Hang, 2000[217]
	Καταστροφή ανθρώπινης επικοινωνίας (αρνητικό)	Jung, 2008)[218]
	Απομόνωση στον κυβερνοχώρο (cyber-egoism)	Wertheim, 1999; Park 2001[219]
Πηγή πληροφοριών	Συστηματοποίηση της πληροφορίας	Wertheim, 1999; Buchanan, 2002
	Χρήστης ως παράγοντας γνώσης	Jung, 2008
	Προσβασιμότητα ηλεκτρονικών τόπων	Hang, 2000; Wertheim, 1999
	Τυποποίηση πληροφοριών	Wertheim, 1999
	Υπερκείμενα (hyper texts)	Jung, 2008
	Μηχανές αναζήτησης (πχ. Bing)	Jung, 2008

217 Βλέπε Hang, S. (2000). Another ego in cyberspace. Seoul: gimyoungsa.

218 Βλέπε Jung, yu-ul(2008). Mobile Odyssey. Seoul: Lionbooks. The Bodley Head Ltd.

219 Βλέπε Park, C (2001). Sociology of cyberspace. Seoul: Junglimsa. The Bodley Head Ltd.

Παράρτημα 5 Πολιτικές προστασίας της ΕΕ για την τρομοκρατία

	Εισηγήσεις-Βελτιώσεις	**Πολιτικές**	**Πολιτικές προστασίας της ΕΕ**[220]	**Κατάσταση**
1.	Αναφορά σε πρακτικές εξωτερικής πολιτικής	**Πρόληψη** **Απάντηση**	Διεθνής διάσταση: προτεραιότητα βοήθειας σε ότι αφορά την ενδυνάμωση της διεθνούς συνεργασίας με τρίτες χώρες.	Ενεργή
2.	Ανάπτυξη μίας συγκροτημένης επικοινωνιακής στρατηγικής.	**Πρόληψη** **Απάντηση**	Εξέταση του ρόλου των Μέσων Ενημέρωσης, καταστολή του εξτρεμισμού	Ενεργή
3.	Προώθηση ιδεολογικών απαντήσεων	**Πρόληψη** **Απάντηση**	Ενίσχυση της κοινής γνώμης και απόδοση λόγου σε μη ακραίες φωνές	Ενεργή
4.	Εφαρμογή κάθε μέτρων καταστολής της τρομοκρατίας	**Πρόληψη** **Προστασία** **Καταδίωξη** **Απάντηση**	Εύνοια σε επίπεδο συνεργασίας και ακαδημαϊκών σπουδών, συλλογή πληροφοριών, ανάλυση και ανταλλαγή με έμφαση στις ευθύνες του κάθε κράτους μέλους, ενίσχυση των θεσμών της	Ενεργή

220 EU Terrorism Action Plan

			Ευρωπαϊκής Ένωσης	
5.	Αναγνώριση και καταπολέμηση των βαθύτερων αιτιών.	**Πρόληψη** **Καταδίωξη**	Καταστολή των δραστηριοτήτων των δικτύων και των ατόμων που προσελκύουν άτομα στην τρομοκρατία: πρόληψη στρατολόγησης και μύησης, πρόνοια για την ασφάλεια, την δικαιοσύνη, την δημοκρατία και την ευκαιρία για κατάργηση ανισοτήτων και διακρίσεων.	Ενεργή
6.	Υιοθέτηση κοινών όρων	**Πρόληψη** **Προστασία** **Καταδίωξη** **Απάντηση**	Προσπάθεια για υιοθέτηση ενός κοινώς αποδεκτού ορισμού για την τρομοκρατία.	Ενεργή

Παράρτημα 6 Δράσεις Διεθνών Οργανισμών Ενάντια στην Τρομοκρατία

ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΙ	**ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ**
Ηνωμένα Έθνη	Πολλαπλοί θεσμοί των Ηνωμένων Εθνών, έχουν λάβει σημαντικές πρωτοβουλίες σχετικά με την καταπολέμηση της τρομοκρατίας και της εγκληματικής χρήσης της πληροφόρησης.

	Μερικοί από αυτοί είναι: 1. Η **Αντιτρομοκρατική Επιτροπή του Συμβουλίου Ασφαλείας**[221] που αποτελεί τον κύριο θώκο δραστηριοτήτων σχετικά με την κατάπαυση των τρομοκρατικών δραστηριοτήτων 2. Το **Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα**[222] που προμηθεύει τα μέλη κράτη του ΝΑΤΟ με νομικές συμβουλές προκειμένου να ενισχύσει το πνεύμα διεθνούς συνεργασίας των χωρών για την αναστολή κάθε είδους τρομοκρατικής δραστηριότητας. 3. Η **Διεθνής Ένωση Πληροφοριών**[223]**,** με την ιδιότητα του πλέον δραστήριου οργάνου για την εναρμόνιση των συνθηκών διεθνούς ασφαλείας. Η δραστηριότητα της καλύπτει τομείς, όπως: **α)** την ανταλλαγή πληροφοριών με στόχο την ασφάλεια των κρατικών υποδομών μίας χώρας, **β)** την νομική καθοδήγηση σε ότι αφορά την καταπολέμηση τρομοκρατικών συμβάντων του κυβερνοχώρου, **γ)** την

221 The United Nations General Assembly Resolution, 4th December 2000
222 Βλέπε www.unodc.org
223 Βλέπε www.itu.int/

	εγκατάσταση μηχανισμών άμεσης απάντησης σε περιπτώσεις τρομοκρατικών επιθέσεων.
Συμβούλιο της Ευρώπης	Το **Συμβούλιο της Ευρώπης,** από το 2001, ασχολείται με την περισυλλογή, την ασφαλή διακίνηση και την προστασία των ηλεκτρονικών δεδομένων στα υπολογιστικά συστήματα.
G8	Η **ομάδα κρατών G8**[224] ασχολείται με την προστασία του κυβερνοχώρου και την αποφυγή χρήσης αυτού για τρομοκρατικές ή άλλες παράνομες επιχειρήσεις
Οικονομικός Σύνδεσμος Ασίας Ειρηνικού (APEC)	Η **Αντιτρομοκρατική Ομάδα Εργασίας** του **Οικονομικός Σύνδεσμος Ασίας Ειρηνικού**[225]**,** επιδίδεται σε ζητήματα τεχνικής προστασίας ενάντια σε τρομοκρατικές επιχειρήσεις
NATO	Η **Επιτροπή Σχεδιασμού Πολιτικής Επικοινωνίας του NATO**[226]**,** έχει να κάνει με την δημιουργία προδιαγραφών προστασίας των κρατικών υποδομών των κρατών μελών. Επιπλέον, το **Κέντρο Ασφαλείας Πληροφοριών**[227] θεωρείται ως η πρώτη γραμμή δράσης ενάντια στην

224 G8 Information Centre, University of Toronto, Canada, www.g7.utoronto.ca

225 Makarim Wibisono, Ambassador and Chair CTTF: APEC´s Strategy to Suσελ.ort International Law Enforcement Cooperation to Counter Terrorism in the Asia-Pacific Region, Bali 2004. Βλέπε www.apec.org

226 The Civil Communication Planning Committee (CCPC)

227 NATO Summit in 2002

	τρομοκρατία του κυβερνοχώρου.
Οργανισμός Αμερικανικών Πολιτειών[228] (1999)	Ο οργανισμός αυτός είναι αρμόδιος για την προμήθεια νομικών μέσων και οργάνων για την καταπολέμηση εγκληματικών και τρομοκρατικών δράσεων στην αμερικανική περιφέρεια.

Βιβλιογραφία

- Alexander, Yonah Swetman, Michael S. (2001). Cyber Terrorism and Information Warfare: Threats and Responses. Transnational Publishers Inc.,U.S
- Arquilla et al. (1999), "Networks, Netwar, and Information-Age Terrorism" in Terrorism and Counterterrorism: Understanding the new security environment (2004) The McGraw-Hill Companies.
- Colarik, Andrew M. (2006). Cyber Terrorism: Political and Economic Implications. Idea Group, U.S.
- CRS Report for Congress Received through the CRS Web. Computer Attack and Cyber Terrorism 2008
- EU urged to deepen cooperation after Estonia cyber-attacks
- Vulnerabilities and Policy Issues for Congress: Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. October 17, 2003 http://www.fas.org/irp/crs/RL32114.pdf
- Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Updated January 29, 2008 http://www.fas.org/sgp/crs/terror/RL32114.pdf
- Chaliand, Gerard. The History of Terrorism: From Antiquity to al Qaeda. Berkeley: University of California Press, 2007. ΣΕΛ. 213.
- Conway M. (2003), "Terrorism and IT: Cyberterrorism and Terrorist Organisations Online" in Terrorism and Counterterrorism: Understanding the new security environment (2005) ed. Rohan Gunaratna. Marshall Cavendish Academic

228 Βλέπε AG/RES. 1840 (XXXII-O/02) adopted on June 3, 2002, www.oas.org

- Gruen M. (2003) "White Ethnonationalist and Political Islamist Methods of Fundraising and Propaganda on the Internet in Terrorism and Counterterrorism: Understanding the new security environment (2005) ed. Rohan Gunaratna. Marshall Cavendish Academic.
- Jacqueline Ching (2010). Cyberterrorism. Rosen Pub Grouσελ.
- Jones, F., & Fong, Y. (1994). Military psychiatry and terrorism. In Department of the Army, Textbook of military medicine (pσελ. 264–269). Washington, D.C.: Department of the Army.
- Kaplan, A. (1981). The psychodynamics of terrorism. In Y. Alexander & J. Gleason (Eds.), Behavioral and quantitative perspectives on terrorism (pσελ. 35–50). New York: Pergamon.
- Nye, Joseph. (2010). Cyberpower . Harvard Kennedy School. In Nye, Joseph "The Future of Power in the 21st Century", (2011), Public Affairs Press
- Oots, K. (1990). Bargaining with terrorists: Organizational considerations. Terrorism, 13, 145–158.
- Taylor, M. (1988). The terrorist. London: Brassey's Defence.
- TE-SAT 2007: EU Terrorism Situation & Trend Report | Europol https://www.europol.europa.eu/sites/default/files/publications/tesat2007.pdf
- Thomas T.L. (2003) Al-Qaeda and the Internet: The Danger of "Cyber-planning" www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf Retrieved on 09/04/2007
- U.S. Department of Justice. (2000). Homicide trends in the U.S. [On-line]. Available: http://www.ojσελ.
- U.S. Department of State. (2000). Patterns of global terrorism, 2000 [On-line].
- U.S. Department of Transportation. (2001). 2000 Annual Assessment—Motor Vehicle Traffic Crash
- Weimann G. (2004) www.terror.net How Modern Terrorism Uses The Internet. United States Institute of Peace www.usiσελ.org/pubs/specialreports/sr116.pdf Retrieved on 09/04/2007.
- Weimann, Gabriel (2006). Terror on the Internet: The New Arena, the New Challenges. United States Institute of Peace, U.S.
- Verton, Dan (2003). Black Ice: The Invisible Threat of Cyber-terrorism. Osborne/McGraw-Hill, U.S.

Πρόσθετο Υλικό

- The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Cosimo, Inc. July 30, 2010
- The Media and Terrorism: A Reassessment Paul Wilkinson. Terrorism and Political Violence, Vol.9, No.2 (Summer 1997), ρσελ.51–64 Published by Frank Cass, London
- U.S Code Title 22.
- Al-Khattar, Aref M. Religion and Terrorism: An Interfaith Perspective. Westport, CT: Praeger, 2003
- Andress, Jason. Winterfeld, Steve. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress
- Arquilla et al. (1999), "Networks, Netwar, and Information-Age Terrorism" in Terrorism and Counterterrorism: Understanding the new security environment (2004) The McGraw-Hill Companies,
- Rabasa Angel, *The Muslim world after 9/11*. Project Air Force. RAND Corporation 2004.
- Boyer Bell, J. *(1975) Transnational Terror, Stanford, CA: Hoover Institution*
- Bridis Ted, " 'Silent Horizon' war games wrap up for the CIA," USA Today, May 26, 2005.
- Buijs, F.J. (2001) 'Political Violence, Threat and Challenge' in *The Netherlands' Journal of Social Science*
- Carr, Jeffrey. (2010). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly
- Chaliand, Gerard. The History of Terrorism: From Antiquity to al Qaeda. Berkeley: University of California Press, 2007.
- Charmon, Christopher. *Five Strategies of Terrorism.*Willett, Edward C. ;Ayatollah Khomeini, 2004, Publisher: The Rosen Publishing Group
- Richard Clarke "War from Cyberspace," The National Interest on line, October 27, 2009
- Denning Dorothy, "A View of Cyberterrorism Five Years Later," 2007, ρσελ. 2–3,[1] Βλέπε Greg Goth, "Terror on the Internet: A Complex Issue, and Getting Harder," IEEE Computer Society, March 2008,
- Easttom C. (2010) *Computer Crime Investigation and the Law*
- Eedle, Paul "Al-Qaeda Takes Fight for 'Hearts and Minds' to the Web," Jane's Intelligence Review, August 2002, rpt. in CNO/IO Newsletter, 5-11 August 2002.
- Furnell and Warren, "Computer Hacking and Cyber-terrorism: The Real Threats in The new Millenium

- Ganor Boaz, von Knop,Katharina, M. Duarte Carlos A(eds). "Hypermedia seduction for terrorist recruiting". IOS Press, 2007, σελ.39
- Amrutha Gayathri. FBI issues warning: Al Qaeda could be plotting an Independence Day attack on US. International Business Times.

- Ganor Boaz, von Knop,Katharina, M. Duarte Carlos A(eds). "Hypermedia seduction for terrorist recruiting". IOS Press, 2007, σελ.39

- Gibson, R. & Ward, S., "Reinvigorating Democracy: British Politics and Internet, Ash gate, Alders hot", 2000, σελ.209.
- Goldsmith Jack, "Can we stop the global cyber arms race?" Washington Post
- Goldsmith Jack and Wu Tim, Who Controls the Internet? Illusions of a Borderless World, Oxford, Oxford University Press, 2006.
- Graff, Garrett. "Robert Mueller: Remaking the FBI", Washingtonian, August 1, 2008
- Hafner Katie & Markoff John (1991). Cyberpunk: Outlaws and Hackers on the Computer Frontier. Simon & Schuster.
- Hang, S. (2000). Another ego in cyberspace. Seoul: gimyoungsa.
- Hart, The Concept of Law Oxford: Oxford University Press: 1961
- Hoffman, Bruce "Inside Terrorism" Columbia University Press 1998 ISBN 0-231-11468-0.
- Hoffman Bruce, T*he Use of Internet by Islamic Extremists.* House Parliamentary Select Committee on Intelligence. May 2006.
- Hoffman, Bruce: *Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations.* Santa Monica, CA: RAND, 2003
- Hoffman Bruce, *The Use of Internet by Islamic Extremists*,
- Honderich, Ted. *Terrorism for Humanity: Inquiries in Political Philosophy*. Rev. ed. London: Pluto Press, 2003.
- Mark Hosenball, "Islamic Cyberterror," *Newsweek*, 20 May 2002
- Huntington, S. 1996. *The clash of civilizations and the remaking of world order*. New York: Simon& Schuster Inc
- David E. A. Johnson and Steve Pettit, "Principles of the Defense for Cyber Networks," Defense Concepts 4, 2 (Jan 2010), 17.

- Jaeger, Carl "The Internet Encyclopedia", Southern Oregon University.

- Jenkins, ΣΕΛ. *Images of Terror: What We Can and Can't Know About Terrorism.* New York: Aldine de Gruyter, 2003.

- Jensen Derrick, *Endgame: Resistance*, Seven Stories Press, 2006

- Jones, F., & Fong, Y. (1994). Military psychiatry and terrorism. In Department of the Army, Textbook of military medicine (ρσελ. 264–269). Washington, D.C.: Department of the Army.

- Johnson, K (2000). Internet Email Protocols: A Developer's Guide. Addison-Wesley Professional
- Philip, A. Karber, *Terrorism as a social protest, 1971.*

- Jung, yu-ul(2008). Mobile Odyssey. Seoul: Lionbooks. The Bodley Head Ltd

- Philip, A. Karber, *Urban Terrorism: Baseline Data and a Conceptual Framework,* Social
- Science Quarterly 52, (December, 1971).

- Anspaha Katrine, The Integration of Islam in Europe: Preventing the radicalization of Muslim diasporas and counterterrorism policy. Riga, Latvia 2008, 25 -27 September

- Kessler, Ronald (1993). The FBI: Inside the World's Most Powerful Law Enforcement Agency. Pocket Books Publications.

- Kollock, ΣΕΛ. Kshetri, Nir, The Global Cybercrime Industry: Economic, Institutional and Strategic. Springer edition and Smith, M. (eds) (1998) Communities in Cyberspace, London: Routledge

- Laquer, W Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind, Woodrow Wilson Center Press, 1998

- Lasker John. "U.S. Military's Elite Hacker Crew," Wired News, April 18, 2005

- Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

- Martin C. Libicki, Cyberdeterrence and Cyberwarfare (Santa Monica: RAND, 2009)

- Mahan, Alfred Thayer. The Influence of Sea Power upon History, 1660–1783 (1890)

- Gregory J Ratrray, "An environmental Approach to Understanding Cyber Power," in Kramer et al, eds. Cyber power and National Security

- Marchetti, Victor; John D. Marks (1974). The CIA and the Cult of Intelligence.

- McCauley, Martin (2004). Russia, America and the Cold War. Pearson Education Limited.

- McQuade, S. (ed) (2009) *The Encyclopedia of Cybercrime*, Westport, CT: Greenwood Press.
- Mirskii, G. 2003. Political Islam and Western society. *Russian Social Science Review* 44:63–78
- Kibble, D. 2002. The attacks of 9/11: Evidence of a clash of religions? *Parameters* 32:34–45
- Mitchell, James "Identifying Potential Terrorist Targets" a study in the use of convergence. G2 Whitepaper on terrorism, copyright 2006, G2. Counterterrorism Conference, June 2006, Washington D.C.
- Mancur Olson, *The Rise and Decline of Nations: Economic Growth, Stagflation, and Social Rigidities*, Yale University Press, 1982
- Markoff John, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," New York Times, April 16, 2010
- Mitnick Kevin and. Simon William L, Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, 2011.
- Markoff John, "Old Trick Threatens Newest Weapons," *New York Times*, October 27, 2009; and Shane Harris, "The Cyberwar Plan," *National Journal*, November 14, 2009, 18ff.
- Moloney, Ed (2002). A Secret History of the IRA. Penguin Books
- "Michael Nacht - Assistant Secretary of Defense for Global Strategic Affairs - WhoRunsGov.com/ The Washington Post
- Nagel Jack, The descriptive Analysis of Power, (New Haven, Yale University Press, 1975), σελ.14
- J.S. Nye, Soft Power: The means to Success in World Politics,(New York, Public Affairs Press, 2004)
- Brent F. Nelsen *Religion and European Unity: Toward a Cultural Theory of Integration. Prepared for delivery at The Annual Meeting of the American Political Science Association,* Chicago I11, 30 August- 2 September 2007.
- Overgaard, Per Baltzer "The Scale of Terrorist Attacks as a Signal of Resources," *Journal of*
- *ConTict Resolution*
- Olesen Thomas, "*Social Movement Theory and Radical Islamic Activism".* Islamist as a. social movement. Centre for Studies in Islamism and Radicalization (CIR). Department of Political Science
- Aarhus University, Denmark, May 2009
- Olesen Thomas, *"Social Movement Theory and Radical Islamic Activism": Islamist as a social movement, σελ. 9.*

- David L. Paletz and Alex ΣΕΛ. Schmid, Terrorism and the Media. How Researcher, Terrorists, Government, Press, Public, Victims View and Use the Media Newbury Park: Sage Publications 1992)

- Park, C (2001). Sociology of cyberspace. Seoul: Junglimsa. The Bodley Head Ltd

- Rapoport David C., ‘‘The Four Waves of Modern Terrorism,’’ in Audrey Kurth Cronin and James M.

- Ludes, Attacking Terrorism: Elements of a Grand Strategy (Washington,D.C.: Georgetown University Press, 2004)

- James, W. Rawles, “High Technology Terrorism” Defense Electronics, January 1990,
- Reinares, F. (2005) ‘Conceptualising International Terrorism’, ARI, no. 82.

- Rollins, J. & Wilson, C. CRS Report for Congress. Terrorist Capabilities for Cyberattack: Overview and Policy Issues, January 22, 2007.

- Ross Jeffrey Ian, Controlling State Crime: Toward an Integrated Structural Model. In: J.I. Ross (Ed.). Controlling State Crime. An Introduction. New York, Garland Publ. Co., 1995.

- Sandler, “Terrorism and Signaling,” *European Journal of Political Economy*, τομ. 9, No. 3 (August 1993)

- Sageman, Marc *Understanding Terror Networks* (Philadelphia, PA: University of Pennsylvania Press, 2004)

- Schmid, ΣΕΛ. Alex, A. J ongman. *Political terrorism: a new guide to actors, authors, concepts, data bases, theories, & literature*.(2005) [1] Schmidt A. and A. Jongman (2005) *Political Terrorism*, *Piscataway*, NJ: Transaction Publishers.

- Schmidt A. and A. Jongman (1988) *Political Terrorism. A new guide to actors, authors, concepts, databases, theories and literature,* Amsterdam: North-Holland Publishing Company

- Schmidt, A. (1988) *Political Terrorism: A new guide to actors, authors, concepts, databases, theories and literature,* Amsterdam: North-Holland Publishing Company.

- Schmidt, Alex P Violence as Communication, (Beverly Hills: Sage, 1982), 60.

- Wilkinson Paul, Terrorism and the Liberal State (New York: New York UP, 1986)

- Schuler, Douglas., Shaping the network society: the new role of civil society in cyberspace, Massachusetts Institute of Technology.

- Schwartau, Winn Terminal Compromise: computer terrorism: when privacy and freedom are the victims: a novel.

- Schwartz John, "Despite 9/11 Warnings, Cyberspace Still at Risk," The Post Standard (Syracuse, N.Y.), 11 September 2002.
- Smith, M., Kollock, ΣΕΛ.(1999). Communities in cyberspace. New York: Routledge. MA: Harvard University Press
- Russell Smith, Grabosky Peter and Urbas Gregor, *Cyber Criminals on Trial: Prosecutorial and Judicial Responses to Computer Crime*. Cambridge: Cambridge University Press, 2004
- Colin Soloway, Rod Nordland, and Barbie Nadeau, "Hiding (and Seeking) Messages on the Web," Newsweek, 17 June 2002
- Speer, D.L. (2000) *Terrorist Motivations and Unconventional Weapons*, in ΣΕΛ.R. Lavoy et al.(eds). *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons*, Ithaca: Cornell University Press.
- Tom Squitieri, "Cyberspace Full of Terror Targets," USA Today, 5 June 2002
- Stuart H. Starr, "Toward a Preliminary Theory of Cyber power
- Taylor & Francis (2010), "Terrorism and Political Violence". Routledge, vol. 23.
- Theoharis, Athan G. (2004). The FBI and American Democracy: A Brief Critical History. Kansas: University Press
- Thornton Thomas Perry, "Terror as a weapon of Political Agitation," in Internal War: Problems and Approaches, ed. Harry Eckstein (New York Free Press of Glencoe, 1964), 73
- Smith Maynard, "The Theory of Games and Evolution in Animal Conΐicts," *Journal of Theoretical*
- *Biology*, τομ. 47 (1974), σελ. 209–211; John J. Mearsheimer, *Conventional Deterrence* (Ithaca,
- Schmidt, A. and A. Jogman (2005) *Political Terrorism*, Piscataway, NJ: Transaction Publishers
- Soloway Colin, Nordland Rod, and Nadeau Barbie, "Hiding (and Seeking) Messages on the Web,"
- Newsweek, 17 June 2002,.
- Talmon, J The Myth of Nation and Vision of Revolution, The Origins of Ideological Polarization in the 20th Century, 1981
- Patrick S. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," unpublished paper, School of Advanced Military Studies, Fort Leavenworth, Kansas, June 2002.
- Vasilenko, V.I. (2004) *Terrorism as a challenge for national and international law: security vs liberty?*, Berlin: Springer.

- Walzer, M. , "Towards a Global Civil Society", International Political Currents, Volume 1, Berghan Books, Oxford, 1995
- Waugh, W.L. Jr. (1982) *International terrorism :how actions respond to terrorists,* Salisbury, N.C.: Documentary Publications
- Weber Max, The Theory of Social and Economic Organization (New York: Oxford UP, 1947), 149
- Weber Max, The Theory of Social and Economic Organization (New York: Oxford UP, 1947), 152
- Weber S, "Cooperation and Discord in U.S."- Soviet Arms Control (Princeton Press, 1991)
- White, J. R. (2002). Terrorism: An introduction, 3rd ed. Stamford, CN: Wadsworth-Thomson Learning
- Gabriel Weimann. (2006). *Terror on the Internet. The New Arena, the New Challenges.* Washington, DC: United States Institute of Peace Press, 309
- Wertheim, M. (1999). The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet. Sydney: Doubleday. MA: Harvard University Press
- Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online*, Routledge, London
- Wibisono Makarim, Ambassador and Chair CTTF: APEC´s Strategy to Support International Law Enforcement Cooperation to Counter Terrorism in the Asia-Pacific Region, Bali 2004. Βλέπε www.apec.org
- Zittrain Jonathan, The Future of the Internet and How to Stop It (New Haven: Yale UP, 2008).

Ελληνική βιβλιογραφία

- Λοβέρδου, Α. *Για την τρομοκρατία και το πολιτικό έγκλημα,* 1987, σελ. 71.
- Αριστοτέλης, *Πολιτικά.*(παρ. 1252α)
- Αριστοτέλης, *Πολιτικά.*(παρ. 1252β[1]
- G8 Information Centre, University of Toronto, Canada, www.g7.utoronto.ca

Ηλεκτρονικό Υλικό

Center for Strategic & International Studies (CSIS)

Cyberterrorism: How Real is the Threat?

Franklin Zimring (2004) on the Vigilante Mindset (doc)

Hackers Hall of Fame

How to Own the Internet in Your Spare Time

InfoSec and InfoWar Portal

Institute for Advanced Study of Information Warfare

Navy Postgraduate School White Paper on Cyberterror (pdf)

Politically Motivated Computer Crime and Hacktivism Blog

Putting Cyberterrorism in Context

Reality Bites: Cyberterrorism and Terrorist Use of the Internet

SocioSite: Power, Conflict, War, CyberWar, Cyberterrorism