



Τετάρτη 29 Δεκεμβρίου 2010
www.geostrategy.gr

Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή

Κοινωνία της πληροφορίας

Ένα χαρακτηριστικό γνώρισμα της μεταψυχροπολεμικής εποχής είναι η διαρκής εξάρτηση της κοινωνίας από την πληροφορία. Η παγκόσμια κοινωνία βιώνει μια μεταβατική περίοδο, κατά την οποία λειτουργεί και δραστηριοποιείται παράλληλα με τα τεχνολογικά επιτεύγματα στο χώρο των πληροφοριών και των επικοινωνιών. Μεταβάλλεται ραγδαία σε μια «κοινωνία της πληροφορίας», καθώς «αισθάνεται την ανάγκη να δικτυωθεί, να επικοινωνήσει δικτυακά, να συλλέξει πληροφορίες και να εκμεταλλευτεί τις πληροφορίες των δικτύων». Η ευρεία χρήση της ψηφιακής τεχνολογίας είναι πραγματικότητα και αποτελεί πλέον απαραίτητο εργαλείο για το δημόσιο τομέα, τον ιδιωτικό τομέα αλλά και την καθημερινότητα του κάθε ανθρώπου. Ένας τεράστιος όγκος πληροφοριών κινείται αδιάκοπα στο διαδίκτυο με τελικό προορισμό το σύγχρονο άνθρωπο, ο οποίος τις αποθηκεύει, τις εκμεταλλεύεται ή τις δρομολογεί προς εκατομμύρια άλλους προορισμούς.

Η πλέον κοινή έκφραση της «κοινωνίας της πληροφορίας» είναι το Internet, το οποίο καθημερινά αυξάνεται ως προς τον αριθμό των ατόμων που το χρησιμοποιούν, ως προς την ποικιλία των παρεχόμενων υπηρεσιών αλλά και ως προς τον αριθμό των διαθέσιμων πηγών πληροφοριών.

Internet και κυβερνοχώρος

Το 1969, η «Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων» (*Advanced Research Projects Agency - ARPA*) του υπουργείου Άμυνας των ΗΠΑ αποφάσισε τη δημιουργία ενός δικτύου τεσσάρων ηλεκτρονικών υπολογιστών (ARPANET), με τρόπο ώστε να εξασφαλίζεται η μεταξύ τους επικοινωνία, ακόμη και στην περίπτωση που ένας από αυτούς θα παρουσίαζε πρόβλημα στη λειτουργία του. Τα επόμενα χρόνια, πραγματοποιήθηκε η επέκταση του δικτύου με τη σύνδεση και άλλων υπολογιστών. Το 1971, ο αριθμός των συνδεδεμένων υπολογιστών στο δίκτυο ανήλθε στους 20, ενώ έως το 1977, συνδέθηκαν επιπλέον 200 υπολογιστές. Το 1974, το δίκτυο αυτό πήρε την ονομασία Internet, και έκτοτε, η ανάπτυξή του ήταν εκπληκτική. Έως το 1997, στο Internet είχαν συνδεθεί περίπου 100.000.000 υπολογιστές, ενώ το 2000, έφτασαν τα 200.000.000. Σήμερα, περισσότεροι από δύο δισεκατομμύρια χρήστες (ιδιώτες, εταιρίες, οργανισμοί, δημόσιο, κτλ) σε παγκόσμιο επίπεδο είναι συνδεδεμένοι στο διαδίκτυο, όπου τους παρέχεται ένα τεράστιο φάσμα υπηρεσιών.

Ο κυβερνοχώρος (cyberspace) αποτελείται από το σύνολο των παγκόσμιων δικτύων υπολογιστών (συμπεριλαμβανομένου του Internet) και των περιφερειακών μηχανημάτων (όπως οι servers, οι routers, τα modems, οι εκτυπωτές, οι ενσύρματες και οι ασύρματες γραμμές, κτλ), τα οποία είναι συνδεδεμένα μεταξύ τους, προκειμένου να πραγματοποιείται η επεξεργασία, η αποθήκευση και η ροή των πληροφοριών (δεδομένων). Εκτός από το διαδίκτυο, ο κυβερνοχώρος περιλαμβάνει και το σύνολο των εσωτερικών δικτύων, τα οποία είναι εγκατεστημένα και λειτουργούν στο δημόσιο τομέα, στις τράπεζες, στους διάφορους οργανισμούς, στις ένοπλες δυνάμεις (εσωτερικά δίκτυα ελέγχου και διοίκησης, δίκτυα οπλικών συστημάτων, όπως αρμάτων, αεροσκαφών, πολεμικών πλοίων, δορυφόρων, κτλ),

αλλά και το σύνολο των μεμονωμένων ηλεκτρονικών υπολογιστών που δεν είναι συνδεδεμένοι σε κανένα δίκτυο.

Ο κυβερνοχώρος θα μπορούσε να χαρακτηριστεί και ως ένας «προσβάσιμος παγκόσμιος ψηφιακός χώρος». Εξάλλου, αναφέρεται και ως ο «πέμπτος κοινός χώρος», μετά το έδαφος, τη θάλασσα, τον αέρα και το διάστημα.

Κυβερνο-απειλή και κυβερνοπόλεμος

Κάθε μη εξουσιοδοτημένη προσπάθεια πρόσβασης σε ένα σύστημα ελέγχου ή δίκτυο, μέσω της χρήσης ενός διαύλου ροής πληροφοριών, ονομάζεται κυβερνο-απειλή (cyber threat). Αξίζει να σημειωθεί ότι η κυβερνο-απειλή δεν έχει ενταχθεί ακόμη στο δίκαιο των ένοπλων συγκρούσεων.

Κάθε ενέργεια που λαμβάνει χώρα στον κυβερνοχώρο και στοχεύει κατά της ισχύος μιας χώρας ή κατά ενός μη κρατικού δρώντα (πρόσωπα, οργανισμούς, εταιρίες, κτλ) ονομάζεται κυβερνοπόλεμος (cyberwarfare). Δεν υπάρχει επίσημος ορισμός του κυβερνοπολέμου στα πλαίσια του ΟΗΕ, παρότι το είδος αυτό του «πολέμου» εμφανίσθηκε σχεδόν ταυτόχρονα με τη δημιουργία του κυβερνοχώρου. Οι hackers και οι crackers εκμεταλλεύονται τις αδυναμίες των δικτύων μπορούν να διεισδύσουν σε αυτά, να υποκλέψουν πληροφορίες, να εισάγουν ψευδείς ή και παραπλανητικές πληροφορίες, να δημιουργήσουν προβλήματα λειτουργίας των δικτύων, και όλα αυτά προκειμένου να οδηγήσουν τα κέντρα αποφάσεων σε λανθασμένες αποφάσεις. Οι τρωτότητες (αδυναμίες) των δικτύων και των συστημάτων πληροφοριών οφείλονται στο κενό μεταξύ της θεωρίας και της πράξης, δηλαδή στις διαφορές που παρουσιάζονται κατά τη φάση της σχεδίασης, της κατασκευής και της λειτουργίας των πληροφοριακών συστημάτων.

Το είδος αυτό του «πολέμου» παρουσιάζει σαφείς διαφορές από τον παραδοσιακό πόλεμο. Συγκεκριμένα:

- Δεν προσδιορίζεται γεωγραφικά.
- Απαιτεί ελάχιστο κόστος.
- Διεξάγεται ταχύτατα.
- Χαρακτηρίζεται ως ακήρυχτος πόλεμος.
- Ανήκει στις μορφές του ασύμμετρου πολέμου (αόρατος ως προς την ταυτότητα του επιτιθέμενου, μη προβλέψιμος και τεράστιας καταστροφικότητας).

Διεθνείς αναλυτές εκτιμούν ότι «μελλοντικά ο κυβερνοπόλεμος θα συνιστά τη μέγιστη παγκόσμια απειλή». Αυτό βέβαια προϋποθέτει την επιβίωση του κυβερνοχώρου. Προς το παρόν, η απειλή του κυβερνοπολέμου θα υφίσταται για όσο χρονικό διάστημα ο κυβερνοχώρος θα παραμένει τρωτός. Το Φεβρουάριο του 2010, ο διευθυντής της υπηρεσίας *National Intelligence* των ΗΠΑ, Dennis Blair, απευθυνόμενος προς τη γερουσία ανέφερε ότι «δεν μπορούμε να είμαστε σίγουροι αν ο κυβερνοχώρος θα παραμείνει διαθέσιμος και αξιόπιστος σε περίοδο κρίσης».

Σήμερα, ο κυβερνοπόλεμος συνιστά μία μείζονα ασύμμετρη απειλή για την εθνική ασφάλεια και την ευημερία των κρατών, επομένως, είναι αναγκαία η σχεδίαση μιας στρατηγικής (cyber-security strategy), που θα εξασφαλίζει στο μέγιστο δυνατό βαθμό την ασφαλή ροή των πληροφοριών, την αποθήκευσή τους και την αντιμετώπιση όλων των μορφών κυβερνο-επιθέσεων (cyber-attacks). Η σημαντικότητα των πληροφοριών συνδέεται άμεσα με τους εθνικούς στόχους και την κυριαρχία μιας χώρας. Για το λόγο αυτό, οι κυβερνήσεις των χωρών επιδιώκουν να ιδρύσουν τις κατάλληλες υπηρεσίες, που θα διαθέτουν τα απαραίτητα τεχνολογικά μέσα και δυνατότητες, προκειμένου να προστατέψουν την ασφάλεια της ροής των ζωτικών διαβαθμισμένων πληροφοριών.

Κυβερνοπόλεμος και ένοπλες δυνάμεις

Όπως είναι φυσικό, οι ένοπλες δυνάμεις εκμεταλλεύονται τα επιτεύγματα της ψηφιακής τεχνολογίας. Δίνουν ιδιαίτερη έμφαση στην επίτευξη του μέγιστου δυνατού ελέγχου του ηλεκτρομαγνητικού φάσματος και του κυβερνοχώρου. Επιδιώκουν να αποκτήσουν την επιχειρησιακή δυνατότητα, η οποία θα τους επιτρέψει να διεισδύουν και να ελέγχουν όλα τα υφιστάμενα και μελλοντικά δίκτυα επικοινωνίας, τους αισθητήρες και τα οπτικά συστήματα που χρησιμοποιούν τον κυβερνοχώρο, σε παγκόσμιο επίπεδο. Για παράδειγμα, μεταξύ άλλων, επιδιώκουν:

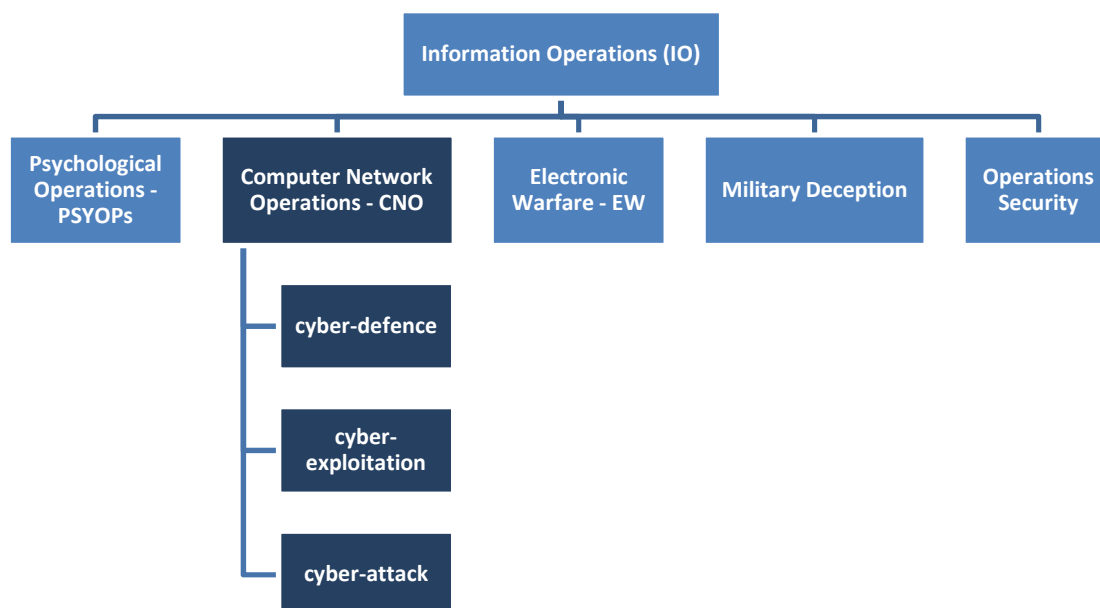
- Να επικρατήσουν στο διάστημα ελέγχοντας τη ναυτιλία των δορυφόρων.
- Να διεισδύσουν σε δίκτυα διοίκησης και ελέγχου (C2).
- Να ελέγξουν τα εχθρικά ραδιο-βοηθήματα.
- Να παρεμβάλουν ή και να παραπλανήσουν τα εχθρικά RADARs με την παροχή ψευδών στόχων.
- Να εμποδίσουν τη χρήση των οπλικών συστημάτων, που λειτουργούν με ηλεκτρομαγνητική ενέργεια ή χρησιμοποιούν δίκτυα υπολογιστών.
- Να εμποδίσουν την καθοδήγηση των μη επανδρωμένων εναέριων οχημάτων (Unmanned Aerial Vehicles - UAVs), τη λειτουργία των εχθρικών robots, κτλ.

Στις ΗΠΑ, την ευθύνη για την επικράτηση στον κυβερνοχώρο (cyber domain), τον κυβερνοπόλεμο και τον ηλεκτρονικό πόλεμο έχει αναλάβει η Air Force Cyber Command (πρόσφατα, απέκλεισε από το δίκτυο υπολογιστών της την πρόσβαση σε τουλάχιστον 25 ιστοσελίδες, μεταξύ των οποίων περιλαμβάνονται οι New York Times και Guardian, επειδή δημοσίευσαν διαβαθμισμένα τηλεγραφήματα της WikiLeaks). Τα τελευταία έτη, η αποστολή της αμερικανικής πολεμικής αεροπορίας, όπως δηλώνει η ηγεσία της, είναι «να πετάει αλλά και να μάχεται στον αέρα, στο διάστημα και στον κυβερνοχώρο».

Στην Ελλάδα, το ΓΕΕΘΑ -ως βασικός φορέας ασφάλειας της χώρας- συνεργαζόμενο με την ΕΥΠ, εκδίδει τον Εθνικό Κανονισμό Ασφάλειας (ΕΚΑ), που αφορά και την ασφάλεια των ηλεκτρονικά επεξεργασμένων διαβαθμισμένων πληροφοριών (εθνικά ευαίσθητων πληροφοριών). Για τη σύνταξη του ΕΚΑ, ο οποίος εφαρμόζεται σε όλους τους δημόσιους φορείς (υπουργεία, περιφέρειες, νομαρχίες, κλπ), έχουν ληφθεί υπόψη οι αντίστοιχοι κανονισμοί του NATO.

Οι ένοπλες δυνάμεις διεξάγουν επιχειρήσεις κυβερνοπολέμου, οι οποίες ανήκουν στην κατηγορία των επιχειρήσεων πληροφοριών (Information Operations – IO) και διαρκούν συγκεκριμένη χρονική περίοδο, προκειμένου να υποστηρίξουν άλλες μορφές στρατιωτικών επιχειρήσεων. Οι επιχειρήσεις αυτές αφορούν ενέργειες, οι οποίες, εκτός λίγων εξαιρέσεων, δεν αποσκοπούν στη στοχοποίηση του προσωπικού ούτε στην καταστροφή των δικτύων, αλλά προσβλέπουν:

- Στην κυβερνο-άμυνα (cyber-defense), δηλαδή στην προστασία των φίλιων πληροφοριακών συστημάτων από πιθανές κυβερνο-επιθέσεις.
- Στην εκμετάλλευση των πληροφοριών (cyber-exploitation) του αντίπαλου δικτύου υπολογιστών, και
- Στην κυβερνο-επίθεση (cyber-attack) κατά του εχθρικού δικτύου.



Κυβερνο-έγκλημα

Η εγκληματικότητα της σύγχρονης εποχής διαπράττεται στον κυβερνοχώρο και στηρίζεται στην τεχνολογική ανάπτυξη. Παρόλα αυτά, το συμβατικό έγκλημα δεν έχει εκλείψει.

Η εμφάνιση της ψηφιακής τεχνολογίας σχεδόν συμπίπτει χρονικά με την εμφάνιση της ψηφιακής εγκληματικότητας. Ο ταχύς ρυθμός ανάπτυξης της εν λόγω τεχνολογίας και οι αδυναμίες του κυβερνοχώρου προσέφεραν νέες ευκαιρίες και επιπρόσθετες επιλογές για τη διάπραξη ψηφιακών εγκλημάτων. Η αύξηση των κυβερνο-εγκλημάτων εμφανίσθηκε με την ευρεία χρήση των δικτύων, τα οποία, αφενός προσέφεραν πρόσβαση στην πληροφορία, και αφετέρου δεν απαιτούσαν τη φυσική παρουσία του εισβολέα.

Για τη διάπραξη ενός ηλεκτρονικού εγκλήματος είναι συνήθως απαραίτητη η ύπαρξη ενός ηλεκτρονικού υπολογιστή, ο οποίος χρησιμοποιείται είτε ως επιθετικό μέσο είτε ως στόχος ενός κυβερνο-εγκλήματος. Υπάρχουν όμως και περιπτώσεις κατά τις οποίες ένας ηλεκτρονικός υπολογιστής εμπλέκεται έμμεσα στη διάπραξη ενός εγκλήματος, δηλαδή χρησιμοποιείται επικουρικά, προκειμένου να διευκολύνει την τέλεση ενός συμβατικού εγκλήματος. Πρέπει να διευκρινισθεί ότι η αναγκαιότητα της ύπαρξης ενός ηλεκτρονικού υπολογιστή για τη διάπραξη ενός ηλεκτρονικού εγκλήματος δεν περιορίζεται στη συνήθη μορφή του ηλεκτρονικού υπολογιστή που διαθέτει ο κοινός χρήστης, αλλά συμπεριλαμβάνει και όλες τις κατηγορίες των ηλεκτρονικών υπολογιστών, που χρησιμοποιούνται στην κινητή τηλεφωνία, στα δίκτυα επικοινωνιών γενικότερα, στα μηχανήματα αυτόματης ανάληψης μετρητών του τραπεζικού τομέα, κτλ.

Το σημαντικότερο μειονέκτημα του κυβερνοχώρου είναι η τρωτότητά του, δηλαδή η αδυναμία παροχής προστασίας των πληροφοριών από πιθανές ενέργειες, που μπορούν να τις αλλοιώσουν ή να τις καταστρέψουν. Οι πιθανές αυτές ενέργειες συνιστούν εν δυνάμει απειλές, οι οποίες στρέφονται κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ενός δικτύου, που συνιστούν τους βασικούς στόχους ασφάλειας και σχετίζονται με το κυβερνο-έγκλημα.

Ο δικηγόρος και καθηγητής του ΤΕΙ Μεσολογγίου, Τσουραμάνης Χρήστος, στο βιβλίο του «ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ - Η (αν)ασφάλής όψη του διαδικτύου» αναφέρει ότι τα ψηφιακά εγκλήματα διαφέρουν από τα παραδοσιακά εγκλήματα στα εξής χαρακτηριστικά σημεία:

- Διαπράττονται συνήθως από μακρινή απόσταση. Η παγκοσμιότητα του ψηφιακού εγκλήματος συνιστά και το κύριο χαρακτηριστικό του.
- Ο εντοπισμός του ψηφιακού εγκληματία είναι τεχνολογικά περίπλοκος.
- Αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη τους.
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.
- Οι οικονομικές απώλειες που προξενούνται στα «ψηφιακά» θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων, και
- Στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμμία επίσημη αρχή.

Ο κυβερνοπόλεμος ως παγκόσμια απειλή

Ο «πέμπτος κοινός χώρος» έχει καταστεί πεδίο αντιπαράθεσης και ανταγωνισμού για την κυριαρχία μεταξύ των κρατικών δρώντων αλλά και μεταξύ των μη κρατικών δρώντων, για την υποστήριξη κυρίως των οικονομικών τους συμφερόντων. Οι κυβερνο-απειλές εκδηλώνονται με μια αυξητική τάση κατά του συνόλου των δικτύων που απαρτίζουν τον κυβερνοχώρο, γεγονός που δημιουργεί μια άναρχη κατάσταση. Η σύγχρονη ψηφιακή τεχνολογία «προσφέρει» διαρκώς νέα και πιο εξελιγμένα κυβερνο-όπλα στους κυβερνο-επιτιθέμενους.

Η παγκόσμια κοινότητα και κυρίως οι χώρες με ανεπτυγμένη ψηφιακή τεχνολογία, αναγνωρίζοντας τη σπουδαιότητα της ασφάλειας του κυβερνοχώρου για την προώθηση των συμφερόντων τους αλλά και τις υπαρκτές κυβερνο-απειλές κατά της εθνικής τους ασφάλειας και ευημερίας, πραγματοποιούν τα πρώτα τους βήματα προκειμένου να καθορίσουν τους κανόνες συμπεριφοράς εντός του κυβερνοχώρου σε εθνικό και παγκόσμιο επίπεδο. Αυτό αποδεικνύεται από τα συμπεράσματα και τις εκτιμήσεις των εμπειρογνομώνων, όπως ότι:

- Η κυβερνοχώρος συνιστά πρόκληση για το παρόν και το μέλλον της παγκόσμιας κοινότητας.
- Η εξάρτηση του δημόσιου και ιδιωτικού τομέα από τον κυβερνοχώρο θα αυξάνεται διαρκώς.
- Προς το παρόν, ο κυβερνοχώρος παραμένει «ευπρόσβλητος» και η απόλυτη προστασία του χαρακτηρίζεται ως «ουτοπία», καθότι αποτελεί πεδίο παγκόσμιου οικονομικού και στρατιωτικού ανταγωνισμού, ενώ η σύγχρονη τεχνολογία «αδυνατεί» να εγγυηθεί την αποτελεσματική κυβερνο-ασφάλεια.
- Η κυβερνο-απειλή είναι μια υπαρκτή παγκόσμια ασύμμετρη απειλή, που στρέφεται κατά της εθνικής ασφάλειας και της ευημερίας των χωρών.
- Η κυβερνο-επίθεση είναι φτηνή και αποτελεσματική, ενώ η κυβερνο-άμυνα είναι δαπανηρή, περίπλοκη, απαιτεί πολυμερή συνεργασία και δεν εγγυάται το αποτέλεσμα.
- Τα μέσα διεξαγωγής του κυβερνοπολέμου είναι ευρέως διαθέσιμα και αναπτύσσονται με ταχείς ρυθμούς.
- Η συντριπτική πλειοψηφία των κυβερνο-απειλών αφορούν το ηλεκτρονικό οικονομικό έγκλημα.

Παρότι όλες οι κυβερνήσεις παρουσιάζονται ως δρώντες στον κυβερνοχώρο που εστιάζουν την προσοχή τους μόνο στην κυβερνο-άμυνα, εντούτοις, εκτιμάται ότι επιδιώκουν να αναπτύξουν τεχνολογία και μέσα (κυβερνο-όπλα), προκειμένου αφενός να εκμεταλλευθούν τις πληροφορίες των αντίπαλων δικτύων, και αφετέρου να διεξάγουν κυβερνο-επιθέσεις, όταν απαιτηθεί. Ο λόγος είναι προφανής. Το πλεονέκτημα σε τεχνολογικό επίπεδο δημιουργεί αντίστοιχο πλεονέκτημα στον παγκόσμιο ανταγωνισμό της κυριαρχίας και της υποστήριξης των συμφερόντων.

*Γιαννακόπουλος Βασίλειος
Ταξίαρχος ε.α. Πολεμικής Αεροπορίας
Πρώην Γεωστρατηγικός Αναλυτής ΓΕΕΘΑ
Απόφοιτος της Σχολής Πολέμου και του
Centre d' Études Diplomatiques et Stratégiques
www.geostrategy.gr*