«Αθηνά»
ΕΛΛΗΝΙΚΟ ΚΕΝΤΡΟ ΕΛΕΓΧΟΥ ΟΠΛΩΝ
Σαλαμίνος 10, Θεσσαλονίκη 54625, Τηλ/Fax: 2310904794 / 6944165341, www.armscontrol.info

ΚΥΒΕΡΝΗΤΙΚΗ ΤΡΟΜΟΚΡΑΤΙΑ:
ΚΥΝΗΓΩΝΤΑΣ ΤΟΥΣ ΑΝΕΜΟΜΥΛΟΥΣ ΤΗΣ ΝΕΑΣ ΧΙΛΙΕΤΗΡΙΔΑΣ

Μανώλης Αστρεινίδης, Διεθνολόγος Ερευνητής του Ε.Κ.Ε.Ο. «Αθηνά»
Σαλαμίνος 10, Θεσσαλονίκη 54625, email:athena@armscontrol.info

Τετάρτη 29 Ιουνίου 2005

ΚΥΒΕΡΝΗΤΙΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

Εισαγωγή

` Αν και δεν υπάρχει συγκεκριμένος ορισμός για την κυβερνητική τρομοκρατία, το αμερικανικό FBI έχει δώσει τον παρακάτω λειτουργικό προσδιορισμό: «κυβερνητική τρομοκρατία είναι μια προσχεδιασμένη επίθεση με πολιτικά κίνητρα κατά των συστημάτων πληροφοριών, των συστημάτων των ηλεκτρονικών υπολογιστών και των προγραμμάτων τους και τα δεδομένα που προκύπτουν από τη βία εις βάρος άμαχων στόχων από μυστικούς πράκτορες ή εθνικές ομάδες». Οι κυβερνητικοί τρομοκράτες μπορεί να είναι εγχώριοι τρομοκράτες ή διεθνείς όπως η Αλ-Κάϊντα. Ως τέτοιοι χαρακτηρίζονται οι τρομοκράτες που είτε στηρίζονται αποκλειστικά στη κυβερνητική τρομοκρατία για την επιδίωξη του σκοπού τους είτε επειδή χρησιμοποιούν τη κυβερνητική τρομοκρατία σε συνδυασμό και με άλλες μορφές συμβατικής τρομοκρατίας. Η κυβερνητική τρομοκρατία αποτελεί σήμερα μεγαλύτερη απειλή από οποτεδήποτε άλλοτε στο παρελθόν χάρη σε αρκετούς παράγοντες. Εν πρώτοις, τα τραγικά γεγονότα της 11 Σεπτεμβρίου 2001 έχουν αποδείξει ότι υπάρχουν τρομοκρατικές ομάδες που διαθέτουν τη πολυτέλεια της γνώσης αλλά και την αλαζονεία να επιτεθούν στις ΗΠΑ εντός των κυριαρχικών ορίων της χώρας. Κατά δεύτερο, κάθε όψη της αμερικανικής ζωής, συμπεριλαμβανομένων και των οικονομικών θεσμών, εγκαταστάσεις παραγωγής και των λειτουργιών της κυβέρνησης έχουν αρχίσει να εξαρτώνται από τη τεχνολογία των ηλεκτρονικών υπολογιστών. Τρίτο, η οικονομία των Η.Π.Α. διαρκώς εξαρτάται από τις ηλεκτρονικές συναλλαγές που φυσικά είναι εξαιρετικά ευάλωτες σε μια ενδεχόμενη επίθεση κυβερνο-τρομοκρατών.

1. Δυνατότητες των κυβερνο-τρομοκρατών

Προκειμένου να αξιολογήσουμε πλήρως την αυξανόμενη απειλή της κυβερνητικής τρομοκρατίας είναι σημαντικό να συζητηθούν οι δυνατότητες των κυβερνο-τρομοκρατών. Για να προσδιορίσουμε τις δυνατότητες των κυβερνο-τρομοκρατών θεωρείται απαραίτητο να εξεταστούν πρώτα αρκετά υποθετικά σενάρια που θέτουν οι ειδικοί στο τομέα της κυβερνητικής τρομοκρατίας και να τονιστούν τα πραγματικά περιστατικά που έχουν συμβεί τα τελευταία χρόνια.

Α. Υποθετικά Σενάρια

Αρκετοί σχολιαστές στο δημόσιο διάλογο για τις δυνατότητες των κυβερνο-τρομοκρατών έχουν θέσει ένα σημαντικό αριθμό υποθετικών σεναρίων όπου οι κυβερνο-τρομοκράτες επιτίθενται κατά σημαντικών υποδομών εντός των ΗΠΑ.

1ο Σενάριο: Μια πιθανή επίθεση κυβερνο-τρομοκρατών θα μπορούσε να έχει στόχο τους επιβάτες μιας αεροπορικής εταιρίας χρησιμοποιώντας τον πύργου ελέγχου εναέριας κυκλοφορίας ενός αεροδρομίου. Ο κυβερνο-τρομοκράτης «σπάει» το λογισμικό πρόγραμμα του πύργου ελέγχου εναέριας κυκλοφορίας και προσθέτει λάθος πληροφορίες σχετικά με τη θέση του αεροσκάφους, τη ταχύτητα κλπ, αναγκάζοντας τον ελεγκτή εναέριας κυκλοφορίας να δώσει στο πιλότο του αεροπλάνου λανθασμένες πληροφορίες. Το αεροσκάφος τότε συγκρούεται με ένα άλλο αεροσκάφος ή συντρίβεται στο έδαφος, ανάλογα με τη λανθασμένη πληροφόρηση.

2ο Σενάριο: Ένας κυβερνο-τρομοκράτης θα μπορούσε να τοποθετήσει βόμβες με ηλεκτρονικό μηχανισμό σε μια ολόκληρη πόλη. Αυτές οι βόμβες μεταδίδουν ένα κώδικα η μια στη άλλη και μπορούν να πυροδοτηθούν με ένα χρονοδιακόπτη ή ένα υπολογιστή. Οι βόμβες είναι επίσης προγραμματισμένες να εκραγούν εάν μια από τις υπόλοιπες αφοπλιστεί.

3ο Σενάριο: Ένας κυβερνο-τρομοκράτης διακόπτει τη λειτουργία του τραπεζικού λογισμικού, διακόπτει οικονομικές συναλλαγές και μπαίνει παράνομα στο δίκτυο του χρηματιστηρίου, διαγράφοντας και αλλάζοντας τις αξίες των μετοχών. Ο κυβερνο-τρομοκράτης εισαγάγει λανθασμένες πληροφορίες στα ΜΜΕ σχετικά με τις συγχωνεύσεις εταιριών, τις αξίες των μετοχών αλλά και τα εταιρικά κέρδη. Η παραπληροφόρηση προκαλεί μια ταχύτατη πτώση των αξιών των μετοχών, μια απώλεια της κεφαλαιοποίησης της αγοράς και μια γενικότερη αποσταθεροποίηση της αγοράς. Οι πολίτες χάνουν την εμπιστοσύνη τους στα οικονομικά συστήματα και έτσι επέρχεται ο οικονομικός κλονισμός και αποσταθεροποίηση.

4ο Σενάριο: Ένας κυβερνο-τρομοκράτης σπάει το δίκτυο του υπολογιστή μια αλυσίδας φαρμακείων και αλλάζει τις πληροφορίες σχετικά με την αλληλεπίδραση μεταξύ φαρμακευτικών ουσιών. Καθώς ένας μεγάλος αριθμός ηλικιωμένων ανθρώπων παίρνουν διάφορα φάρμακα που έχουν αρνητική επίδραση σε συνδυασμό με άλλα φάρμακα, πολλοί αρρωσταίνουν και κάποιοι οδηγούνται στο θάνατο.

Οι παραπάνω κυβερνο-τρομοκρατικές επιθέσεις δεν έχουν ποτέ μέχρι σήμερα πραγματοποιηθεί και πολλοί ειδικοί διαφωνούν ως προς τη δυσκολία και τη περιπλοκότητα

που απαιτείται από ένα κυβερνο-τρομοκράτη να επιτύχει αυτού του είδους τις επιθέσεις. Ωστόσο, για λόγους σκοπιμότητας της συζήτησης δεν έχει τόση σημασία το ότι αυτές οι επιθέσεις ποτέ δεν πραγματοποιήθηκαν αλλά αυτό που έχει σημασία είναι το γεγονός ότι αυτά τα σενάρια είναι πιθανά. Εάν υπάρχει μια πιθανότητα οι κυβερνο-τρομοκράτες να είναι σε θέση να ενορχηστρώσουν αυτές τις καταστρεπτικές επιθέσεις, τότε η κυβερνητική τρομοκρατία θα πρέπει να ληφθεί σοβαρά υπ' όψιν.

Β. Πραγματικά Περιστατικά

Προκειμένου να εκτιμήσουμε τη σοβαρότητα της κυβερνητικής τρομοκρατίας, είναι σημαντικό να συζητηθεί τί μπορούν να κάνουν οι κυβερνο-τρομοκράτες, εξετάζοντας περιστατικά που πραγματικά έχουν συμβεί στο παρελθόν. Τα περισσότερα από τα ακόλουθα περιστατικά δεν μπορούν να χαρακτηριστούν ως ενέργειες κυβερνητικών τρομοκρατών καθώς τα περισσότερα δεν έγιναν με σκοπό την επίτευξη ενός πολιτικού ή κοινωνικού σκοπού. Ωστόσο αυτά τα περιστατικά καταδεικνύουν τί θα μπορούσε να πετύχει ένας κυβερνο-τρομοκράτης με τη κατάλληλη εκπαίδευση. Το 1998, ο Ρόμπερτ Μόρις «απελευθέρωσε» έναν ιό η/υ που «μόλυνε» περίπου 3.000-4.000 από τους συνολικά 60.000 εξυπηρετητές του Διαδικτύου. Το 1989, μια ομάδα χάκερς γνωστή ως «Λεγεώνα του Θανάτου» στην ουσία «κατέλαβε» το τηλεφωνικό σύστημα των νοτιανατολικών Πολιτειών των ΗΠΑ. Η ομάδα παγίδευσε τηλεφωνικές γραμμές, έκανε εκτροπή τηλεφωνικών κλήσεων ενώ προσποιούνταν τους τεχνικούς στο τηλέφωνο. Το 1996, ένας χάκερ, με διασυνδέσεις στο κίνημα της υπεροχής της Λευκής φυλής, έθεσε εκτός λειτουργίας ένα προμηθευτή υπηρεσίας διαδικτύου στη Μασσαχουσέτη και κατέστρεψε μέρος του συστήματος τήρησης αρχείων. Ο χάκερ προσπαθούσε να αποστείλει ρατσιστικά μηνύματα σε ολόκληρο τον κόσμο. Έκλεινε δε με το μήνυμα «Έχετε ακόμα να δείτε πραγματική ηλεκτρονική τρομοκρατία. Κι αυτό είναι απλά υπόσχεση.»

Το 1997, ένας χάκερ αχρήστευσε το σύστημα του η/υ ενός πύργου ελέγχου στο αεροδρόμιο του Worcester στη Μασσαχουσέτη. Ευτυχώς δεν υπήρξαν θύματα, ωστόσο αυτό είχε επιπτώσεις στην υπηρεσία του πύργου ελέγχου. Την ίδια χρονιά, ένας χάκερ στη Σουηδία μπλόκαρε το σύστημα κλήσεων προς τον αριθμό έκτακτης ανάγκης (**911**) σε ολόκληρη τη δυτική και κεντρική Φλόριντα. Το 1998, οι υπολογιστές της NASA, του Ναυτικού και των πανεπιστημίων δέχθηκαν επίθεση. Οι εξυπηρετητές εμποδίζονταν να ανταποκριθούν στις συνδέσεις του δικτύου και πολλοί υπολογιστές καταστράφηκαν. Επίσης το 1998, το Υπουργείο Άμυνας δέχθηκε επίθεση και οι χάκερς απέκτησαν πρόσβαση στις πληροφορίες και τα δεδομένα του προσωπικού και της μισθοδοσίας. Το 2001, δύο φοιτητές έσπασαν ένα τραπεζικό σύστημα που χρησιμοποιούσαν οι τράπεζες και οι εταιρίες πιστωτικών καρτών για να ασφαλίζουν τους προσωπικούς κωδικούς των λογαριασμών των πελατών τους. Μέσα από αυτά τα παραδείγματα φαίνεται ξεκάθαρα ότι ένας κυβερνο-τρομοκράτης με τη σωστή εκπαίδευση μπορεί να προξενήσει εξαιρετικά σοβαρή ζημιά στη κυβέρνηση, τις ιδιωτικές εταιρίες αλλά και τους πολίτες.

2. Ομάδες που πιθανό να χρησιμοποιούν κυβερνητική τρομοκρατία

Προκειμένου να αξιολογήσουμε με ακρίβεια την απειλή της κυβερνητικής τρομοκρατίας, ένα άλλο θέμα που πρέπει να λάβει κανείς υπ᾽ όψιν είναι το ποιες ομάδες είναι πιθανό να χρησιμοποιούν κυβερνητική τρομοκρατία για την επιδίωξη των πολιτικών και κοινωνικών σκοπών τους. Αξίζει να αναγνωρίσουμε και να επισημάνουμε αυτές τις ομάδες προκειμένου να προσδιορίσουμε την απειλή και να κρίνουμε τη νοοτροπία και κουλτούρα των κυβερνο-τρομοκρατών. Δυστυχώς μια κυβερνο-τρομοκρατική απειλή θα μπορούσε να προέρχεται από αναρίθμητες πηγές. Άτομα, χώρες, ομάδες διεθνούς τρομοκρατίας, εγχώριες ομάδες καθώς και μεγάλος αριθμός άλλων φορέων έχει τη δυνατότητα να διενεργήσει κυβερνητική τρομοκρατία. Έχει αναφερθεί ότι μόνο 2002, το FBI διεξήγε περισσότερες από 10.000 έρευνες για τρομοκρατικές ενέργειες. Για να έχουμε μια γενική ιδέα του ποιες ομάδες θα μπορούσαν να καταφύγουν στη κυβερνο-τρομοκρατία είναι σημαντικό να εξετάσουμε αρκετές ομάδες διεθνούς τρομοκρατίας αλλά και αρκετές εγχώριες ομάδες.

Α. Διεθνείς Ομάδες

Το Υπουργείο Δικαιοσύνης των ΗΠΑ ανέφερε ότι το 1997 υπήρξαν 48 αναφορές για δίωξη διεθνών τρομοκρατών. Ο ρυθμός δίωξης των διεθνών τρομοκρατών παρέμεινε σταθερός μέχρι το 2001 οπότε και ο ρυθμός αυξήθηκε δραματικά στις 204. Ενώ πολλοί διαφωνούν ως προς τους λόγους αυτής της δραματικής αύξησης, οι περισσότεροι συμφωνούν ότι εν μέρει οφείλεται στην αυξημένη δημόσια επίγνωση της απειλής και σε ένα αυξημένο κονδύλιο που δόθηκε στην αντιτρομοκρατική υπηρεσία του FBI.

Η ομάδα διεθνούς τρομοκρατίας που έχει τραβήξει τη μεγαλύτερη προσοχή τα τελευταία λίγα χρόνια είναι η **Αλ-Κάϊντα**. Η Αλ-Κάϊντα πολύ πιθανό να κάνει χρήση κυβερνητικής τρομοκρατίας για να φέρει σε πέρας τους σκοπούς της. Το αμερικανικό ΥΠΕΞ έχει χαρακτηρισμένη την Αλ-Κάϊντα στη λίστα των ξένων τρομοκρατικών οργανώσεων. Η Αλ-Κάϊντα μάχεται εναντίον όλων των μη-ισλαμικών καθεστώτων και είναι ιδιαίτερα αντι-δυτικού προσανατολισμού. Ο κύριος στόχος τους είναι η επανεγκαθίδρυση του μουσουλμανικού καθεστώτος σε ολόκληρο το Περσικό Κόλπο. Διαθέτουν τρομοκρατικούς πυρήνες σε ολόκληρο τον κόσμο και είναι υπεύθυνοι για τους βομβαρδισμούς της αμερικανικής πρεσβείας στην Αν. Αφρική το 1998, το βομβαρδισμό του αμερικανικού αεροπλανοφόρου Cole το 2000 καθώς θεωρούνται υπεύθυνοι και για τις επιθέσεις στο Κέντρο Παγκόσμιου Εμπορίου αλλά και στο Πεντάγωνο το 2001. Η Αλ-Κάϊντα φαίνεται να έχει υιοθετήσει εν πολλοίς τη τεχνολογία της πληροφορικής. Επίσης η ίδια τρομοκρατική οργάνωση έχει αναπτύξει ένα δίκτυο επικοινωνιών που βασίζεται στο Διαδίκτυο, τα ηλεκτρονικά έντυπα και τα ηλεκτρονικά μηνύματα σε μια προσπάθεια να αποφεύγει τη σύλληψη από αντιτρομοκρατικές υπηρεσίες.

Μια δεύτερη ομάδα διεθνούς τρομοκρατίας είναι η **Ένοπλη Ισλαμική Ομάδα**. Η ομάδα αυτή θεωρείται μια ακραία ισλαμική ομάδα και ενεργεί κυρίως από την Αλγερία και τη Γαλλία. Μάχονται κατά των μη μουσουλμάνων και ξένων, κατά της αλγερινής κυβέρνησης και επιδιώκουν την εγκαθίδρυση ενός ισλαμικού κράτους. Είναι γνωστοί για τις συχνές κατά καιρούς σφαγές πολιτών εν ονόματι του σκοπού τους.

Μια τρίτη ξένη τρομοκρατική ομάδα είναι η **Aum Shinrikyo**. Η ομάδα αυτή ενεργεί με έδρα την Ιαπωνία και τη Ρωσία. Η ομάδα επιδιώκει να επιφέρει την Αποκάλυψη και είναι υπεύθυνη για την επίθεση με τη χημική ουσία sarin σ' ένα μετρό του Τόκυο το 1995. Η επίθεση εκείνη είχε ως αποτέλεσμα 12 νεκρούς και 5.000 τραυματίες. Το επίπεδο των δυνατοτήτων της Aum Shinrikyo στη κυβερνητική τρομοκρατία αποκαλύφθηκε το 2000, όταν ένα ιαπωνικό αστυνομικό τμήμα έμαθε ότι ένα από τα ηλεκτρονικά συστήματα εντοπισμού οχημάτων είχε κατασκευαστεί από την Aum Shinrikyo. Μέχρι εκείνη την αποκάλυψη, η τρομοκρατική αυτή ομάδα συγκέντρωνε απόρρητα δεδομένα που αφορούσαν τη θέση των χαρακτηρισμένων και μη αστυνομικών οχημάτων μέσα από το πρόγραμμα που είχαν κατασκευάσει για την αστυνομία. Επίσης αποκαλύφθηκε ότι η Aum Shinrikyo εμφανιζόταν ως υπεργολάβοι για εταιρίες προγραμματισμού ηλεκτρονικών συστημάτων και είχε κατασκευάσει λογισμικό για τουλάχιστον 80 ιαπωνικές επιχειρήσεις και 10 κυβερνητικές υπηρεσίες. Επειδή λειτουργούσαν ως υπεργολάβοι, ήταν σχεδόν αδύνατο να εντοπίσει η κυβέρνηση ποια προγράμματα είχαν κατασκευαστεί από τη τρομοκρατική οργάνωση.

Μια τέταρτη τρομοκρατική ομάδα είναι η **Χεζμπολά** η οποία έχει μια παρουσία στις ΗΠΑ και στο Λίβανο. Είχαν πάρει την ευθύνη για τους βομβαρδισμούς της αμερικανικής πρεσβείας και των καταυλισμών των Πεζοναυτών το 1983 και το βομβαρδισμό της αμερικανικής πρεσβείας στη Βηρυτό το 1984. Ο σκοπός τους είναι η εγκαθίδρυση της ισλαμικής θεοκρατίας στο Λίβανο και η εκρίζωση μη-ισλαμικών επιρροών στη Μ. Ανατολή. Η Χεζμπολά προς το παρόν διαχειρίζεται τη δική της ιστοσελίδα όπου η αποστολή της οργάνωσης περιγράφεται σε παγκόσμιο επίπεδο. Επίσης είναι γνωστό ότι η ίδια τρομοκρατική οργάνωση διαθέτει τη τεχνική κατάρτιση να καταστρέφει και να εξαφανίζει ιστοσελίδες αλλά δεν είναι ξεκάθαρο αν είναι σε θέση να διενεργήσουν μεγάλες επιθέσεις κυβερνητικής τρομοκρατίας σε δίκτυα και συστήματα.

Μια τελευταία ομάδα διεθνούς τρομοκρατίας είναι η **Χαμάς** η οποία ενεργεί στο Ισραήλ και στην Ιορδανία. Μάχονται κατά του κράτους του Ισραήλ και στόχος τους είναι η δημιουργία ενός ισλαμικού παλαιστινιακού κράτους. Η κύρια τακτική τους είναι μεγάλης κλίμακας εκρήξεις με τη μέθοδο των επιθέσεων αυτοκτονίας. Η Χαμάς σήμερα κάνει χρήση του Διαδικτύου με σκοπό την αποστολή ηλεκτρονικών μηνυμάτων, το σχεδιασμό δραστηριοτήτων, τη διάδοση της φιλοσοφίας τους και τη στρατολόγηση.

Β. Εγχώριες Ομάδες

Η κυβέρνηση των ΗΠΑ δεν χαρακτηρίζει τις εγχώριες ομάδες ως τρομοκράτες, ωστόσο ελέγχουν και επιτηρούν ομάδες που είναι αναμεμειγμένες σε εγκληματικές δραστηριότητες. Το FBI ορίζει την εγχώρια τρομοκρατία ως « τη παράνομη χρήση ή επαπειλούμενη χρήση βίας εκ μέρους μιας ομάδας ή ατόμου που εδρεύει και ενεργεί εντός των ΗΠΑ ή των εδαφών τους χωρίς ξένη καθοδήγηση και που διενεργείται εις βάρος προσώπων ή περιουσίας με τη πρόθεση του εκφοβισμού ή του εξαναγκασμού μιας κυβέρνησης ή του πληθυσμού της σε επιδίωξη πολιτικών ή κοινωνικών στόχων».

Το Υπουργείο Δικαιοσύνης ανέφερε ότι το 1997 υπήρξαν 147 αναφορές για δίωξη εγχώριων τρομοκρατών. Οι αριθμοί των αναφορών ανήλθαν τα τελευταία χρόνια στις

166(1998), στις 187 (1999), 194(2000) και 259 (2001). Το FBI αναφέρει ότι η τρέχουσα εγχώρια τρομοκρατική απειλή προέρχεται από ξεχωριστές και διαφορετικές ομάδες. Πρώτα, οι ομάδες των εξτρεμιστών της άκρας δεξιάς όπως **η Παγκόσμια Εκκλησία του Δημιουργού και του Έθνους των Αρίων** που πιστεύουν στην υπεροχή της Λευκής φυλής και συνδυάζουν αντικυβερνητικές με αντικανονικές πεποιθήσεις, συνιστούν μια απειλή εγχώριας τρομοκρατίας. Δεύτερον, οι εξτρεμιστές της Αριστεράς και των Πορτορικάνων όπως για παράδειγμα, το **Παγκόσμιο Εργατικό Κόμμα και οι Ένοπλες Δυνάμεις για την Εθνική Απελευθέρωση του Πουέρτο Ρίκο**, που συνδυάζουν ένα σοσιαλιστικό δόγμα μέσα από βίαιη καταστροφή ως μέσο για την επιδίωξη των σκοπών τους, συνιστούν μια απειλή εγχώριας τρομοκρατίας.

Το FBI έχει επίσης αναφέρει ότι ενώ οι δραστηριότητες των εξτρεμιστών της άκρας Αριστεράς βαθμιαία ατονούν, οι δραστηριότητες των ακροδεξιών εξτρεμιστών και οι δραστηριότητες εξτρεμιστών ειδικού ενδιαφέροντος παρουσιάζουν αύξηση, καθιστώντας αυτές τις δύο ομάδες τη κύρια απειλή εγχώριας τρομοκρατίας σήμερα. Η αναφορά του FBI βρήκε ότι αυτές οι τρομοκρατικές ομάδες βελτιώνουν την ικανότητά τους να στρατολογούν, να επικοινωνούν, και να συγκεντρώνουν χρήματα. Στην ίδια αναφορά βρέθηκε ότι οι ομάδες εγχώριας τρομοκρατίας αποκτούσαν ολοένα και μεγαλύτερο ενδιαφέρον και πειραματίζονταν με μη συμβατικά μέσα τρομοκρατίας, όπως τα χημικά όπλα, τα βιολογικά όπλα και τα κυβερνο-όπλα όπως οι ιοί των ηλεκτρονικών υπολογιστών. Επιπλέον, η αναφορά του FBI αποκάλυψε αρκετούς πιθανούς στόχους της εγχώριας τρομοκρατίας, όπως «οι στρατιωτικές εγκαταστάσεις, τα κτίρια και το προσωπικό του Ο.Η.Ε., όργανα σχετικά με τις κοινότητες των Αφροαμερικανών και των Εβραίων και άλλες φυλετικές και θρησκευτικές μειονότητες, οι ομοφυλόφιλοι και οι λεσβίες και οι ξένες στρατιωτικές μονάδες με έδρα τις αμερικανικές βάσεις».

Υπάρχουν αρκετές ειδικές ομάδες που ενεργούν εντός των Ηνωμένων Πολιτειών, που μπορεί να διαθέτουν την ικανότητα να χρησιμοποιούν το κυβερνοχώρο ως μέσο για τη διενέργεια εγχώριας τρομοκρατίας. Μια ομάδα που θα μπορούσε να καταφύγει στη κυβερνητική τρομοκρατία είναι το «**Hammerskin Nation**». Αυτή η ομάδα αποτελείται από εξτρεμιστές της λευκής δύναμης. Ισχυρίζεται ότι διαθέτει μέλη στις Η.Π.Α, στο Καναδά, στην Αυστραλία, στη Γερμανία και στην Αγγλία. Το «Hammerskin Nation» διαθέτει κάποια κατάρτιση στους υπολογιστές, όπως έχει αποδειχθεί από τη χρήση του διαδικτύου για τη διάδοση πληροφοριών στα μέλη του, τη στρατολόγηση και τη προμήθεια συνδέσμων σε πωλητές μουσικής της λευκής δύναμης.

Μια άλλη ομάδα που θα μπορούσε να καταφύγει στη κυβερνο-τρομοκρατία προκειμένου να προαγάγει τη πολιτική της ατζέντα είναι το «**Stormfront**» που είναι επίσης μια ομάδα εξτρεμιστών της λευκής δύναμης. Κι αυτή η ομάδα έχει επιδείξει κατάρτιση στους υπολογιστές μέσα από τη χρήση του Διαδικτύου. Διαθέτει στο Διαδίκτυο μια εικονική κοινότητα για οικογένειες λευκών εξτρεμιστών και ελεύθερους λευκούς εξτρεμιστές. Η ομάδα διατηρεί επίσης συνδέσμους με άλλες ομάδες λευκών εξτρεμιστών όπως οι νέο-ναζί και οι skinheads.

Μια τρίτη εγχώρια ομάδα που πιθανόν να χρησιμοποιεί τη κυβερνο-τρομοκρατία είναι το Έθνος των Αρίων. Το **Έθνος των Αρίων** διέθετε μια αρκετά μεγάλη ιστοσελίδα μέχρι που έχασαν μια ακριβή δικαστική μάχη και η ιστοσελίδα τους κατέληξε να είναι ανενεργή. Η

ιστοσελίδα τους περιλάμβανε συνδέσμους με άλλες ομάδες μίσους, συνδέσμους με λανθασμένες πληροφορίες σχετικά με την Αγία Γραφή και σχετικά με μειονοτικές ομάδες καθώς και συνδέσμους με σελίδες σχετικές με τη κατασκευή βομβών ενώ οι χρήστες της σελίδας μπορούσαν να κατεβάσουν ιούς ηλεκτρονικών υπολογιστών.

Μια τελευταία εγχώρια ομάδα ικανή να διενεργήσει κυβερνητική τρομοκρατία είναι η «**Εθνική Συμμαχία**». Αυτή η ομάδα είναι νεο-ναζιστική και διαθέτει τη δική της ιστοσελίδα. Επειδή η σελίδα της δεν είναι πολύ περίπλοκη και σύνθετη, οι περισσότερες ομάδες εξτρεμιστών της λευκής δύναμης και οι αντι-σημιτικές ομάδες παρέχουν συνδέσμους στην Εθνική Συμμαχία.

3. Τα οφέλη των τρομοκρατών που κάνουν χρήση της κυβερνητικής τρομοκρατίας

Η κυβερνητική τρομοκρατία είναι ένα πολύ ελκυστικό μέσο κατατρομοκράτησης μιας κυβέρνησης, μια εταιρίας ή των πολιτών μιας χώρας. Υπάρχουν πολλοί λόγοι για τους οποίους η κυβερνητική τρομοκρατία αποτελεί μια ελκυστική επιλογή για τους τρομοκράτες. Πρώτον είναι η φτηνότερη από τις παραδοσιακές τρομοκρατικές μεθόδους. Πολλές φορές αυτό που χρειάζεται ο τρομοκράτης είναι μόνο ένας υπολογιστής και μια απλή τηλεφωνική σύνδεση. Οι τρομοκράτες δεν χρειάζεται να αγοράζουν παραδοσιακά επιθετικά όπλα όπως πιστόλια και βόμβες, αντίθετα μπορούν να δημιουργήσουν και να διασπείρουν ηλεκτρονικούς ιούς μέσω μιας τηλεφωνικής γραμμής. Επίσης οι τρομοκράτες δεν χρειάζεται να ενοικιάζουν οχήματα ή να πληρώνουν για τη διανομή των εκρηκτικών τους, μπορούν να σπείρουν το τρόμο από τον υπολογιστή του σπιτιού τους.

Δεύτερον, η κυβερνητική τρομοκρατία είναι πιο ανώνυμη από τις παραδοσιακές τρομοκρατικές μεθόδους καθώς είναι δύσκολος ο εντοπισμός ενός κυβερνο-τρομοκράτη. Επίσης δεν υπάρχουν φυσικοί φραγμοί όπως τα σημεία ελέγχου, τελωνειακοί υπάλληλοι ή σύνορα. Είναι επίσης δυσκολότερο να αναγνωριστεί κάποιος από ένα ψευδώνυμο ή από το όνομα ενός φιλοξενούμενου χρήστη. Επιπλέον ο κυβερνο-τρομοκράτης θα μπορούσε να δραστηριοποιείται από οπουδήποτε στο κόσμο.

Τρίτο, υπάρχει ένας ενδεικτικά μεγάλος αριθμός στόχων. Ο κυβερνο-τρομοκράτης θα μπορούσε να στοχεύει τους υπολογιστές μιας κυβέρνησης, μιας εταιρίας, ατομικούς, δημόσια έργα τους υπολογιστές ιδιωτικών αερογραμμών κλπ. Επίσης, μέσα σε κάθε μια από τις κατηγορίες αυτές ενυπάρχουν υπο-κατηγορίες συστημάτων και δικτύων όπου ενδιαφέρεται να μπει παράνομα ο κυβερνο-τρομοκράτης. Ένας άλλος ελκυστικός παράγοντας είναι ότι σύμφωνα με το νόμο των πιθανοτήτων, ανάμεσα σε τόσους πολλούς υπολογιστές και συστήματα, θα υπάρχει μεγάλος αριθμός αδυναμιών και ευκαιριών τις οποίες μπορούν να εκμεταλλευτούν οι τρομοκράτες.

Τέταρτο, η κυβερνητική τρομοκρατία μπορεί να διενεργηθεί από μακριά. Αυτό το χαρακτηριστικό της κυβερνο-τρομοκρατίας είναι ιδιαίτερα ελκυστικό για τους κυβερνο-τρομοκράτες. Συνήθως οι τρομοκράτες που χρησιμοποιούν παραδοσιακές μεθόδους, όπως οι επιθέσεις αυτοκτονίας με εκρηκτικά, δαπανούν πολύ χρόνο και χρήμα για τη στρατολόγηση και εκπαίδευση των τρομοκρατών που τελικά θα σκοτωθούν φέροντας σε πέρας τις επιθέσεις τους.

Η κυβερνητική τρομοκρατία μπορεί να έχει μεγαλύτερο αριθμό οπαδών στους κόλπους των τρομοκρατικών οργανώσεων.

Τέλος, η κυβερνητική τρομοκρατία έχει τη δυνατότητα να επηρεάζει μεγαλύτερο αριθμό ανθρώπων απ΄ ό,τι οι παραδοσιακές τρομοκρατικές μέθοδοι. Για παράδειγμα, εκτιμάται ότι ο ιός I LOVE YOU επηρέασε περισσότερους από 20 εκατομμύρια χρήστες του Διαδικτύου και κόστισε δισεκατομμύρια δολάρια σε βλάβες. Επειδή η κυβερνο-τρομοκρατία μπορεί να επηρεάσει περισσότερους ανθρώπους υπάρχει μεγαλύτερη δυνατότητα για πιο εκτεταμένη ειδησεογραφική κάλυψη που αποτελεί το τελικό ζητούμενο των τρομοκρατών. Είναι πολύ πιθανό το τρομοκρατικό περιστατικό να μη καλυφθεί μόνο από τα τοπικά ΜΜΕ αλλά και από τα εθνικά καθώς η κυβερνητική τρομοκρατία αποτελεί ένα προσφιλές και επίκαιρο θέμα.

4. Ο ρόλος των κυβερνήσεων στη καταπολέμηση της κυβερνητικής τρομοκρατίας

Η κυβερνητική τρομοκρατία είναι μια σχετικά πρόσφατη απειλή, για το λόγο αυτό γίνονται ακόμα εκτιμήσεις και εικασίες για το ποιος τελικά είναι υπεύθυνος για τη καταπολέμησή της. Ωστόσο η αδυναμία των κυβερνήσεων να αντιμετωπίσουν τη κυβερνητική τρομοκρατία αποτελεί απλά μέρος του προβλήματος. Αυτό οφείλεται στην έλλειψη ανθρώπινου δυναμικού (ειδικών) και οικονομικών κονδυλίων των κυβερνήσεων. Αυτό το γεγονός είναι εξαιρετικά εξαντλητικό για τις ιδιωτικές εταιρίες που έχουν απώλειες περίπου 10 εκ. δολάρια ετησίως εξαιτίας της ηλεκτρονικής εγκληματικότητας. Σε μια προσπάθεια να δημιουργήσει ετοιμότητα έναντι της κυβερνητικής τρομοκρατίας, η αμερικανική κυβέρνηση έχει αναπτύξει την Εθνική Στρατηγική για την Ασφάλεια του Κυβερνοχώρου. Οι τρεις στόχοι του σχεδίου είναι να α) προλαμβάνει τις κυβερνο-επιθέσεις εις βάρος θεμελιωδών αμερικανικών υποδομών, β) ελαχιστοποιεί τις εθνικές αδυναμίες έναντι κυβερνο-επιθέσεων και γ) ελαχιστοποιεί τη βλάβη και το χρόνο αποκατάστασης από κυβερνο-επιθέσεις όταν αυτές συμβαίνουν.

Προκειμένου να είναι η στρατηγική αποτελεσματική απαιτείται ενεργός συμμετοχή όλων των χρηστών του Κυβερνοχώρου, ακόμα και των μέσων χρηστών, των μικρών επιχειρήσεων αλλά και μεγάλων εταιριών καθώς και όλων των κυβερνητικών υπηρεσιών. Εξαιτίας της φύσης της απειλής και της φύσης της στρατηγικής που αποσκοπεί στη καταπολέμηση της συγκεκριμένης απειλής, φαίνεται ότι απαιτείται μια συνδυασμένη προσπάθεια των διεθνών, ομοσπονδιακών και τοπικών αστυνομικών δυνάμεων προκειμένου να υπάρξει μια αποτελεσματική άμυνα κατά της κυβερνητικής τρομοκρατίας.

- **Διεθνείς Υπηρεσίες**

Στη μάχη κατά της κυβερνητικής τρομοκρατίας, η Ιντερπόλ έχει παίξει ένα σημαντικό ρόλο σε διεθνές επίπεδο. Η Ιντερπόλ έχει 178 χώρες-μέλη που την καθιστούν τη μεγαλύτερη διεθνή οργάνωση, αμέσως μετά τον Ο.Η.Ε. Η Ιντερπόλ λειτουργεί ως σύνδεσμος μεταξύ των δυνάμεων τήρησης της τάξης των κρατών μελών. Οι χώρες-μέλη παρέχουν πληροφορίες στην Ιντερπόλ για να διανεμηθούν μεταξύ των άλλων χωρών-μελών, όπως οι καταζητούμενοι εγκληματίες, αγνοούμενοι και κλεμμένα περιουσιακά στοιχεία. Επίσης η Ιντερπόλ επιδοτεί ομάδες εργασίας σε πολλά εγκληματολογικά θέματα όπως π.χ. ηλεκτρονική εγκληματικότητα,

διαφθορά, έγκλημα κατά του περιβάλλοντος, παράνομη διακίνηση γυναικών και παιδιών καθώς και άλλα θέματα. Επιπλέον η Ιντερπόλ διαθέτει μια βάση δεδομένων που περιέχει πάνω από 300.000 φακέλους εγκληματιών.

Προκειμένου να καταπολεμήσει την κυβερνητική τρομοκρατία, η Ιντερπόλ προσπαθεί να διευκολύνει το μοίρασμα των δεδομένων μεταξύ των χωρών-μελών, διενεργώντας επιχειρησιακή ανάλυση πληροφοριών, επιδοτώντας την εκπαίδευση σε θέματα κυβερνητικής τρομοκρατίας και παρέχοντας υλικό κατασκοπείας στα κράτη-μέλη.

Ένα άλλο μέτρο που λαμβάνεται σε διεθνές επίπεδο για τη καταπολέμηση της κυβερνητικής τρομοκρατίας είναι η μορφοποίηση κοινών ομάδων εργασίας. Ένα παράδειγμα είναι η κοινή ομάδα εργασίας Ινδίας-ΗΠΑ στην αντιτρομοκρατία. Οι κοινές ομάδες εργασίας είναι πλέον σε θέση να αυξήσουν την ανταλλαγή πληροφοριών μεταξύ των 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. Η κοινή ομάδα εργασίας Ινδίας-ΗΠΑ εγκαινίασε επίσης ένα διμερή διάλογο κυβερνο-ασφάλειας, που εστιάζεται ειδικά σε θέματα κυβερνητικής τρομοκρατίας και ασφάλειας των πληροφοριών.

5. Δυσκολίες στην εφαρμογή των μέτρων ασφαλείας

Αν και υπάρχουν πολλά προστατευτικά μέτρα παρουσιάζονται αρκετές δυσκολίες στην εφαρμογή τους από πλευράς των εταιριών. Πρώτον, η εφαρμογή όλων των διαθέσιμων προστατευτικών μέτρων είναι πολυδάπανη για τις ιδιωτικές εταιρίες. Ανάλογα με το μέγεθος της εταιρίας, μπορεί να κοστίσει εκατοντάδες χιλιάδες δολάρια για ένα σύμβουλο που θα προσδιορίσει τις αδυναμίες της εταιρίας και να εγκαταστήσει τα προστατευτικά μέτρα. Επιπρόσθετα, η τεχνολογία της ασφάλειας βαδίζει με σχετικά ταχείς ρυθμούς και το κόστος των νέων και αναβαθμισμένων συστημάτων ασφαλείας και λογισμικών μπορεί να αποβεί πολυέξοδο. Επιπλέον, η εκπαίδευση της πλειοψηφίας των υπαλλήλων μιας εταιρίας σε θέματα κυβερνητικής τρομοκρατίας και προληπτικών μέτρων είναι εξίσου πολυδάπανη.

Δεύτερον, ο εντοπισμός των αδυναμιών των συστημάτων των η/υ μιας εταιρίας και η εγκατάσταση λογισμικού ασφαλείας καθώς και η αναβάθμιση είναι διαδικασία πολύ χρονοβόρα. Παίρνει χρόνο από το σκοπό για το οποίο αρχικά δημιουργήθηκε η εταιρία και κατά συνέπεια μειώνει τα κέρδη.

Τρίτο, πολλά από τα συστήματα ασφαλείας και τις περίπλοκες τεχνολογικές εξελίξεις στο προστατευτικό λογισμικό κατά της κυβερνο-τρομοκρατίας είναι δυσνόητα και δύσκολα στην εκμάθηση.

Τέλος, πολλές ιδιωτικές εταιρίες δεν επιθυμούν να αναφέρουν τα κρούσματα κυβερνητικής τρομοκρατίας στις Αρχές. Θεωρείται εξευτελιστικό για μια ιδιωτική εταιρία να μαθευτεί ότι η ασφάλεια των δικτύων της έχει παραβιαστεί και επομένως είναι ευπρόσβλητη. Επίσης, τέτοια γεγονότα δημιουργούν αρνητική εικόνα για την εταιρία. Οι ανταγωνιστές της μπορούν εύκολα να χρησιμοποιήσουν αυτές τις πληροφορίες εις βάρος της και η εταιρία θα χάσει σίγουρα την επιχειρηματικότητά της.

Αν και οι παραπάνω δυσκολίες καθιστούν δύσκολη τη προετοιμασία και τη προστασία έναντι μιας επίθεσης κυβερνητικής τρομοκρατίας, ο παρών κίνδυνος των αυξανόμενων επιθέσεων τύπου κυβερνο-τρομοκρατίας είναι τόσο υψηλός ώστε να παραβλέπεται η εφαρμογή ενός συστήματος ασφαλείας. Αυτό που χρειάζεται απλώς μια σύνθετη και ευρηματική επίθεση για να καταστρέψει μια μεγάλη, μεσαία ή μικρή εταιρία. Εάν η επίθεση δεν καταστρέψει την εταιρία, τότε το κόστος των επισκευών μπορεί να είναι εξαιρετικά υψηλό και έτσι να χαθεί η καλή θέληση της εταιρίας.

Συμπέρασμα

Συμπερασματικά, υπάρχει μεγάλος αριθμός διεθνών και εγχώριων κυβερνο-τρομοκρατών που είναι ικανοί να προξενήσουν σοβαρές ζημίες στους κυβερνητικούς και οικονομικούς οργανισμούς σε παγκόσμιο επίπεδο. Αυτές οι τρομοκρατικές ομάδες σταδιακά θα στηρίζονται στη κυβερνητική τρομοκρατία για να επιτύχουν τους πολιτικούς και κοινωνικούς τους σκοπούς εξαιτίας των πολυάριθμων πλεονεκτημάτων της κυβερνητικής τρομοκρατίας. Παρόλο που αυτοί κυβερνο-τρομοκράτες θα εξαπολύουν τις επιθέσεις τους, υπάρχουν ωστόσο υπηρεσίες όπως η Ιντερπόλ που έχουν αναπτύσσουν δυνατότητες και ικανότητες κατά της κυβερνο-τρομοκρατίας. Επιπλέον, αν και ακριβά και δύσκολα στην εφαρμογή τους, ωστόσο υπάρχουν διαθέσιμα προστατευτικά μέτρα που μπορούν οι ιδιωτικές εταιρίες να εφαρμόσουν προκειμένου να προστατευτούν.