ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ & ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ
(Critical Infrastructures & Cyber Centric Warfare)

Σχετικά πρόσφατες αναφορές στις κατά τόπους δράσεις πρακτόρων ξένων μυστικών υπηρεσιών, σε συνδυασμό με την δραστηριότητα των διπλωματικών αρχών, αλλά και μεμονωμένων προσώπων που έδρασαν «ανεξάρτητα» στον κύκλο των επαγγελματικών τους δραστηριοτήτων (βλ. Edward Snowden, Julian Assange), η ροή της τρέχουσας επικαιρότητας και αναταράξεων σε παγκόσμιο επίπεδο, ανακαλούν στο προσκήνιο θέματα αντικατασκοπίας, ασφάλειας πληροφοριών, εγκαταστάσεων κρισίμων υποδομών και λοιπών δραστηριοτήτων που συνάδουν με την καθημερινή μας ζωή, ασφάλεια και ευημερία.

Οι εκφάνσεις που προσλαμβάνει το θέμα τέτοιων δράσεων, άπτονται εξειδικευμένων θεματικών περιοχών, μία εκ των οποίων είναι η Ασφάλεια των Κρισίμων Υποδομών από δραστηριότητες «Κυβερνοπολέμου» ή/και «Δικτυο-κεντρικού πολέμου», ο οποίος αναλύεται από τη σκοπιά και την μέχρι σήμερα εμπειρία του εν μέρει «ειδικού» στις ακολουθούσες ενότητες.

Ο στρατιωτικός στόχος κατά την διάρκεια συρράξεων στις κύριες περιόδους εξέλιξης του ανθρώπου, έχει όπως παρακάτω :

- Στην Αγροτική περίοδο στόχο αποτελεί το Ανθρώπινο Δυναμικό.
- Στην Βιομηχανική περίοδο στόχο αποτελεί το Υλικό και οι Εγκαταστάσεις.
- Στην μετα-βιομηχανική περίοδο ή περίοδο της Πληροφορίας στόχο αποτελούν τα Μέσα και οι Δυνατότητες.

Η Κρίσιμη Δικτυακή Υποδομή (Critical Infrastructures)

Με τον όρο Κρίσιμη Δικτυακή Υποδομή ενός κράτους ή/και οργανισμού, πλέον δεν αναφερόμαστε αποκλειστικά σε δίκτυα Η/Υ, αλλά και σε άλλα Δίκτυα όπως :

- Συλλογής, Μεταφοράς και Επεξεργασίας Πληροφοριών
- Υποστήριξης, Διοικητικής Μέριμνας και Ανεφοδιασμού
- Συγκοινωνιών (Χερσαίων, Θαλασσίων και Εναέριων)
- Παραγωγής και Διανομής Ενέργειας
- Επικοινωνιών (Ενσύρματων και Ασύρματων)
- Διαχείρισης και Ασφάλειας Ηλεκτρομαγνητικού Φάσματος
- Διαχείρισης των Υδάτινων Πόρων και Αποθεμάτων
- Διοικήσεως και Ελέγχου (Command & Control – C2)
- Γνώσης, Πληροφόρησης και Ενημέρωσης
- Παραχωρήσεων και Κοινωνικών Παροχών
- Διεθνών Αγορών και Συμφερόντων
- Σχέσεων, Γνωριμιών και Κοινωνικής ή/και Θρησκευτικής Δικτύωσης

Τόσο αυτά, όσο και πολλά άλλα, αποτελούν ελκυστικούς στόχους για τον «άγνωστο εχθρό», όχι μόνο κατά τις περιόδους κρίσεων, αλλά και κατά την ροή της τρέχουσας περιόδου.

Επιπλέον, η εκτεταμένη εξάρτηση μας από τα πάσης φύσεως ή μορφής δίκτυα, καθώς και η ανάγκη προστασίας τους, ανέδειξε ένα νέο πεδίο Στρατιωτικού Ενδιαφέροντος, τις Πληροφοριακές Επιχειρήσεις (Information Operations – Info Ops).

Πληροφοριακές Επιχειρήσεις (Info Ops)

Οι Πληροφοριακές Επιχειρήσεις περιλαμβάνουν έξι (6) συνεργαζόμενους τομείς, χωρίς αλληλεξάρτηση ή ιεραρχική δομή μεταξύ τους, αλλά σαφή αλληλεπίδραση και εκμετάλλευση των αποτελεσμάτων του ενός από τους άλλους. Αυτοί οι τομείς είναι οι ακόλουθοι:

- Πληροφορίες
- Ψυχολογικές Επιχειρήσεις (ΨΕ).
- Κοινή Γνώμη
- Ηλεκτρονικός (Η/Ν) Πόλεμος
- Επιχειρήσεις Διοικήσεως και Ελέγχου (Command & Control Warfare – C2W)
- Κυβερνοπόλεμος (Cyber Warfare) ή Δικτυοκεντρικός πόλεμος (Network Centric Warfare)

Οι Πληροφοριακές Επιχειρήσεις (Info Ops) δεν αντικαθιστούν τις Επιχειρήσεις Διοικήσεως και Ελέγχου (C2W), αλλά δρουν σε επικάλυψη και συντονισμένα με αυτές, ανεξάρτητα από το διαλαμβανόμενο επίπεδο (στρατηγικό, επιχειρησιακό, ή τακτικό). Εκμεταλλευόμενες δε ταυτόχρονα την (απαραίτητα καλή) γνώση της πολιτικής, κοινωνικής και στρατιωτικής κατάστασης, λειτουργούν συμπληρωματικά προκειμένου να ενισχύσουν την διαδικασία λήψεως αποφάσεων, επηρεάζοντας παράλληλα με διάφορους τρόπους την αντίστοιχη του αντιπάλου.

Διεθνώς ο γρηγορότερα αναπτυσσόμενος τομέας των Πληροφοριακών Επιχειρήσεων, είναι ο Κυβερνοπόλεμος (Cyber Centric Warfare), ή Δικτυοκεντρικός πόλεμος (Network Centric Warfare).

Πληροφορικός Πόλεμος (Information Warfare) vs Κυβερνοπόλεμος (Cyber Warfare)

«Πληροφορικός Πόλεμος» (Information Warfare) [1]

Είναι η επιθετική και αμυντική χρήση της πληροφορίας και των Πληροφορικών Συστημάτων (ΠΣ) με σκοπό να απορρίψει, αλλοιώσει, καταστρέψει και εκμεταλλευτεί την πληροφορία του αντιπάλου, καθώς και τις διαδικασίες που στηρίζονται στην πληροφορία, τα Πληροφορικά Συστήματα (ΠΣ) και τα δίκτυα Η/Υ, προστατεύοντας ταυτόχρονα τα αντίστοιχα φίλια.

«Κυβερνοπόλεμος» (Cyber Warfare) [2]

Είναι η εφαρμογή των παραπάνω για Στρατιωτικούς σκοπούς.

Εισαγωγή στον «Κυβερνοπόλεμο» (Cyber Warfare)

Ο «Κυβερνοπόλεμος» (Cyber Warfare) θα μπορούσε να χαρακτηριστεί σαν τον πόλεμο κατά της (κρισίμου) υποδομής του αντιπάλου. (αδόκιμα).

Έχει σκοπό να προκαλέσει σύγχυση στον αντίπαλο, να τον κάνει ανίκανο να χρησιμοποιήσει την/τις (κρίσιμη/ες) υποδομή/ες που έχει δημιουργήσει και να τον αποσυντονίσει σε σημείο που να μην δύναται να εκτελέσει επιχειρήσεις.

Επιτυγχάνει όλα τα παραπάνω, θέτοντας εκτός λειτουργίας τον κρατικό μηχανισμό, τις επικοινωνίες, τα συστήματα συλλογής και επεξεργασίας των πληροφοριών, τα ΜΜΕ, την

[1] Ατομική Διατριβή «Ο Κυβερνοπόλεμος» Ανχης (ΕΠ) Ιωάννης Α. Κολομβάκης – Σχολή Εθνικής Ασφάλειας Οκτ 2006.
[2] Ατομική Διατριβή «Ο Κυβερνοπόλεμος» Ανχης (ΕΠ) Ιωάννης Α. Κολομβάκης – Σχολή Εθνικής Ασφάλειας Οκτ 2006.

οργάνωση, την εγχώρια βιομηχανία και εν γένει όλα τα στοιχεία που απαιτούνται για να υποστηριχθούν οι επιχειρήσεις.

Στον Κυβερνοπόλεμο κάθε επιθετική προσπάθεια επιδιώκει να έχει σαν αποτέλεσμα τα ακόλουθα:

- Στέρηση Παροχής Υπηρεσιών (DoS – Denial of Service)
- Υποκλοπή
- Παραπλάνηση

Ο «Κυβερνοπόλεμος» υπόκειται στους ίδιους περιορισμούς με τον συμβατικό πόλεμο, ενώ ταυτόχρονα δρα ως πολλαπλασιαστής ισχύος.

Τελικά ο «Κυβερνοπόλεμος» :

- Δεν είναι «hacking».
- Οι «hackers» έχουν στόχο Πληροφορικά Συστήματα (ΠΣ).
- Οι «Κυβερνοπολεμιστές» έχουν στόχο ανθρώπους.
- Είναι η διαδικασία σχεδιασμού και εκτέλεσης επιχειρήσεων για την επίτευξη συγκεκριμένου στόχου.
- Ισχύουν οι ίδιες αρχές και μεθοδολογίες με τον συμβατικό πόλεμο :
  - εμμονή στον σκοπό
  - παραπλάνηση
  - συγκέντρωση προσπαθειών
  - απλότητα
  - αιφνιδιασμός
  - άμυνα σε πολλά επίπεδα

<u>Δραστηριότητες «Κυβερνοπολέμου»</u>

Οι δραστηριότητες του Κυβερνοπολέμου διακρίνονται σε :

- Επιθετική Δραστηριότητα (Offensive), η οποία έχει σκοπό να απορρίψει, να διαστρέψει, να καταστρέψει και να εκμεταλλευτεί την πληροφορία του αντιπάλου ώστε να επηρεάσει την αντίληψή του και να του μειώσει τις δυνατότητες κατά τις επιχειρήσεις.
- Αμυντική Δραστηριότητα (Defensive), η οποία έχει σκοπό να προστατεύσει εμάς και τους συμμάχους μας από παρόμοια δραστηριότητα και ταυτόχρονα να εξασφαλίσει την δυνατότητά μας να εκμεταλλευτούμε την/τις διαθέσιμη/ες πληροφορία/ες κατά την διεξαγωγή των επιχειρήσεων.
- Υποστήριξης των Επιθετικών Επιχειρήσεων, με σκοπό να συλλέξει κατά την διάρκεια της ειρήνης πληροφορίες που θα χρησιμοποιήσει για την επίτευξη των παραπάνω ενεργειών του, να βελτιώσει τον κύκλο απόφασης – δράσης και να διαταράξει τον ανάλογο κύκλο του αντιπάλου, ώστε να αποκτηθεί Υπεροχή στην Πληροφορία (Information Superiority).

<u>Υπεροχή στην Πληροφορία (Information Superiority)</u>

Υπεροχή στην Πληροφορία είναι η ικανότητα :

- Συλλογής
- Επεξεργασίας και
- Διασποράς της πληροφορίας στις ημέτερες δυνάμεις,

εξασφαλίζοντας ταυτόχρονα την αδυναμία του εχθρού να πράξει το ίδιο.

Η ενεργοποίηση του νέου αυτού είδους πολέμου, έχει σαν αποτέλεσμα να έχει ήδη αλλάξει σημαντικά η έννοια και ο τρόπος που αντιμετωπίζουμε τα θέματα ασφαλείας, τόσο σήμερα, όσο και στο άμεσο μέλλον.

Η Έννοια και η Σημασία του Απορρήτου

Η έννοια και η σημασία του «Απορρήτου» έχει αλλάξει. Μέχρι τώρα η προσπάθεια ήταν να «υποκλαπεί» πληροφορία. Τώρα πια η πληροφορία είναι διαθέσιμη ελεύθερα και σε μεγάλες ποσότητες.

Η πληροφορία όμως δεν αποτελεί γνώση. Γνώση αποτελεί η επεξεργασμένη πληροφορία.

Αυτός που έχει την δυνατότητα να την ταξινομήσει γρήγορα και να την μετατρέψει σε εκμεταλλεύσιμη μορφή έχει το πλεονέκτημα.

Στο σύγχρονο πόλεμο, η προσπάθεια του αντιπάλου δεν επικεντρώνεται μόνο στην υποκλοπή της πληροφορίας, αλλά και στο να μας στερήσει τα συστήματα και τις διαδικασίες, όπου βασίζουμε την οργάνωση μας και με τα οποία εκμεταλλευόμαστε την πληροφορία.

Η αναφορά της έννοιας του πολέμου δεν εστιάζει αποκλειστικά στις διάφορες μορφές ενόπλων συγκρούσεων, αλλά αναφέρεται κυρίως στην καθημερινή τρέχουσα οικονομική, πολιτική, διπλωματική και όχι μόνο δραστηριότητα, κρατών, συνασπισμών συμφερόντων ή/και οργανισμών.

Έτσι, η προετοιμασία αποτελεί μια συνεχή και αέναη διαδικασία σε τρέχουσα καθημερινή βάση σ' όλα τα επίπεδα, με αποκλειστικό σκοπό τη διαρκή ετοιμότητα αντιμετώπισης οποιουδήποτε περιστατικού «αστάθειας» ή/και «εισβολής».

Επιπλέον, η έγκαιρη κι επιτυχής αντιμετώπιση των καθημερινών μικρών ή μεγαλύτερων «περιστατικών», προσομοιάζει «επ' έργω» τις πραγματικές ή σχεδόν πραγματικές συνθήκες αντιμετώπισης καταστάσεων κρίσεων. Παράλληλα, αργά αλλά σταθερά, διαμορφώνει ένα βαθμό ή κατάσταση ετοιμότητος, η οποία εκφράζεται με την ικανότητα αντίδρασης ή/και αντι-αντίδρασης σε ανάλογο αριθμό «περιστατικών», που ενδέχεται να εκδηλωθούν ταυτόχρονα ή/και σε συνδυασμό χρονικής ακολουθίας εξέλιξής τους.

Επειδή δε, η εποχή μας και το προσεχές μέλλον χαρακτηρίζεται από τις παραμέτρους ακαριαία «ταχύτητα» και σημειολογική ή χειρουργική «ακρίβεια», οποιαδήποτε όχι άμεση αντίδραση, καθίσταται βραδεία και αναποτελεσματική.

Ας υποθέσουμε ότι «άγνωστος εχθρός» προσβάλλει και διακόπτει για σημαντικό διάστημα κάποιων ωρών το σύστημα παραγωγής και διανομής ενέργειας – ισχύος (ηλεκτροδότησης) σε μια ευρεία γεωγραφική περιοχή της χώρας. Αυτή η περιοχή παραλύει κυριολεκτικά, καθότι η διακοπή παροχής ενέργειας διακόπτει την λειτουργία εκατοντάδων δραστηριοτήτων, με αποτέλεσμα την δημιουργία χαοτικών καταστάσεων σε διαφορετικά πολλαπλά επίπεδα. Ταυτόχρονα δημιουργεί και διασπείρει γεωμετρικά συνθήκες πανικού στον πληθυσμό, ο οποίος κατά κανόνα αντιδρά σπασμωδικά (όχι συντεταγμένα) και κατά το δοκούν, με ότι αυτό συνεπάγεται. Πολλά συστήματα παροχής κοινωφελών υπηρεσιών σταματούν ξαφνικά να λειτουργούν, διακόπτοντας χιλιάδες δραστηριοτήτων που ήδη βρίσκονται σε εξέλιξη, όπως τραπεζικές ή χρηματο-οικονομικές συναλλαγές, κυκλοφοριακές ρυθμίσεις, επεμβάσεις ή παροχές υγείας, εμπορίου, εκπαίδευσης, επικοινωνιών και συγκοινωνιών, ενημέρωσης και ασφάλειας, αλλά και τις όποιες καθημερινές δραστηριότητες εργασίας ή ρουτίνας του πληθυσμού, με απίστευτες συνέπειες ή παρενέργειες.

Αντίστοιχες ενέργειες με συναφή επακόλουθα μπορεί να προκληθούν σε άλλες κρίσιμες υποδομές όπως οι τηλεπικοινωνίες, η ύδρευση, το χρηματοπιστωτικό (δια-τραπεζικό) σύστημα, οι συγκοινωνίες, κλπ.

Κάτω από αυτές τις συνθήκες ο «αντίπαλος» καθίσταται ευάλωτος σε πολλά και διαφορετικά μέτωπα ή επίπεδα, καθότι καλείται να αντιμετωπίσει εκτός της πολλαπλής εσωτερικής αστάθειας στην συγκεκριμένη περιοχή και ότι αυτή επηρεάζει, ταυτόχρονα με την οποιαδήποτε άλλη/ες «απειλή/ες», όπου και όποτε ενδεχομένως εκδηλωθεί. Κι αυτό από μόνο του, συνιστά μια ασύμμετρη απειλή αν όχι την κυριότερη από αυτές που μπορεί να είναι συνδυασμός «Κυβερνοπολέμου», με παράλληλη χρήση όπλων νέας τεχνολογίας όπως τα βουβά ή σιωπηλά όπλα (silent weapons).

Εδώ διαφαίνεται η αξία της «ετοιμότητας» με την αμεσότητα αντίδρασης ή/και αντι-αντίδρασης, χωρίς τη γενίκευση του συναγερμού (και του πανικού που θα ρυμουλκήσει), αλλά την δυνατότητα αντιμετώπισής του σε τοπικό επίπεδο, ως καθημερινό «περιστατικό» ή συμβάν, ταυτόχρονα με παράλληλη κατακόρυφη και οριζόντια ενημέρωση και ετοιμότητα αντίδρασης. Αυτό συνάδει με μια διαρκή κατάσταση αναμονής η οποία δεν είναι παθητική στάση, αλλά ενεργητική δηλ. στάση επιχειρησιακής ετοιμότητας, διότι έχει συνεχώς την κουλτούρα κι εναλλαγή αντιμετώπισης οποιουδήποτε περιστατικού ήθελε παρουσιαστεί (βλ. Incident Response Capabilities).

Η παραπάνω διαδικασία διαφαίνεται απλοϊκή, εφόσον αντιμετωπίζεται καθημερινά σε επίπεδο τρέχουσας διαδικασίας ή εργασίας από το αρμόδιο προσωπικό, το οποίο παράλληλα εκπαιδεύεται επ' έργω (on the job training), χωρίς να διακατέχεται από το άγχος του αιφνιδιασμού και του αποτελέσματος των ενεργειών, διατηρώντας νηφαλιότητα, ψυχραιμία, αυτοπεποίθηση και επάρκεια αντιμετώπισης και ελέγχου της όποιας κατάστασης. Η συνήθεια αντιμετώπισης «περιστατικών εισβολών» σε τρέχουσα βάση, οποιαδήποτε ώρα του 24ώρου, επαυξάνει εκθετικά την αποτρεπτική ικανότητα του συνόλου (ανθρώπων – διαδικασιών – μηχανισμών ελέγχου των καταστάσεων), και δημιουργεί ηθικό έρισμα και συνείδηση ετοιμότητας. Παράλληλα δημιουργεί και συνθέτει ένα πολυδιάστατο υπόβαθρο διαδικασιών ελέγχου ασφαλείας, παρασύροντας σ' αυτό και παράπλευρους τομείς πάσης φύσεως δραστηριοτήτων, οι οποίοι επηρεάζουν ούτως ή άλλως τη ζωή και ευημερία του τόπου.

Η ικανότητα συντεταγμένης, άμεσης και συμπαγούς αντίδρασης, ταυτόχρονα από πολλούς διαφορετικούς μηχανισμούς, διαμορφώνει εκτός από πνεύμα ή κουλτούρα ασφάλειας σε πολλούς, ένα ικανό «πλέγμα διαδικασιών ασφάλειας», οι οποίες περιβάλουν τις καθημερινές συνθήκες ζωής, δραστηριοτήτων και συνηθειών της κοινωνίας στο σύνολό της, διαχέοντας σιγουριά κι αισιοδοξία.

Επιπλέον, έμμεσα πλην σαφώς «πιέζουν» κι άλλους τομείς δραστηριοτήτων να ενταχθούν ενεργά στη θέσπιση και ακολουθία κοινών κανόνων ασφαλείας υπό ενιαία διοίκηση και έλεγχο.

Ακόμα, στον Κυβερνοπόλεμο, η απόσταση δεν έχει ουσιαστικά νόημα και γι' αυτό το λόγο η προσέγγισή πρέπει να είναι τοπολογική. Στην πραγματικότητα και την πράξη, αυτό που έχει σημασία είναι καθαρά ο χρόνος. Και στην κρυπτασφάλεια ο χρόνος είναι ο σημαντικός και κυρίαρχος παράγοντας, γιατί η ασφάλεια έχει ημερομηνία λήξης, αφού κάθε κώδικας σπάζεται και το σπάσιμο είναι αποκλειστικά θέμα χρόνου. Κατά συνέπεια δεν υπάρχει λόγος να αναζητούμε την πληρότητα.

Επειδή στον «Κυβερνοπόλεμο» δεν υπάρχει γραμμικότητα στην εξέλιξη αλλά ούτε και συνέχεια, η ασυνέχεια δημιουργεί προβλήματα στις προβλέψεις. Επίσης, επειδή ο «Κυβερνοπόλεμος» λειτουργεί ως «*Ασύμμετρη Απειλή*» που έχει ελάχιστο κόστος, δεν

επαρκούν ενδιάμεσες λύσεις. Όποιες δε επιλεγούν και εφαρμοσθούν, πρέπει να είναι ταυτόχρονα έξυπνες, αλλά και αποτελεσματικές. Αυτό δεν σημαίνει απαραίτητα ότι χρειάζονται μεγάλα ή/και ακριβά σε οικονομικό επίπεδο μέσα. Πρώτα πρέπει να αντιμετωπίσουμε την νοητική αδράνεια και ν' αναζητήσουμε την καινοτομία, η οποία βασίζεται στην προσαρμοστικότητα και στην πλαστικότητα του εγκεφάλου μας. Έχει σημασία λοιπόν να αναπτύξουμε την στρατηγική μας και να μάθουμε πώς να μαθαίνουμε για να μπορέσουμε όχι μόνο να ανταποκριθούμε αλλά να έχουμε ανάδραση και ανθεκτικότητα στις επιθέσεις. Διότι, δεν έχει αξία μόνο η επίθεση, αλλά και το πώς καταφέρνεις και κρατάς μια θέση σε βάθος χρόνου. Η διαχρονικότητα είναι ο μόνος τρόπος να είσαι αξιόπιστος στον «Κυβερνοπόλεμο» γιατί αποδεικνύεις με τρόπο βιωματικό ότι ξέρεις να επιβιώσεις και σε εχθρικό περιβάλλον. Συνεπώς μπορείς να περάσεις και στην αντεπίθεση, η οποία είναι η καλύτερη επίθεση, αφού έχει όλα τα δεδομένα.

Έτσι ο «Κυβερνοπόλεμος» σχετίζεται άμεσα με τη νοημοσύνη και δεν υπάρχει λόγος να θεωρούμε ότι δεν μπορούμε να παίξουμε ένα ρόλο ακόμα και αμυντικό για να προστατέψουμε τις αξίες μας.

Εκτίμηση Κινδύνων (Risk Assessment)

Εδώ υπεισέρχεται ένας όρος υπό την έννοια της διαρκούς διαδικασίας εκτίμησης – επανεκτίμησης των συνθηκών, που συνθέτουν τους κινδύνους που διατρέχει οποιαδήποτε χρονική στιγμή, η οντότητα, αυτοτέλεια, αλλά και απρόσκοπτη λειτουργία της κάθε μιας κρίσιμης υποδομής της χώρας. Συνίσταται και αποτελεί αλληλένδετο μέρος, μαζί με την ετοιμότητα αντίδρασης σε κάθε περίπτωση, της συνολικής ικανότητας αποτροπής κρίσεων σε οποιοδήποτε επίπεδο, εφόσον οι μηχανισμοί και διαδικασίες που υποστηρίζουν την αδιάλειπτη 24ωρη λειτουργία της, λειτουργούν στο πνεύμα των παραπάνω αναφερθέντων προϋποθέσεων λειτουργικής ετοιμότητος.

Η ρευστότητα των συνθηκών σε τρέχουσα βάση επιβάλλει τη διαμόρφωση περιβάλλοντος διαρκούς σταθερότητας και ασφάλειας, το οποίο προδιαγράφει η ικανότητα και επάρκεια του προσωπικού που διαχειρίζεται κάθε κρίσιμη υποδομή ή το πληροφορικό σύστημα (ΠΣ) ελέγχου της, σε αδιάλειπτη 24ωρη βάση.

Συνοψίζοντας, οι Κρίσιμες Υποδομές μιας χώρας διαχειρίζονται από ΠΣ, τα οποία θα πρέπει να είναι εξασφαλισμένα από κάθε περίπτωση εισβολών που θα δεχθούν, μέσα από τις χαώδεις διαστάσεις του διαδικτύου (Internet), στο οποίο επ’ ουδενί τρόπω ή χρόνω, δεν πρέπει να διασυνδέονται. Ούτως ή άλλως αυτές καθ’ αυτές αποτελούν «στόχο» σε κάθε επιτήδειο (hackers επιστρατευμένοι από μυστικές υπηρεσίες κρατών κι όχι μόνο αλλά και crackers), ο οποίος διαθέτει την απαραίτητη τεχνογνωσία (know how) προκειμένου να τις προσβάλλει, χωρίς να αφήσει ψηφιακά ίχνη.

Η μέχρι σήμερα εμπειρία μας απέδειξε ότι ο μεγαλύτερος κίνδυνος εντοπίζεται στον πυρήνα (κέντρο ελέγχου) του κάθε συστήματος, παρά στην περιφέρεια («περιμετρική» ασφάλεια-υποσυστήματα), η οποία ελέγχεται ούτως ή άλλως από αυτόν. Κι αυτό εστιάζεται στην υπερεκτίμηση των μέσων, των δυνατοτήτων ή/και κτηθέντων γνώσεων, αλλά και την διαρκή επανάληψη, η οποία πολλές φορές μεταπίπτει σε «ρουτίνα» που ρυμουλκεί ο ανθρώπινος παράγοντα, με ότι αυτό συνεπάγεται.

Ούτως ή άλλως η διασφάλιση των Κρισίμων Υποδομών εδράζεται σε ΠΣ, τα οποία κάτω από ανθρώπινη διαχείριση, εξασφαλίζουν την σε 24ωρη βάση αδιάλειπτη παροχή υπηρεσιών, μέσων, δυνατοτήτων ή αγαθών, που απαιτεί η εύρυθμη λειτουργία κάθε σύγχρονης ευνομούμενης και ευημερούσας κοινωνίας.

Άρα αυτές θα πρέπει να θωρακίζονται δυναμικά (κι όχι στατικά) από συνδυασμό συστημάτων, διαδικασιών και προσωπικού, με κατάλληλη συγκρότηση κι εξειδίκευση, αλλά και απαιτούμενου αριθμού επάνδρωσης κι εναλλακτικής (εξ)υπηρέτησης, συνεχή επικαιροποίηση, εστιασμένα στο διαρκές αποτρεπτικό αποτέλεσμα.

Ιωάννης Α. Κολομβάκης
Ταξχος (ΕΠ) ε.α.
Μηχ/κος Δικτύων-MSc
Μέλος ΕΛΙΣΜΕ
i.kolomvakis@yahoo.gr

Πηγές

1 «Ασφάλεια Πληροφοριακών Συστημάτων» Σ. Κάτσικας – Δ. Γκρίτζαλης – Σ. Γκρίτζαλης Εκδόσεις Νέων Τεχνολογιών 2004.
2 «Ψηφιακή Εγκληματικότητα Η ανασφαλής όψη του Διαδικτύου» Χρ. Τσουραμάνης, Εκδόσεις Βασ. Ν. Κατσαρού 2005.
3 «Η Τέχνη της Απάτης» Κέβιν Μίτνικ – Ουίλιαμ Σάιμον, Εκδόσεις Ωκεανίδα 2006
4 Διδακτορική Διατριβή «Η Επανάσταση στις Σύγχρονες Στρατιωτικές Εξελίξεις (Revolution In Military Affairs – RMA)» Κώστας Γρίβας 2004.
5 Ατομική Εργασία «Ο Κυβερνοπόλεμος» Ανχης (ΕΠ) Ιωάννης Α. Κολομβάκης – Σχολή Εθνικής Ασφάλειας Οκτ 2006.
6 «Γεωπολιτική Προσέγγιση για ένα νέο Ελληνικό Αμυντικό Δόγμα» Ι. Μάζης Εκδόσεις Παπαζήση 2006.
7 «Critical Foundations Protecting America's Infrastructures» The Report of the President's Commission on Critical Infrastructure Protection October 1997.
8 «Threat & Vulnerability Model for Information Security» The Report of the President's Commission on Critical Infrastructure Protection 1997.
9 «Security in the Information Age: New Challenges, New Strategies» The Joint Economic Committee United States Congress 2002.
10 «Vulnerability Assessment Framework» Critical Infrastructure Assurance Office 1998.
11 «National Strategy for Critical Infrastructure and Cyberspace Security» Information & Communication Sector National Strategy Input May 2002.
12 «Defending America's Cyberspace National Plan for Information Systems Protection» White House 2000.
13 «The National Strategy to Secure Cyberspace» February 2002.
14 Computer Incident Response Capabilities (CIRC) NATO, Brussels Belgium 2004.
15 Computer Emergency Response Team (CERT) NATO, Brussels Belgium 2005.
16 Cyber Defense Exercises NATO, Krakow Poland 2005.
17 www.lygeros.org
18 Βασικές Αρχές Ασφάλειας Δικτύων, Εφαρμογές & Πρότυπα William Stallings © 2008
19 Διαχείριση Έργων Πληροφορικής Δρ Ευάγγελος Κιουντούζης Καθηγητής ΟΠΑ