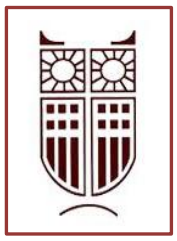
ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES



ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ ΑΣΦΑΛΕΙΑΣ»

Κυβερνοπόλεμος και Ελληνικές ΕΔ: Παρούσα κατάσταση, μελλοντικές προοπτικές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Στέργιος Αναστασιάδης

Αθήνα, 2019

Τριμελής Επιτροπή

Χαράλαμπος Παπασωτηρίου, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)

Κωνσταντίνος Κολιόπουλος, Καθηγητής Παντείου Πανεπιστημίου

Κώστας Υφαντής, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου

Στη γυναίκα μου και στα τρία μου αγόρια
που αποτελούν την πηγή ενέργειας σε ό,τι πράττω στη ζωή μου.

Σελίδα σκόπιμα κενή

Συντομογραφίες

ΣΕΠ	Συστημάτων Επικοινωνιών και Πληροφορικής
ΣΚΑΚ	Στρατιωτικό Κέντρο Αντιμετώπισης Κυβερνοπεριστατικών
ΣΠΗΥ	Σχολή Προγραμματιστών Ηλεκτρονικών Υπολογιστών
ΤΠ	Τεχνολογία Πληροφορικής
CCD-CoE	Cooperative Cyber Defense Center of Excellence
CERT	Computer Emergency Response Team
CIS	Communication and Information Systems
CISA	Cyber security and Infrastructure Security Agency
CSIRT	Computer Security Incident Response Team
CSOC	Cyber Security Operations Center
DDoS	Distributed Denial of Service
DoS	Denial of Service or Destruction –
ENISA	European Network and Information Security Agency
ICT	Information and communications technology
IP	Internet Protocol
NCIA	NATO Communications and Information Agency
NCIRT	NATO Computer Incident Response Team
NIS	Network and Information System
NPPD	National Protection and Programs Directorate
PLC	Programmable Logic Controller
SCADA	System Control and Data Acquisition

Περιεχόμενα

Κεφάλαιο Δεύτερο

Έννοια και στοιχεία κυβερνοπολέμου

Κεφάλαιο Τρίτο

Κυβερνοπόλεμος και Εθνική Ασφάλεια

Κεφάλαιο Τέταρτο

ΝΑΤΟ και Κυβερνοπόλεμος

Κεφάλαιο Πέμπτο

Ελλάδα και Κυβερνοπόλεμος

Περίληψη

Η παρούσα εργασία αναλύει το φαινόμενο του Κυβερνοπολέμου, ως ένα βασικό παράγοντα της σχεδίασης και διεξαγωγής των σύγχρονων επιχειρήσεων, εστιάζοντας στην παρούσα ελληνική πραγματικότητα και τις μελλοντικές προοπτικές της στο πεδίο αυτό.

Αρχικά αναφέρονται βασικές έννοιες που σχετίζονται με τις Κυβερνοεπιθέσεις, τα μέσα με τα οποία αυτές εκδηλώνονται και τους κύριους σκοπούς που μπορεί να εξυπηρετήσουν. Δεν κρίνεται σκόπιμο να εμβαθύνω στο σημείο αυτό καθώς πρόκειται κυρίως για τεχνικούς όρους. Το κεφάλαιο καταλήγει στις παράθεση πραγματικών περιστατικών, ώστε να μπορέσει ο αναγνώστης να αντιληφθεί τον επικείμενο κίνδυνο που διατρέχει ο εκάστοτε κρατικός ή μη δρών.

Συνεχίζοντας η μελέτη αναφέρεται στον Κυβερνοπόλεμο, στα χαρακτηριστικά του και στο τεχνολογικό πλαίσιο του πολέμου. Τέλος αναφέρονται ενδεικτικά οι θέσεις μερικών εκ των επικρατέστερων κρατικών δρώντων στο χώρο του Κυβερνοπολέμου, σε παγκόσμιο επίπεδο.

Το επόμενο κεφάλαιο διαπραγματεύεται την έννοια του Κυβερνοπολέμου σαν τμήμα της Πολιτικής Εθνικής Ασφάλειας. Επικεντρώνεται στο θεσμικό πλαίσιο του Κυβερνοπολέμου στους σκοπούς που εξυπηρετεί και στις κρίσιμες κρατικές και ιδιωτικές υποδομές, οι οποίες αποτελούν τους κύριους στόχους του.

Το ΝΑΤΟ και ο Κυβερνοπόλεμος αποτελούν το θέμα της επόμενης ενότητας, η οποία μας δίνει μια γενική εικόνα για τη γενική στρατηγική της συμμαχίας απέναντι στη σύγχρονη αυτή απειλή. Εδώ επίσης αναφέρεται η έννοια της ενεργητικής άμυνας που αποτελεί την νεότερη επικρατούσα επιχειρησιακή αντίληψη, η οποία έχει ήδη υιοθετηθεί από τις ΗΠΑ.

Η εργασία στη συνέχεια πραγματεύεται θέματα που άπτονται του Ελληνικού ενδιαφέροντος, καθώς διανύουμε μια χρονική περίοδο όπου ‘’γράφεται ιστορία’’ στο χώρο του Κυβερνοπολέμου στη χώρα μας. Αναφέρεται αρχικά στο εντελώς νέο νομοθετικό πλαίσιο που πλέον αναθέτει το έργο της αποκλειστικής αντιμετώπισης κυβερνοπεριστατικών στη ΓΕΕΘΑ/ΔΙΚΥΒ. Στη συνέχεια αναλύονται δύο θεσμικά κείμενα που περιγράφουν τη στρατηγική Κυβερνοπολέμου των Ελληνικών ΕΔ και καταλήγει στην παρουσίαση της νέας ΓΕΕΘΑ/ΔΙΚΥΒ. Επισημαίνονται δε οι σημαντικότατες εξελίξεις που έχουν δρομολογηθεί στο Ελληνικό περιβάλλον.

Στο επόμενο κεφάλαιο κρίθηκε σκόπιμο να αναφερθούν περιληπτικά οι

δυνατότητες Κυβερνοπολέμου της γείτονος και των εγγύς γειτονικών καρτών. Διαφαίνεται το πόσο μεγάλη σημασία έχει δώσει η Τουρκία στην αμυντική θωράκιση των κρίσιμων υποδομών της από επιθέσεις Κυβερνοπολέμου, καθώς και η προτεραιότητα της Κυβέρνησης να καταστήσουν τη χώρα παγκόσμια δύναμη στο νέο αυτό πεδίο πολέμου.

Τέλος παραθέτονται συμπεράσματα που εξήλθαν από τη συγγραφή του παρόντος πονήματος και καταθέτονται προτάσεις που θεωρώ ότι είναι προς την κατεύθυνση αναβάθμισης των Ελληνικών ΕΔ στο κρίσιμο πεδίο του Κυβερνοπολέμου, η οποία κρίνεται απαραίτητη στο σύγχρονο περιβάλλον που καλούνται να επιχειρούν.

Λέξεις-κλειδιά: Κυβερνοπόλεμος, Κρίσιμες Υποδομές, Διοίκηση Κυβερνοπολέμου, Νομοθετικό πλαίσιο Κυβερνοπολέμου, Κυβερνοάμυνα

Cyberwar and Greek Armed Forces: Present situation, future prospects

Stergios Anastasiadis

Abstract

The present work analyzes the phenomenon of cyber warfare as a key factor in the design and development of modern business, focusing on the present Greek reality and its future prospects in this field.

Initially, basic concepts related to Cyber Attacks are mentioned, the means by which they are manifested, and the main purposes they may serve. It does not seem appropriate to delve deeper into this point as it is mainly about technical terms. The chapter concludes with a list of facts so that the reader can understand the imminent danger of the state or non-state actors are.

Continuing the study refers to the cyberwar, its characteristics and the technological context of the war. Last but not least, the positions of some of the most dominant government actors in the field of cyber warfare at global level are mentioned.

The next chapter discusses the concept of cyber warfare as part of National Security Policy. It focuses on the institutional context of the cyber warfare for the purposes it serves and the critical public and private infrastructure, which are its main objectives.

NATO and the Cyber War is the subject of the next section, which gives us an overview of the alliance's overall strategy against this modern threat. Also what mentioned here is the concept of active defense, which is the newest dominant business concept already, adopted by the US.

The work then deals with issues of Greek interest as we go through a period where 'history is being written' in the cyber war in our country. It refers first to the completely new legislative framework that now entrusts the task of exclusively addressing cyber incidents to National Defence/Cyberwarfare Command. Following there are two institutional texts that outline the Hellenic Armed Force’s Cyber Warfare strategy and conclude with the presentation of the new National Defence/Cyberwarfare Command The most significant developments in the Greek environment are highlighted.

In the next chapter, it is appropriate to summarize briefly our Neighborhood’s and near neighbors’ states Cyber War possibilities. It is clear depicted how important

Turkey has been in defending its critical infrastructures from cyberattacks, as well as the government's priority to make the country a global force in this new field of war.

Finally, conclusions are drawn from the writing of this article and proposals are put forward which I believe are in the direction of upgrading the Greek Armed Forces in the critical field of Cyberwar, which is deemed necessary in the modern environment that they are called upon to operate.

Keywords: Cyber War, Critical Infrastructure, Cyber Warfare Command, Cyberwar Legislative Framework, Cyber Defense

Εισαγωγή

> …δεν υπάρχουν πλέον αυτοκίνητα, δεν υπάρχουν πλέον αεροπλάνα, δεν υπάρχουν πλέον ακουστικά βαρηκοΐας. Υπάρχουν υπολογιστές με τέσσερις τροχούς, υπολογιστές με φτερά και υπολογιστές που σε βοηθάνε να ακούς[1]

Το επιχείρημα αυτό που ίσως σε κάποιους να ακούγεται ως υπεραπλουστευμένη προσέγγιση ενός πολύπλοκου θέματος, της διείσδυσης των υπολογιστών σε κάθε έκφανση της καθημερινότητας, αποτελεί προϊόν συζήτησης μεταξύ του πρωταγωνιστή της υπόθεσης, ορισμένοι το χαρακτήρισαν «σκάνδαλο» Wikileaks, Julian Assange και ορισμένων εκ των συνεργατών του. Είναι πράγματι εξαιρετικά δύσκολο να φανταστούμε τη ζωή μας χωρίς την παρουσία υπολογιστών.

Από την εμφάνιση του Διαδικτύου και έπειτα, νέοι όροι άρχισαν να εμφανίζονται με καταιγιστικό ρυθμό στη ζωή μας αφού η επικοινωνία δια μέσω την υπολογιστών ήταν πλέον καθημερινότητα. Οι περισσότεροι από αυτούς έχουν τεχνική αφετηρία, σε μια προσπάθεια να ακολουθήσουν την εξέλιξη της ίδιας της τεχνολογίας των υπολογιστικών συστημάτων και των τεχνολογιών δικτύωσης. Όπως χαρακτηριστικά αναφέρει ο Jeremie Zimmermann, συνιδρυτής και εκπρόσωπος της ομάδας υποστήριξης πολιτών La Quadrature du Net.[2]«όλα όσα έγιναν στο διαδίκτυο απλά εκτινάχθηκαν από εκεί που ήταν άγνωστα πριν λίγους μήνες ή λίγα χρόνια, άρα δεν μπορείς να προβλέψεις ποια θα είναι η επόμενη καινοτομία και η εξέλιξη της καινοτομίας είναι τόσο γρήγορη, ώστε είναι πολύ πιο γρήγορη από τη διαδικασία δημιουργίας πολιτικής».[3] Το ίδιο το Διαδίκτυο αποτελεί κομβικής σημασία έννοια. Ως Διαδίκτυο νοείται κάθε συνένωση δύο ή περισσότερων δικτύων, όχι κατ' ανάγκη ίδιας τεχνολογίας, έτσι ώστε να επιτυγχάνεται η επικοινωνία μεταξύ τους και να λειτουργούν σε λογικό επίπεδο, σαν ένα δίκτυο. Αρχικά τα δίκτυα ήταν απομονωμένα και κατά συνέπεια πρόσφεραν σημαντική προστασία από κακόβουλους χρήστες. Η ανάπτυξη της πληροφορικής όμως, καθώς και η ανάγκη να γίνουν όλες αυτές οι υπηρεσίες προσιτές στον πολίτη, σε συνδυασμό με τη χρήση της νέας τεχνολογίας, τα κατέστησε ευρέως προσβάσιμα οδηγώντας μοιραία στην αύξηση της τρωτότητάς τους.

---

[1] Julian Assange and others, *Cypherpunks, Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των WikiLeaks,* Αθήνα, Ποιότητα, 2013

[2] La Quadrature du Net: http://laquadrature.net, ευρωπαϊκή οργάνωση που υπερασπίζεται τα δικαιώματα της ανωνυμίας στο διαδίκτυο.

[3] Julian Assange and others, *Cypherpunks, Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των WikiLeaks,* Αθήνα, Ποιότητα, 2013

Οι πόλεμοι, όπως ήταν φυσιολογικό, ήταν ανάμεσα στις δράσεις του ανθρώπου που επηρεάστηκαν πρωτίστως από τη ραγδαία αυτή τεχνολογική ανάπτυξη. Οι πόλεμοι δε των τελευταίων δεκαετιών δεν περιορίστηκαν στο φυσικό πεδίο αλλά σταδιακά επεκτάθηκαν και στο δικτυακό, με αποτέλεσμα σήμερα να αναμένουμε ότι ο επόμενος πόλεμος θα είναι κυρίως, αν όχι μόνο, δικτυακός. Τα δίκτυα και τα συστήματα των υπολογιστών αποτελούν τις πραγματικές λεωφόρους της σύγχρονης οικονομίας, στις οποίες διακινείται η πολυτιμότερη πρώτη ύλη του σύγχρονου κόσμου: η πληροφορία. Παράλυση της ροής των πληροφοριών οδηγεί αυτομάτως σε οικονομική κατάρρευση. Αυτός είναι άλλωστε και ο στόχος των πολεμιστών του κυβερνοχώρου, που ξεκίνησαν ως χάκερς αλλά θα καταλήξουν πραγματικοί κυβερνοπολεμιστές.

Σκοπός

Σκοπός της παρούσης εργασίας, αρχικά είναι να διερευνηθούν οι απειλές και η ασφάλεια στο σύγχρονο και δυναμικά εξελισσόμενο διαδικτυακό περιβάλλον. Η ασφάλεια του διαδικτύου εξετάζεται σε συνδυασμό με τις δυνατότητες προσβολής μέσω κυβερνοεπιθέσεων, τόσο στις κρίσιμες υποδομές, όσο και στις ένοπλες δυνάμεις της χώρας.

Επιδιώκεται να αποτυπωθεί η υφιστάμενη δυνατότητα αντίδρασης των ενόπλων δυνάμεων σε μια τέτοιου είδους απειλή λαμβάνοντας προληπτικά μέτρα ασφαλείας. Επιπλέον θα προσπαθήσω να διαπιστώσω την τρέχουσα εθνική κατάσταση στο πεδίο του Κυβερνοπολέμου, τις προοπτικές για μελλοντική εξέλιξη, καθώς και τις επερχόμενες προκλήσεις που θα πρέπει να ολοκληρώσουν οι Ελληνικές ένοπλες δυνάμεις στον ευαίσθητο αυτό τομέα.

Προϋποθέσεις

Για τη σύνταξη της διατριβής τέθηκαν οι παρακάτω προϋποθέσεις:

α. Η υφιστάμενη συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το διαδίκτυο αλλά και το μεγαλύτερο ποσοστό των εμπορικών δικτύων, είναι το TCP/IP[4] και δεν θ' αλλάξει στο εγγύς μέλλον.

β. Τα διεθνές νομικό πλαίσιο που ασχολείται με τα θέματα του διαδικτύου, θα εξακολουθήσει να εφαρμόζεται με υστέρηση σε σχέση με τη τεχνολογική εξέλιξη, ενώ τα επιμέρους εθνικά νομικά πλαίσια θα συνεχίσουν να έχουν σημαντικές διαφοροποιήσεις σε συνάρτηση με την τεχνολογική και οικονομική ανάπτυξη των κρατών που τα εκπονούν.

γ. Η κακόβουλη χρήση του διαδικτύου από εθνικούς και μη δρώντες θα εξακολουθήσει να υφίσταται και μάλιστα με εντονότερους ρυθμούς, καθιστώντας την προστασία των δικτυακών υπολογιστών όλο και δυσκολότερο επίτευγμα.

δ. Η δικτύωση που έχει αναπτυχθεί, τόσο στις κρίσιμες υποδομές της σύγχρονης κοινωνίας, όσο και στις ένοπλες δυνάμεις των κρατών και ειδικότερα της χώρας μας, θα συνεχίσει να αυξάνεται.

ε. Οι πολύ σημαντικές εξελίξεις που λαμβάνουν χώρα σε εθνικό επίπεδο, την περίοδο που εκπονείται αυτή η εργασία, θα έχουν ολοκληρωθεί μέσα στα προβλεπόμενα χρονικά περιθώρια που έχουν τεθεί.

[4] Transmission Control Protocol/Internet Protocol, Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου

Κεφάλαιο Πρώτο
Γενικά

1.1 Ιστορική ανασκόπηση

Αν γνωρίζεις τον εχθρό και τον εαυτό σου, δεν χρειάζεται να φοβάσαι για την έκβαση εκατό μαχών[5]

Η αξία των πληροφοριών στην έκβαση μιας αναμέτρησης δεν αμφισβητήθηκε από κανέναν στο βάθος των αιώνων. Αντίθετα οι αυτοκρατορίες που άντεξαν περισσότερο διαχρονικά (Μογγόλοι, Κινέζοι) διέθεταν ιδιαίτερες υπηρεσίες που είχαν ως αποστολή τη συλλογή, επεξεργασία και εκμετάλλευση των κάθε είδους πληροφοριών.

Ενώ η φυσική παρουσία στην περιοχή ενδιαφέροντος ήταν αρχικά απαραίτητη προϋπόθεση για τη συλλογή των πληροφοριών, η εξέλιξη της τεχνολογίας αποκάλυψε νέους τρόπους δράσης που εξασφάλισαν την ασφάλεια και κυρίων την ανωνυμία των εκάστοτε δρώντων.

Η ανακάλυψη δε του ηλεκτρονικού υπολογιστή, μείωσε κατά πολύ τους χρόνους επεξεργασίας των δεδομένων, ενώ παράλληλα επέτρεψε την αποθήκευση μεγάλου όγκου πληροφοριών σε ηλεκτρονικά μέσα. Όσο οι υπολογιστές αυτοί ήταν απομονωμένοι, μοναδικός τρόπος υποκλοπής πληροφοριών ήταν, όπως και παλαιότερα, η φυσική παρουσία στο χώρο όπου ήταν εγκατεστημένοι. Αυτό όμως μπορούσε εύκολα να αντιμετωπιστεί βελτιώνοντας τα μέτρα φυσικής ασφάλειας, οπότε οι μέθοδοι συλλογής πληροφοριών, θα έλεγε κανείς ότι ελάχιστα άλλαξαν.

Αυτό που έφερε την τεράστια αλλαγή στον τομέα της ασφάλειας των πληροφοριών ήταν η εμφάνιση των πρώτων δικτύων ηλεκτρονικών υπολογιστών. Αυτή η διασύνδεση έδινε τη δυνατότητα στον χρήστη του κάθε υπολογιστή να έχει πρόσβαση σε όλες τις πληροφορίες του δικτύου, είτε τοπικά, είτε στους διακομιστές του. Έτσι λοιπόν ήταν ευκολότερο για κάποιον να υποκλέψει πληροφορίες χωρίς να είναι καν παρόν. Μπορούσε ένας χρήστης που βρισκόταν στην Ευρώπη να υποκλέψει στοιχεία που ήταν αποθηκευμένα σε κάποιο δίκτυο της Αμερικής και το αντίστροφο.

[5] Ρένα, Λέκκου, Δάντου, Sun Tzu, *The Art of War*, Αθήνα, Περίπλους, 2007

1.2 Κυβερνοχώρος (Cyberspace)

Ο Κυβερνοχώρος είναι ένα παγκόσμιο πεδίο (global domain) εντός του πληροφοριακού περιβάλλοντος αποτελούμενος από ένα δίκτυο αλληλεξαρτώμενων και διασυνδεδεμένων υποδομών πληροφοριακής τεχνολογίας, των δικτύων τηλεπικοινωνιών, συστημάτων πληροφορικής και ενσωματωμένων επεξεργαστών (processors) και ελεγκτών (controllers)[6].

Εντός αυτού του κατασκευασμένου από τον άνθρωπο πεδίου βρίσκονται διασυνδεδεμένα επικοινωνιακά και πληροφοριακά δίκτυα, στα οποία είναι αποθηκευμένες παντός είδους πληροφορίες και όπου συνδέονται οι υποδομές όλων των χωρών, όπως επίσης και ο «κόσμος» που δημιουργείται γύρω τους (εκπομπές από ασύρματα δίκτυα, χειριστές, προγραμματιστές, ερευνητές και καθηγητές που διδάσκουν σχετικά αντικείμενα). Μέσω του Κυβερνοχώρου διεξάγεται προοδευτικά όλο και μεγαλύτερο μέρος της ανθρώπινης δραστηριότητας.[7]

Ουσιαστικά θα μπορούσε να θεωρηθεί ως ένας ψηφιακός κόσμος, που παράγεται από τους υπολογιστές και τα δίκτυα υπολογιστών, στους οποίους οι άνθρωποι και οι υπολογιστές συνυπάρχουν και που περιλαμβάνει όλες τις διασυνδεμένες δραστηριότητες. Το διαδίκτυο λοιπόν έχει οδηγήσει σε μία απίστευτη έκρηξη της ποσότητας πληροφοριών που είναι διαθέσιμες στο κοινό. Οι πληροφορίες αυτές είναι, μαζί με την τεχνική υποδομή του διαδικτύου, τα βασικά συστατικά μέρη του λεγόμενου κυβερνοχώρου (cyberspace). Ο κυβερνοχώρος, σύμφωνα με τον Timothy Luke, είναι ο αποκλειστικός χώρος της ψηφιακής πληροφορίας.[8] Πρόκειται για ένα σύμπαν δεδομένων χωρίς όρια που διαπερνά κάθε φυσικό περιορισμό. Οι άνθρωποι μπορούν να επικοινωνούν και να αλληλεπιδρούν ανεξάρτητα της ώρας και της τοποθεσίας τους.[9] Βέβαια, πρόκειται επίσης για έναν χώρο στον οποίο δεν υπάρχει καμιά υπέρτατη ρυθμιστική αρχή, εκτός ίσως από κάποιες αρχές με χαμηλού επιπέδου τεχνικές αρμοδιότητες. Υπό αυτή την έννοια, ο κυβερνοχώρος έχει αρκετά κοινά σημεία με την άναρχη κοινωνία του HedleyBull. Το ποιος ελέγχει ποιόν, τι υπακούει σε ποιους κανόνες και που αρχίζουν και που τελειώνουν οι όποιοι κανόνες, παραμένει αναπάντητο ερωτηματικό.

---

[6] ΠαΔ 1-26/2019 περί *Διαχείρισης Ασφαλείας Πληροφοριακών Συστημάτων και Τοπικών Δικτύων Δεδομένων*

[7] Κατευθυντήριο πλαίσιο ανάπτυξης κυβερνοάμυνας στις ΕΔ, ΓΕΕΘΑ, ΔΙΚΥΒ, 2013

[8] Timothy W. Luke, *Cyberspace as Meta Nation: The Net Effects of Online E Publicanism*, Alternatives: Global, Local, Political 26, 2001

[9] Στο ίδιο

Ο Κυβερνοχώρος αποτελείται από το σύνολο των παγκόσμιων δικτύων υπολογιστών (συμπεριλαμβανομένου και του Internet) και των περιφερειακών μηχανημάτων (εξυπηρετητές, δρομολογητές, μόντεμ, εκτυπωτές, ενσύρματες και ασύρματες γραμμές κλπ), 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 διοίκησης και ελέγχου, δίκτυα οπλικών συστημάτων όπως αρμάτων, αεροσκαφών, πολεμικών πλοίων, δορυφόρων κλπ) αλλά και το σύνολο των μεμονωμένων ηλεκτρονικών υπολογιστών που δεν είναι συνδεδεμένοι σε κανένα δίκτυο.

Ο κυβερνοχώρος αναφέρεται και ως ο "πέμπτος κοινός χώρος" μετά το έδαφος, τη θάλασσα, τον αέρα και το διάστημα.[10] Αντιλαμβανόμαστε λοιπόν ότι είναι κάτι πολύ ευρύτερο του Internet, το οποίο άλλωστε είναι ένα μόνο από τα στοιχεία του κυβερνοχώρου. Επίσης, η αλληλεξάρτηση και η αλληλεπίδραση τόσο πολλών και ενίοτε ετερόκλητων στοιχείων όπως οι τράπεζες και οι ένοπλες δυνάμεις, καταδεικνύουν ακριβώς την ιδιαίτερη υπόσταση του κυβερνοχώρου.

Για τον έλεγχο του κυβερνοχώρου, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, γίνεται μια μάχη διαρκείας. Η μάχη αυτή μπορεί να προσομοιαστεί με τις μάχες του παρελθόντος για τα νέα εδάφη ή, αργότερα, για τις μάχες επικράτησης και ελέγχου των πρώτων υλών ή, τέλος, τις μάχες για την εξασφάλιση φθηνού εργατικού δυναμικού. Το μήλο της έριδος στην μάχη επικράτησης του κυβερνοχώρου είναι η πληροφορία. Αυτή ακριβώς η πληροφορία και η διαχείρισή της είναι που, σχεδόν πάντα αποτελεί τον στόχο των κυβερνοεπιθέσεων.

1.3 Κυβερνοεπίθεση (Cyberattack)

Τα σύγχρονα κράτη καθώς αναπτύσσονται, αυξάνουν την εξάρτησή τους από μια σειρά διασυνδεδεμένων και όλο και περισσότερο τρωτών κρίσιμων υποδομών, για την αποτελεσματική τους λειτουργία. Αυτές οι αλληλεξαρτώμενες υποδομές έχουν διευκολύνει σε μεγάλο βαθμό την καθημερινότητα των πολιτών και την αποτελεσματικότητα της διοίκησης, έχουν όμως ταυτόχρονα εισαγάγει νέα είδη

[10] Βασίλειος, Γιαννόπουλος, «Κυβερνοπόλεμος. Υπαρκτή παγκόσμια ασύμμετρη απειλή», *Ελεύθερη Ζώνη,*3 Ιανουαρίου 2011, http://www.elzoni.gr/html/ent/321/ent.5321.asp, (έγινε πρόσβαση στις 6 Μαρ 2019)

τρωτότητας. Η προσβολή τους με στόχο την εξουδετέρωση και όχι απαραίτητα τη φυσική καταστροφή τους, μπορεί να παραλύσει την κοινωνία. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι κρίσιμες υποδομές, των οποίων η παρακολούθηση και ο έλεγχος γίνεται με πληροφοριακά συστήματα SCADA[11] (Συστήματα βιομηχανικού ελέγχου).[12]

Οι σύγχρονες κρίσιμες υποδομές των χωρών λοιπόν όπως, η ενέργεια, τα δίκτυα πετρελαίου και φυσικού αερίου, ο οικονομικός τομέας, τα δίκτυα ύδρευσης και οι υπηρεσίες εκτάκτων αναγκών, αντιμετωπίζουν αυτή την απειλή και αποτελούν τους κύριους στόχους των κυβερνοεπιθέσεων.

Οι Κυβερνοεπιθέσεις αυτές μπορεί να είναι από μια απλή εισβολή σ' ένα σύστημα προκειμένου να αναλάβουν τον έλεγχό του για λόγους πρόκλησης και περιέργειας, μέχρι την εισβολή σ' ένα σύστημα για λόγους εκδίκησης, κλοπής πληροφοριών, παρενόχλησης, υπεξαίρεσης χρημάτων ή καταστροφής μεγαλύτερης έκτασης.

Σύμφωνα με το Κατευθυντήριο πλαίσιο ανάπτυξης Κυβερνοάμυνας στις ΕΔ (Αυγ 2013), η Κυβερνοεπίθεση είναι ένα κυβερνοπεριστατικό[13] που πραγματοποιείται με σκοπό να προκαλέσει ζημιά ή να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα, ή τη διαθεσιμότητα ενός αυτοματοποιημένου πληροφοριακού συστήματος. Η ενέργεια αυτή μπορεί να συνιστά παράνομη ή άδικη πράξη υπό το πρίσμα του εθνικού ή διεθνούς δικαίου και κάτω από συγκεκριμένες συνθήκες μπορεί να εξισωθεί με ένοπλη επίθεση.

1.4 Μέσα εκδήλωσης Κυβερνοεπιθέσεων[14]

Υπάρχουν δύο μέσα τα οποία μια χώρα, μια οργάνωση ή κάποιο άτομο θα μπορούσε να χρησιμοποιήσει για την εκδήλωση Κυβερνοεπιθέσεων εντός ή μέσω του Κυβερνοχώρου· ο υπολογιστής και τα κακόβουλα προγράμματα. Στη διεθνή βιβλιογραφία και αρθρογραφία, τα μέσα αυτά αποκαλούνται Κυβερνοόπλα (Cyberweapons).

1.4.1 Υπολογιστής. Ο υπολογιστής αποτελεί σήμερα το βασικό εργαλείο με το οποίο σχεδιάζονται και από το οποίο εκδηλώνονται οι Κυβερνοεπιθέσεις. Στο

[11] SCADA: System Control and Data Acquisition
[12] Παναγιώτης, Μαυρόπουλος, *Κυβερνοπόλεμος,* Διάλεξη ΣΕΘΑ, 25 Ιαν 17
[13] Είναι οποιαδήποτε αναγνωρισμένη ανωμαλία στον κυβερνοχώρο, η οποία είναι δυνατόν να προκαλέσει ζημιά ή να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός αυτοματοποιημένου πληροφοριακού συστήματος
[14] Παναγιώτης, Μαυρόπουλος, *Κυβερνοπόλεμος και Εθνική Στρατηγική*

πλαίσιο αυτό του ρόλου του, ο υπολογιστής μπορεί να χαρακτηριστεί ως όπλο διεξαγωγής Κυβερνοπολέμου (Κυβερνοόπλο). Μια συνηθισμένη περίπτωση χρήσης του υπολογιστή σήμερα είναι αυτή στην οποία ο έλεγχός του έχει αναληφθεί από άγνωστο άτομο με την εγκατάσταση κατάλληλου λογισμικού, ώστε να χρησιμοποιηθεί για την εκτόξευση επιθέσεων DDoS,[15] εν αγνοία του χειριστή του, για λόγους απόκρυψης της ταυτότητας του δράστη. Στην ορολογία του Κυβερνοπολέμου ένας τέτοιος υπολογιστής ονομάζεται zombie.

1.4.2 Κακόβουλα προγράμματα (malware – malicious software). Ο όρος κακόβουλα προγράμματα είναι ένας γενικός όρος ο οποίος αναφέρεται σε ενοχλητικό ή επιβλαβές λογισμικό (προγράμματα, δέσμες ενεργειών ή μακροεντολές) που έχει σχεδιαστεί για να μολύνει, να καταστρέψει, να τροποποιήσει ή να προκαλέσει άλλου είδους προβλήματα σ' έναν υπολογιστή ή πρόγραμμα, χωρίς να το γνωρίζει ο ιδιοκτήτης του. Ο χαρακτηρισμός «κακόβουλο» αναφέρεται στην πρόθεση του δημιουργού του λογισμικού. Υπάρχουν διάφοροι τύποι κακόβουλων προγραμμάτων, το κάθε ένα με δικό του τρόπο λειτουργίας, όπως παρακάτω:

1.4.2.1 Δούρειοι Ίπποι (TrojanHorse).[16] Οι δούρειοι ίπποι είναι προγράμματα που προσφέρουν ή εμφανίζονται να προσφέρουν εντυπωσιακές λειτουργίες ή χαρακτηριστικά, όμως εκτελούν αθόρυβα επιβλαβείς ενέργειες στο παρασκήνιο. Έχοντας πάρει το όνομά τους από τον γνωστό Δούρειο Ίππο, οι ιοί αυτοί είναι σχεδιασμένοι να φαίνονται ελκυστικοί στον χρήστη. Μπορεί να έχουν τη μορφή παιχνιδιών, screensaver, ενημερώσεων εφαρμογών ή άλλων χρήσιμων προγραμμάτων ή αρχείων οποιουδήποτε είδους. Ορισμένοι δούρειοι ίπποι μιμούνται ή αντιγράφουν απόλυτα δημοφιλή ή γνωστά προγράμματα, ώστε να εμφανίζονται πιο αξιόπιστοι. Σκοπός αυτής της εξαπάτησης είναι να παρασύρει τον χρήστη να εγκαταστήσει τον δούρειο ίππο. Μετά την εγκατάσταση, οι δούρειοι ίπποι μπορούν επίσης να χρησιμοποιήσουν "αντιπερισπασμούς", για να συνεχίσουν να δίνουν την ψευδαίσθηση ότι είναι νόμιμοι. Για παράδειγμα, ένας δούρειος ίππος που κρύβεται σ' ένα screensaver ή αρχείο εγγράφου θα εμφανίζει μια εικόνα ή ένα έγγραφο. Όσο αποσπά την προσοχή του χρήστη, ο δούρειος ίππος εκτελεί αθόρυβα άλλες ενέργειες στο παρασκήνιο.

---

[15] Distributed Denial of Service

[16] https://help.f-secure.com/product.html?home/internet-security/latest/el/concept_AD66CB676C2749B8A235B6D7E63BB4C2-internet-security-latest-el, (έγινε πρόσβαση στις 14 Μαρ 2019)

1.4.2.2 Σκουλήκια (Worms).[17]Οι ιοί τύπου worms είναι προγράμματα που στέλνουν αντίγραφα του εαυτού τους από μία συσκευή σε μια άλλη συσκευή σ' ένα δίκτυο. Ορισμένοι ιοί τύπου worm εκτελούν επίσης επιβλαβείς ενέργειες στις συσκευές που έχουν προσβληθεί. Πολλοί ιοί τύπου worm έχουν σχεδιαστεί να φαίνονται ελκυστικοί στον χρήστη. Μπορεί να έχουν τη μορφή εικόνας, βίντεο, εφαρμογής ή άλλων χρήσιμων προγραμμάτων ή αρχείων. Σκοπός αυτής της εξαπάτησης είναι να παρασύρουν τον χρήστη να εγκαταστήσει τον ιό τύπου worm. Άλλοι ιοί τύπου worm έχουν σχεδιαστεί να δρουν εντελώς μυστικά, καθώς εκμεταλλεύονται τα ελαττώματα μιας συσκευής για να εγκατασταθούν χωρίς να γίνουν αντιληπτοί από τον χρήση. Μετά την εγκατάσταση, οι ιοί τύπου worm χρησιμοποιούν τους φυσικούς πόρους της συσκευής για να δημιουργήσουν αντίγραφα του εαυτού τους και μετά να τα στείλουν σε όλες τις άλλες συσκευές που μπορούν να προσεγγίσουν σ' ένα δίκτυο. Αν γίνεται αποστολή πολλών αντιγράφων ιών τύπου worm, μπορεί να επιβαρυνθεί η απόδοση της συσκευής. Αν προσβληθούν πολλές συσκευές σ' ένα δίκτυο και στέλνουν αντίγραφα του ιού, μπορεί να επηρεαστεί το ίδιο το δίκτυο.

1.4.2.3 Κερκόπορτες (Trapdoors).[18] Κερκόπορτα είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης. Οι κερκόπορτες χρησιμοποιήθηκαν νόμιμα για πολλά χρόνια από τους προγραμματιστές, για να απαλλάξουν από σφάλματατα συστήματα και να δοκιμάσουν προγράμματα.

1.4.2.4 Παραπλάνηση (IPspoofing).[19]Με την τεχνική αυτή (γνωστή και ως IPaddressforgery ή hostfilehijack) ο επιτιθέμενος παρίσταται ψευδώς ως ο κατασκευαστής και διαχειριστής νόμιμων και ακίνδυνων σελίδων και ιστότοπων.Ο επισκέπτης που πληκτρολογεί στον Η/Υ του μία διεύθυνση ορισμένης ιστοσελίδας στο διαδίκτυο, οδηγείται σε μία άλλη ιστοσελίδα, παραποιημένη. Κατά την επικοινωνία του με αυτήν τη φαινομενικά νόμιμη και φυσιολογική, αλλά στην πραγματικότητα κατασκευασμένη από τρίτους, ιστοσελίδα, όλα τα στοιχεία που τυχόν εισάγει ο χρήστης καταλήγουν στους ‘’πλαστογράφους’’, οι οποίοι μπορούν

[17] Στο ίδιο
[18] http://ebackspace.blogspot.com/2013/04/blog-post_9252.html, (έγινε πρόσβαση στις 14 Μαρ 2019)
[19] https://www.ip.gr/el/dictionary/215-Spoofing, (έγινε πρόσβαση στις 14 Μαρ 2019)

ακόμη και να αναλάβουν τον έλεγχο του Η/Υ του ή του δικτύου στο οποίο αυτός ανήκει, με ότι αυτό συνεπάγεται.

1.4.2.5 Κατασκοπεία (Spyware).[20]Το spyware είναι λογισμικό (από τις λέξεις spy software, δηλαδή λογισμικό κατασκοπείας), που συνήθως περιλαμβάνεται ως κρυμμένο στοιχείο σε εφαρμογές shareware ή freeware που λαμβάνονται από το Internet. Αυτό σημαίνει ότι ενώ εγκαθίστανται αυτές τις εφαρμογές, ενδεχομένως να εγκαθίστανται και spyware, χωρίς να το γνωρίζει ο χρήστης. Το spyware μπορεί επίσης να φιλοξενηθεί σε ιστοσελίδες. Στη συνέχεια, μπορεί να εγκατασταθεί στους υπολογιστές των χρηστών που επισκέφτηκαν τις σελίδες. Το λογισμικό spyware επιχειρεί να αντλήσει πληροφορίες από τον Η/Υ χωρίς την άδειά του χρήστη, συνήθως για διαφημιστικούς λόγους. Αφού το spyware εγκατασταθεί στον Η/Υ, παρακολουθεί τη δραστηριότητά του στο Internet και αναφέρει τις πληροφορίες που συγκέντρωσε στο δημιουργό του. Μερικές φορές, οι πληροφορίες που συγκεντρώνονται είναι απόρρητες: κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, διευθύνσεις e-mail, κλπ.

1.4.2.6 Δικτυακό ρομπότ (Bot).Ένα Διαδικτυακό μποτ ή αλλιώς ρομπότ είναι μια μηχανή που εφαρμόζει αυτοματοποιημένες λειτουργιές μέσα στο διαδίκτυο όπως η διαδικτυακή αναζήτηση. Μέσω της αναζήτησης μερικές φορές φέρνουν στην επιφάνεια κακόβουλα λογισμικά (malware), που με αυτόν τον τρόπο μολύνουν τους υπολογιστές ή τον καταλαμβάνουν εξολοκλήρου. Υπάρχουν δυο κατηγορίες από μποτ, η μια κατηγορία είναι το «καλό» μποτ και η άλλη το «κακό». Τα «καλά» μας βοηθούν να αναζητήσουμε δεδομένα από το διαδίκτυο, λόγο του ότι το διαδίκτυο είναι ένας μεγάλος ιστός . Έτσι το μποτ σαν αράχνη, αναζητεί τα πάντα μέσα σ' αυτό, σε κάθε μορφή και μας παρουσιάζει τα δεδομένα. Ακόμα μπορεί να αλληλοεπιδρά με τις ιστοσελίδες ώστε να βρίσκει αυτό που επιθυμούμε. Τα «κακά» μποτ μολύνουν το χρηστή μ' ένα κακόβουλο λογισμικό και στέλνουν τα δεδομένα που συλλέξανε από τον υπολογιστή κωδικοποιημένα πίσω σε εξυπηρετητή (server) που τα αποκωδικοποιεί. Ο εξυπηρετητής αυτός λειτουργεί ως «κέντρο διοίκησης και ελέγχου» για ένα μεγαλύτερο μποτ με όνομα Μπότνετ (botnet) ή αλλιώς δημιουργείται ένα μεγάλο δίκτυο υπολογιστών.

[20] https://www.pandasecurity.com/homeusers/downloads/docs/product/help/ap/2013/el/675.htm, (έγινε πρόσβαση στις 14 Μαρ 2019)

1.4.2.7 Stuxnex.[21] Το Stuxnet είναι ένα πρόγραμμα υπολογιστή που δημιουργήθηκε το 2008 και σκοπό έχει να ελέγχει ένα απομακρυσμένο σύστημα σχεδόν αυτόνομα. Τα χτυπήματα γίνονταν με επαφή ,όπως για παράδειγμα με την βοήθεια ενός ενδιάμεσου USB stick με σκοπό την πρόσβαση στον έλεγχο του συστήματος που θέλαμε να επιτεθούμε. Έγινε γνωστός από την κυβερνοεπίθεση στο εργοστάσιο εμπλουτισμένου ουρανίου στη Νατάνζ (Natanz) του Ιράν το 2010. Το Stuxnet μόλυνε τα συστήματα ελέγχου του εργοστασίου μέσω ενός USB stick, άρα μιλάμε για την επέμβαση του ανθρώπινου παράγοντα. Ο υπολογιστής που προσβλήθηκε ήταν συνδεδεμένος με συγκεκριμένα μοντέλα PLC (Programmable Logic Controller) ελέγχου εργοστασιακών εγκαταστάσεων που κατασκευάζονται από την Siemens. Τα μοντέλα PLC έλεγχαν σταθμούς παραγωγής ηλεκτρικής ενέργειας. Ο ιός σταμάτησε τον προγραμματισμό του PLC με αποτέλεσμα οι φυγοκεντρητές να στροβιλίζονται πιο γρήγορα σε σύγκριση με αυτό που έχει προγραμματιστεί, προκαλώντας κατ' αυτόν τον τρόπο ζημία και ενδεχομένως την καταστροφή τους. Το Stuxnet κατέγραφε τη φυσιολογική δραστηριότητα των φυγοκεντρητών για 13 ημέρες και μετά επιτέθηκε και άλλαξε τη συχνότητα περιστροφής τους. Σημαντικό είναι να σημειωθεί ότι το Stuxnet έστελνε μήνυμα στους υπολογιστές του πυρηνικού εργοστασίου τα δεδομένα της προηγούμενης φυσιολογικής δραστηριότητας που είχε καταγράψει και όχι τα δεδομένα της πραγματικής. Αυτό είχε ως αποτέλεσμα οι φυγοκεντρητές να καταστρέφονται, αλλά οι μηχανικοί να μην γνωρίζουν την αιτία.

1.5. Σκοπός των Κυβερνοεπιθέσεων[22]

Η χρήση των Κυβερνοόπλων και οι τεχνικές για την προσβολή διαφόρων στόχων δεν αποτελούν αυτοσκοπό. Οι Κυβερνοεπιθέσεις διεξάγονται για την επίτευξη κάποιου συγκεκριμένου σκοπού. Ο σκοπός αυτός διαφέρει κατά περίπτωση, γενικώς όμως ανήκει σε μία από τις παρακάτω κατηγορίες:

1.5.1 Εκμετάλλευση (exploitation). Στην περίπτωση της εκμετάλλευσης βασικός στόχος του δράστη είναι η υποκλοπή πληροφοριών από το στόχο ή τις πηγές πληροφοριών που είναι συνδεδεμένες με αυτόν.

1.5.2 Παραπλάνηση (deception). Στην περίπτωση αυτή ο δράστης επιτρέπει στο στόχο του να εξακολουθεί να λειτουργεί, αλλά παραποιεί τις

[21] Νίνα, Παρθενοπούλου, «Ο ιός Stuxnetκαι το πυρηνικό πρόγραμμα του Ιράν», *Κέντρο Διεθνών Στρατηγικών Αναλύσεων,* https://kedisa.gr/o-ιός-stuxnet-και-το-πυρηνικό-πρόγραμμα-του-ν/, (έγινε πρόσβαση στις 14 Μαρ 2019)
[22] Παναγιώτης, Μαυρόπουλος, *Κυβερνοπόλεμος και Εθνική Στρατηγική*

πληροφορίες τις οποίες αυτός συλλέγει, αναλύει ή παράγει, στοχεύοντας ουσιαστικά στο σύστημα λήψης αποφάσεων του αντιπάλου.

1.5.3 Καταστροφή (destruction).Στην περίπτωση της καταστροφής ο επιτιθέμενος, μέσω της χρήσης πληροφοριακών συστημάτων, καθιστά αδύνατη τη λειτουργία του στόχου, καταστρέφοντας τον ίδιο ή τα συστήματα υποστήριξης που είναι απαραίτητα για τη λειτουργία του. Στην περίπτωση αυτή πρωταρχικός στόχος δεν είναι τα πληροφοριακά συστήματα του αντιπάλου, αλλά η κρίσιμη υποδομή του.

1.5.4 Διακοπή λειτουργίας ή εξουδετέρωση (denial of service or destruction – DoS). Στην περίπτωση επιθέσεων διακοπής λειτουργίας ή εξουδετέρωσης, ο επιτιθέμενος δεν καταστρέψει το στόχο αλλά τον θέτει εκτός λειτουργίας ή τον καθιστά αναξιόπιστο για κάποια χρονική περίοδο, απαγορεύοντας στους νόμιμους χρήστες την εξυπηρέτησή τους ή την πρόσβαση σε πηγές πληροφοριών.

1.6 Περιστατικά Κυβερνοεπιθέσεων

Με την πρόοδο του ICT[23] παρατηρούνται όλο ένα και περισσότερα περιστατικά κυβερνοεπιθέσεων. Οι νέες τεχνολογίες τοποθετούν το λιθαράκι τους υποβοηθώντας στο να γίνει ένα βήμα πιο μπροστά, για την αύξηση των επιθέσεων στον Κυβερνοχώρο, κατατάσσοντάς το σ' ένα από τα πιο επίκαιρα φαινόμενα στην σημερινή εποχή.

1.6.1 Εσθονία 2007.Η Εσθονία δέχθηκε επίθεση επί 19 ημέρες, από τέλη Απριλίου ως αρχές Μαΐου του 2007, με αφορμή την απομάκρυνση ενός μνημείου του Β΄ ΠΠ της πρώην ΕΣΣΔ από την κεντρική πλατεία του Ταλίν. Η επίθεση αυτή έγινε με την χρήση των Bots όπου Ρώσοι εγκληματικοί φορείς χτύπησαν τα κοινωνικά δίκτυα της Εσθονίας. Μετά από αυτές τις επιθέσεις, η Εσθονία προσέγγισε το ΝΑΤΟ για στρατιωτική βοήθεια αλλά το ΝΑΤΟ δεν μπορούσε να χρησιμοποιήσει την τότε αρμοδιότητα και πολιτική του για να παρέμβει. Έως ότου δημιουργηθεί στην Εσθονία το Κέντρο Αριστείας Κυβερνοάμυνας, η χώρα υιοθέτησε μια εντελώς νέα νομοθεσία και πολιτική για να αντιμετωπίσει τις όποιες μελλοντικές παρόμοιες κυβερνοεπιθέσεις στις κρίσιμες υποδομές της. Η επίθεση είχε σαν αποτέλεσμα τη μείωση του ΑΕΠ της χώρας κατά 7%.[24]

[23] Information and communications technology
[24] Παναγιώτης, Μαυρόπουλος, *Κυβερνοπόλεμος,* Διάλεξη ΣΕΘΑ, 25 Ιαν 2017

Για την επίθεση αυτή του 2007 ο Jaak Aaviksoo, Υπουργός Άμυνας της Εσθονίας, αναφέρει: «οι περισσότερες επιθέσεις στόχευαν στους διακομιστές της κυβέρνησης και των ειδησεογραφικών γραφείων, αλλά και οι δύο μεγαλύτερες τράπεζες της Εσθονίας υπέστησαν βαριά επίθεση. Στις σημαντικότερες στιγμές, η ποσότητα της κυβερνοκυκλοφορίας που στόχευε κυβερνητικά ιδρύματα, απ' έξω από την Εσθονία ήταν 400 φορές υψηλότερη από το φυσιολογικό επίπεδο. Μερικές από τις επιθέσεις πραγματοποιήθηκαν σε κύματα και εκτελέστηκαν με πολύ ακριβή χρονισμό. Ήταν ασυνήθιστα καλά συντονισμένες και απαιτούσαν πόρους μη διαθέσιμους στον μέσο άνθρωπο. Σε κάποιο σημείο, οι επιθέσεις πραγματοποιούνταν σ' ένα πολύ ακριβές χρονοδιάγραμμα και περιλάμβαναν ομάδες υπολογιστών – «προγράμματα ρομπότ» - τα οποία πιθανόν να ενοικιάστηκαν νωρίτερα γι' αυτό το σκοπό».[25]

Βλέποντας το αποτέλεσμα της επίθεσης ο Jaak Aavikso συμπληρώνει: «Λαμβάνοντας υπόψη το μέγεθος των υποδομών της Εσθονίας και την έκταση των επιθέσεων, ήταν μια από τις πιο σημαντικές και συντονισμένες κυβερνοεπιθέσεις ενάντια σ' ένα κυρίαρχο κράτος στον κόσμο. Παρόλο που η επίθεση ανατράπηκε χωρίς μακροπρόθεσμες επιπτώσεις, υπήρξαν κάποιες άμεσες επιδράσεις που επηρέασαν όλους τους πολίτες της Εσθονίας, όπως η μη διαθεσιμότητα των διαδικτυακά τραπεζικών υπηρεσιών και οι δυσκολίες στις επικοινωνίες. Σε μια χώρα που το 98% των τραπεζικών συναλλαγών γίνονται διαδικτυακά και όπου η πλειοψηφία των πολιτών συμπληρώνουν τα φορολογικά έντυπα διαδικτυακά, είμαι σίγουρος ότι μπορείτε να συνειδητοποιήσετε τον αντίκτυπο που τέτοια παρατεταμένα περιστατικά μπορεί να έχουν. Ο αντίκτυπος των επιθέσεων μεγεθύνθηκε από την ψυχολογική επίδραση και εκφοβισμό που είχε στον γενικό πληθυσμό. Εκτός από την απευθείας επίδραση του στόχου, οι κυβενοεπιθέσεις δημιούργησαν ευρεία σύγχυση και κακή επικοινωνία στο ευρύ κοινό, καθώς ήταν αδύνατη η πρόσβαση από το εξωτερικό σε πληροφορίες σχετικά με τα γεγονότα στην Εσθονία».[26]

1.6.2 Γεωργία 2008.Επίσης είναι σημαντικό να αναφερθεί και ο πόλεμος μεταξύ Ρωσίας και Γεωργίας το 2008. Η Ρωσία χτύπησε τις ιστοσελίδες της κυβέρνησης και τα μέσα ενημέρωσης της Γεωργίας με σκοπό να μην μπορεί η κυβέρνηση να επικοινωνήσει με τον πληθυσμό της. Με την επίθεση αυτή παρέλυσαν

[25] Reich, Pauline, *Cyber Warfare: A Review Of Theories, Law, Policies, Actual Incidents – And The Dilemma Of Anonymity*, European Journal of Law and Technology 1.2, 2010
[26] Στο ίδιο

την δημόσια διοίκηση της Γεωργίας. Οι επιθέσεις αυτές δεν έλειπαν από το επίκεντρο των συζητήσεων. Πολλοί αναλυτές παραθέτουν σειρά προτάσεων για την αντιμετώπιση των θυμάτων –περιοχών των κυβερνοεπιθέσεων μέσα από την μελέτη τους και το έργο τους. Προτείνουν ότι νέες προσεγγίσεις στο παραδοσιακό Δίκαιο των Ένοπλων Συγκρούσεων πρέπει να αναπτυχθούν ώστε να μπορεί να παρέχει αποτελεσματικές νομικές επιδιορθώσεις. Ο Jon Bumgarner (2009), ο Γενικός Διευθυντής του Τεχνικού Τμήματος της Μονάδας Κυβερνοεπιπτώσεων των ΗΠΑ, έκανε μια σειρά από εντυπωσιακές παρατηρήσεις για την Γεωργία το καλοκαίρι του 2008: «Πολλές από τις κυβερνοεπιθέσεις ήταν τόσο κοντά χρονικά στις αντίστοιχες στρατιωτικές επιχειρήσεις που πρέπει να υπήρχε κοντινή συνεργασία μεταξύ των ανθρώπων στον Ρωσικό στρατό και τους πολίτες επιτιθέμενους μέσα από τον κυβερνοχώρο. Όταν οι κυβερνοεπιθέσεις ξεκίνησαν δεν περιλάμβαναν στάδια αναγνώρισης ή χαρτογράφησης αλλά κατευθείαν πέρασαν στο είδος πακέτων που ήταν το καταλληλότερο για την εμπλοκή των ιστότοπων υπό επίθεση. Αυτό υποδεικνύει ότι η απαραίτητη αναγνώριση και η εγγραφή των σεναρίων επίθεσης έπρεπε να είχαν γίνει εκ των προτέρων. Πολλές από τις πράξεις των δραστών, όπως η εγγραφή νέων ονομάτων ιστοχώρου και η δημιουργία νέων ιστοσελίδων, πραγματοποιήθηκαν τόσο γρήγορα που όλα τα βήματα έπρεπε να είχαν προετοιμαστεί νωρίτερα».[27] Προσθέτει επίσης ότι «οι διοργανωτές των κυβερνοεπιθέσεων είχαν εκ των προτέρων ειδοποίηση των προθέσεων του Ρωσικού στρατού και πληροφορήθηκαν για τη χρονική στιγμή των επιχειρήσεων του Ρωσικού στρατού ενώ αυτές οι επιχειρήσεις πραγματοποιούνταν».

Τέλος καταλήγει στο συμπέρασμα ότι: «Από την κυβερνοεκστρατεία ενάντια στην Εσθονία τον Απρίλιο και Μάιο του 2007, οι Ρώσοι είχαν ήδη μάθει ότι μια κυβερνοεκστρατεία που πραγματοποιείται από πολίτες μπορεί να προκαλέσει σοβαρές οικονομικές και ψυχολογικές διαταραχές σε μια χώρα, χωρίς να προκαλέσει κάποια σοβαρή διεθνή απόκριση. Αυτό το μάθημα ενισχύθηκε από τις εμπειρίες τους με τις κυβερνοεκστρατείες ενάντια στη Λιθουανία στο τέλος του Ιουνίου 2008 και ενάντια στο Καζακστάν τον Ιανουάριο του 2009, όπου μεγάλες τοπικές διαταραχές είχαν εντυπωσιακά μικρή κάλυψη από τον διεθνή τύπο. Η εκστρατεία ενάντια στη Γεωργία έλαβε χώρα κάτω από διαφορετικές συνθήκες, γιατί η Ρωσία είχε εμπλακεί σε απροκάλυπτη στρατιωτική δράση ενάντια στη χώρα, αλλά η συνιστώσα του

[27] Στο ίδιο

κυβερνοχώρου πραγματοποιούνταν από πολίτες και δεν υπήρχαν διεθνή αντίποινα. Με δεδομένο αυτή την ιστορία, θα ήταν πολύ αναπάντεχο αν οι μελλοντικές διενέξεις και συγκρούσεις που θα περιλαμβάνουν τη Ρωσία και τις πρώην κτήσεις ή δορυφόρους της δεν συνοδεύονται από κυβερνοεκστρατείες».[28]

1.6.3 Ιαπωνία 2010.Στις 19 Σεπτεμβρίου του 2010 η Ιαπωνία υποψιαζόταν ότι μία κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DoS)''χτυπούσε'' τις ιστοσελίδες του Υπουργείου Αμύνης και της Υπηρεσίας Εθνικής Αστυνομίας λόγω μιας διένεξης που είχε με τη Λαϊκή Δημοκρατία της Κίνας, όπως ανέφεραν τα μέσα. Η Ιαπωνική κυβέρνηση πήρε τα μέτρα της διατάζοντας τις κυβερνητικές οντότητες να λάβουν μέτρα αυτοάμυνας, όπως να κλείσουν τις ιστοσελίδες τους, για σύντομο χρονικό διάστημα. Οι υποψίες της Ιαπωνίας βασίζονταν σ' ένα περιστατικό που έγινε στις 7 Σεπτέμβρη 2010, όπου μιας Κινέζικη τράτα και δύο Ιαπωνικά σκάφη της ακτοφυλακής, συγκρούστηκαν κοντά σε μια αμφιλεγόμενη σειρά νησιών, στην Ανατολική Θάλασσα της Κίνας. Η σύγκρουση αυτή δεν τελείωσε ειρηνικά καθώς η μεγαλύτερη ομάδα πειρατείας της Κίνας είχε προειδοποιήσει ότι θα επιτίθονταν σε Ιαπωνικές ιστοσελίδες, ως διαμαρτυρία για το περιστατικό».[29]

1.6.4 Νατάνζ 2010.Το πρώτο χτύπημα όπου έκανε την εμφάνισή του ο ιός Stuxnet ήταν τον Ιούνιο του 2010 στις Ιρανικές πυρηνικές εγκαταστάσεις που χτυπήθηκαν στο Νατάνζ. Μόλυνε πάνω από 60.000 υπολογιστές που οι περισσότεροι από αυτούς βρίσκονταν στο Ιράν, χωρίς να περιοριστεί μόνο εκεί. Από το χτύπημα αυτό επηρεάστηκαν επίσης και άλλες χώρες όπως η Ινδία, η Ινδονησία, η Κίνα, το Αζερμπαϊτζάν, η Φινλανδία και η Γερμανία. Ο ιός δεν έμεινε εκεί. Προχώρησε μέσα από το διαδίκτυο και σε άλλα συστήματα υπολογιστών χωρίς βέβαια να προκαλέσει τον ίδιο βαθμό ζημίας αφού η χρήση αντιδότων περιόρισε σημαντικά την εξάπλωση του μέχρι και τις 24 Ιουνίου του 2012.

1.6.5 ChostNet 2009.Τον Μάρτιο του 2009 ανακαλύφθηκε μία μεγάλης κλίμακας επιχείρηση κατασκοπείας από τους ερευνητές στο Information Warfare Monitor που ονομάστηκε GhostNet. Η υποδομή διοίκησης και ελέγχου αυτής της επιχείρησης βρίσκεται κυρίως στην Λαϊκή Δημοκρατία της Κίνας και έχει εισχωρήσει σε υψηλής σημασίας πολιτικές, οικονομικές και ΜΜΕ τοποθεσίες σε 103 χώρες. Αν και η δραστηριότητα έχει βάση κυρίως στην Κίνα, δεν υπάρχουν ισχυρές αποδείξεις ότι η Κινέζικη κυβέρνηση εμπλέκεται στην επιχείρηση. Τα υπολογιστικά συστήματα

[28] Στο ίδιο
[29] Στο ίδιο

που ανήκουν σε πρεσβείες, υπουργεία εξωτερικών και άλλα κυβερνητικά γραφεία ανά τον κόσμο κινδύνευσαν από το GhostNet.

Στις 6 Απρίλιου του 2010, το ίδρυμα Shadow server και το Information Warfare Monitor εξέδωσαν μια κοινή αναφορά σχετικά με έρευνα στο κομμάτι της κατασκοπείας στον Κυβερνοχώρο. Στην αναφορά τονίζεται το ολοένα και αυξανόμενο πρόβλημα που τίθεται από την αυξανόμενη ενσωμάτωση του εγκλήματος και της κατασκοπείας στον ιστό του παγκόσμιο κυβερνοχώρου. Η αναφορά κάνει έκκληση για ένα παγκόσμιο συνέδριο στον κυβερνοχώρο προκειμένου να τεθεί μια τάξη σ' αυτό που αυξανόμενα μετατρέπεται σ' έναν επικίνδυνα διαταραγμένο χώρο.[30]

[30] Στο ίδιο

Κεφάλαιο Δεύτερο

Έννοια και στοιχεία κυβερνοπολέμου

2.1 Ορισμός

Για τον όρο «Κυβερνοπόλεμος» υπάρχουν διάφοροι ορισμοί που μπορούν να τον εξηγήσουν. Ο Αντισμήναρχος της Πολεμικής Αεροπορίας των ΗΠΑ, Gregory J. Rattray, στο βιβλίο του ‘’Strategic Warfarein Cyberspace’’[31], ορίζει τον κυβερνοπόλεμο ως «στρατιωτικές επιχειρήσεις στον κυβερνοχώρο με σκοπό την επίθεση εναντίον του εχθρού και την προστασία των φίλιων κέντρων βάρους».[32]

Επιπρόσθετα ένας άλλος ορισμός που τον εξηγεί είναι:

«Ένας αγώνας μεταξύ αντιτιθέμενων πλευρών που κάνουν χρήση τεχνολογίες και μεθόδους δικτύου για να αγωνιστούν για ένα πλεονέκτημα πληροφοριών στα πεδία της πολιτικής, οικονομικών, στρατιωτικών υποθέσεων και τεχνολογίας».[33]

Τέλος ο πρώην σύμβουλος ασφαλείας του Λευκού Οίκου, Richard Clarke, αναφέρει ότι «Ο κυβερνοπόλεμος είναι η καταστροφή, η αναστάτωση ή η πρόκληση ζημιάς σε συστήματα του πραγματικού κόσμου μέσω των επιθέσεων με συστήματα υπολογιστών, κάτι που συμβαίνει μόνο κατά τη διάρκεια κάποιου πολέμου ή, υποθέτω, κάποιας μυστικής δράσης. Άρα, πρόκειται να συμβεί όταν κράτη θα πάνε σε πόλεμο μεταξύ τους».[34]

2.2 Χαρακτηριστικά

Ο Κυβερνοπόλεμος, όπως και κάθε άλλη μορφή πολέμου έχει κάποια χαρακτηριστικά που τον κάνει να ξεχωρίζει από τους άλλους πολέμους. Ορισμένα από αυτά είναι τα ακόλουθα.[35]

---

[31] Gregory J. Rattray, *Strategic Warfare in Cyberspace*, Cambridge, MIT press, 2001

[32] Κέντρο Βάρους, στην στρατηγική είναι, κατά τον Carl von Clausewitz, όλα εκείνα τα σημεία του εχθρού εναντίον των οποίων πρέπει να συγκεντρωθεί όλη η φίλια επίθεση. Σύμφωνα με την ανάλυση του Κωνσταντίνου Κολλιόπουλου στο βιβλίο του “Η Υψηλή Στρατηγική της Αρχαίας Σπάρτης”, σ. 64, η έννοια του κέντρου βάρους μπορεί να πάρει διάφορες μορφές, είτε υλικές είτε ψυχολογικές. Παραδείγματα κέντρου βάρους διαφόρων πολεμικών προσπαθειών μπορεί να είναι οι ένοπλες δυνάμεις του αντιπάλου, η βιομηχανική του παραγωγή, μια σημαντική εδαφική περιοχή, η θέληση της ηγεσίας του να συνεχίσει τον πόλεμο, η ικανότητα της πολιτικής ηγεσίας του να εξασφαλίσει την υπακοή του λαού κλπ.

[33] Reich, Pauline, *Cyber Warfare: A Review Of Theories, Law, Policies, Actual Incidents – And The Dilemma Of Anonymity*, European Journal of Law and Technology 1.2 , 2010

[34] Eleanor, Hall, «Former White House security advisor warns og cyber war», *The World today*,7 September 2010, http://www.abc.net.au/worldtoday/content/2010/s3086792.htm, (έγινε πρόσβαση στις15 Μαρ 2019)

[35] Dipert, Randall, *The Ethics Of Cyberwarfare: Journal Of Military Ethics: Vol 9, No 4*, Journal of Military Ethics, 2016

α. Δεν υπάρχουν ενήμερες, ανοιχτές, δημόσιες ή πολιτικές συζητήσεις για το τι θα συνιστούσε μία δεοντολογική και συνετή πολιτική χρήσης τέτοιων όπλων.

β. Είναι πολύ δύσκολο να προσδιοριστεί η πηγή των κυβερνοεπιθέσεων, το λεγόμενο «πρόβλημα της απόδοσης (attribution problem)».

γ. Πολλές κυβερνοεπιθέσεις δεν θα είναι φονικές και δεν θα προκαλέσουν καν μόνιμη ζημιά σε φυσικά (υλικά) αντικείμενα. Αυτό είναι βέβαια άκρως ανόμοιο με τα πυρηνικά όπλα και με όλα σχεδόν τα παραδοσιακά όπλα του πολέμου.

δ. Δεν υπάρχουν «εξωτικές» μονάδες κυβερνοόπλων (cyberweapons), γεγονός που τα καθιστά και πάλι πολύ ανόμοια με τα πυρηνικά και τα άλλα όπλα προηγμένης τεχνολογίας, ή ακόμα και με τα χημικά ή τα βιολογικά όπλα.

ε. Οποιοσδήποτε υπολογιστής είναι ένα δυνητικό κυβερνοόπλο και οποιοσδήποτε με προχωρημένη γνώση πληροφοριακών συστημάτων είναι ένας δυνητικός κυβερνοπολεμιστής.

στ. Η άμυνα είναι ακριβή και ευπαθή σε αποτυχία, ενώ η επίθεση είναι περίπου το ίδιο φθηνή: αυτό είναι παρόμοιο με την πυρηνική προστασία, με τις αντι-πυραυλικές τεχνολογίες, τη θωράκιση του σώματος, την προστασία απέναντι σε αυτοσχέδιους εκρηκτικούς μηχανισμούς.

ζ. Υπάρχει πολύ χαμηλός βαθμός βεβαιότητας για το τι θα συμβεί με μία επίθεση, ή σ' έναν πόλεμο.

η. Οι μακρινές σε βάθος χρόνου, βλαβερές παρενέργειες (παράπλευρες απώλειες), δεν μπορούν επαρκώς να προβλεφθούν, όπως ασθένειες, οικονομικές συνέπειες και ούτω καθεξής.

2.3 Τεχνολογικό πλαίσιο του πολέμου

Με το πέρασμα του χρόνου και με την πρόοδο της κυβερνοτεχνολογίας ο κυβερνοπόλεμος γίνεται όλο και πιο εξειδικευμένος και προσαρμόζεται σε κάθε περίσταση ξεχωριστά, με αποτέλεσμα οι επιπτώσεις στο θύμα κράτος να απέχουν πολύ από εποχή σε εποχή, λόγω του τεχνολογικού υποβάθρου. Στον 21ο αιώνα που ζούμε παρατηρείται αλματώδης πρόοδος στις τεχνολογίες πληροφοριών. Ο αριθμός των ενεργών χρηστών στον κυβερνοχώρο είναι πολύ μεγάλος. Στατιστικές δείχνουν ότι από το 2000 μέχρι και σήμερα παρατηρείται αύξηση ποσοστού κατά 566%.

Η Διεθνής Ένωση Τηλεπικοινωνιών είχε αναφέρει ότι «στο τέλος του 2018, θα υπάρχουν σχεδόν 3 δισεκατομμύρια χρήστες του Διαδικτύου, με τα δύο τρίτα από αυτούς να προέρχονται από τον αναπτυσσόμενο κόσμο…ο αριθμός των κινητών-ευρυζωνικών συνδρομών θα φθάσει τις 2,3 δισεκατομμύρια παγκοσμίως…πενήντα πέντε τοις εκατό από αυτές τις συνδρομές αναμένεται να είναι στον αναπτυσσόμενο κόσμο».[36]

2.4 Διεθνείς θέσεις για τον Κυβερνοπόλεμο

Παρακάτω θα αναφερθούν σε αδρές γραμμές, οι βασικές αρχές κυβερνοπολέμου για τρεις από τους βασικότερους κρατικούς δρώντες σε παγκόσμια κλίμακα.

2.4.1 Ηνωμένες Πολιτείες Αμερικής.[37] Σύμφωνα με μία έκθεση στο Κογκρέσο οι κυβερνοεπιθέσεις που γίνονταν εναντίων της Κυβέρνησης των ΗΠΑ αυξάνονται ραγδαία από το 2009. Η έκθεση αυτή αναφέρει:

α. Την ύπαρξη υποψίας ότι πολλές από αυτές τις επιθέσεις προέρχονταν από το Κινέζικο κράτος και κρατικοεπιδοτούμενες οντότητες.

β. Κατά τη διάρκεια του 2008, υπήρξαν συνολικά 54640 κυβερνοεπιθέσεις ενάντια στο Υπουργείο Άμυνας των ΗΠΑ.

γ. Κατά το πρώτο μισό του 2009, υπήρξαν 43785 κυβερνοπεριστατικά που στόχευαν το Υπουργείο Άμυνας.

Με βάση τις προτάσεις και τα προβλήματα που ειπώθηκαν στην έκθεση, βγήκαν κάποια συμπεράσματα, τα σημαντικότερα από τα οποία είναι τα εξής:

α. Οι κυβερνοεπιθέσεις που προέρχονται από την Κίνα δεν είναι εύκολο να ταξινομηθούν.

β. Η κυβερνοεπίθεση μπορεί να αναγνωριστεί από ποιον προήλθε, αφού τα κυβερνοπεριστατικά αφήνουν πίσω τους υπογραφές που μπορούν, με την εγκληματολογική ανάλυση, να αποκαλύψουν κάποιες φορές την υπαγωγή των υπεύθυνων δραστών σ' έναν λογικό βαθμό βεβαιότητας, γεγονός που βοηθά να συμπληρωθεί η κατανόηση των επιτιθέμενων και των συνδέσμων τους.

Τέλος ενδιαφέρον ήταν και οι παρατηρήσεις που έγιναν από τον Dennis Blair[38]στην επιτροπή:

---

[36] Φλώρα, Σίμου, Διπλωματική Εργασία του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, *Κυβερνοπόλεμος και επιθέσεις στο διαδίκτυο,* Οκτώβριος 2016

[37] Στο ίδιο

α. Ευαίσθητες πληροφορίες «κλέβονται καθημερινά τόσο από τα δίκτυα της κυβέρνησης, όσο και του ιδιωτικού τομέα».

β. Οι ΗΠΑ δεν μπορούν να είναι βέβαιες ότι οι υποδομές του κυβερνοχώρου τους θα είναι διαθέσιμες και αξιόπιστες σε μια κρίση.

γ. Οι ΗΠΑ και ο κόσμος γενικότερα παρουσιάζουν μια μεγαλύτερη τρωτότητα στη διαταραχή ως αποτέλεσμα της τάσης προς σύγκλιση των υπολογιστών και των ελέγχων με τα οποία λειτουργούν οι κρίσιμες υποδομές σ' ένα μόνο δίκτυο: το Διαδίκτυο.

δ. Οι κυβερνοαπειλές είναι όλο και πιο διακριτικές και περίπλοκες. Τον προηγούμενο χρόνο είδαμε την ανάπτυξη του «αυτοτροποποιούμενου κακόβουλου λογισμικού, το οποίο εξελίσσεται για να καταστήσει τις παραδοσιακές τεχνολογίες ανίχνευσης ιού λιγότερο αποτελεσματικές».

Η κυβέρνηση των ΗΠΑ έχει πλέον επικεντρωθεί στην έννοια της κυβερνοασφάλειας, υλοποιώντας λύσεις υψηλής τεχνολογίας, τέτοιες ώστε να μπορεί να αντιμετωπίσει τις διάφορες προκλήσεις του κυβερνοπολέμου και να προστατέψει τα ιδιωτικά συστήματά της.

«Μια από τις πιο σοβαρές προκλήσεις των ΗΠΑ για την εθνική ασφάλεια είναι η κυβερνοασφάλεια», αναφέρει ο πρόεδρος των ΗΠΑ, Barack Obama και συνεχίζει «οι ΗΠΑ δεν είναι ολοκληρωτικά προετοιμασμένες να ανταπεξέλθουν σ' αυτήν αφού δεν υπάρχει μια συγκεκριμένη εθνική πολιτική κυβερνοασφάλειας και κάποιος οργανισμός που να στοχεύει στο σκοπό αυτό με κάποιες ευθύνες και αρμοδιότητες».[39]

Μόλις στις 16 Νοεμβρίου 2018 ο πρόεδρος Trump υπέγραψε τον νόμο για την ασφάλεια στον κυβερνοχώρο και τον Οργανισμό Ασφάλειας Υποδομών του 2018. Αυτή η νομοθεσία ορόσημο, αναδεικνύει την αποστολή της πρώην Διεύθυνσης Εθνικής Προστασίας και Προγραμμάτων (National Protection and Programs Directorate – NPPD) και ιδρύει τον Οργανισμό Κυβερνοασφάλειας και Υποδομών (Cyber security and Infrastructure Security Agency – CISA). Ο CISA εγκαινιάζει την εθνική ικανότητα να αμύνεται των κυβερνοεπιθέσεων και να συνεργάζεται με την

[38] Είναι ο πρώην των Διευθυντής της Εθνικής Υπηρεσίας Πληροφοριών των ΗΠΑ, απόστρατος ναύαρχος, ο οποίος ήταν ο διοικητής των αμερικανικών δυνάμεων στην περιοχή του Ειρηνικού

[39] Dan, Fayutkin, «The American and Russian Approaches to Cyber Challenges», *Journal of Defence Management*, 2012, https://www.omicsonline.org/open-access/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (έγινε πρόσβαση στις16 Μαρ 2019)

ομοσπονδιακή κυβέρνηση για την παροχή εργαλείων για την ασφάλεια στον κυβερνοχώρο, για υπηρεσίες αντιμετώπισης περιστατικών, καθώς και δυνατότητες αξιολόγησης των δικτύων ‘’.gov” που υποστηρίζουν τις βασικές λειτουργίες των διάφορων υπηρεσιών και οργανισμών.[40]

Την τελευταία εξέλιξη στην εθνική στρατηγική των ΗΠΑ, αποτελεί η μετάβαση από την ενεργητική άμυνα (active defense), στην προωθημένη άμυνα (forward defense). Πρόκειται για μια νέα στρατηγική στο πεδίο του κυβερνοχώρου, βασιζόμενη σε επιχειρήσεις εκτός δικτύων των ΗΠΑ, για την ανατροπή εχθρικών ενεργειών. Η εκτίμηση των ειδικών είναι ότι η συγκεκριμένη πολιτική υπονοεί μια χαλάρωση των νομικών περιορισμών στις στρατιωτικές επιχειρήσεις και την ενίσχυση των ικανοτήτων τους για αποτελεσματικότερη προστασία των δικτύων τους[41]. Επιπλέον, η προσωπική μου άποψη είναι ότι προετοιμάζει το έδαφος για την επίσημη υιοθέτηση του «προληπτικού πολέμου» και στον κυβερνοχώρο.

Λαμβάνοντας υπόψη το βασικό ρόλο που διαδραματίζουν οι ΗΠΑ στον τομέα της κυβερνοασφάλειας, ενδεχομένως η τάση αυτή να υιοθετηθεί σύντομα και από άλλα κράτη ή οργανισμούς (πχ. NATO).

2.4.2 Ρωσία.[42]Το πανεπιστήμιο της Μόσχας και ειδικά το τμήμα διεθνούς πολιτικής σε συνεργασία με το ινστιτούτο προβλημάτων διεθνούς ασφάλειας (IISP) διεξήγαγαν μελέτη σχετικά με τους κυβερνοπολέμους και τη διεθνή ασφάλεια, η οποία εγκρίθηκε από το υπουργείο άμυνας της χώρας. Η έρευνα αυτή ενσωμάτωσε τον κυβερνοπόλεμο σ’ έναν πόλεμο πληροφορίας που επικεντρώνεται σε επιθέσεις κατά των συστημάτων διοίκησης – ελέγχου και λήψης αποφάσεων, χωρίς να παραλείπει και τις ανθρώπινες διεργασίες.

Πιο συγκεκριμένα εστίασε στις αρχές των κυβερνοεπιχειρήσεων και άλλων δραστηριοτήτων στον κυβερνοχώρο. Ανέλυσε τις κύριες ιδεολογικές και οργανωτικές δομές του κυβερνοπολέμου καθώς και την ανάπτυξη μίας στρατιωτικής δύναμης και των βασικών αρχών των κινεζικών στρατηγικών του κυβερνοπολέμου. Συμπερασματικά, σύμφωνα με την προαναφερθείσα έρευνα, η ανάπτυξη μίας αντίδρασης σ’ αυτές τις περιπτώσεις πρέπει να οργανωθεί πάνω σε μία διεπιστημονική βάση και να περιλαμβάνει ερευνητές από διαφορετικούς κλάδους,

[40] https://www.dhs.gov/topic/cybersecurity, (έγινε πρόσβαση στις 16 Μαρ 2019)
[41] Ελένη, Καψοκόλη, *ΝΑΤΟ και Κυβερνοάμυνα,* Διάλεξη στο 6ο Συνέδριο Ελληνικής Υψηλής Στρατηγικής, ΛΑΕΔ, 27 Μαρτίου 2019
[42] Φλώρα, Σίμου, Διπλωματική Εργασία του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, *Κυβερνοπόλεμος και επιθέσεις στο διαδίκτυο,*, Οκτώβριος 2016

πολιτικούς αναλυτές, κοινωνιολόγους, ψυχολόγους, στρατιωτικούς ειδικούς εκπροσώπους των ΜΜΕ, αφού υπάρχουν επιπτώσεις σε όλο το εύρος της ανθρώπινης δραστηριότητας.[43]

Συμπληρωματικά στη συνεργασία μεταξύ της Ρωσίας και των ΗΠΑ συζητήθηκαν:

α. Η ανάληψη της ευθύνης στα κράτη ξεχωριστά, προκειμένου εκείνα να παρακολουθούν τα δικά τους δίκτυα.

β. Η υιοθέτηση ενός εγχώριου δικαίου κυβερνοπολέμου σε σχέση με το δίκαιο του πολέμου και τις άλλες μορφές δικαίου (της θάλασσας, του διαστήματος κλπ).

Είναι οφθαλμοφανές ότι οι περισσότερες κυβερνοεπιθέσεις που γίνονται στις κρίσιμες υποδομές ενός έθνους κράτους δεν θα είναι ανιχνεύσιμες και παρόλο που μπορεί να είναι δυνατόν να εντοπιστεί η τοποθεσία από όπου εξαπολύθηκε η επίθεση, τα υπεύθυνα άτομα και οι υπεύθυνοι για τη λήψη αποφάσεων είναι πολύ πιο δύσκολο να ανιχνευθούν δεδομένου των τρεχόντων τεχνολογικών εργαλείων και τεχνικών.

Σε μία τέτοια εποχή που οι κυβερνοεπιθέσεις και οι αμυντικές επιθέσεις των εθνών αυξάνονται ολοένα και πιο πολύ, το γνωμικό του Γκάντι «οφθαλμός αντί οφθαλμού και σύντομα όλος ο κόσμος θα είναι τυφλός» βρίσκει απόλυτη εφαρμογή.

2.4.3 Λιθουανία.[44]Η Λιθουανία γίνεται στόχος κυβερνοεπίθεσης περίπου 55 χιλιάδες φορές κάθε χρόνο, ενώ σε ολόκληρη την ΕΕ καταγράφονται 4 χιλιάδες κυβερνοεπιθέσεις κάθε μέρα. Τα μεγαλύτερα ποσοστά των επιθέσεων αυτών αφορούν στο δημόσιο τομέα (28%), στον τομέα της ενέργειας (20%), στον τομέα της εξωτερικής πολιτικής και δημόσιας ασφάλειας (19%) και τέλος στον οικονομικό τομέα (11%), ενώ οι κρίσιμες υποδομές της κυβέρνησης, της ενέργειας και του στρατού, είναι εκείνες που στοχοποιούνται περισσότερο.

Προκειμένου να ανταποκριθεί η κυβέρνηση στις σύγχρονες πρακτικές κυβερνοασφάλειας, ίδρυσε το εθνικό κέντρο κυβερνοπολέμου, το οποίο αποτελεί την εθνική CERT[45] και υπάγεται απευθείας στο ΥΠΕΘΑ. Από την 1η Ιανουαρίου 2018

[43] Dan, Fayutkin, «The American and Russian Approaches to Cyber Challenges», *Journal of Defence Management*, 2012, https://www.omicsonline.org/open-access/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (έγινε πρόσβαση στις16 Μαρ 2019)
[44] ΥΦΕΘΑ της Λιθουανίας, ομιλία, παρουσίαση στη ΣΕΘΑ, 13 Φεβ 2019
[45] Computer Emergency Response Team

υπεύθυνος για τη λειτουργία του κέντρου είναι ο ίδιος ο ΥΦΕΘΑ. Το κέντρο είναι υπεύθυνο να ενσωματώσει όλους του κυβερνητικούς, στρατιωτικούς και δημόσιους φορείς κάτω από μια ενιαία αρχή και να τους συντονίσει ώστε να υπάρχει κοινή πολιτική στα θέματα που αφορούν τον κυβερνοπόλεμο.

Οι βασικοί πυλώνες της εθνικής πολιτικής κυβερνοασφάλειας της Λιθουανίας είναι:

α. Ενίσχυση των εθνικών δυνατοτήτων κυβερνοάμυνας.

β. Αποτροπή και εξιχνίαση όλων των κυβερνοεγκλημάτων.

γ. Αύξηση της ευαισθητοποίησης σε θέματα κυβερνοχώρου και ενίσχυση της καινοτομίας.

δ. Στενή συνεργασία δημόσιου και ιδιωτικού τομέα.

ε. Διεθνής συνεργασία.

Μαζί με τη χώρα μας συμμετέχει ενεργά σε όλα τα προγράμματα της ΕΕ (PESCO) που έχουν να κάνουν με τον κυβερνοχώρο.

Επιπλέον έχει συνάψει με τις ΗΠΑ συμφωνία που αφορά στους εξής τομείς:

α. Δημιουργία περιφερειακού κέντρου κυβερνοάμυνας, εμπλέκοντας τις ΗΠΑ στην υπεράσπιση του εθνικού κυβερνοχώρου.

β. Συνεργασία που αφορά στην εξασφάλιση του ενεργειακού τομέα από κυβερνοεπιθέσεις.

γ. Στενότερη συνεργασία με την εθνική φρουρά της Πενσυλβάνια σε θέματα πληροφορικής, παρακολούθησης εκλογών, κυβερνοασκήσεων κλπ.

Αυτή τη στιγμή η κυβέρνηση της χώρας έχει εφαρμόσει συγκεκριμένες πολιτικές στο χώρο της κυβερνοασφάλειας, μερικές από τις οποίες είναι:

α. Χορήγηση και έλεγχος κάθε IP address,[46] σε χρήστες που αφορούν κρίσιμες υποδομές, μόνο μέσα από τη εθνικό CERT.

β. Έχουν ενταχθεί μαθήματα που αφορούν τη σωστή συμπεριφορά και χρήση των Η/Υ, σε όλο το φάσμα της εκπαίδευσης, ξεκινώντας από τους μαθητές των 6-7 ετών.

γ. Το ίδιο έχει συμβεί και σε όλες τις στρατιωτικές ακαδημίες της χώρας, καθώς και στα εθνικά μέσα ενημέρωσης, προκειμένου να χειρίζονται με το σωστό τρόπο τις ευαίσθητες πληροφορίες.

[46] Διεύθυνση IP - διεύθυνση διαδικτυακού πρωτοκόλλου (*IP address - Internet Protocol address*) είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol standard για τη μεταξύ τους αναγνώριση και συνεννόηση).

Βλέπουμε πως μια μικρή χώρα που θέτει, πολύ ορθά, ως προτεραιότητα τη διασφάλιση των κρίσιμων υποδομών και την ασφάλεια των πληροφοριών, μπορεί να εξελιχθεί ως πρότυπο σε διεθνή επίπεδο. Η Λιθουανία θεωρείται πρωτοπόρος πλέον σε θέματα κυβερνοπολέμου σε παγκόσμιο επίπεδο.

Κεφάλαιο Τρίτο

Κυβερνοπόλεμος και Εθνική Ασφάλεια

3.1 Είναι ο Κυβερνοπόλεμος πόλεμος;

Σύμφωνα με την επικρατούσα ερμηνεία, «ο όρος επίθεση αφορά στις ενέργειες που μπορεί να προβεί ένα κράτος, το οποίο διαθέτει οργανωμένες στρατιωτικές δυνάμεις και δύναται να υποστηρίξει μια στρατιωτική επιχείρηση τέτοιου μεγέθους που θα απειλήσει την εδαφική κυριαρχία ή την πολιτική ανεξαρτησία ενός άλλου κράτους».[47] Τα ενδιαφέροντα σημεία είναι:

α. Η ύπαρξη δύο τουλάχιστον εμπλεκομένων.

β. Οι εμπλεκόμενοι να είναι κράτη.

γ. Η επιχείρηση να είναι στρατιωτική.

δ. Το μέγεθος της επιχείρησης να είναι τέτοιο που να απειλεί την εδαφική κυριαρχία ή την πολιτική ανεξαρτησία του άλλου κράτους.

Τα παραπάνω απαιτείται να ισχύουν σωρευτικά, ώστε να μπορεί μια πράξη βίας να θεωρηθεί επίθεση και έτσι το κράτος που την υφίσταται να έχει δικαίωμα στην άμυνα, μεμονωμένα ή συλλογικά.

Ο Κλαούζεβιτς από την άλλη, ορίζει τον πόλεμο «ως πράξη βίας με σκοπό την επιβολή της θέλησης στον αντίπαλο». Σήμερα, η εξέλιξη της επιστήμης, της τεχνολογίας, το γεγονός ότι τα σύγχρονα κράτη εξαρτώνται όλο και περισσότερο από αυτή, καθώς επίσης και η δομή λειτουργίας των σύγχρονων κρατών, δημιούργησε δυνατότητες χρήσης νέων μέσων προκειμένου να ασκηθεί η επιβολή της θέλησης του ενός επί του αντιπάλου. Αυτές τις δυνατότητες προσφέρει ο Κυβερνοπόλεμος, οι οποίες προσβάλλουν τον αντίπαλο στόχο όχι καταλαμβάνοντας έδαφος αλλά μέσω της απομείωσης της επικοινωνιακής και πληροφοριακής του υποδομής. Ο Κυβερνοπόλεμος είναι δυνατόν να επηρεάσει τη θέληση του αντιπάλου, είτε με την αποτροπή είτε με τον πειθαναγκασμό, από τη στιγμή που οι στόχοι που μπορούν να προσβληθούν είναι πάρα πολλοί και οι επιπτώσεις πολύ σοβαρές. Το να χρησιμοποιεί λοιπόν κάποιος τις Κυβερνοδυνατότητες εναντίον κάποιου αντιπάλου, είναι σαν να διεξάγει πόλεμο, σύμφωνα με τον ορισμό του πολέμου, όπως τον έθεσε ο Κλαούζεβιτς.

[47] Κώστας, Χατζηκωνσταντίνου και Χαράλαμπος, Αποστολίδης και Μιλτιάδης, Σαρηγιάννης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο,* Αθήνα, Σάκκουλα, 2014

3.2 Σκοπός Κυβερνοπολέμου

Ο Κυβερνοπόλεμος, όπως και κάθε πόλεμος διεξάγεται προκειμένου να εξυπηρετήσει συγκεκριμένους πολιτικούς σκοπούς, οι οποίοι προσδιορίζονται στα πλαίσια της Υψηλής Στρατηγικής, από την εκάστοτε πολιτική ηγεσία. Για να έχει όμως πιθανότητες να επιτύχει μια Κυβερνοεπιχείρηση θα πρέπει να τεθεί ο τελικός σκοπός αυτής. Σ' αυτή την περίπτωση δεν μιλάμε πλέον για κατάληψη και κατοχή εδαφών ή καταστροφή ενόπλων δυνάμεων. Αυτές είναι αποστολές που αναλαμβάνουν οι καθαρά συμβατικές ένοπλες δυνάμεις, σε συμβατικό είδος πολέμου. Κάποια παραδείγματα πολιτικών σκοπών που δύναται να εξυπηρετήσει ο Κυβερνοπόλεμος είναι τα ακόλουθα:

α. Απλή παρενόχληση πληροφοριακών υποδομών, προκειμένου να υπενθυμίσουμε στον αντίπαλο τις δυνατότητές μας.

β. Πειθαναγκασμός αντιπάλου, πριν τη λήψη σημαντικών αποφάσεων.

γ. Εκδίκηση για αποφάσεις που πάρθηκαν ενάντια στα συμφέροντα της χώρας που εκτελεί την Κυβερνοεπίθεση. Το πλέον πρόσφατο παράδειγμα αποτελεί η επίθεση που έγινε στην Εσθονία το 2007.

3.3 Στόχοι Κυβερνοπολέμου

3.3.1 Γενικά.Η χρήση του Κυβερνοπολέμου δύναται να επιτύχει τον πολιτικό σκοπό ενός πολέμου. Η χρήση αυτή όμως απαιτεί τη συντονισμένη εκδήλωση Κυβερνοεπιθέσεων σε στόχους, η προσβολή των οποίων θα επιφέρει το επιθυμητό αποτέλεσμα. Τέτοιους στόχους αποτελούν οι κρίσιμες υποδομές μιας χώρας.

3.3.2 Κρίσιμες Υποδομές. Ως Κρίσιμες υποδομές χαρακτηρίζονται εκείνες οι φυσικές και ηλεκτρονικές υποδομές οι οποίες εξασφαλίζουν όλες τις βασικές λειτουργίες ενός κράτους. Οι σύγχρονες κοινωνίες αυξάνουν συνεχώς την άμεση εξάρτησή τους από κρίσιμες υποδομές οι οποίες μάλιστα, λόγω της εξελιγμένης τεχνολογίας, είναι διασυνδεδεμένες μεταξύ τους, σαν ένα ενιαίο δίκτυο. Η διασυνδεσιμότητα αυτή, από τη μία αυξάνει την αποτελεσματικότητα λειτουργίας των υποδομών αυτών και επομένως διευκολύνει την καθημερινότητα του πολίτη, από την άλλη όμως αποτελεί την ''αχίλλειο πτέρνα'' τους, καθιστώντας αυτές ιδανικούς στόχους Κυβερνοεπιθέσεων. Κάθε πρόβλημα στη λειτουργία τους έχει πολλαπλάσιο αντίκτυπο στην κοινωνία, χωρίς καν να είναι απαραίτητη η καταστροφή τους.

Τέτοιου τύπου επιθέσεις δεν έχουν σαν σκοπό την πρόκληση απωλειών σε ανθρώπινο δυναμικό. Στοχεύουν στον πειθαναγκασμό του λαού ή της εκάστοτε κυβέρνησης, ώστε αυτή, αντιλαμβανόμενη το μη αποδεκτό ρίσκο ενδεχόμενων ενεργειών της, να αναθεωρήσει τις αποφάσεις της και να πράξει ανάλογα. Μια διακοπή ηλεκτρικής ενέργειας, μετά από προσβολή ενός κρίσιμου υποσταθμού, θα επέφερε σημαντικό πλήγμα στο εθνικό σύστημα υγείας. Οποιαδήποτε παρεμβολή σε εθνικό σύστημα αντιμετώπισης εκτάκτων αναγκών, θα προκαλούσε πρωτίστως απώλειες ανθρωπίνων ζωών, αλλά οι πολίτες θα έχαναν την εμπιστοσύνη προς το κράτος, αφού το τελευταίο θα αδυνατούσε να τους παράσχει οποιαδήποτε βοήθεια.

3.3.3 Στοχοποίηση των κρίσιμων υποδομών. Η διάταξη των κρίσιμων υποδομών μιας χώρας στόχου θα μπορούσε να παραλληλισθεί με το χάρτη πληροφοριών του αντιπάλου, όπου εκεί φαίνεται η διάταξη μάχης στην περίοδο των επιχειρήσεων.

Θα αναρωτηθεί κανείς πως είναι δυνατόν να αποκρύψει ή εκάστοτε κυβέρνηση τις υποδομές αυτές αφού, πλήθος πληροφοριών που τις αφορούν είναι προσβάσιμες ακόμα και από τις ανοιχτές πηγές. Η τρωτότητα της κάθε υποδομής όμως εξαρτάται από το βαθμό διασυνδεσιμότητάς της με δίκτυα πληροφοριακών συστημάτων. Αν δηλαδή δεν διαθέτει συστήματα πληροφορικής ή επικοινωνιών, τότε πιθανότατα δεν μπορεί να γίνει θύμα κυβερνοεπίθεσης. Επίσης η λειτουργία των σύγχρονων συστημάτων ελέγχου εγκαταστάσεων δεν είναι προσβάσιμη και γνωστή από όλους. Επομένως δεν αρκεί απλά και μόνο η γνώση ύπαρξης μιας υποδομής για να καταστεί στόχος.

Επόμενο στάδιο στη στοχοποίηση αποτελεί η ιεράρχηση των στόχων του κυβερνοπολέμου. Αυτό γίνεται για δύο λόγους, πρώτον για να επιλεχθεί ο τρόπος και το μέσο προσβολής, ανάλογα με τη διαθεσιμότητα και δεύτερον για να αποφασιστεί ο χρόνος προσβολής. Για παράδειγμα, όταν βρισκόμαστε στην αρχή μιας κρίσης ή όταν η κρίση δεν έχει αποκαλυφθεί ακόμα, προσβάλλονται κυρίως οικονομικοί στόχοι του αντιπάλου. Όταν η κρίση κλιμακώνεται, σειρά έχουν οι υποδομές που υποστηρίζουν επικοινωνίες, συγκοινωνίες και το μηχανισμό αντιμετώπισης εκτάκτου αναγκών. Τέλος όταν η κρίση ξεσπά, προσβάλλονται υποδομές που σχετίζονται καθαρά με τις Ένοπλες Δυνάμεις του εχθρού.

Κρίσιμες υποδομές που θα μπορούσαν να αποτελέσουν στόχους του Κυβερνοπολέμου, είναι υποδομές.[48]

α. Πληροφορικής και επικοινωνιών.

β. Οικονομικών υπηρεσιών.

γ. Συστήματος παραγωγής-διάθεσης ηλεκτρικής ενέργειας.

δ. Συστήματος παραγωγής – αποθήκευσης-διάθεσης φυσικού αερίου.

ε. Συγκοινωνιών (οδικών, αεροπορικών, θαλάσσιων κ.α.).

στ. Υδάτινων πόρων.

ζ. Εξυπηρέτησης πολιτών.

η. Παροχής υγειονομικών υπηρεσιών.

Επομένως, ως αποστολή του κυβερνοπολέμου μπορεί να ορισθεί η προστασία των κρίσιμων υποδομών του κράτους μέσω της προστασίας όλων των δικτυοκεντρικών συστημάτων, δημόσιων και ιδιωτικών, από ενδεχόμενες επιθέσεις που θα είχαν ως στόχο την υποβάθμιση της λειτουργίας τους και την πρόκληση λειτουργικών ή φυσικών βλαβών, καθώς επίσης και η πρόκληση ανάλογων αποτελεσμάτων στον αντίπαλο, στα πλαίσια πάντα καθορισμένης εθνικής στρατηγικής ασφαλείας.

[48] Παναγιώτης, Μαυρόπουλος, *Κυβερνοπόλεμος και Εθνική Στρατηγική*

Κεφάλαιο Τέταρτο
NATOκαι Κυβερνοπόλεμος

4.1 Γενικά

Μέχρι την κυβερνοεπίθεση που δέχτηκε η Εσθονία το 2007 το NATO θεωρούσε τον κυβερνοπόλεμο μια πιθανή αλλά μακρινή απειλή. Το γεγονός ότι τα κράτη χρησιμοποιούσαν την πληροφοριακή τεχνολογία για να εισβάλουν σε δίκτυα άλλων χωρών με σκοπό τον εντοπισμό τρωτών σημείων και τη συλλογή πολιτικών, στρατιωτικών, οικονομικών, βιομηχανικών και τεχνολογικών πληροφοριών, ήταν ανεκτό ως φυσιολογική δραστηριότητα. Η κυβερνοεπίθεση εναντίον της Εσθονίας έδωσε νέες διαστάσεις στο φαινόμενο. Ήταν μια προσπάθεια αποσταθεροποίησης της χώρας με οικονομικές επιπτώσεις. Μετά τη σύνοδο της Πράγας το 2002, το NATO ξεκίνησε την πρωτοβουλία ‘’πρόγραμμα κυβερνοάμυνας’’ (Technical NATO Cyber Defense), η οποία οδήγησε στην ίδρυση του NATO Computer IncidentResponse Team (NCIRT), κάτι αντίστοιχο με τα CERT[49]. Στις αρχές του 2008, μετά από πρόταση των Εσθονικών αρχών, το NATO συμφώνησε στην ίδρυση του Κέντρου Αριστείας Κυβερνοάμυνας, CCD-CoE[50]στο Ταλίν.

Το NATO Cooperative Cyber Defense Centre of Excellence (CCD-CoE) είναι ένα αναγνωρισμένο από το NATO κέντρο αλληλεγγύης στον κυβερνοχώρο με επίκεντρο την έρευνα, την εκπαίδευση και τις ασκήσεις. Αντιπροσωπεύει μια κοινότητα 21 χωρών παρέχοντας μια σφαιρική ματιά στην άμυνα στον κυβερνοχώρο, με τεχνογνωσία στους τομείς της τεχνολογίας, της στρατηγικής, των επιχειρήσεων και του νόμου. Η καρδιά του Κέντρου είναι μια διαφορετική ομάδα διεθνών εμπειρογνωμόνων με στρατιωτικό, κυβερνητικό, ακαδημαϊκό και βιομηχανικό υπόβαθρο.

Το CCD-CoE φιλοξενεί το Εγχειρίδιο του Ταλλίν 2.0, τον πιο ολοκληρωμένο οδηγό για τον τρόπο με τον οποίο το Διεθνές Δίκαιο εφαρμόζεται στις επιχειρήσεις του κυβερνοχώρου. Το Κέντρο διοργανώνει τη μεγαλύτερη και πιο πολύπλοκη διεθνή άσκηση προστασίας από απειλές στον κυβερνοχώρο, Locked Shields. Κάθε άνοιξη το Κέντρο φιλοξενεί στο Ταλίν το Διεθνές Συνέδριο για τις Κυβερνοσυμπλοκές, (CyCon), μια μοναδική εκδήλωση που συγκεντρώνει τους βασικούς εμπειρογνώμονες και τους υπεύθυνους λήψης αποφάσεων της παγκόσμιας κοινότητας άμυνας στον

[49] Στο ίδιο
[50] Cooperative Cyber Defense Center of Excellence

κυβερνοχώρο. Από τον Ιανουάριο του 2018, το CCD-CoE είναι υπεύθυνο για τον προσδιορισμό και τον συντονισμό των λύσεων εκπαίδευσης και κατάρτισης στον τομέα των επιχειρήσεων Κυβερνοάμυνας για όλα τα όργανα του NATO σε ολόκληρη τη Συμμαχία. Το Κέντρο στελεχώνεται και χρηματοδοτείται από τα κράτη μέλη του, τα οποία σήμερα είναι: Αυστρία, Βέλγιο, Τσεχική Δημοκρατία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιταλία, Λετονία, Λιθουανία, Σουηδία, Τουρκία, το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες.

Συγκεντρώνει δε ερευνητές, αναλυτές και εκπαιδευτικούς από το στρατό, την κυβέρνηση, τον ακαδημαϊκό κόσμο και τη βιομηχανία.[51] Το κέντρο πρακτικά αποτελεί ένα χώρο ανταλλαγής πληροφοριών και ενημέρωσης μεταξύ των ειδικών, καθώς και εκπαίδευσης αξιωματικών του NATO σε θέματα κυβερνοπολέμου.

Η Συμμαχία έχει αντιληφθεί ότι αντιμετωπίζει πλέον ένα εξελισσόμενο και περίπλοκο περιβάλλον απειλής. Το NATO και οι σύμμαχοί του βασίζονται σε ισχυρές και ανθεκτικές κυβερνητικές άμυνες για την εκπλήρωση των βασικών καθηκόντων της συμμαχίας, για συλλογική άμυνα, διαχείριση κρίσεων και συνεταιριστική ασφάλεια. Το NATO πρέπει να είναι έτοιμο να υπερασπιστεί τα δίκτυα και τις επιχειρήσεις του ενάντια στην αυξανόμενη πολυπλοκότητα των απειλών του κυβερνοχώρου και των επιθέσεων που αντιμετωπίζει.[52]

Η πολιτική αυτή, που έχει πλέον υιοθετήσει το NATO, βασίζεται στη συλλογική άμυνα (άρθρο 5 του NATO), τη βοήθεια/ενίσχυση στα κράτη-μέλη, την εφαρμογή του διεθνούς δικαίου, τον επιχειρησιακό προγραμματισμό, τη κατάρτιση και την εκπαίδευση του προσωπικού μέσω κοινών ασκήσεων, καθώς και την ενισχυμένη ανταλλαγή πληροφοριών.

4.2 Κέντρο συνεργασίας και ασφάλειας στον κυβερνοχώρο[53]

Οι κυβερνοπολεμιστές της συμμαχίας έχουν, από την 12 Φεβρουαρίου 2019, μια νέα κοινότητα που δημιουργήθηκε από τον Οργανισμό Επικοινωνιών και Πληροφοριών του NATO (NCIA).[54]Οι ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης θα συνδέονται μεταξύ τους με προστατευμένο δίκτυο για τις επιχειρήσεις και θα

[51] https://ccdcoe.org/about-us/, (έγινε πρόσβαση στις 28 Μαρ 2019)
[52] https://www.nato.int/cps/en/natohq/topics_78170.htm, (έγινε πρόσβαση στις 28 Μαρ 2019)
[53] Cyber Security Collaboration Hub
[54] NATO Communications and Information Agency

προέρχονται από το Βέλγιο, τη Γαλλία, τις Κάτω Χώρες, το Ηνωμένο Βασίλειο και τις ΗΠΑ.[55]

Τα κράτη-μέλη της συμμαχίας έχουν πλέον ένα χώρο, στον οποίο μπορούν:

α. Να ανταλλάσσουν πληροφορίες.

β. Να μοιράζονται τις βέλτιστες πρακτικές,

γ. Να συνεργάζονται σ' ένα κρυπτογραφημένο περιβάλλον για την αντιμετώπιση και αποτροπή πιθανών μελλοντικών απειλών.

Προβλέπεται να υπάρχει ολοκληρωμένη πρόσβαση από όλα τα κράτη-μέλη, πριν το τέλος του 2019. Η χώρα μας εργάζεται πάνω σ' αυτό το σκοπό.

4.3 Από την παθητική στην ενεργητική άμυνα[56]

Το 2013, μέσω του Tallinn manual I, έγινε η πρώτη αναφορά στο νομικό πλαίσιο της ενεργητικής άμυνας (active defense). Η ενεργητική άμυνα αποτελείται από μια σειρά προληπτικών μέτρων με σκοπό τον εντοπισμό ή τη συλλογή πληροφοριών σχετικά με μια πιθανή κυβερνοεπίθεση» ή κυβερνοεισβολή, η οποία εκδηλώνει μια προληπτική κυβερνο-αντι-επιχείρηση (cyber counter operation) εναντίον του δρώντα. Αναλύεται επιπλέον η εφαρμογή του δικαίου ενόπλων συγκρούσεων (law of armed conflict) σε πιθανές συγκρούσεις. Πότε δηλαδή βρισκόμαστε σε απειλή και πότε όχι.

Το 2017, μέσω του Tallinn manual II, γίνεται η δεύτερη αναφορά στο νομικό πλαίσιο της ενεργητικής άμυνας, το οποίο πραγματεύεται τη διεξαγωγή επιχειρήσεων στον κυβερνοχώρο, οι οποίες είναι συμβατές με το διεθνές δίκαιο. Τα ερωτήματα που τέθηκαν ήταν:

α. Ποιος ο νομιμοποιημένος στόχος;

β. Πως προσδιορίζεται η αμυντική και η επιθετική δράση στον κυβερνοχώρο;

Όλα τα παραπάνω θέματα απασχολούν το τρέχον διάστημα τη συμμαχία, η οποία έχει αποδεχτεί πλήρως το ρόλο της για την άμυνα και την ασφάλεια στον κυβερνοχώρο.

---

[55] https://www.nato.int/cps/en/natohq/news_163358.htm?selectedLocale=en, (έγινε πρόσβαση στις 28 Μαρ 2019)

[56] Ελένη, Καψοκόλη, *ΝΑΤΟ και Κυβερνοάμυνα,* Διάλεξη στο 6ο Συνέδριο Ελληνικής Υψηλής Στρατηγικής, ΛΑΕΔ, 27 Μαρτίου 2019

Κεφάλαιο Πέμπτο
Ελλάδα και Κυβερνοπόλεμος

5.1 Γενικά

Η εξέλιξη της τεχνολογίας τα τελευταία χρόνια, που έχει οδηγήσει στην καθημερινή χρήση των δικτύων Η/Υ σχεδόν σε όλες τις μορφές της ανθρώπινης δραστηριότητας, καθιστούν τον κυβερνοχώρο που εμπεριέχει τα ανωτέρω δίκτυα εξαιρετικά σημαντικό για την ασφάλεια της χώρας. Ο κυβερνοχώρος ενώ αποτελεί την πέμπτη διάσταση διεξαγωγής των σύγχρονων επιχειρήσεων, είναι εξίσου ή και κατά περίπτωση περισσότερο σημαντική από αυτές. Η οποιαδήποτε λοιπόν ενέργεια ή εμπλοκή στο πεδίο αυτό, προκειμένου να επιτευχθούν οι επιδιωκόμενοι στόχοι, θα πρέπει να σχεδιάζεται σε επίπεδο Υψηλής Στρατηγικής από κατάλληλα κυβερνητικά όργανα. Ακολούθως αναφέρονται οι τελευταίες νομοθετικές εξελίξεις που πρόσφατα έλαβαν χώρα σε εθνικό επίπεδο, προκειμένου η χώρα να εξασφαλίσει την κυβερνοασφάλεια, όσο αυτό καθίσταται εφικτό, των κρίσιμων υποδομών της.

5.2 Νομοθετικό πλαίσιο και διατάξεις[57]

5.2.1 Γενικά. Σύμφωνα με το άρθρο 7 του νόμου 4577 της 3 Δεκεμβρίου 2018, ως «Εθνική Αρμόδια Αρχή για την ασφάλεια των συστημάτων δικτύου και πληροφοριών»[58]ή «Εθνική Αρχή Κυβερνοασφάλειας», ορίζεται η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης. Η Εθνική Αρχή καλύπτει τους τομείς της ενέργειας, των μεταφορών, των τραπεζών, των υποδομών χρηματοπιστωτικών αγορών, της υγείας, της προμήθειας και διανομής πόσιμου νερού και των ψηφιακών υποδομών.

Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT), η οποία καλύπτει τους παραπάνω τομείς και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, είναι η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ (ΓΕΕΘΑ/ΔΙΚΥΒ).

---

[57] Αρ. ΦΕΚ 199

[58] «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, με δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών

Οι αρμοδιότητες της Ελληνικής CSIRTείναι οι εξής:

α. Η παρακολούθηση των συμβάντων[59] σε εθνικό επίπεδο.

β. Η παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων επαγρύπνησης και ανακοινώσεων, καθώς και η διάδοση πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους[60] και συμβάντα.

γ. Η παρέμβαση σε περίπτωση συμβάντος.

δ. Η παροχή δυναμικής ανάλυσης κινδύνων και συμβάντων, καθώς και η επίγνωση της κατάστασης.

ε. Η συμμετοχή στο δίκτυο CSIRT και η συνεργασία με τις αντίστοιχες υπηρεσίες των υπόλοιπων κρατών–μελών στο πλαίσιο του δικτύου CSIRT.

στ. Η εγκαθίδρυση σχέσεων συνεργασίας με τον ιδιωτικό τομέα.

ζ. Η προώθηση, η υιοθέτηση και η χρήση κοινών ή τυποποιημένων πρακτικών για τις διαδικασίες χειρισμού συμβάντων και κινδύνων.

Η CSIRT συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στην οδηγία του Ευρωπαϊκού Κοινοβουλίου με την οποία θεσπίστηκαν μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

5.2.2 Ασφάλεια των συστημάτων δικτύου και πληροφοριών των φορέων εκμετάλλευσης βασικών υπηρεσιών.[61]Επιπλέον, η Εθνική Αρχή Κυβερνοασφάλειας σε συνεργασία με την CSIRT, και τους λοιπούς, ανά φορέα βασικής υπηρεσίας, εμπλεκόμενους φορείς:

α. Αξιολογεί τα τεχνικά και οργανωτικά μέτρα που λαμβάνουν οι φορείς εκμετάλλευσης βασικών υπηρεσιών για τη διαχείριση των κινδύνων που αφορούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους, ως προς την καταλληλότητα και την αναλογικότητά τους.

β. Αξιολογεί την καταλληλότητα των μέτρων που λαμβάνουν οι φορείς εκμετάλλευσης βασικών υπηρεσιών για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου

[59] «συμβάν»: κάθε γεγονός που έχει στην πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών

[60] «κίνδυνος»: κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός με ενδεχομένως δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών

[61] «φορέας εκμετάλλευσης βασικών υπηρεσιών»: δημόσια ή ιδιωτική οντότητα

και πληροφοριών που χρησιμοποιούνται για την παροχή των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειάς τους.

γ. Καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν οι φορείς εκμετάλλευσης βασικών υπηρεσιών, προκειμένου να κοινοποιήσουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT συμβάντα με σοβαρές επιπτώσεις στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών που αυτοί παρέχουν. Οι ανωτέρω κοινοποιήσεις εκ μέρους των φορέων εκμετάλλευσης βασικών υπηρεσιών πρέπει να πραγματοποιούνται χωρίς αδικαιολόγητη καθυστέρηση και να περιλαμβάνουν πληροφορίες που να επιτρέπουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT να προσδιορίσουν τόσο τη σοβαρότητα όσο και τις διασυνοριακές επιπτώσεις, λόγω του κοινοποιούμενου περιστατικού.

Προκειμένου να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος, λαμβάνονται υπόψη οι εξής παράμετροι:

α. Ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας.

β. Η διάρκεια του συμβάντος.

γ. Το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν.

Βάσει των πληροφοριών που κοινοποιούνται από το εκάστοτε φορέα εκμετάλλευσης βασικών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας ενημερώνει το ή τα άλλα επηρεαζόμενα κράτη-μέλη, εφόσον το κοινοποιούμενο συμβάν έχει σοβαρό αντίκτυπο στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών στο εν λόγω κράτος-μέλος. Στο πλαίσιο της ανωτέρω ενημέρωσης, διαφυλάσσεται, σύμφωνα με το ενωσιακό δίκαιο ή με την εθνική νομοθεσία, η ασφάλεια και τα εμπορικά συμφέροντα του κοινοποιούντος φορέα εκμετάλλευσης βασικών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που ενδεχομένως εμπεριέχονται στην κοινοποίησή του. Όταν οι περιστάσεις το επιτρέπουν, η Εθνική Αρχή Κυβερνοασφάλειας ή η αρμόδια CSIRT παρέχει στον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών, πληροφορίες όσον αφορά τις ενέργειες που έλαβαν χώρα σε συνέχεια της κοινοποίησής του, όπως πληροφορίες που θα μπορούσαν να υποστηρίξουν την αποτελεσματική διαχείριση του περιστατικού από τούδε και στο εξής.

Ύστερα από διαβούλευση με τον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να ενημερώνει το

κοινό σχετικά με μεμονωμένα συμβάντα, αν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη μελλοντικού συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη.

Η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να καταρτίζει και να εκδίδει κατευθυντήριες οδηγίες σχετικά με τις περιστάσεις υπό τις οποίες οι φορείς εκμετάλλευσης βασικών υπηρεσιών είναι υποχρεωμένοι να κοινοποιούν συμβάντα, συμπεριλαμβανομένων μεταξύ άλλων των παραμέτρων που προσδιορίζουν τη σοβαρότητα των επιπτώσεων ενός συμβάντος.

5.2.3 Ασφάλεια των συστημάτων δικτύου και πληροφοριών των παρόχων ψηφιακών υπηρεσιών.[62]Επιπλέον, η Εθνική Αρχή Κυβερνοασφάλειας σε συνεργασία με την CSIRT, και τους λοιπούς, εμπλεκόμενους φορείς:

α. Αξιολογεί τα τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που πρέπει να λάβουν οι πάροχοι ψηφιακών υπηρεσιών, όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στο πλαίσιο της παροχής, εντός της Ευρωπαϊκής Ένωσης. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο και να συνεκτιμούν ιδίως τα εξής στοιχεία:

(1) Την ασφάλεια των συστημάτων και των εγκαταστάσεων.

(2) Τη διαχείριση συμβάντων.

(3) Τη διαχείριση της επιχειρησιακής συνέχειας.

(4) Την παρακολούθηση, τους ελέγχους και τις δοκιμές δικτύων και πληροφοριακών συστημάτων.

(5) Τη συμμόρφωση με τα διεθνή πρότυπα.

β. Αξιολογεί τα μέτρα για την αποτροπή και την ελαχιστοποίηση των επιπτώσεων συμβάντων, τα οποία πρέπει να λάβουν οι πάροχοι ψηφιακών υπηρεσιών και επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν, σε σχέση με τις υπηρεσίες οι οποίες προσφέρονται εντός της Ευρωπαϊκής Ένωσης, με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειάς τους.

γ. Καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν οι πάροχοι ψηφιακών υπηρεσιών, προκειμένου να κοινοποιούν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT, χωρίς αδικαιολόγητη καθυστέρηση,

[62] «πάροχος ψηφιακών υπηρεσιών»: νομικό πρόσωπο που παρέχει ψηφιακή υπηρεσία

κάθε συμβάν που έχει σημαντικές επιπτώσεις στην παροχή της υπηρεσίας που παρέχεται από αυτούς εντός της Ευρωπαϊκής Ένωσης. Οι ανωτέρω κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT να προσδιορίσουν τόσο τη σοβαρότητα του συμβάντος όσο και τις διασυνοριακές επιπτώσεις.

Για να προσδιοριστεί αν οι επιπτώσεις ενός συμβάντος είναι σημαντικές, λαμβάνονται υπόψη οι εξής παράμετροι:

α. Ο αριθμός των χρηστών που επηρεάζονται από το συμβάν, ιδίως αυτών που εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών.

β. Η διάρκεια του συμβάντος.

γ. Το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν.

δ. Το μέγεθος της διατάραξης της λειτουργίας της υπηρεσίας.

ε. Η έκταση των επιπτώσεων στις οικονομικές και κοινωνικές δραστηριότητες.

Κατά περίπτωση, και συγκεκριμένα αν το συμβάν με σημαντικές επιπτώσεις αφορά δύο ή περισσότερα κράτη-μέλη, η Εθνική Αρχή Κυβερνοασφάλειας ενημερώνει τα άλλα κράτη-μέλη που επηρεάζονται από το συμβάν. Στο πλαίσιο της ενημέρωσης αυτής, το ενιαίο κέντρο επαφής σε συνεργασία με την αρμόδια CSIRT πρέπει, σύμφωνα με το ενωσιακό δίκαιο και την εθνική νομοθεσία που είναι σύμφωνη προς το ενωσιακό δίκαιο, να διαφυλάσσουν την ασφάλεια και τα εμπορικά συμφέροντα του παρόχου ψηφιακών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που ο τελευταίος έχει παράσχει. Το εθνικό ενιαίο κέντρο επαφής[63] διαβιβάζει τις κοινοποιήσεις συμβάντων στα αντίστοιχα ενιαία κέντρα επαφής των άλλων επηρεαζόμενων κρατών-μελών.

Ύστερα από διαβούλευση με τον ενδιαφερόμενο πάροχο ψηφιακών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT, και κατά περίπτωση, οι αρμόδιες αρχές ή τα αρμόδια CSIRT άλλων ενδιαφερόμενων κρατών-μελών μπορούν να ενημερώνουν το κοινό σχετικά με μεμονωμένα συμβάντα ή να απαιτούν από τον πάροχο ψηφιακών υπηρεσιών να το πράξει, όταν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος

[63] Η Εθνική Αρχή Κυβερνοασφάλειας ορίζεται ως το εθνικό ενιαίο κέντρο επαφής

ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη ή αν η αποκάλυψη του συμβάντος εξυπηρετεί το δημόσιο συμφέρον.

5.3 Κατευθυντήριο πλαίσιο ανάπτυξης κυβερνοάμυνας στις Ελληνικές Ένοπλες Δυνάμεις[64]

Η προστασία των εθνικών στρατιωτικών υποδομών που ανήκουν στον κυβερνοχώρο πρέπει να αποτελεί αναπόσπαστο μέρος της γενικής αμυντικής σχεδίασης των ΕΔ. Κατά συνέπεια, ο καθορισμός των βασικών στόχων που θα πρέπει να εκπληρώνονται από τις δράσεις της κυβερνοάμυνας θα πρέπει να είναι μία από τις βασικές προτεραιότητες σε επίπεδο στρατηγικής σχεδίασης. Το πρώτο βήμα αυτής της σχεδίασης είναι ο καθορισμός ενός κατευθυντήριου πλαισίου ανάπτυξης κυβερνοάμυνας στις ΕΔ. Σκοπός του κατευθυντήριου πλαισίου ανάπτυξης κυβερνοάμυνας στις ΕΔ είναι ο καθορισμός των Στρατηγικών και των Επιχειρησιακών στόχων της κυβερνοάμυνας.

5.3.1 Στόχοι κυβερνοάμυνας στις ΕΔ. Το πεδίο της κυβερνοάμυνας στις ΕΔ έχει ως κύριες αποστολές

α. Να διασφαλιστεί η ικανότητα λήψης αποφάσεων της ηγεσίας, μέσω της προστασίας των πληροφοριών.

Η ηγεσία και οι αρμόδιοι φορείς διαχείρισης των κρίσεων, πρέπει να έχουν τους πόρους για να επικοινωνούν με απόλυτη ασφάλεια σε οποιαδήποτε κατάσταση. Συνεπώς, τα δίκτυα πρέπει να επεκταθούν και να ασφαλιστούν, τόσο σε τοπικό επίπεδο (δίκτυο ΕΔ) όσο και σε Εθνικό επίπεδο. Η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που διανέμονται μέσω αυτών των δικτύων, είναι επιτακτική ανάγκη. Πρέπει να αναπτυχθεί και να διατηρηθεί η απαραίτητη τεχνογνωσία, ώστε να επιτευχθεί η τεχνολογική μας ανεξαρτησία.

Η διατήρηση της στρατηγικής ανεξαρτησίας της χώρας εξαρτάται από την ικανότητά μας να διαθέτουμε εγχώριες κρυπτογραφικές τεχνολογίες και μεθόδους, οι οποίες θα αξιοποιούνται στο σχεδιασμό εγχώριων προϊόντων ασφάλειας. Ως εκ τούτου, πρέπει να εξασφαλίσουμε ότι το πεδίο της ασφάλειας των συστημάτων πληροφορικής, παραμένει ελκυστικό για τους νέους

[64] Κατευθυντήριο Πλαίσιο Ανάπτυξης Κυβερνοάμυνας στις ΕΔ, ΓΕΕΘΑ/ΔΙΚΥΒ, Αυγ 2013

επιστήμονες, με σκοπό την απόκτηση εθνικής τεχνογνωσίας και τεχνολογικής εμπειρίας.

Εκτός από την ανάγκη ασφαλούς και εμπιστευτικής επικοινωνίας της ηγεσίας και των φορέων που εμπλέκονται στη διαχείριση των κρίσεων, θα πρέπει να διασφαλίζεται και η ύπαρξη εναλλακτικών διαύλων επικοινωνίας μεταξύ αυτών. Επιπλέον, θα πρέπει να σχεδιαστούν και να αναπτυχθούν ασφαλείς πόροι για την ηλεκτρονική ανταλλαγή δεδομένων, τηλεφωνίας και τηλεδιάσκεψης. Ειδικότερα για τους φορείς εκμετάλλευσης των υποδομών ζωτικής σημασίας, η ανάπτυξη των πόρων θα πρέπει να συνεχιστεί και τα επόμενα χρόνια.

β. Να ενισχυθεί η ασφάλεια των στρατιωτικών πληροφοριακών υποδομών και να υπάρξει συμβολή στην ασφάλεια των κρίσιμων εθνικών υποδομών στον κυβερνοχώρο.

Για την εκπλήρωση της αποστολής τους οι ΕΔ βασίζονται στη σωστή λειτουργία των πληροφοριακών τους υποδομών. Αυτό ισχύει, σε πολύ μεγαλύτερο ποσοστό, και στην λειτουργία του κρατικού μηχανισμού αλλά και της κοινωνίας γενικότερα. Πολλά αντικείμενα του πραγματικού κόσμου έχουν ενσωματωμένα πληροφοριακά συστήματα ή ελέγχονται από λογισμικό και αποτελούν πλέον στόχο κυβερνοεπιθέσεων. Οι επιθέσεις περιορίζονται στο επίπεδο δικτυακών εφαρμογών, αλλά έχουν μεταφερθεί και στο λογισμικό ελέγχου συστημάτων. Μια επιτυχημένη επίθεση στα εθνικά πληροφοριακά συστήματα και στον εθνικό κυβερνοχώρο, θα έχει σοβαρές κοινωνικές, πολιτικές και οικονομικές συνέπειες.

Οι ΕΔ θα πρέπει να λειτουργούν με υποδειγματικό τρόπο και να αποτελούν πρότυπο στην ασφάλεια των πληροφοριακών υποδομών τους. Θα πρέπει να βρίσκονται σε στενή συνεργασία με τους εθνικούς παρόχους, τους κατασκευαστές υλικού και λογισμικού ασφαλείας και τους αντίστοιχους φορείς χρήσης - εκμετάλλευσης των πληροφοριακών συστημάτων, ώστε να βελτιώνουν συνεχώς και να επιτυγχάνουν υψηλό επίπεδο ασφάλειας, των δικών τους πληροφοριακών συστημάτων αλλά και κατ' επέκταση των κρίσιμων Εθνικών πληροφοριακών υποδομών. Τα στελέχη θα πρέπει να είναι σε θέση να εμπιστεύονται τις ηλεκτρονικές υπηρεσίες που παρέχονται μέσα από τα πληροφοριακά συστήματα των ΕΔ.

γ. Να γίνουν οι ΕΔ μια ανταγωνιστική δύναμη στο διεθνή χώρο της κυβερνοάμυνας.

Σε αντίθεση με τον φυσικό χώρο, οι συγκρούσεις στον κυβερνοχώρο δεν γνωρίζουν σύνορα. Έτσι, αξιόπιστη κυβερνοάμυνα δεν μπορεί να επιτευχθεί με δράσεις που περιορίζονται μόνο σε εθνικό επίπεδο. Θα πρέπει, η όλη προσπάθεια, να στηρίζεται σ' ένα δίκτυο από συμμάχους με τους οποίους σε πραγματικό χρόνο θα μπορούν να ανταλλάσσονται πληροφορίες για τρωτότητες, μηχανισμούς προστασίας, επιθέσεις καθώς και πιθανά αντίμετρα που μπορούν να εφαρμοστούν. Οι ΕΔ θα πρέπει να αναπτύξουν και να ενισχύσουν συνεργασίες με συμμάχους και βασιζόμενες στην εμπειρία τους να συμβάλουν ενεργά στη διαμόρφωση των πολιτικών κυβερνοάμυνας στο πλαίσιο τόσο των Εθνικών φορέων, όσο και των Διεθνών οργανισμών, ιδίως του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης.

Διατηρώντας επιπλέον τη στρατηγική ανεξαρτησία της η Ελλάδα, μέσω των ΕΔ πρέπει να εργαστεί σκληρά για να ενταχθεί και να παραμείνει στον κύκλο των ανεπτυγμένων και ισχυρών κρατών στον τομέα της κυβερνοάμυνας. Η συνεργασία με τα μέλη αυτού του κύκλου, τόσο σε επιχειρησιακό επίπεδο, όσο και σε επίπεδο εφαρμογής μιας ενιαίας στρατηγικής για την αντιμετώπιση των κοινών απειλών, θα έχει πολλαπλά οφέλη για την χώρα.

5.4 Πολιτική κυβερνοάμυνας στις Ελληνικές Ένοπλες Δυνάμεις[65]

Η εκπλήρωση της αποστολής των ΕΔ βασίζεται σε μεγάλο βαθμό στην απρόσκοπτη λειτουργία των κρίσιμων Συστημάτων Επικοινωνιών και Πληροφορικής (ΣΕΠ) (Communication and Information Systems, CIS). Οι εξελίξεις στο τομέα της πληροφορικής προσφέρουν σημαντικές δυνατότητες στην βελτιστοποίηση της οργάνωσης και της λειτουργίας των ΕΔ. Ταυτόχρονα, όμως, η ολοένα αυξανόμενη εξάρτηση από την τεχνολογία δημιουργεί νέες απειλές και τρωτότητες. Ως εκ τούτου, καθίσταται προφανές ότι η ασφαλής και αξιόπιστη χρήση του κυβερνοχώρου είναι ζωτικής σημασίας για την εθνική άμυνα της χώρας.

Οι απειλές στον κυβερνοχώρο αντιπροσωπεύουν μια βαθιά πρόκληση για τη σταθερότητα, την ευημερία και την ασφάλεια της χώρας και μπορεί να προέρχονται τόσο από εχθρικά κράτη όσο και από τρομοκρατικές ομάδες, εγκληματικές οργανώσεις ή χάκερς. Η κλίμακα και η πολυπλοκότητα των κυβερνοεπιθέσεων τα τελευταία χρόνια αυξάνονται σταθερά και μπορούν να οδηγήσουν σε διαρροή διαβαθμισμένων πληροφοριών, δυσλειτουργία του συστήματος διοίκησης και

[65] Πολιτική Κυβερνοάμυνας στις ΕΔ, ΓΕΕΘΑ/ΔΙΚΥΒ, Φεβ 2014

ελέγχου, δυσχέρεια στην εκτέλεση επιχειρήσεων ή ακόμα και σε καταστροφή υλικού και απώλεια ανθρώπινων ζωών. Συνεπώς, η χώρα θα πρέπει να έχει τη δυνατότητα να αποτρέψει και να αμυνθεί ενάντια σε οποιαδήποτε κυβερνοαπειλή και κυβερνοεπίθεση.

Οι Ελληνικές ΕΔ, αυτή την περίοδο που γράφεται η παρούσα διατριβή, διαθέτουν μια συγκεκριμένη πολιτική κυβερνοάμυνας ή οποία καθορίζει το βασικό πλαίσιο, ώστε μέσα από συγκεκριμένες διαδικασίες και μέτρα να παρέχεται στα φίλια ΣΕΠ η απαιτούμενη προστασία από τις ραγδαία εξελισσόμενες κυβερνοαπειλές. Σε γενικές γραμμές αυτή περιγράφεται στις ακόλουθες παραγράφους.

5.4.1 Αντιμετώπιση Κυβερνοπεριστατικών. Η κυβερνοάμυνα προϋποθέτει μηχανισμούς, διαδικασίες και ικανότητες για την αποτροπή, εντοπισμό, αξιολόγηση, αντιμετώπιση, επαναφορά και ανάλυση/εξαγωγή συμπερασμάτων από κυβερνοεπιθέσεις, οι οποίες επηρεάζουν την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) των ΣΕΠ. Η υλοποίηση των ανωτέρω γίνεται μέσω του ΣΚΑΚ (Στρατιωτικό Κέντρο Αντιμετώπισης Κυβερνοπεριστατικών - Cyber Security Operations Center, CSOC). και συντονίζεται μέσω της ΓΕΕΘΑ/ΔΙΚΥΒ. Συγκεκριμένα:

α. Προετοιμασία και Εκπαίδευση: Ανάπτυξη προτύπων και διαδικασιών που καλύπτουν όλο τον κύκλο εργασιών αντιμετώπισης κυβερνοπεριστατικών και προγραμματισμός εκπαίδευσης και ασκήσεων που επικεντρώνονται στην αντιμετώπιση τόσο μεμονωμένων κυβερνοεπιθέσεων όσο και εκτεταμένου κυβερνοπολέμου.

β. Αποτροπή: Κοινοποίηση των πολλαπλών επιπτώσεων (υπηρεσιακές, ποινικές, κλπ) από ενδεχόμενη μη εφαρμογή των κανόνων ασφαλείας ή προσπάθεια παραβίασης των συστημάτων, τόσο στους έμπιστους εσωτερικούς χρήστες, όσο και σε κακόβουλους εξωτερικούς όλων των ΣΕΠ. Ταυτόχρονη υλοποίηση πολλαπλών μηχανισμών άμυνας, έτσι ώστε να εξασφαλίζεται ότι η αποτυχία ή η αστοχία ενός μέτρου προστασίας θα καλυφθεί από τα υπόλοιπα [εφαρμογή της αρχής «άμυνα σε βάθος» («defence in depth»)].

γ. Διενέργεια σε όλα τα στρατιωτικά δίκτυα, από τη ΓΕΕΘΑ/ ΔΙΚΥΒ, ελέγχων ασφαλείας, εκτιμήσεων τρωτοτήτων και ελέγχων διείσδυσης. Οι έλεγχοι είναι τακτικοί (προγραμματισμένοι) ή έκτακτοι (μη προγραμματισμένοι).

δ. Εντοπισμός, Αξιολόγηση-Ανάλυση και Αντιμετώπιση: Εντοπισμός σε πραγματικό ή κοντά στον πραγματικό χρόνο και αποτελεσματική

αντιμετώπιση κάθε ύποπτης δραστηριότητας στον κυβερνοχώρο από το ΣΚΑΚ. Το ΣΚΑΚ αναφέρεται στη ΓΕΕΘΑ/ΔΙΚΥΒ, την οποία εξετάζω λεπτομερώς στη συνέχεια της διατριβής.

ε. Επαναφορά και Ανάλυση/Εξαγωγή Συμπερασμάτων: Πλήρης λειτουργική αποκατάσταση του πληγέντος συστήματος/υποδομής, μετά την αποτελεσματική αντιμετώπιση ενός κυβερνοπεριστατικού, καθώς και επαναφορά των δεδομένων από τους αρμόδιους διαχειριστές αυτού, σε συνεργασία με το ΣΚΑΚ. Επίσης, ταυτόχρονα με την αντιμετώπιση ενός κυβερνοπεριστατικού, γίνεται πλήρης καταγραφή όλων των ενεργειών που πραγματοποιήθηκαν και των δεδομένων που συλλέχθηκαν με σκοπό την ανάλυση της επίθεσης και την εξαγωγή χρήσιμων συμπερασμάτων (lessons learned).

5.4.2 Ρόλοι και Ευθύνες. Οι ρόλοι και οι ευθύνες των φορέων των ΕΔ σχετικά με την κυβερνοάμυνα και ανάλογα με το επίπεδο κάλυψης των υποδομών είναι οι εξής:

α. Υποδομές ΣΕΠ των ΕΔ: Οι ΕΔ πρέπει να έχουν την ικανότητα να προστατεύουν τις δικές τους κρίσιμες πληροφοριακές υποδομές. Το ΓΕΕΘΑ/ΔΙΚΥΒ συντονίζει την εφαρμογή της πολιτικής Κυβερνοάμυνας στις ΕΔ, η οποία υλοποιείται από τα τμήματα πληροφορικής των ΓΕ.

β. Εθνικές επεκτάσεις των υποδομών ΣΕΠ των ΕΔ: Απαραίτητη θεωρείται η επέκταση της ομπρέλας προστασίας της κυβερνοάμυνας και σε κόμβους διασύνδεσης των στρατιωτικών συστημάτων με υποδομές άλλων εθνικών φορέων (π.χ. Υπουργεία, Πρεσβείες, ΕΥΠ, Αστυνομία, κλπ). Σ’ αυτές τις περιπτώσεις η ΓΕΕΘΑ/ΔΙΚΥΒ λειτουργεί ως συντονιστικό όργανο και ως σημείο επαφής των αρμοδίων φορέων, σε θέματα κατανομής υποχρεώσεων και αρμοδιοτήτων κατά περίπτωση.

γ. Διεθνείς επεκτάσεις των υποδομών ΣΕΠ των ΕΔ: Η ΓΕΕΘΑ/ΔΙΚΥΒ και τα αρμόδια τμήματα των ΓΕ, είναι υπεύθυνα για τον έλεγχο συμβατότητας της πολιτικής κυβερνοάμυνας με τις αντίστοιχες των οργανισμών ή των χωρών με τις οποίες υπάρχει διασύνδεση (π.χ. ΝΑΤΟ, ΕΕ, κλπ) σύμφωνα με τις ισχύουσες διεθνείς συμβάσεις και συμφωνίες.

5.4.3 Εφαρμογή Κυβερνοάμυνας. Για την εφαρμογή της κυβερνοάμυνας στις ΕΔ απαιτείται η υλοποίηση συγκεκριμένων βημάτων και δράσεων από τα αρμόδια τμήματα πληροφορικής των ΓΕ σε συντονισμό με τη ΓΕΕΘΑ/ΔΙΚΥΒ, τα οποία είναι σε συμφωνία με τον ΕΚΑ. Συγκεκριμένα:

α. Πλήρης απογραφή όλων των συσκευών (hardware) που χρησιμοποιούνται σε ΣΕΠ, τόσο σε τακτική βάση όσο και οποτεδήποτε γίνονται αλλαγές, όπως η αναβάθμιση υλικού. Δημιουργία καταλόγου εγκεκριμένου εξοπλισμού και παρακολούθηση για χρήση μη εγκεκριμένου υλικού.[66]

β. Πλήρης απογραφή όλου του εγκατεστημένου λογισμικού (software) που χρησιμοποιείται σε ΣΕΠ, τόσο σε τακτική βάση όσο και οποτεδήποτε γίνονται αλλαγές (π.χ. προμήθεια νέου λογισμικού). Επίσης, δημιουργία καταλόγου εγκεκριμένου λογισμικού και απαγόρευση στο χρήστη της δυνατότητας εγκατάστασης μη εγκεκριμένου λογισμικού.

γ. Ασφαλής διαμόρφωση (configuration) όλου του εξοπλισμού (hardware & software) που χρησιμοποιείται σε ΣΕΠ. Δημιουργία προτύπων ασφαλούς διαμόρφωσης εξοπλισμού για όλα τα ΣΕΠ ανάλογα με τη χρήση και το επίπεδο διαβάθμισης ασφαλείας και υποχρεωτική χρήση από όλους.

δ. Εκτίμηση Τρωτοτήτων (Vulnerability Assessment) σε περιοδική βάση. Ανάλογα με τη κρισιμότητα του συστήματος, αυτή θα πραγματοποιείται σε ημερήσια ή εβδομαδιαία βάση το μέγιστο και θα περιλαμβάνει εντοπισμό τρωτοτήτων και έλεγχο εφαρμογής ενημερώσεων ασφαλείας.

ε. Εγκατάσταση λογισμικού εντοπισμού και αντιμετώπισης «ιομορφικού» λογισμικού σε όλα τα συστήματα ΣΕΠ με δυνατότητα κεντρικής διαχείρισης.

στ. Ασφάλιση λογισμικού και διαδικτυακών εφαρμογών. Δημιουργία τυποποιημένων διαδικασιών που περιλαμβάνουν κατ' ελάχιστο τα εξής: έλεγχος λαθών στα δεδομένα εισόδου των χρηστών, περιορισμός εμφάνισης μηνυμάτων λάθος στους χρήστες, αφαίρεση μη αναγκαίων τμημάτων λογισμικού, διενέργεια δοκιμών ασφαλείας των δικτυακών εφαρμογών και εγκατάσταση τείχους προστασίας δικτυακών εφαρμογών (web application firewall).

ζ. Έλεγχος ασφαλείας ασύρματων συσκευών, όπου αυτές κρίνεται σκόπιμο και επιτρέπεται να χρησιμοποιούνται με βάση τις απαιτήσεις και τη διαβάθμιση των δικτύων. Εντοπισμός και απενεργοποίηση των μη προβλεπομένων ασύρματων συσκευών.

[66] Η συγκεκριμένη πολιτική υλοποίησης κυβερνοάμυνας και κυβερνοασφάλειας σε τεχνικό επίπεδο, περιγράφεται στο ΄΄Τεχνικό σχέδιο δράσης για την ανάπτυξη κυβερνοάμυνας στις ΕΔ΄΄, που έχει εκδοθεί από τη ΓΕΕΘΑ/ΔΙΚΥΒ το 2014 και δεν αποτελεί αντικείμενο της παρούσης διατριβής.

η. Εφαρμογή διαδικασιών τήρησης αντιγράφων ασφαλείας των ΣΕΠ, σε τουλάχιστον εβδομαδιαία βάση και αποθήκευση αυτών σύμφωνα με συγκεκριμένα πρότυπα ασφαλείας.

θ. Κατάλληλη εκπαίδευση σε θέματα κυβερνοασφάλειας κυβερνοάμυνας και περιοδική αξιολόγηση ικανοτήτων και γνώσεων όλου του προσωπικού που εμπλέκεται με συστήματα ΣΕΠ.

ι. Ασφαλής διαμόρφωση όλων των δικτυακών συσκευών [δρομολογητές (routers) και μεταγωγείς (switches)] και περιοδική αναθεώρηση αυτών των διαμορφώσεων. Χρήση διαδικτυακού λογισμικού ασφάλειας όπως «Τείχος Προστασίας» (firewall), τουλάχιστον στα κομβικά σημεία των δικτύων.

ια. Περιοδικός έλεγχος των υπηρεσιών (services), πρωτοκόλλων και θυρών δικτύων (ports) σε όλα τα συστήματα ΣΕΠ και περιορισμός αυτών μόνο στα απολύτως απαραίτητα για την εκτέλεση της αποστολής τους.

ιβ. Έλεγχος των δικαιωμάτων διαχείρισης με εφαρμογή συγκεκριμένων διαδικασιών και κανόνων, όπως η σωστή επιλογή και η περιοδική αλλαγή του κωδικού και η χρήση λιστών πρόσβασης.

ιγ. Εφαρμογή Περιμετρικών Μηχανισμών Άμυνας σε πολλαπλά επίπεδα. Κατανομή των συστημάτων ΣΕΠ - με βάση την υπηρεσία που παρέχουν και τη διαβάθμιση των δεδομένων που επεξεργάζονται - σε ξεχωριστές ζώνες ή υποδίκτυα, με σκοπό την προστασία των κρίσιμων συστημάτων και το διαχωρισμό τους από υπηρεσίες που εκτίθενται σε απειλές.

ιδ. Εφαρμογή διαδικασιών καταγραφής συμβάντων (logs) σε όλα τα συστήματα ΣΕΠ και περιοδική παρακολούθηση και ανάλυση αυτών.

ιε. Ελεγχόμενη πρόσβαση σε όλους τους χρήστες με βάση την ελάχιστη απαιτούμενη γνώση και αρμοδιότητα (αρχή των ελάχιστων προνομίων, Principle Of Least Privilege - POLP).

ιστ. Παρακολούθηση και έλεγχος των λογαριασμών χρηστών. Εφαρμογή συγκεκριμένων κανόνων ασφαλείας όπως η εφαρμογή ημερομηνίας λήξης λογαριασμού, το κλείδωμα αυτού σε περιπτώσεις παραβίασης ασφαλείας, ταύτιση με τον χρήστη, δημιουργία προφίλ, κλπ.

ιζ. Εφαρμογή διαδικασιών αποτροπής διαρροής πληροφοριών που θα περιλαμβάνει κρυπτογράφηση δεδομένων, αποκλεισμό εξωτερικών αποθηκευτικών συσκευών, επιτήρηση ηλεκτρονικής αλληλογραφίας, κλπ.

ιη. Ενοποίηση όλων των στρατιωτικών δικτύων και μεταφορά της εικόνας τους στο ΣΚΑΚ με σκοπό τον εντοπισμό κυβερνοπεριστατικών και την καλύτερη αντιμετώπιση αυτών.

ιθ. Περιοδική εκτέλεση ελέγχων διείσδυσης (penetration testing) και ασκήσεων κυβερνοεπιθέσεων από κατάλληλα εκπαιδευμένες ομάδες, σε όλα τα συστήματα ΣΕΠ των ΕΔ.

5.4.4 Περιοδική Αναθεώρηση. Η πολιτική κυβερνοάμυνας αποτελεί ένα ενδιάμεσο στάδιο στην αλυσίδα υλοποίησης της κυβερνοάμυνας, μεταφράζοντας τις γενικές κατευθύνσεις της στρατηγικής κυβερνοάμυνας, που παρουσιάστηκαν σε προηγούμενη ενότητα, σε χαμηλότερου επιπέδου κατευθύνσεις, οι οποίες αποτελούν τη βάση για την εκπόνηση των οδηγιών του τεχνικού σχεδίου δράσης κυβερνοάμυνας.

Σε αντίθεση με τη στρατηγική, η πολιτική θα πρέπει να αξιολογείται περιοδικά και να αναθεωρείται, όταν αυτό απαιτείται, από κατάλληλη διακλαδική επιτροπή. Η ανάγκη αναθεώρησης της πολιτικής μπορεί να προκύψει είτε λόγω του περιορισμένου βαθμού υλοποίησης των γενικών κατευθύνσεων της στρατηγικής στην υλοποίηση της κυβερνοάμυνας στο τακτικό επίπεδο, είτε λόγω εξελίξεων στην τεχνολογία και τις μορφές απειλών που επιβάλλουν την επικαιροποίηση του τεχνικού πλαισίου που περιγράφει το τεχνικό σχέδιο δράσης.

5.5 Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ (ΓΕΕΘΑ/ΔΙΚΥΒ)[67]

5.5.1 Παρούσα Κατάσταση. Αποστολή της Διεύθυνσης είναι ο συντονισμός και η διεξαγωγή επιχειρήσεων κυβερνοάμυνας σε στρατηγικό, επιχειρησιακό και τακτικό επίπεδο, σε περίοδο ειρήνης, κρίσης ή πολέμου.

Την παρούσα χρονική περίοδο η ΓΕΕΘΑ/ΔΙΚΥΒ είναι επανδρωμένη με μόνιμα στελέχη και λειτουργεί με τα παρακάτω τέσσερα τμήματα:

α. Τμήμα Πολιτικής και Στρατηγικής Κυβερνοπολέμου.

β. Τμήμα Αντιμετώπισης Περιστατικών Κυβερνοπολέμου.

γ. Τμήμα Επιχειρήσεων Κυβερνοπολέμου.

δ. Τμήμα Έρευνας και Ανάπτυξης.

Η βασική εκπαίδευση του προσωπικού για τα νεοτοποθετημένα στελέχη γίνεται μέσω των δύο σχολείων που διοργανώνονται εσωτερικά από την ίδια

[67] Οι πληροφορίες που καταγράφονται στο παρόν τμήμα προέρχονται από την άμεση επικοινωνία με στελέχη της ΓΕΕΘΑ/ΔΙΚΥΒ

τη Δνση, το Βασικό και το Προκεχωρημένο. Κάθε ένα από τα δύο αυτά σχολεία είναι διάρκειας δύο εβδομάδων και τα αντικείμενα που διδάσκονται αφορούν σ' όλο το φάσμα των επιχειρήσεων όπως: Ασφάλεια Η/Υ και δικτύων, ψηφιακή σήμανση, εντοπισμός και αντιμετώπιση κυβερνοεπιθέσεων, έλεγχος διείσδυσης, ανάλυση ιομορφικών λογισμικών και ασφάλεια κινητών τηλεφώνων.

Η εκπαίδευση όμως δεν σταματά εκεί αλλά συνεχίζεται σε δύο φάσεις. Η πρώτη φάση διαρκεί ένα χρόνο και αφορά στη βασική εκπαίδευση σε θέματα δικτύων και λειτουργικών συστημάτων. Στη δεύτερη φάση γίνεται εκπαίδευση επ' έργω, η οποία διαρκεί ένα χρόνο και γίνεται υπό την επίβλεψη ενός έμπειρου στελέχους. Αφορά την πρώτη εξειδίκευση σε συγκεκριμένο τομέα. Επιχειρησιακά «εκμεταλλεύσιμο» ένα στέλεχος γίνεται σε δύο χρόνια μετά την ένταξή του στη ΔΙΚΥΒ.

Η Δνση επίσης συμμετέχει σε αριθμό διεθνών (ΝΑΤΟ και ΕΕ) ασκήσεων όπως «Cyber Coalition», «Locked Shields», «Crossed Swords» οι οποίες της προσδίδουν μεγάλη εμπειρία σε ό,τι αφορά το χρησιμοποιούμενο λογισμικό και τις διαδικασίες, ενώ ανταλλάσσονται πολύτιμες απόψεις με τις αντίστοιχες Δνσεις άλλων χωρών πάνω σε θέματα κοινού ενδιαφέροντος.

Επιπλέον, σε ετήσια βάση από το 2010, πραγματοποιείται η Εθνική Διακλαδική Άσκηση Κυβερνοάμυνας «ΠΑΝΟΠΤΗΣ». Έχουν πραγματοποιηθεί οχτώ τέτοιες ασκήσεις μέχρι τώρα. Υπεύθυνη για το συντονισμό της άσκησης είναι η ΓΕΕΘΑ/ΔΙΚΥΒ. Η τελευταία άσκηση «ΠΑΝΟΠΤΗΣ» έλαβε χώρα από 22 έως 25 Μαΐου 2018. Στην άσκηση συμμετείχε προσωπικό από τις ΕΔ και τα Σώματα Ασφαλείας, καθώς και φορείς του δημόσιου και του ιδιωτικού τομέα και της ακαδημαϊκής κοινότητας. Περισσότεροι από 200 συμμετέχοντες από 25 φορείς από όλη τη χώρα ασκήθηκαν στην αντιμετώπιση διαφόρων περιστατικών κυβερνοασφάλειας, καλύπτοντας τόσο μεμονωμένα συμβάντα όσο και περιστατικά ευρύτερης έκτασης που απαιτούσαν συντονισμένη ανταπόκριση σε πολλαπλά επίπεδα. Τα επεισόδια κάλυψαν πλειάδα αντικειμένων κυβερνοάμυνας, όπως ανάλυση ιομορφικού λογισμικού, ψηφιακή διερεύνηση πειστηρίων σε διαφορετικά λειτουργικά συστήματα Η/Υ και έξυπνων κινητών τηλεφώνων, έλεγχο ευπαθειών

εφαρμογών διαδικτύου και ιστού και εντοπισμό και ανάλυση παραβίασης δικτυακής υποδομής.[68]

Η Δνση επίσης συμμετέχει σε αριθμό πολύ σημαντικών Ευρωπαϊκών Προγραμμάτων τα οποία προσδίδουν επιπλέον τεχνογνωσία και συνεισφέρουν στην απόκτησης εμπειριών. Μερικά από αυτά είναι τα εξής: DOGANA[69], CERTCOOP[70], CYBER RANGES[71] και DePoCyTE.[72]

5.5.2 Μόνιμη Διαρθρωμένη Συνεργασία (PESCO) και οδηγίες ΕΕ. Η Δνση αυτή την περίοδο ηγείται ενός πρόγραμμα της ΕΕ στα πλαίσια της PESCO, με την επωνυμία «Cyber Threats and Incident Response Information Sharing Platform».[73] Στο πρόγραμμα συμμετέχουν ακόμα εφτά χώρες ενώ επιπλέον έξι είναι παρατηρητές. Σκοπός του εν εξελίξει προγράμματος είναι:

α. Επαύξηση διαμοιρασμού πληροφορίας απειλών κυβερνοχώρου.

β. Επέκταση των συνεργατικών μηχανισμών μεταξύ των συμμετεχόντων Ευρωπαϊκών κρατών μελών.

γ. Ανάπτυξη πλατφόρμας διαμοιρασμού πληροφορίας σχετικά με απειλές στον κυβερνοχώρο με δυνατότητες αναζήτησης κυβερνοαπειλών (Threat Hunting capabilities).

δ. Αντιμετώπιση κυβερνοπεριστατικών με βάση τις σχετικές πληροφορίες (Ενεργητική Κυβερνοάμυνα – Active Defence).

Το πρόβλημα που επιχειρείται να επιλυθεί μέσω της ανάπτυξης της πλατφόρμας είναι ο έγκαιρος εντοπισμός και αντιμετώπιση τόσο των γνωστών όσο και των άγνωστων απειλών (κυβερνοεπιθέσεις).

Μετά την ψήφιση του Ν.4577-2018 από τις 03 Δεκ 2018, όπως έχει ήδη αναφερθεί, η ΓΕΕΘΑ/ΔΙΚΥΒ έχει οριστεί ως Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών σε εθνικό επίπεδο (CSIRT). Αυτό

[68] http://www.geetha.mil.gr/el/briefing-el/press-el/6640-askhsh-«panopths-2018».html, (έγινε πρόσβαση στις 23 Μαρ 2019)
[69] https://www.dogana-project.eu/, (έγινε πρόσβαση στις 22 Μαρ 2019)
[70] https://www.certcoop.eu/, (έγινε πρόσβαση στις 22 Μαρ 2019)
[71] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, (έγινε πρόσβαση στις 22 Μαρ 2019)
[72] Demand Pooling for the Cyber Defence Training and Exercise
[73] https://www.consilium.europa.eu/media/32079/pesco-overview-of-first-collaborative-of-projects-for-press.pdf, (έγινε πρόσβαση στις 23 Μαρ 2019)

είναι αποτέλεσμα της εφαρμογής της οδηγίας NIS[74] (Network and Information System).

Η NIS Directive, προβλέπει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου ασφάλειας στον κυβερνοχώρο στην ΕΕ, εξασφαλίζοντας:

α. Την ετοιμότητα των κρατών μελών, απαιτώντας τους να είναι κατάλληλα εξοπλισμένα, αφενός με αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT) και αφετέρου με αρμόδια εθνική αρχή κυβερνοασφάλειας.

β. Συνεργασία όλων των κρατών μελών, με τη σύσταση ομάδας συνεργασίας, προκειμένου να υποστηριχθεί και να διευκολυνθεί η στρατηγική συνεργασία και η ανταλλαγή πληροφοριών μεταξύ τους. Θα χρειαστεί επίσης να δημιουργήσουν ένα δίκτυο CSIRT, προκειμένου να προωθηθεί η ταχεία και αποτελεσματική επιχειρησιακή συνεργασία σε ειδικά περιστατικά ηλεκτρονικής ασφάλισης και η ανταλλαγή πληροφοριών σχετικά με τους κινδύνους.

γ. Μια κουλτούρα ασφαλείας σε διάφορους τομείς που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία που όλο και περισσότερο εξαρτάται σε μεγάλο βαθμό από ICTs[75], όπως η ενέργεια, οι μεταφορές, το νερό, οι τραπεζικές υπηρεσίες, οι υποδομές χρηματοπιστωτικών αγορών, η υγειονομική περίθαλψη και η ψηφιακή υποδομή. Οι επιχειρήσεις σ' αυτούς τους τομείς, οι οποίες χαρακτηρίζονται από τα κράτη μέλη ως φορείς βασικών υπηρεσιών θα πρέπει να λάβουν τα κατάλληλα μέτρα ασφαλείας και να κοινοποιούν σοβαρά περιστατικά στην αρμόδια εθνική αρχή. Επίσης, οι βασικοί πάροχοι ψηφιακών υπηρεσιών (μηχανές αναζήτησης, υπηρεσίες cloud computing[76] και online αγορές) θα πρέπει να συμμορφωθούν με τις απαιτήσεις ασφαλείας, βάσει της νέας οδηγίας.

Αυτό πρακτικά, για την Ελληνική πραγματικότητα, σημαίνει ότι η ΓΕΕΘΑ/ΔΙΚΥΒ είναι υπεύθυνη για τον έλεγχο ασφαλείας και την προστασία των κρίσιμων υποδομών της χώρας. Με γνώμονα λοιπόν την οδηγία της ΕΕ προς όλα τα κράτη μέλη και στο πλαίσιο υλοποίησης αντισταθμιστικών ωφελημάτων, αυτή τη στιγμή βρίσκεται σε εξέλιξη η αναβάθμιση ενός νέου εθνικού ΣΚΑΚ.

---

[74] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive,(έγινε πρόσβαση στις 23 Μαρ 2019)

[75] Information Communication Technologies

[76] Υπολογιστικό Νέφος ονομάζεται η κατ' αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων (όπως δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία, ελάχιστη προσπάθεια από τον χρήστη και υψηλή αυτοματοποίηση

Το πρόγραμμα αναμένεται να ολοκληρωθεί σύντομα και τότε θα έχουμε ένα από τα καλύτερα συστήματα επιτήρησης κυβερνοασφάλειας στην περιοχή των Βαλκανίων, ενώ θα αυξηθούν κατακόρυφα οι δυνατότητες της χώρας στον αμυντικό τομέα του κυβερνοπολέμου.

5.5.3 Μελλοντικές Προοπτικές. Άλλες σημαντικές δραστηριότητες που βρίσκονται σε εξέλιξη είναι:

α. Ολοκλήρωση διαδραστικού σχολείου ενημέρωσης στελεχών σε θέματα κυβερνοάμυνας και κυβερνοασφάλειας.

β. Επικαιροποίηση του τεχνικού εγχειριδίου ασφάλειας προσωπικού ηλεκτρονικού υπολογιστή.

γ. Ανάπτυξη λογισμικού συλλογής πληροφοριών για τον εντοπισμό κυβερνοεπιθέσεων.

δ. Συνδρομή στη σύνταξη της Εθνικής Στρατηγικής κυβερνοασφάλειας.

ε. Η Ευρωπαϊκή υπηρεσία για την Ασφάλεια Δικτύων και Πληροφοριών,[77] με έδρα το Ηράκλειο της Κρήτης, έχει ήδη ζητήσει από όλα τα κράτη μέλη, εκτίμηση κινδύνου το προσεχές διάστημα, προκειμένου να καταστεί εφικτή η ενιαία στρατηγική της Ευρωπαϊκής Ένωσης στον τομέα του κυβερνοπολέμου και των κυβερνοαπειλών. Η χώρα μας πρέπει να δρομολογήσει αρκετές ενέργειες τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, ώστε να μην είναι εκπρόθεσμη στις ημερομηνίες που έχουν τεθεί.

Αναφορικά με τα γενικά επιτελεία των τριών κλάδων των ΕΔ, έχουν αντίστοιχο τμήμα το οποίο έχει ως αποστολή την κυβερνοάμυνα στα δίκτυα για τα οποία το εκάστοτε γενικό επιτελείο (ΓΕΣ-ΓΕΝ-ΓΕΑ) είναι υπεύθυνο. Λειτουργούν και αυτά με εξειδικευμένο προσωπικό. Μεταξύ των τεσσάρων δνσεων υπάρχει στενή και άμεση συνεργασία διότι οι απειλές είναι κοινές για όλους.

Σημαντική εξέλιξη αποτελεί το γεγονός ότι από το νέο έτος διοργανώνεται στη Σχολή Προγραμματιστών Ηλεκτρονικών Υπολογιστών (ΣΠΗΥ), διακλαδικό σχολείο σε θέματα Κυβερνοπολέμου και Ασφαλείας Πληροφοριακών Συστημάτων Η/Υ. Την ευθύνη της εκπαίδευσης έχει το ΓΕΣ και συγκεκριμένα η Δνση Έρευνας – Πληροφορικής. Το σχολείο θα είναι διάρκειας 4 εβδομάδων και θα

[77] ENISA – European Network and Information Security Agency

λειτουργήσει σε δύο εκπαιδευτικές σειρές το χρόνο, με τη συμμετοχή Αξκων, Ανθστων, Υπξκων, ΕΠΟΠ και ΜΥ.

Πολύ πρόσφατα (Δεκ 2019) είχαμε την έκδοση από το ΓΕΣ/ΔΕΠΛΗ, την νέας ΠαΔ περί ‘’Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων και Τοπικών Δικτύων Δεδομένων’’. Σκοπός της είναι ο καθορισμός της Πολιτικής Ασφάλειας των υπηρεσιών Τεχνολογίας Πληροφορικής (ΤΠ) του ΣΞ, ανεξαρτήτως της διαβάθμισής τους, ενώ ως πεδίο εφαρμογής ορίζονται όλες οι Υπηρεσίες - Μονάδες και Σχηματισμούς του ΣΞ.

Τελική επιθυμητή κατάσταση, σε ό,τι αφορά την πληροφοριακή υποστήριξη του ΣΞ, είναι για κάθε στέλεχός του, να παρέχονται εν είδει εργαλείων, οι αναγκαίες ασφαλείς υπηρεσίες ΤΠ, οι οποίες θα του εξασφαλίσουν τη δυνατότητα να εκτελεί την αποστολή του αποδοτικότερα, ταχύτερα και ευκολότερα, ανεξάρτητα από το χρόνο και το τόπο, λειτουργώντας με τον τρόπο αυτό, ως πολλαπλασιαστής ισχύος. Σημαντικός αριθμός υπηρεσιών ΤΠ έχουν ήδη αναπτυχθεί και είναι διαθέσιμες για αξιοποίηση από το προσωπικό του ΣΞ, ενώ η ανάπτυξη και διάθεσή τους θα συνεχιστεί, μέχρις ότου επιτευχθεί η τελική επιθυμητή κατάσταση.[78]

5.4.4 Προκλήσεις. Πέρα όμως από τις πολύ καλές προοπτικές εξέλιξης που υπάρχουν αυτή τη στιγμή στο πεδίο της κυβερνοάμυνας, η Δνση αντιμετωπίζει τις εξής προκλήσεις:

α. Προσωπικό: Δεδομένης της γενικότερης έλλειψης προσωπικού και της ελλιπούς στελέχωσης του συνόλου των ελληνικών ΕΔ, λείπουν από τη Δνση εξειδικευμένα στελέχη. Επίσης σοβαρό πρόβλημα είναι και το γεγονός ότι τέτοια στελέχη αναγκάζονται να φύγουν από την Δνση για να γράψουν χρόνο διοικήσεως στα όπλα ή σώματα που ανήκουν και ο οποίος είναι απαραίτητος για τη βαθμολογική τους εξέλιξη, με αποτέλεσμα να χάνεται η εμπειρία που έχουν αποκτήσει.

β. Εξειδίκευση: Δεν αποδίδεται σε κανένα κλάδο η ειδικότητα «Ασφάλεια Πληροφορικής», ούτε υποστηρίζεται με μεταπτυχιακές σπουδές ή ανάλογα σεμινάρια εξειδίκευσης.

γ. Εκπαίδευση: Σε συνέχεια του προηγούμενου, η εκπαίδευση του τοποθετημένου προσωπικού πρέπει να είναι συνεχής, καθώς οι σύγχρονες κυβερνοαπειλές εξελίσσονται και αλλάζουν καθημερινά με ταχύτατους ρυθμούς.

---

[78] ΠαΔ 1-26/2019 περί *Διαχείρισης Ασφαλείας Πληροφοριακών Συστημάτων και Τοπικών Δικτύων Δεδομένων*

Κεφάλαιο Έκτο

Σύγκριση με πιθανούς ανταγωνιστές

6.1 Γενικά

Οι επιχειρήσεις κυβερνοπολέμου ενώ στη μορφή συλλογής πληροφοριών, διεξάγονται ήδη από τον καιρό της ειρήνης, αναμένεται να αυξηθούν σε περιόδους κρίσεων (οικονομικών, διπλωματικών ή στρατιωτικών) ή ενδεχόμενου πολέμου. Μια τέτοια κατάσταση απαιτεί από μέρους της Ελλάδος μια εγρήγορση και μια κατάλληλη προετοιμασία σε όλα τα επίπεδα του Κυβερνοπολέμου. Στην περιοχή που βρισκόμαστε, υπάρχουν δρώντες που ήδη διεξάγουν ή ενδεχομένως να διεξάγουν στο μέλλον επιχειρήσεις κυβερνοπολέμου εις βάρος της χώρας μας. Αυτοί μπορούν να προσδιοριστούν όπως παρακάτω:[79]

α. Δρώντες που ήδη αποτελούν στρατιωτική απειλή (Τουρκία).

β. Δρώντες των οποίων οι διπλωματικές σχέσεις με τη χώρα μας βιώνουν περιόδους κρίσεως (Β. Μακεδονία).

γ. Δρώντες που πρέπει να βρίσκονται συνεχώς στο άμεσο ενδιαφέρον της Ελλάδος, παρά την κατά περιόδους ομαλότητα που επικρατεί στις σχέσεις μεταξύ τους (Βουλγαρία, Αλβανία).

ε. Δρώντες που διαδραματίζουν παγκόσμια ρόλο σε όλα τα επίπεδα (ΗΠΑ, Ρωσία, Κίνα).

στ. Δρώντες των οποίων τα συμφέροντα δεν έπαψαν ποτέ να περιστρέφονται γύρω από τα Βαλκάνια και την ευρύτερη περιοχή της ανατολικής Μεσογείου (Ιταλία, Μεγάλη Βρετανία, Γαλλία).

ζ. Δρώντες των οποίων οι ελληνικής καταγωγής πληθυσμοί που διαβιούν εκεί, διαδραμάτιζαν και διαδραματίζουν σοβαρό ρόλο (Γεωργία).

η. Μεμονωμένοι δρώντες ή οργανώσεις που ενδέχεται να στραφούν κατά της χώρας λόγω συμμετοχής της τελευταίας στο ΝΑΤΟ, στην ΕΕ ή σε άλλους διεθνής οργανισμούς.

6.2 Σύγκριση με την Τουρκία[80]

Σύμφωνα με την έκθεση του Εθνικού Οργανισμού για την Ασφάλεια στον Κυβερνοχώρο από τα 80,8 εκ. του πληθυσμού της Τουρκίας, το 67% είναι χρήστες

[79] Παναγιώτης, Μαυρόπουλος, *Κυβερνοπόλεμος και Εθνική Στρατηγική*

[80] Seker Ensar, Tolga Ihsan Bukar, *National Cyber Security Organisation:Turkey*, CCDCOE, Tallinn 2018

του διαδικτύου, ενώ το 61% από αυτούς είναι μεταξύ 16 και 74 ετών. Οι Τούρκοι πολίτες έχουν διαδικτυακή πρόσβαση από το σπίτι τους σε ποσοστό 76%, ενώ από το σύνολο των χρηστών του διαδικτύου, το 72,4% έχει πρόσβαση από κινητές συσκευές και το 40% μέσω ενσύρματης σύνδεσης.

6.2.1 Ψηφιακές δημόσιες υπηρεσίες. Οι υπηρεσίες ηλεκτρονικής διακυβέρνησης καθιστούν δυνατή την αποτελεσματική, εύκολη και αξιόπιστη αλληλεπίδραση με κυβερνητικούς οργανισμούς, διευκολύνοντας την πρόσβαση σε ακριβείς και ενημερωμένες πληροφορίες για όλες τις δημόσιες υπηρεσίες που παρέχονται από δημόσια ιδρύματα και οργανισμούς. Η ηλεκτρονική διακυβέρνηση της Τουρκίας επιτρέπει την ταχεία και εύκολη ανταλλαγή πληροφοριών και εγγράφων μεταξύ των ιδρυμάτων. Στοχεύει να απαλλάξει τους πολίτες από τη μετακίνηση, μειώνοντας ταυτόχρονα τον φόρτο εργασίας των θεσμικών οργάνων. Η αξιοπιστία των συναλλαγών μέσω της ηλεκτρονικής διακυβέρνησης διασφαλίζεται με μέσα όπως ιδιωτικοί κωδικοί, και ηλεκτρονικές υπογραφές. Αυτά τα συστήματα ελέγχου ταυτότητας και ασφάλειας ενσωματώνονται κυρίως στις επίσημες συναλλαγές, όπως χρηματοδότηση, αγορές πολύτιμων αντικειμένων, συμβολαιογραφικές υπηρεσίες, φορολογικά συστήματα, υπογραφή επίσημων εγγράφων και επικοινωνίες μεταξύ κυβερνήσεων.

Το 2017, σχεδόν το ήμισυ του ενήλικου πληθυσμού (42% μεταξύ 16-74 ετών) χρησιμοποίησε το διαδίκτυο για να αλληλεπιδράσει με κυβερνητικούς οργανισμούς και να χρησιμοποιήσει κυβερνητικές υπηρεσίες για προσωπικούς σκοπούς. Ο αριθμός αυτός έχει αυξηθεί ταχύτατα από το 37% του προηγούμενου έτους. Τα τελευταία χρόνια, οι πιο διαδεδομένες υπηρεσίες ηλεκτρονικής διακυβέρνησης παρέχονται από δημόσιους οργανισμούς όπως το Ίδρυμα Κοινωνικής Ασφάλισης, τη Διοίκηση Εσόδων, το Υπουργείο Δικαιοσύνης, την Εθνική Αστυνομία και τη Γενική Διεύθυνση Κτηματολογίου.

Από το 2018, οι υπηρεσίες ηλεκτρονικής διακυβέρνησης της Τουρκίας καλύπτουν κυρίως:

α. διάφορες υπηρεσίες διοικητικού και δικαστικού συστήματος - παρακολούθηση εγγράφων, φορολογία και τελωνειακές υποθέσεις.

β. επίσημα μητρώα - ατομικές υπηρεσίες αρχείων, όπως η διεύθυνση κατοικίας, τα προσωπικά αρχεία, τα αρχεία οικογενειών ή εξαρτημένων προσώπων, πληροφορίες περί στρατολόγησης, μισθούς κ.λ.π.

γ. υπηρεσίες κοινωνικής πρόνοιας και προγράμματα συνταξιοδότησης και παρακολούθησης των συντάξεων.

δ. υπηρεσίες που σχετίζονται με το εκπαιδευτικό σύστημα, όπως τα εκπαιδευτικά αρχεία, η παρακολούθηση των υποτροφιών, οι συντάξεις στα εκπαιδευτικά ιδρύματα κ.λ.π.

ε. επιχειρηματικές και ακίνητες υπηρεσίες - επιχειρηματική δραστηριότητα, αρχεία και υπηρεσίες οχημάτων, προσωπικά χρέη.

στ. γεωργικά αρχεία, πληροφορίες κτηματογράφησης και

ζ. αρχεία ψηφοφορίας.

Το Υπουργείο Μεταφορών και Υποδομών (UAB) είναι υπεύθυνο για την εγκατάσταση, την υλοποίηση και τη διοίκηση του κυβερνητικού κόμβου υπηρεσιών (e-government). Το Υπουργείο εποπτεύει την τακτική λειτουργία ολόκληρων υπηρεσιών ηλεκτρονικής διακυβέρνησης, αναθέτει ευθύνες σχετικά με την ασφάλεια στον κυβερνοχώρο σε άλλες κυβερνητικές οργανώσεις και διατηρεί το συντονισμό μεταξύ συναφών υπηρεσιών άλλων υπουργείων και κυβερνητικών φορέων. Σύμφωνα με τα στοιχεία του 2015, οι επενδύσεις στον τομέα της πληροφορικής του δημόσιου τομέα ανήλθαν σε 1,38 δισεκατομμύρια δολάρια ετησίως και κατέχουν το 6,9% όλων των επενδύσεων του δημόσιου τομέα.

6.2.1 Ψηφιοποίηση στις επιχειρήσεις. Το ηλεκτρονικό εμπόριο κερδίζει σταθερά δημοτικότητα στην Τουρκία και το 25% των ανθρώπων μεταξύ 16-74 ετών χρησιμοποίησε τις ηλεκτρονικές εμπορικές υπηρεσίες για να αγοράσει προϊόντα ή υπηρεσίες για προσωπικούς σκοπούς το 2016. Αυτό ήταν 21% υψηλότερο από ό, τι το προηγούμενο έτος. Ο όγκος του ηλεκτρονικού εμπορίου έχει επίσης αυξηθεί κατά τη διάρκεια των τελευταίων ετών και το 2016 ο συνολικός όγκος της αγοράς του ηλεκτρονικού εμπορίου ανήλθε στα 10,6 δισ. δολάρια. Στο λιανικό εμπόριο, ο όγκος της αγοράς ηλεκτρονικού εμπορίου αυξήθηκε κατά 34% από το 2013 έως το 2016. Οι δραστηριότητες ηλεκτρονικού εμπορίου ρυθμίζονται από το νόμο για τη ρύθμιση του ηλεκτρονικού εμπορίου που εγκρίθηκε από την Μεγάλη Εθνοσυνέλευση της Τουρκίας το 2014.

Μέχρι το Σεπτέμβριο του 2017, το 96% των νεοσυσταθεισών εταιρειών στην Τουρκία είχε πρόσβαση στο διαδίκτυο, παρουσιάζοντας μια ελαφρά αύξηση από 94% το 2016. Μεταξύ των εταιρειών αυτών, η πρόσβαση και η χρήση του διαδικτύου είναι σχεδόν καθολική (99,7%) για όσες έχουν πάνω από 250 εργαζόμενους.

6.3 Το 2008 Pipeline Attack και το 2015 Blackout: Μια κλήση αφύπνισης για την Τουρκία[81]

Όσον αφορά τις άμεσες επιθέσεις στον κυβερνοχώρο και τις εχθρικές δραστηριότητες που απευθύνονται στην Τουρκία, διακρίνονται δύο επεισόδια: η έκρηξη του 2008 στον αγωγό πετρελαίου Baku-Tblisi-Ceyhan και οι διακοπές ρεύματος το 2015. Το πρώτο συμβάν είναι οι εκρήξεις του 2008 στη γραμμή Baku-Tbilisi-Ceyhan (BTC) κοντά στην ανατολική τουρκική πόλη Erzincan. Οι σωληνώσεις ήταν πάντα ευάλωτες σε τρομοκρατικές επιθέσεις στην Τουρκία. Μια έρευνα ασφαλείας δείχνει ότι μεταξύ των ετών 1987 και 2010 διεξήχθησαν 59 δολιοφθορές με στόχο τους τουρκικούς, εκ των οποίων οι 19 μεταξύ του 2007 και του 2010.

Η επίθεση του 2008, ωστόσο, δεν ήταν συνήθης. Σύμφωνα με ορισμένες πηγές ειδήσεων, οι "χάκερ" είχαν κλείσει τους συναγερμούς, διέκοψαν τις επικοινωνίες και αύξησαν υπερβολικά την πίεση του αργού πετρελαίου στη γραμμή. Το κύριο όπλο στο σταθμό βαλβίδων 30 στις 5 Αυγούστου 2008 ήταν ένα πληκτρολόγιο που μετατόπισε την εσωτερική πίεση των συστημάτων αγωγών, η οποία οδήγησε στη μαζική έκρηξη. Η επίθεση στον αγωγό πετρελαίου συνέπεσε με την εκστρατεία της Ρωσίας στη Γεωργία το 2008, εγείροντας υποψίες, αφού ο αγωγός της BTC ερχόταν σε αντίθεση με τα ενεργειακά γεωστρατηγικά συμφέροντα της Μόσχας στην Ευρασία. Αποκαλύφθηκε ότι υπήρχαν πράγματι έντονες προσπάθειες για ‘’χακάρισμα’’ της εγκατάστασης αγωγών, διακοπή των συστημάτων συναγερμού και όλων των επικοινωνιών, συμπεριλαμβανομένων εκείνων που συνδέουν τα δεδομένα με τα δορυφορικά συστήματα.

Οι χάκερ διέγραψαν όλα τα αρχεία κάμερας ασφαλείας, εκτός από ένα που καταγράφηκε από μια υπέρυθρη κάμερα που δείχνει σαφώς δύο άτομα με φορητούς υπολογιστές που περπατούν κοντά στην εγκατάσταση. Πριν από τον Ρωσο-Γεωργιανό πόλεμο το 2008, οι δεσμοί της Άγκυρας με την Τιφλίδα ήταν αρκετά καλοί και η τουρκική κυβέρνηση υποστήριξε την ένταξη της Γεωργίας στο ΝΑΤΟ. Από την άποψη αυτή, είναι εξίσου σημαντικό ότι, κατά τη διάρκεια του πολέμου, κάποιες ρωσικές πηγές κατηγόρησαν ανοιχτά την Τουρκία, υποστηρίζοντας ότι η Άγκυρα διαδραμάτισε σημαντικό ρόλο στη βελτίωση και την ενθάρρυνση των στρατιωτικών δυνατοτήτων της Γεωργίας.

[81] Can Kasapoglu, Asst. Prof, *Turkey’s Future Cyber Defence Landscape*

Η δεύτερη εντυπωσιακή επίθεση στον κυβερνοχώρο εμφανίστηκε μετά τις διακοπές ρεύματος που έπληξαν 44 από τις 81 επαρχίες στην Τουρκία στις 31 Μαρτίου 2015. Αυτή τη φορά, για τον ύποπτο για τις επιθέσεις στον κυβερνοχώρο ανέφερε ανοιχτά ο Πρωθυπουργός Αχμέτ Νταβούτογλου και κάποιες πηγές τύπου ισχυρίστηκαν ότι το Ιράν βρισκόταν πίσω από αυτές ως απάντηση στις κατηγορίες του προέδρου Ερντογάν και τους ισχυρισμούς του κατά της Τεχεράνης για περιφερειακή κυριαρχία και υποστήριξη των συνεχιζόμενων επιχειρήσεων στην Υεμένη. Οι πολύωρες ημερήσιες διακοπές ρεύματος σταμάτησαν την παραγωγή σε 298 οργανωμένες βιομηχανικές ζώνες και κόστισαν περίπου 700 εκατομμύρια δολάρια. Ορισμένοι εμπειρογνώμονες παρουσίασαν μια ακόμη πιο απαισιόδοξη εκτίμηση ζημιών, που ανερχόταν σε 1 δισ. δολάρια ημερησίως. Το γεγονός ότι η ανατολική πόλη Van, η οποία δέχεται απευθείας ηλεκτρική ενέργεια από το ιρανικό ηλεκτρικό δίκτυο, δεν επηρεάστηκε από τη συσκότιση προκαλεί ακόμη μεγαλύτερη υποψία. Ωστόσο, δεν υπάρχουν επαρκή αποδεικτικά στοιχεία για να κατηγορηθεί ανοιχτά η Τεχεράνη.

6.4 Η αναζήτηση της Τουρκίας για την ενίσχυση των δυνατοτήτων της στον κυβερνοχώρο[82]

Η πιθανότητα ότι η συσκότιση του Μαρτίου του 2015 ήταν επιθέσεις στον κυβερνοχώρο δεν λήφθηκε τόσο σοβαρά υπόψη όσο η έκρηξη του αγωγού του 2008. Ακόμη και αν η συσκότιση δεν προκλήθηκε από επιθέσεις στον κυβερνοχώρο, θα πρέπει να αναγνωριστεί ως αφύπνιση και να αποδειχθεί η δυνατότητα μιας επίθεσης που μπορεί να κοστίσει περίπου 1 δισεκατομμύριο δολάρια την ημέρα, να παραλύσει τη ζωή στα αστικά κέντρα της Τουρκίας και να προκαλέσει ζημιές.

Η αναφερθείσα επίθεση πετρελαϊκών αγωγών του Baku-Tblisi-Ceyhan το 2008 προσέφερε ανεκτίμητα μαθήματα στους Τούρκους φορείς λήψης αποφάσεων. Πρώτον, ήταν σημαντική γιατί έδειξε τις επιπτώσεις μιας εχθρικής κυβερνοεπίθεσης. Δεύτερον, η επίθεση επεσήμανε τη σχέση μεταξύ των περιφερειακών ζητημάτων ασφαλείας, της γεωπολιτικής της ενέργειας και του πολιτικού / στρατιωτικού ανταγωνισμού. Τρίτον, η επιδρομή στον κυβερνοχώρο αποκάλυψε την ευπάθεια της κρίσιμης εθνικής υποδομής στις αναδυόμενες απειλές του πέμπτου τομέα πολέμου.

Σε απάντηση της επίθεσης της BTC, η Άγκυρα αποφάσισε να ενισχύσει τις ικανότητές της στον κυβερνοχώρο. Το 2010, το Συμβούλιο Εθνικής Ασφάλειας της

[82] Στο ίδιο

Τουρκίας (MGK-Milli Güvenlik Kurulu) έκανε τα πρώτα του βήματα για την οικοδόμηση κυβερνοδυνατοτήτων, οδηγώντας στην ίδρυση της Διοίκησης Κυβερνοάμυνας (ΔΙΚΥΒ) των Τουρκικών Ενόπλων Δυνάμεων το 2012. Το 2011 η Τουρκία διεξήγαγε την πρώτη εθνική άσκηση ασφαλείας στον κυβερνοχώρο που περιλάμβανε τόσο υποθετικά σενάρια όσο και πραγματικές δραστηριότητες από ‘’εχθρικές’’ ομάδες. Τέσσερα χρόνια αργότερα, η ασφάλεια στον κυβερνοχώρο υποτίθεται ότι ενσωματώθηκε στο διάσημο "Κόκκινο Βιβλίο" της Τουρκίας, το διαβαθμισμένο Έγγραφο Πολιτικής Εθνικής Ασφαλείας (Milli Güvenlik Siyaset Belgesi), το οποίο παρέχει δογματικές αρχές και στρατηγική καθοδήγηση στις υπηρεσίες και τους θεσμούς του τουρκικού κράτους.

6.5 Εθνική στρατηγική στον τομέα της ασφάλειας στον κυβερνοχώρο και νομικό πλαίσιο[83]

6.5.1 Εθνική στρατηγική. Η τρέχουσα εθνική στρατηγική στον τομέα της ασφάλειας στον κυβερνοχώρο καθορίστηκε με το σχέδιο δράσης του Μαρτίου 2016, από το Εθνικό Συμβούλιο Ασφαλείας. Καλύπτει τη χρονική περίοδο 2016-2019 και αποτελεί κατευθυντήρια γραμμή για όλες τις κυβερνητικές οργανώσεις, τους οργανισμούς, τους υπαλλήλους και τα νομικά πρόσωπα. Η αποστολή της τρέχουσας στρατηγικής και των σχεδίων δράσης συνοψίζεται στην αρχική δήλωση: «θέσπιση εθνικής ασφάλειας στον κυβερνοχώρο, καθορισμός και συντονισμός αποτελεσματικών και βιώσιμων πολιτικών και εφαρμογή στην άσκηση αυτών των πολιτικών». Η στρατηγική και το σχέδιο δράσης υπογραμμίζουν ότι η ασφάλεια στον κυβερνοχώρο αποτελεί αναπόσπαστο τμήμα της εθνικής ασφάλειας και απαιτεί όλες τις διοικητικές και τεχνικές προφυλάξεις όλων των εθνικών φορέων στον κυβερνοχώρο.

Η Τουρκική στρατηγική κυβερνοασφάλειας χωρίζεται σε τρία μέρη:

α. Εξασφάλιση της ασφάλειας, της μυστικότητας και της ιδιωτικής ζωής όλων των δεδομένων, των υπηρεσιών, των συναλλαγών και των συστημάτων στον τομέα των τεχνολογιών των πληροφοριών, καλύπτοντας ταυτόχρονα ολόκληρο τον εθνικό κυβερνοχώρο.

β. Καθορισμός δράσεων για την ασφάλεια στον κυβερνοχώρο που σχετίζονται, με τη διατήρηση των επιπτώσεων των επιθέσεων σε ένα εύλογο

[83] Seker Ensar, Tolga Ihsan Bukar, *National Cyber Security Organisation: Turkey*, CCDCOE, Tallinn 2018

κατώτατο επίπεδο με τα διαθέσιμα και τρέχοντα συστήματα, καθώς και με την παροχή βοήθειας σε κυβερνητικούς οργανισμούς και υπηρεσίες επιβολής του νόμου στον τομέα της έρευνας και της εγκληματολογίας με συναφή εγκλήματα στον κυβερνοχώρο.

γ. Λήψη των απαραίτητων μέτρων ώστε να καταστούν επαρκή τα συστήματα και οι υποδομές που είναι κρίσιμες για την ασφάλεια στον κυβερνοχώρο.

Η εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο και το σχέδιο δράσης πρέπει να επικαιροποιηθούν όσον αφορά την ταχεία εξέλιξη της τεχνολογίας και των κανονισμών.

6.6 Διακυβέρνηση στον κυβερνοχώρο (Τουρκικά CERTs)[84]

6.6.1 Διαχείριση πολιτικού και στρατηγικού επιπέδου. Με την απόφαση του Υπουργικού Συμβουλίου τον Οκτώβριο του 2012 για την εφαρμογή, τη διαχείριση και το συντονισμό των εθνικών ενεργειών στον κυβερνοχώρο, δόθηκε στο Υπουργείο Μεταφορών και Υποδομών η αρμοδιότητα προετοιμασίας και συντονισμού πολιτικών, στρατηγικών και σχεδίων δράσης σχετικά με τη διακυβέρνηση της εθνικής ασφάλειας στον κυβερνοχώρο, ορίζοντάς το ως υπεύθυνη κυβερνητική υπηρεσία η οποία επιβλέπει όλες τις άλλες οντότητες ασφαλείας μέσω του κράτους.

Το Υπουργείο εποπτεύει και διεξάγει δραστηριότητες για την ασφάλεια στον κυβερνοχώρο σε στρατηγικό επίπεδο μαζί με το Εθνικό Συμβούλιο Ασφαλείας στον Κυβερνοχώρο[85] (που ιδρύθηκε το 2013) και το USOM,[86]που αποτελεί το Τουρκικό Εθνικό CERT, το οποίο συντονίζεται από την BTK,[87] την Αρχή Τεχνολογιών Πληροφοριών και Επικοινωνιών. Ως εκ τούτου, όλες οι κυβερνητικές οργανώσεις, οι οργανισμοί, οι υπάλληλοι και οι νομικές οντότητες έχουν την εντολή να ακολουθούν τις πολιτικές και τα πρότυπα που έχει θέσει το Εθνικό Συμβούλιο Ασφαλείας στον Κυβερνοχώρο.

Με απόφαση του τουρκικού υπουργικού συμβουλίου τον Ιούνιο του 2012, το Υπουργείο Μεταφορών και Υποδομών είναι υπεύθυνο για την εθνική ασφάλεια στον κυβερνοχώρο και είναι σε θέση να συγκροτεί συμβούλια και ομάδες εργασίας για τη διεξαγωγή πρακτικών για την εκπλήρωση της αποστολής αυτής.

[84] Στο ίδιο
[85] National Cyber Security Board
[86] Ulusal Siber Olaylara Müdahale Merkezi - Turkish National CERT
[87] Bilgi Teknolojileri ve Iletişim Kurumu - Information and Communication Technologies Authority

6.6.2 Πρόληψη και ανταπόκριση σε επιχειρησιακό επίπεδο. Ενώ η χάραξη πολιτικής εμπίπτει στην αρμοδιότητα του Υπουργείου Μεταφορών και Υποδομών, η ρυθμιστική λειτουργία ανατίθεται στην Αρχή Τεχνολογιών Πληροφοριών και Επικοινωνιών (BTK).

6.6.2.1 Εθνικές και τομεακές ομάδες CERT. Σύμφωνα με το Εθνικό Σχέδιο Δράσης για την Ασφάλεια στον Κυβερνοχώρο 2013-2014, αποφασίστηκε η σύσταση εθνικής CERT και τομεακών και θεσμικών υπο-CERT μεταξύ των κορυφαίων κυβερνητικών - τομεακών φορέων και οργανισμών. Το Νοέμβριο του 2013 δημοσιεύθηκε επίσημη ανακοίνωση για την ίδρυση της εθνικής υπηρεσίας USOM (Εθνική CERT) και τομεακών - θεσμικών SOME,[88] παρέχοντας κατευθυντήριες γραμμές και λεπτομέρειες σε όλες τις ομάδες αντίδρασης ασφαλείας που αφορούν τον κυβερνοχώρο. Από το 2018, σε σχέση με την τρέχουσα Εθνική Στρατηγική Ασφάλειας στον Κυβερνοχώρο και το Σχέδιο Δράσης 2016-2019, οι οργανισμοί που διαθέτουν δικές τους CERT είναι:

α. Υπουργείο Εσωτερικών

β. Υπουργείο Δικαιοσύνης

γ. Υπουργείο Οικονομικών

δ. Υπουργείο Εμπορίου

ε. Υπουργείο Περιβάλλοντος και Πολεοδομίας

στ. Υπουργείο Εργασίας, Κοινωνικών Υπηρεσιών και Οικογένειας

ζ. Υπουργείο Γεωργίας και Δασών

η. Υπουργείο Υγείας

θ. Υπουργείο Μεταφορών και Υποδομών

ι. Αρχή τεχνολογιών πληροφοριών και επικοινωνιών (BTK)

ια. Τραπεζικός Κανονισμός και Οργανισμός Εποπτείας (BDDK)

ιβ. Ρυθμιστική Αρχή για την Αγορά Ενέργειας (EPDK)

ιγ. Συμβούλιο Αγορών Κεφαλαίων (SPK)

6.6.3 Άλλοι φορείς του δημόσιου τομέα. Παρόλο που το Υπουργείο Μεταφορών και Υποδομών ενεργεί ως κορυφαία υπεύθυνη κυβερνητική υπηρεσία

[88] Sektörelve Kurumsal Siber Olaylara Müdahale Ekipleri

και εποπτεύει τις άλλες οντότητες για την ασφάλεια του κυβερνοχώρου μέσω του κράτους, υπάρχει ένα φάσμα κυβερνητικών υπηρεσιών που συμβάλλουν στη διασφάλιση της ασφάλειας του κυβερνοχώρου στην Τουρκία. Οι πιο σημαντικές από αυτές αναφέρονται παρακάτω.

6.6.3.1 Η Προεδρία των Αμυντικών Βιομηχανιών, SSB.[89] Η άμυνα της βιομηχανίας στον κυβερνοχώρο θεωρείται τμήμα της εθνικής αμυντικής βιομηχανίας, επομένως τα έργα άμυνας στον κυβερνοχώρο εποπτεύονται και συνάπτονται από την SSB σε σχέση με τις απαιτήσεις και το στρατηγικό σχέδιο των τουρκικών ενόπλων δυνάμεων και της εθνικής ασφαλείας. Η SSB, μαζί με άλλα κυβερνητικά όργανα όπως η BTK, διοργανώνει ετήσιες διασκέψεις για την ασφάλεια στον κυβερνοχώρο με διαφορετική εστίαση κάθε χρόνο.

6.6.3.2 Το Επιστημονικό και Τεχνολογικό Ερευνητικό Συμβούλιο της Τουρκίας, TUBITAK[90] Δραστηριοποιείται στον τομέα της πληροφορικής, της ασφάλειας των πληροφοριών και των προηγμένων ηλεκτρονικών. Στόχος του είναι να υποστηρίξει τις εθνικές δραστηριότητες έρευνας και ανάπτυξης και ταυτόχρονα να ασκεί ανάλογες δραστηριότητες στο εσωτερικό της χώρας. Έχει επιτύχει εκατοντάδες επιτεύγματα έργων στους τομείς της ασφάλειας των πληροφοριών, του λογισμικού και των τηλεπικοινωνιών.

6.6.3.2 Το Τμήμα της Τουρκική Εθνικής Αστυνομίας υπεύθυνο για τα εγκλήματα στον κυβερνοχώρο. Παρέχει υποστήριξη για τη διερεύνηση των εγκλημάτων που διαπράττονται μέσω της τεχνολογίας των πληροφοριών και εξετάζει - διαχειρίζεται ψηφιακά δεδομένα, προκειμένου να καταπολεμηθεί αποτελεσματικά η εγκληματικότητα στον κυβερνοχώρο. Η Τουρκία έχει επίσης υπογράψει και επικυρώσει τη Σύμβαση της Βουδαπέστης του 2001 για τα εγκλήματα στον κυβερνοχώρο (με κάποιες επιφυλάξεις), η οποία αφορά την εγκληματικότητα στο Διαδίκτυο και την πληροφορική, εναρμονίζοντας τις εθνικές νομοθεσίες, βελτιώνοντας τις τεχνικές διερεύνησης και αυξάνοντας τη συνεργασία μεταξύ των κρατών. Έχει επίσης εγκρίνει εθνικούς νόμους σύμφωνα με τις διατάξεις της Σύμβασης.

[89] Savunma Sanayii Başkanlığı
[90] Türkiye Bilimselve Teknolojik Araştırma Kurumu – The Scientific and Technological Research Council of Turkey

6.6.3.3 Η Αρχή Προστασίας Προσωπικών Δεδομένων, KVKK.[91]

Παρέχει προστασία για τα προσωπικά δεδομένα και αναπτύσσει την ευαισθητοποίηση του κοινού στο θέμα αυτό σύμφωνα με τα θεμελιώδη δικαιώματα που σχετίζονται με την ιδιωτική ζωή και την ελευθερία, που αναφέρονται στο Σύνταγμα.

6.7 Στρατιωτική κυβερνοάμυνα[92]

6.7.1 Πλαίσιο πολιτικής. Οι τουρκικές ένοπλες δυνάμεις (TSK),[93] εφαρμόζουν την πολιτική και στρατηγική για την κυβερνοάμυνα σύμφωνα με τα υφιστάμενα εθνικά, διεθνή πρότυπα και πρότυπα του NATO. Η διατήρηση ενός συνεχούς συγχρονισμού με το Υπουργείο Μεταφορών και Υποδομών ως η κορυφαία εθνική CERT (USOM) κατέχουν κορυφαίες προτεραιότητες, επιτρέποντας στις TSK να ενημερώνονται για τις τρέχουσες εξελίξεις όσον αφορά τις απειλές στον κυβερνοχώρο, τις επιθέσεις και την τεχνολογία, για να αποφευχθεί έτσι η διπλή προσπάθεια.

Οι πολιτικές και τα μέτρα της τουρκικής στρατιωτικής ασφάλειας στον κυβερνοχώρο περιγράφονται από τους κανονισμούς του Γενικού Επιτελείου της Τουρκίας, οι οποίοι ακολουθούν τις εθνικές αποφάσεις ασφαλείας και τους συναφείς νόμους. Για να συμβαδίσουν με τη συνεχή εξέλιξη της ασφάλειας στον κυβερνοχώρο, ιδιαίτερα τα τελευταία 20 χρόνια, οι τουρκικές ένοπλες δυνάμεις αντιλαμβάνονται την άμυνα στον κυβερνοχώρο ως ξεχωριστό στρατιωτικό τομέα, συμβαδίζοντας έτσι με την αναγνώριση του κυβερνοχώρου από το NATO ως τομέα των επιχειρήσεων, όπως αυτό καθορίστηκε στη σύσκεψη κορυφής στη Βαρσοβία τον Ιούλιο του 2016.

Για να αντιμετωπίσουν τις αυξανόμενες απειλές και την εχθρότητα στον κυβερνοχώρο, είτε από κρατικούς είτε μη κρατικούς φορείς, η δημιουργία και διατήρηση ισχυρών και ανθεκτικών στάσεων και δυνατοτήτων στον κυβερνοχώρο είναι από τις κορυφαίες προτεραιότητες της αμυντικής στρατηγικής της Τουρκίας.

Οι εθνικές ασκήσεις στον κυβερνοχώρο διενεργούνται ετησίως από διαφορετικούς φορείς για να μετρήσουν την ανταγωνιστικότητα των δημοσίων ιδρυμάτων κατά των απειλών στον κυβερνοχώρο, τόσο για στρατιωτικούς όσο και για μη στρατιωτικούς σκοπούς. Ο κύριος σκοπός των ασκήσεων είναι να εκπαιδεύσουν,

[91] Kişisel Verileri Koruma Kurumu – Personal Data Protection Authority
[92] Seker Ensar, Tolga Ihsan Bukar, *National Cyber Security Organisation: Turkey*, CCDCOE, Tallinn 2018
[93] Türk Silahlı Kuvvetleri – Turkish Armed Forces (TAF)

ώστε να μπορούν να ενεργούν προληπτικά ενάντια σε απειλές προς τα εθνικά συμφέροντα ή τους πολίτες, να αποτρέπουν επιθέσεις, να τους εξαλείφουν και να αναπτύσσουν αντίμετρα. Αυτό αποτελεί μία από τις κορυφαίες προτεραιότητες των τουρκικών ενόπλων δυνάμεων σε σχέση με τον κυβερνοχώρο.

6.7.2 Δομή και οντότητες-κλειδιά. Το Υπουργείο Εθνικής Άμυνας διατηρεί τη γενική ευθύνη για τη στρατιωτική άμυνα στον κυβερνοχώρο και κατέχει την υψηλότερη θέση σε σχέση με τον στρατιωτικό κυβερνοχώρο.

Η Τουρκική Στρατιωτική Διοίκηση Κυβερνοάμυνας[94] είναι η ανώτατη αρχή για την προάσπιση των στρατιωτικών δικτύων στην Τουρκία και η κορυφαία στρατιωτική CERT (TAF-CERT). Το TAF-CERT λειτουργεί ως το εξωτερικό στρώμα των στρατιωτικών δικτύων των TAF αλλά και ως η επαφή μεταξύ του NATO (NCIRC), του εθνικού CERT και των στρατιωτικών υπό CERT. Στη δομή διοίκησης, η Διοίκηση Κυβερνοάμυνας των Τουρκικών Ενόπλων Δυνάμεων βρίσκεται υπό τη Διεύθυνση Επικοινωνιών, Ηλεκτρονικών και Πληροφοριακών Συστημάτων (J6 - Turkish: MEBS)[95] του Τουρκικού Γενικού Επιτελείου.

Η Διοίκηση Κυβερνοάμυνας είναι μια κοινή διακλαδική διοίκηση που διαθέτει προσωπικό από όλες τις υπηρεσίες. Για να διατηρηθεί ένα υψηλό επίπεδο συγχρονισμού και συντονισμού, διατηρείται ένας ενεργός δίαυλος επικοινωνίας μεταξύ του Υπουργείου Μεταφορών και Υποδομών (TÜBİTAK) και άλλων κυβερνητικών οργανώσεων. Η Διοίκηση Κυβερνοάμυνας διεξάγει επίσης κοινές δραστηριότητες με οντότητες και οργανισμούς του NATO στον κυβερνοχώρο και συμμετέχει σε πολυεθνικές ασκήσεις και αποστολές σε αυτό το πλαίσιο.

Η τρέχουσα στρατηγική στον κυβερνοχώρο για την άμυνα δίνει προτεραιότητα στην ενίσχυση των εθνικών δυνατοτήτων στον αμυντικό τομέα μέσω της στρατολόγησης και της κατάρτισης νέου προσωπικού. Για να υποστηρίξουν αυτό το στόχο, τα πανεπιστήμια και τα τεχνολογικά ινστιτούτα περιλαμβάνονται στα νέα μελλοντικά εθνικά αμυντικά σχέδια ανάπτυξης. Προκειμένου να βελτιωθούν ταυτόχρονα αυτά τα σχέδια, η ανάδραση από αυτούς τους παράγοντες ενσωματώνεται συνεχώς σε αυτές τις αναπτυξιακές προσπάθειες.

6.7.3 Έρευνα Ανάπτυξη και χρηματοδότηση. Στο πλαίσιο του προγράμματος εκσυγχρονισμού της Διοίκησης Κυβερνοάμυνας, αναπτύχθηκε ένα νέο στρατολογικό υπό CERT, ένα εξειδικευμένο εργαστήριο επιμόρφωσης στο

[94] Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı
[95] Communications, Electronics and Information Systems Directorate (J6)

κυβερνοχώρο, ένα σύστημα παρακολούθησης στρατιωτικών δικτύων με όλες τις σχετικές δομές υποστήριξης. Η χρηματοδότηση αυτών των διαδικασιών και μετασχηματισμών προέρχεται από τον προϋπολογισμό της εθνικής άμυνας. Έργα έρευνας και ανάπτυξης στο πλαίσιο της εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο και του σχεδίου δράσης για το διάστημα 2016-2019 έχουν ανατεθεί σε κορυφαίες εταιρείες και πανεπιστήμια στον τομέα της αμυντικής βιομηχανίας.

6.8 Κυβερνοάμυνα και Πληροφορίες[96]

Ειδικό τμήμα της Τουρκικής Εθνικής Υπηρεσίας Πληροφοριών, MİT[97] είναι υπεύθυνο για την εποπτεία των τηλεπικοινωνιών, όπως εξουσιοδοτείται από το νόμο, καθώς επίσης και για την ανάλυση, αποθήκευση των πληροφοριών επικοινωνίας για σκοπούς αντιπληροφοριών και καταπολέμησης τρομοκρατικών ενεργειών. Ο οργανισμός λειτουργεί κάτω από τις κρατικές υπηρεσίες πληροφοριών και τον νόμο περί εθνικών υπηρεσιών πληροφοριών του 2014.Ασχολείται με ανάλυση εικόνας και ήχου (IMINT), αποκρυπτογραφεί κρυπτογραφημένα δεδομένα και ασκεί δραστηριότητες εναντίον απειλών στον κυβερνοχώρο.

6.9 Εμπλοκή του ιδιωτικού τομέα[98]

Ο αριθμός των ιδιωτικών εταιρειών ασφαλείας στον κυβερνοχώρο στην Τουρκία αυξήθηκε ραγδαία τα τελευταία δύο χρόνια. Σήμερα, περισσότερες από 100 εταιρείες ασκούν δραστηριότητες στον τομέα της ασφάλειας στον κυβερνοχώρο. Μόλις πριν από 5-6 χρόνια, ο αριθμός αυτός ήταν μεταξύ 10 και 20. Ο ιδιωτικός τομέας έχει επίσης εξελιχθεί σημαντικά. Ενώ τα πρώτα χρόνια ήταν ως επί το πλείστον σύμβουλοι παγκοσμίων εταιρειών, που προσέφεραν συμβουλές ασφάλειας πληροφοριών στις βιομηχανίες, έχουν πλέον ωριμάσει ώστε πλέον αναπτύσσουν προϊόντα και τεχνολογίες που σχετίζονται με θέματα ασφάλειας στον κυβερνοχώρο των επιχειρήσεων.

Με τη συμβολή του ιδιωτικού τομέα που δραστηριοποιείται στην εθνική αμυντική βιομηχανία, δημοσιεύονται συνεχώς νέα ερευνητικά αποτελέσματα και εκθέσεις. Για παράδειγμα, η έκθεση για την κατάσταση της απειλής του κυβερνοχώρου στην Τουρκία δημοσιεύεται αρκετές φορές το χρόνο και έχει ως στόχο

[96] Seker Ensar, Tolga Ihsan Bukar, *National Cyber Security Organisation: Turkey*, CCDCOE, Tallinn 2018
[97] Millİstihbarat Teşkilatı Başkanlığı
[98] Seker Ensar, Tolga Ihsan Bukar, *National Cyber Security Organisation: Turkey*, CCDCOE, Tallinn 2018

να ενημερώσει τους δημόσιους και κυβερνητικούς αξιωματούχους σχετικά με τη δυναμική και τα πρόσφατα περιστατικά που αφορούν την εθνική ασφάλεια στον κυβερνοχώρο.

Σχετική εκπαίδευση παρέχεται από ακαδημαϊκά ιδρύματα, κυβερνητικούς και ιδιωτικούς οργανισμούς, ενώ ορισμένα πανεπιστήμια στην Τουρκία προσφέρουν διδακτορικά προγράμματα στον κυβερνοχώρο. Μερικές αξιοσημείωτες σχολές που προσφέρουν τέτοια προγράμματα είναι το Τεχνικό Πανεπιστήμιο της Μέσης Ανατολής, το Τεχνικό Πανεπιστήμιο Gebze, το Πανεπιστήμιο Hacettepe και το Πανεπιστήμιο του Μαρμαρά.

Τα τελευταία χρόνια, η Τουρκία κατέβαλε σημαντικές προσπάθειες στη διαδικασία συγκέντρωσης διαφόρων παραγόντων υπό ένα εθνικό τομέα στον κυβερνοχώρο. Τον Οκτώβριο του 2017, η Προεδρία των Αμυντικών Βιομηχανιών (SSB) κάλεσε τις κυριότερες ιδιωτικές εταιρείες ασφάλειας στον κυβερνοχώρο να συζητήσουν περαιτέρω το ζήτημα αυτό και την πιθανή συνεργασία μεταξύ αυτών των φορέων.

Αν και δεν υπάρχει νομική υποχρέωση για τη συμμετοχή της ιδιωτικής βιομηχανίας σε αυτή τη συνεργασία, δίνεται έμφαση στην αμοιβαία εμπιστοσύνη και τη συνεργασία μεταξύ δημόσιων και ιδιωτικών φορέων. Το βασικό κίνητρο αυτών των προσπαθειών είναι να ενισχυθούν οι σχέσεις αγοραστή-προμηθευτή, τα κοινά κανάλια διανομής, οι κοινές ομάδες εργασίας και οι δραστηριότητες έρευνας και ανάπτυξης που διεξάγονται από πανεπιστήμια με εταιρείες που μπορούν να δημιουργήσουν καλύτερες ευκαιρίες και οφέλη και για τις δύο πλευρές. Λόγω των κοινών οικονομικών συμφερόντων, οι εταιρείες του τομέα είναι πιο παραγωγικές, πιο καινοτόμες και επομένως πιο ανταγωνιστικές από τις εταιρείες που λειτουργούν μόνες τους.

6.10 Εκτίμηση της μη κρατικής απειλής για την Τουρκία[99]

Καθώς τα κράτη στη Μέση Ανατολή βρίσκονται σε παρακμή σε ότι αφορά τη "Διαδικτυακή Σκηνή", οι μη κρατικοί δρώντες δείχνουν σημαντικό ενδιαφέρον για τις επιχειρήσεις στον κυβερνοχώρο, οδηγώντας στην εξάπλωση των συγκρούσεων.

Αξίζει να δοθεί προσοχή στο Συριακό Ηλεκτρονικό Στρατό (SEA). Ο κύριος πυρήνας του κυβερνητικού δικτύου επιχειρήσεων βρίσκεται στο Ντουμπάι με άλλα

[99] Seker Ensar, Tolga Ihsan Bukar, *National Cyber Security Organisation: Turkey*, CCDCOE, Tallinn 2018

μέλη στη Συρία. Χρηματοδοτημένος από τον ξάδερφο του Basselal-Assad, Rami Makhlouf, ο SEA ονομάζεται "πραγματικός στρατός στην εικονική πραγματικότητα" από τον συριακό δικτάτορα Basselal-Assad.[100] Η ενημέρωση του IHS Jane'sδείχνει ότι ο τρόπος λειτουργίας της SEA πραγματοποιείται κυρίως μέσω ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing emails), προσελκύοντας τους παραλήπτες να κάνουν κλικ σε συνδέσμους ή εισάγοντας στοιχεία σύνδεσης για τοποθεσίες που η SEA προσπαθεί να βανδαλίσει και τις οποίες συλλαμβάνει. Έχει ένα εντυπωσιακό σύνολο στόχων που περιλαμβάνει τη "The Washington Post", τη "UNICEF", την ιστοσελίδα του Στρατού των ΗΠΑ, τη "LeMonde", τους "International Business Times" και τους "Reuters".

Είναι επίσης γνωστό ότι η Συριακή Εταιρεία Πληροφορικής (SCS),[101] μια τεχνολογική ομάδα που ιδρύθηκε από τον Basselal-Assad, παρείχε τη βάση για τον SEA.

Οι τρέχουσες ικανότητες του SEAστον κυβερνοχώρο, σε συνδυασμό με την υποστήριξη της SCS μπορούν να βελτιωθούν σε απειλητικό βαθμό. Επιπλέον, οι σύμμαχοι του καθεστώτος, ιδιαίτερα η Κίνα και το Ιράν, απολαμβάνουν τεράστιες δυνατότητες κυβερνοπολέμου, οι οποίες θα μπορούσαν να μεταφραστούν σε ξένη βοήθεια στις εχθρικές κυβερνητικές δραστηριότητες του καθεστώτος.

Εκτός από την SEA και την SCS, το Cyber caliphate που συνδέεται με το ISIS είναι ένας άλλος σημαντικός παράγοντας στον οποίο η Τουρκία πρέπει να δώσει προσοχή. Η πιο συγκλονιστική ενέργεια του ομίλου ήταν η πειρατεία του γαλλικού τηλεοπτικού δικτύου TV5 Monde στις 8 Απριλίου 2015 με το πειρατικό μήνυμα του "Jesuis ISIS".[102] Το Cyber caliphate ανέβασε προσωπικές ταυτότητες και τα βιογραφικά των γάλλων στρατιωτών οι οποίοι πολεμούσαν σε επιχειρήσεις κατά του ISIS. Επιπλέον η ριζοσπαστική ομάδα εξτρεμιστών χάκερ προσέβαλλε επίσημο λογαριασμό Twitter της Κεντρικής Διοίκησης των ΗΠΑ στις αρχές του 2015.[103]

Οι δραστηριότητες του Cyber caliphate θα μπορούσαν να αποτελέσουν μεγάλη απειλή για την Τουρκία, ανυψώνοντας περισσότερο τον εξτρεμισμό ανάμεσα στη θρησκευτική νεολαία, ειδικά επειδή η χρήση του Διαδικτύου στην Τουρκία είναι υψηλότερη από τους γείτονές της στη Μέση Ανατολή. Η Τουρκία θα μπορούσε

[100] Jane's Intelligence Review, *Middle East Conflict Spills into Cyber space*, 2015, page 3-4
[101] Syrian Computer Society
[102] http://rt.com/news/248073-islamic-state-hackers-french-tv/ (έγινε πρόσβαση στις 20 Οκτ 2019)
[103] http://rt.com/usa/221927-central-command-hackedcybercaliphate/(έγινε πρόσβαση στις 20 Οκτ 2019

επίσης να αντιμετωπίσει επιθέσεις στον κυβερνοχώρο, οι οποίες ενδέχεται να στοχεύουν σε επίσημους δικτυακούς τόπους και σε παραδοσιακά δίκτυα μέσων.

Κεφάλαιο Έβδομο
Συμπεράσματα

7.1 Γενικά

Ένα υψηλού επιπέδου κυβερνοόπλο μοιάζει, από τη μια με ένα πυρηνικό όπλο στην ικανότητά του να καταστρέφει την κρίσιμη εθνική υποδομή και από την άλλη είναι παρόμοιο με ένα βιολογικό όπλο σε ότι αφορά στις πληροφορίες που απαιτούνται για την ανίχνευση του χτυπήματος και τον εντοπισμό του δράστη. Σε κάποιο βαθμό, θυμίζουν ωρολογιακές βόμβες για τη χρονική διαφορά μεταξύ του χρόνου επίθεσης και της στιγμής του αντίκτυπου που μπορεί να σχεδιάσει ο επιτιθέμενος. Επειδή τα κυβερνοόπλα είναι μυστικά επιχειρησιακά όπλα, είναι συγκρίσιμα με τις σύγχρονες Ειδικές Δυνάμεις.

Ο πόλεμος στον κυβερνοχώρο είναι ένα πολύπλοκο φαινόμενο που προσδίδει στον πόλεμο κάτι παραπάνω από μια απλή τεχνολογική αλλαγή. Ο πόλεμος στον κυβερνοχώρο συνίσταται σε μια τεχνολογική επανάσταση όσον αφορά τις κινητικές και μη κινητικές στρατιωτικές ικανότητες που έχουν επιφέρει τα νέα δόγματα, οι οργανώσεις, οι έννοιες, οι στρατηγικές και τακτικές, οι επιθετικές και αμυντικές προσεγγίσεις και κυρίως, μια νέα κατηγορία πολεμιστών.

Ο πόλεμος στον κυβερνοχώρο τέλος αναφέρεται πλέον σ' ένα νέο τομέα επιχειρήσεων. Οι τομείς του πολέμου είναι αλληλένδετοι μιλώντας για κοινές έννοιες πολέμου και συνδυασμένων επιχειρήσεων. Με άλλα λόγια, οι έννοιες όπως η Air-Land Battle, η Air-Sea Battle, αναγκάζουν τις αεροπορικές, χερσαίες και ναυτικές μονάδες να υιοθετήσουν όλο και περισσότερο κοινό χαρακτήρα και να προωθήσουν περαιτέρω τις διαδικτυακές επιχειρήσεις. Τον τελευταίο αιώνα, το διάστημα έχει ενσωματωθεί σε αυτή τη σύνθετη εικόνα και έχει γίνει ένα ανεκτίμητο μέρος των επιχειρήσεων. Αποστολές, όπως η πυραυλική άμυνα ή ο διηπειρωτικός βαλλιστικός πύραυλος (ICBM), δεν μπορούν να υλοποιηθούν χωρίς τη χρήση μέσων στο διάστημα. Τα συστήματα πυροβολικού, οι μονάδες τεθωρακισμένων, ακόμη και το σύγχρονο πεζικό επωφελούνται από τα συστήματα που βασίζονται στο GPS, τα συστήματα καθοδήγησης όπλων και από τα δίκτυα παροχής πληροφοριών στο θέατρο των επιχειρήσεων.

Λόγω των δραστικών αλλαγών που έχει επιφέρει η διασύνδεση όλων τον μέσων, μέσω της υψηλής τεχνολογίας, ο κυβερνοχώρος είναι στενά ενσωματωμένος σε όλους τους τομείς του πολέμου. Από την άποψη αυτή, οι μονάδες ελέγχου όπλων

γίνονται ολοένα και πιο μηχανογραφημένες όσον αφορά την υποδομή C4ISR.[104] Κάτω από αυτές τις συνθήκες, τα όπλα στον κυβερνοχώρο εισέρχονται στο προσκήνιο με την ικανότητά τους να παραλύουν και να τυφλώνουν τους κόμβους διοικήσεως και ελέγχου του εχθρού. Επιπλέον, ο ηλεκτρονικός πόλεμος (EW), που αποτελεί αναπόσπαστο στοιχείο όλων των στρατιωτικών κλάδων αλλά κυρίως για τις σύγχρονες αεροπορικές δυνάμεις, έχει μια στενότερη σχέση με τον κυβερνοπόλεμο. Το ίδιο θα μπορούσε να λεχθεί και για τις πληροφοριακές επιχειρήσεις και τον ψυχολογικό πόλεμο.

7.2 Συναγόμενα Συμπεράσματα

Από τη μελέτη του θέματος προκύπτουν ορισμένα συμπεράσματα:

α. Από τη στιγμή που η ζωή του σύγχρονου ανθρώπου βασίζεται όλο και περισσότερο στη χρήση και τη δικτύωση υπολογιστών κάθε είδους, η κυβερνοαπειλή θα υφίσταται, τα κυβερνοόπλα θα εξελίσσονται συνεχώς και οι κυβερνοεπιθέσεις θα πραγματοποιούνται σε όλο το φάσμα της ανθρώπινης δραστηριότητας, από τώρα και στο εξής.

β. Βρισκόμαστε πλέον στην εποχή που οι κυβερνοπολεμιστές έχουν πάρει τη μορφή επαγγελματιών που δρουν στον κυβερνοχώρο και οι οποίοι μπορούν να πλήξουν κρίσιμες υποδομές οποιασδήποτε χώρας, προκαλώντας πλείστα όσα προβλήματα στην κανονικότητα της καθημερινής ζωής των πολιτών της.

γ. Το παρόν νομικό πλαίσιο παγκοσμίως δεν έχει συμπεριλάβει ακόμα την έννοια του κυβερνοπολέμου μέσα στις διατάξεις του. Ως εκ τούτου τα όρια μεταξύ επίθεσης και μη επίθεσης, εγκλήματος και μη εγκλήματος είναι δυσδιάκριτα και όχι σαφώς καθορισμένα. Δεν έχουν θεσπιστεί, στα πλαίσια διεθνών συμφωνιών, νόμοι από όλα τα κράτη, που να σχετίζονται με κρίσιμα θέματα που αφορούν στον κυβερνοπόλεμο. Κάποια κράτη όπως η Εσθονία, λόγω σοβαρής κρίσης που υπέστη εξαιτίας κυβερνοεπίθεσης, έχει αρχίσει να διαμορφώνει εθνική συνείδηση κυβερνοασφάλειας, αλλά σε συλλογικό επίπεδο δεν έχει επιτευχθεί ακόμα κάποια σημαντική πρόοδος.

δ. Αποτελώντας σημαντικό πυλώνα ισχύος κάθε σύγχρονου κράτους, η κυβερνοάμυνα εντάσσεται στον εθνικό σχεδιασμό Υψηλής Στρατηγικής προκειμένου να εξυπηρετήσει και να εξασφαλίσει τα εθνικά συμφέροντα.

[104] Command-Control-Communications-Computers-Intelligence-Surveillance-Reconnaisance

ε. Μέσω της αποκλειστικής προσφυγής στον κυβερνοπόλεμο, ένας δρων, κρατικός ή μη, μπορεί να εκπληρώσει πολιτικούς σκοπούς που θα ήταν αδύνατο να επιτευχθούν με συμβατικές δυνάμεις. Θα μπορούσαμε να πούμε δηλαδή ότι είναι μια μορφή πολέμου που μπορεί να εφαρμοστεί και από τις μικρές χώρες που υστερούν σε συμβατικές στρατιωτικές δυνάμεις ή ακόμα και από μεμονωμένους παίχτες.

στ. Όπως και στις συμβατικές επιχειρήσεις, για να μπορέσει ένα κράτος να εντάξει την έννοια της αποτροπής στη στρατηγική κυβερνοπολέμου που ακολουθεί, θα πρέπει να διαθέτει αξιόπιστες επιθετικές δυνατότητας.

ζ. Οι κυβερνοεπιθέσεις δεν έχουν σαν στόχο μόνο τις υποδομές του δημόσιου τομέα. Είναι δυνατόν να στραφούν και εναντίον ιδιωτικών εγκαταστάσεων. Η στενή σχέση και συνεργασία μεταξύ των φορέων αυτών θα αποτελέσει την καλύτερη αποτροπή για κάθε πιθανή κυβερνοεπίθεση. Από την άλλη πλευρά θα ωφελήσει αμφοτέρους τους εθνικούς δρώντες αφού συνεργασίες τέτοιου είδους θα τους κάνει να αποκτήσουν πλήρη γνώση των κρίσιμων αδυναμιών τους, τις οποίες καλούνται να προστατέψουν.

η. Οι ένοπλες δυνάμεις έχουν μια σχέση υποστηρίζοντος-υποστηριζομένου με τον κυβερνοπόλεμο. Στο σύγχρονο θέατρο επιχειρήσεων φαντάζει αδύνατη μια ενέργεια συμβατικών δυνάμεων, χωρίς πριν ή κατά τη διάρκειά της, να έχει εκτελεστεί κάποιου είδους κυβερνοεπιχείρηση, είτε για παραπλάνηση, είτε για συλλογή πληροφοριών, είτε στα πλαίσια κάποιας υποβοηθητικής αποστολής.

θ. Η όλο και μεγαλύτερη αλληλεξάρτηση των σύγχρονων κρατών μεταξύ τους, καθιστά επιτακτική την αυστηρή επιλογή των κρίσιμων υποδομών του αντιπάλου που θα επιλεγούν ως κυβερνοστόχοι, καθώς μια λάθος επίθεση δύναται να επηρεάσει δρώντες που έως τότε δεν αποτελούσαν στόχο. Αυτό μπορεί να έχει τα ακριβώς αντίθετα αποτελέσματα για το δρώντα που εκδηλώνει την κυβερνοεπίθεση.

ι. Είναι φανερό ότι ο κυβερνοπόλεμος από μόνος του μπορεί να λειτουργήσει αποτρεπτικά ώστε να μην προχωρήσουν οι αντίπαλοι σε συμβατικές επιχειρήσεις. Από την άλλη όμως θα μπορούσε να λειτουργήσει σαν προπαρασκευαστική φάση εκτεταμένων συμβατικών επιχειρήσεων, για την επίτευξη του επιθυμητού αντικειμενικού σκοπού.

ια. Για μη κρατικούς δρώντες, όπως οι διάφορες τρομοκρατικές οργανώσεις, ή μεμονωμένοι χάκερς, ο κυβερνοχώρος αποτελεί έναν ιδανικό χώρο παράνομης δράσης, καθώς εκεί μπορούν να κρύψουν πολύ εύκολα τα ίχνη τους. Αυτό σημαίνει

πως το ίδιο το διαδίκτυο δεν φαίνεται να αποτελεί στόχο αφού την ίδια στιγμή αποτελεί το χώρο δράσεως και αποκρύψεώς τους.

ιβ. Το κόμματι της κυβερνοασφάλειας που κοστίζει πιο πολύ σ' ένα σύγχρονο κράτος είναι εκείνο που αφορά στο ανθρώπινο δυναμικό. Η εκπαίδευση ικανού αριθμού ανθρώπων είναι ακριβή και σίγουρα πολύ χρονοβόρα διαδικασία. Το προσωπικό αυτό επίσης είναι δυσεύρετο και δυσαναπλήρωτο. Αποτελεί όμως την καλύτερη και πιο εγγυημένη επένδυση στο χώρο της κυβερνοασφάλειας.

ιγ. Κράτη με φτωχή ή ανύπαρκτη πληροφοριακή υποδομή, δεν αποτελούν ελκυστικούς στόχους για κυβερνοεπιθέσεις. Υπό αυτή την έννοια η χώρα μας δεν είναι ψηλά στη λίστα των κυβερνοστόχων αφού η διασύνδεση των κρίσιμων υποδομών μεταξύ τους δεν έχει ακόμα ολοκληρωθεί. Από την άλλη όμως, αυτό σημαίνει πως αν τελικά δεχτεί ευρείας κλίμακας κυβερνοεπίθεση, οι δυνατότητες άμυνας μειώνονται δραματικά.

ιδ. Σήμερα σημαντικά βήματα έχουν γίνει στον τομέα της κυβερνοασφάλειας, αφού έχει οριστεί ως Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT), η οποία καλύπτει τους τομείς της ενέργειας, των μεταφορών, των τραπεζών, των υποδομών χρηματοπιστωτικών αγορών, της υγείας, της προμήθειας και διανομής πόσιμου νερού και των ψηφιακών υποδομών και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ (ΓΕΕΘΑ/ΔΙΚΥΒ). Συνεργαζόμενη δε άμεσα με τη Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, προβλέπεται ότι το αποτέλεσμα θα είναι προς όφελος του εθνικού συμφέροντος. Μένει να υλοποιηθούν αρκετά στάδια προς αυτή την κατεύθυνση, τα οποία είναι σε εξέλιξη αυτή τη στιγμή, αλλά οι ενδείξεις είναι άκρως ενθαρρυντικές καθώς κατάλληλα στελέχη, γνώστες του αντικειμένου, έχουν τοποθετηθεί στις κατάλληλες θέσεις, ώστε να φέρουν σε πέρας τις τρέχουσες διαδικασίες.

ιε. Γενικότερα και σε διεθνές επίπεδο ο κυβερνοχώρος θεωρείται το πέμπτο πεδίο πολέμου. Για χώρες με μικρό προϋπολογισμό ο κυβερνοχώρος προσφέρει πολλές δυνατότητες με σχετικά περιορισμένα κόστη. Γι' αυτό και αποτελεί ευκαιρία για την χώρα μας να επενδύσει σ' αυτό το πεδίο. Οι πολύ καλές σχέσεις που διατηρούμε με σοβαρούς παίκτες όπως ΗΠΑ και Ισραήλ, μας επιτρέπουν να έχουμε πρόσβαση σε εκπαιδεύσεις και ασκήσεις που είναι πολύτιμες.

ιστ. Στην Ελλάδα υπάρχουν τεράστιες δυνατότητες από πλευράς προσωπικού οι οποίες δυστυχώς δεν αξιοποιούνται στο έπακρο. Η δυσχερής οικονομική κατάσταση έχει επηρεάσει αρνητικά την πρόοδο της χώρας στον τομέα του κυβερνοχώρου, ενώ αξιόλογα ‘’μυαλά’’ αναγκάζονται να μεταναστεύσουν στο εξωτερικό.

Κεφάλαιο Όγδοο
Προτάσεις

8.1 Γενικά

Ο σταθερά αυξανόμενος όγκος, η πολυπλοκότητα της κακόβουλης δραστηριότητας στον κυβερνοχώρο, καθώς επίσης και η ταχύτητα με την οποία συμβαίνουν τα γεγονότα στο χώρο αυτό, υπογραμμίζουν την ανάγκη για μεγαλύτερη έμφαση στην πρόληψη και στην ανθεκτικότητα και λιγότερο στην αντίδραση και στην άμεση αντιμετώπιση. Οι ΕΔ θα πρέπει να είναι ικανές να αντέχουν σε κυβερνοεπιθέσεις και να εξασφαλίσουν τη συνέχεια στις υπηρεσίες των επικοινωνιακών και πληροφοριακών συστημάτων τους για το πλήρες φάσμα των αποστολών τους.

8.2 Συναγόμενες Προτάσεις

Από την παραπάνω ανάλυση προκύπτουν κάποιες προτάσεις σχετικά με τις ενέργειες που πρέπει να γίνουν και τα μέτρα που πρέπει να ληφθούν, τόσο σε κυβερνητικό επίπεδο, όσο και σε επίπεδο ενόπλων δυνάμεων. Τις στιγμές που γράφεται αυτή η διατριβή, πολλά «ιστορικά» πράγματα έχουν ήδη αρχίσει να υλοποιούνται στη χώρα μας στο πεδίο του κυβερνοπολέμου. Αρκετά υπολείπονται να γίνουν για να ολοκληρωθεί η όλη προσπάθεια. Κατά την άποψή μου αυτά είναι:

α. Η επιτυχής διεξαγωγή επιχειρήσεων κυβερνοπολέμου προϋποθέτει θεμελιώδη αλλαγή νοοτροπίας του προσωπικού των Ενόπλων Δυνάμεων και ειδικότερα της πολιτικής και στρατιωτικής ηγεσίας, στενή συνεργασία όλων των εμπλεκόμενων φορέων σε εθνικό και ιδιωτικό επίπεδο, κατάλληλη επιλογή και εκπαίδευση προσωπικού και συμμετοχή στη διαδικασία Εθνικής Αμυντικής Σχεδίασης, μέσω ειδικής επιτροπής.

β. Οι ΕΔ θα πρέπει να αποφύγουν την αλληλοκάλυψη των υφιστάμενων προσπαθειών που λαμβάνουν χώρα αυτή την περίοδο και ταυτόχρονα να επιδιώξουν τη διαλειτουργικότητα, τη διασυνδεσιμότητα και τη μέγιστη αξιοποίηση του εξειδικευμένου και κατάλληλα καταρτισμένου προσωπικού που διαθέτουν.

γ. Η Ελλάδα οφείλει να εφαρμόσει ένα ενιαίο δόγμα για την προστασία των κρίσιμων υποδομών της, αναβαθμίζοντας την προστασία των συστημάτων πληροφοριών.

δ. Προκειμένου να φτάσει η χώρα σε υψηλό επίπεδο τεχνολογικής ανωτερότητας, πρέπει να επενδύσει στην ανίχνευση ταλέντων. Ο τομέας της

τεχνολογίας απαιτεί άτομα τα οποία σκέφτονται και ενεργούν έξω από στεγανά και ιεραρχημένες δομές. Η κυβέρνηση αλλά και οι Ελληνικές Ένοπλες Δυνάμεις μπορούν να δημιουργήσουν αυτό το φυτώριο του τεχνολογικά εκπαιδευμένου προσωπικού. Πολλές χώρες έχουν εφαρμόσει αντίστοιχο πρόγραμμα:

(1) Το Ισραήλ διαθέτει την Ομάδα 8200[105], η οποία εκπαιδεύει το προσωπικό που υπηρετεί πάνω στην τεχνολογία. Αυτό το προσωπικό όταν απολυθεί είναι οι δημιουργοί των φημισμένων τεχνολογικών καινοτομιών της χώρας.

(2) Την ίδια λογική ακολουθεί και η Αγγλία, η οποία άνοιξε το ιστορικό Bletchley Park[106]. Το κτίριο της κρυπτογραφίας κατά τον Β΄ ΠΠ ανακαινίστηκε για να εκπαιδεύει η Αγγλία τους αυριανούς «καλούς χάκερς», τους οποίους και αναζητάει ακόμα και από τα θρανία του Γυμνασίου.

(3) Πολλές χώρες, μεταξύ των οποίων και κάποιοι Έλληνες με δική τους πρωτοβουλία, συμμετέχοντας στο ετήσιο παγκόσμιο συνέδριο[107] «χάκερς» που διοργανώνεται κάθε χρόνο στα καζίνο του Λας Βέγκας, αναγνωρίζουν τους μελλοντικούς συνεργάτες τους στον τομέα του κυβερνοχώρου. Είναι αυτοί που θα δουλέψουν στο δημόσιο ή ιδιωτικό τομέα επ' ωφελεία της Αμερικάνικης κυβέρνησης.

ε. Οι χώρες – οργανώσεις οι οποίες πρέπει να αποτελέσουν άμεσα αντικείμενο ελληνικού κυβερνοενδιαφέροντος, λόγω της πιθανής εξέλιξής τους σε στρατιωτικές απειλές ή κυβερνοαπειλές είναι, η Τουρκία, η Β. Μακεδονία, η Αλβανία, η Βουλγαρία, η Μεγάλη Βρετανία, η Ιταλία, η Γαλλία, οι ΗΠΑ, η Ρωσία, η Κίνα, η Γεωργία και η Al Qaeda.

στ. Η Ελλάδα θα πρέπει να προβεί στην υιοθέτηση, αναθεώρηση, συμπλήρωση του εθνικού νομικού πλαισίου που αφορά στη δραστηριότητα στον Κυβερνοχώρο.

ζ. Θα πρέπει να συναφθούν συμφωνίες με άλλες χώρες για την παροχή υποστήριξης στον εντοπισμό του ίχνους των κυβερνοεπιθέσεων και στην πηγή τους, έτσι ώστε να εντοπιστούν οι μελλοντικοί δράστες και να προσαχθούν σε δίκη ή να εκδοθούν.

---

[105] https://en.wikipedia.org/wiki/Unit_8200, (έγινε πρόσβαση στις 3 Απρ 19)
[106] https://el.wikipedia.org/wiki/Μπλέτσλεϊ_Παρκ, (έγινε πρόσβαση στις 3 Απρ 19)
[107] Γιάννης, Παπαδόπουλος, «Η μεγάλη διεθνής σύναξη των χάκερ», Κ*αθημερινή,* 20 Αυγούστου 2018, http://www.kathimerini.gr/980573/gallery/texnologia/diadiktyo/h-megalh-die8nhs-syna3h-twn-xaker, (έγινε πρόσβαση στις 3 Απρ 19)

η. Θεωρείται επιβεβλημένη η εισαγωγή κλάδου Κυβερνοασφάλειας στα τμήματα Πληροφορικής των πανεπιστημίων με σκοπό την παροχή εκπαιδεύσεων μέσω μεταπτυχιακών και διδακτορικών σπουδών. Αυτό θα εξυπηρετούσε την απόλυτη εξειδίκευση προσωπικού που θα μπορούσε αργότερα να στελεχώσει αντίστοιχες θέσεις τόσο στον ιδιωτικό, όσο και στο δημόσιο τομέα, στην Ελλάδα ή και σε διεθνής οργανισμούς που ασχολούνται με τον κυβερνοχώρο. Στο ίδιο πνεύμα κρίνεται αναγκαία η εισαγωγή ανάλογων μαθημάτων και στις παραγωγικές σχολές των Ενόπλων Δυνάμεων καθώς όλα τα στελέχη συχνά χειρίζονται ευαίσθητες πληροφορίες και ενδέχεται να αποτελέσουν στόχους κυβερνοεπίθεσης.

θ. Απαιτείται εκστρατεία ενημέρωσης των χρηστών πληροφοριακών συστημάτων, με σκοπό να αυξηθεί η κατανόηση των κινδύνων και η έκταση των προκλήσεων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, τόσο σε επίπεδο ΕΔ όσο και σε εθνικό επίπεδο.

ι. Είναι απαραίτητη η εκπόνηση μελέτης όπου να φαίνονται καταγεγραμμένες όλες οι υποδομές τις οποίες η χώρα καθορίζει ως κρίσιμες, τόσο στον ιδιωτικό, όσο και στο δημόσιο τομέα, ώστε να μπορέσει να γίνει σωστός καθορισμός έργου με σκοπό την κυβερνοασφάλειά τους. Μια τέτοια μελέτη απαιτεί ετήσια επικαιροποίηση ώστε η βάση δεδομένων που αφορά στην οργάνωση της κυβερνοάμυνας να παραμένει πάντα ενημερωμένη. Επιπλέον θα πρέπει να γίνεται συνεχής έλεγχος αυτών των υποδομών ώστε να διαπιστώνονται τα σημεία τρωτότητάς τους. Θεωρώ ότι η εθνική στρατηγική κυβερνοπολέμου θα πρέπει να στηρίζεται πρωτίστως στην τακτική της προληπτικής άμυνας και δευτερευόντως στην προληπτική επίθεση.

ια. Επειδή όπως έχω ήδη αναφέρει βρισκόμαστε ήδη εν μέσω σοβαρών εξελίξεων – αποφάσεων, στον τομέα του κυβερνοχώρου και εξαιτίας του σαφούς καθορισμού ως εθνικού CSIRT της ΓΕΕΘΑ/ΔΙΚΥΒ, θα πρέπει, αν δεν της έχει ήδη εκχωρηθεί η μέγιστη δυνατή πρωτοβουλία αντιδράσεων σε περίπτωση κάποιου κυβερνοεπεισοδίου, χωρίς να παρεμβάλλονται πολλά επίπεδα λήψης απόφασης, καθώς οι ενέργειες και οι εξελίξεις των συμβάντων αυτών είναι ταχύτατες και σύντομες. Η "ομίχλη" δε που καλύπτει τον επιτιθέμενο καθιστά ακόμα περισσότερο επιβεβλημένη αυτή την ταχύτητα λήψης απόφασης.

ιβ. Όπως υφίσταται θεσμικά κείμενα που αφορούν στην πολιτική κυβερνοασφάλειας στις ΕΔ, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, θα

πρέπει να εκπονηθεί ξεκάθαρη Εθνική Στρατηγική Κυβερνοπολέμου σε εθνικό επίπεδο.

ιγ. Βρίσκεται σε πολύ καλό επίπεδο η σχεδίαση – εκτέλεση της ετήσια εθνικής άσκησης κυβερνοπολέμου «ΠΑΝΟΠΤΗΣ». Ανάλογη θα πρέπει να είναι και η συμμετοχή μας σε αντίστοιχες διεθνείς ασκήσεις (ΝΑΤΟϊκές ή της Ευρωπαϊκής Ένωσης), ώστε να ανταλλάσσονται απόψεις και να αποκτώνται παραστάσεις προς βελτίωση όλων. Οι ενοποιημένες προσπάθειες και η συνεργασία για την αντιμετώπιση των απειλών στον κυβερνοχώρο είναι κρίσιμης σημασίας. Πρέπει να διεξάγονται τακτικές ασκήσεις στον κυβερνοχώρο όπου να υπάρχει αποτελεσματική "κόκκινη" δραστηριότητα.

ιδ. Μέσα από τη ΓΕΕΘΑ/ΔΙΚΥΒ απαιτείται ο σχεδιασμός ενός εθνικού προγράμματος, ώστε να μπορέσει η χώρα να καταστεί ικανή να παράγει απολύτως εγχώριες κυβερνοδυνατότητες ώστε σταδιακά να μπορέσουμε να γίνουμε αυτάρκεις σε συστήματα κυβερνοπολέμου. Ανάλογη στόχευση έχει η Λιθουανία, μετά την ρωσική κυβερνοεπίθεση που δέχτηκε το 2008.

ιε. Προτείνεται η αύξηση της συνεργασίας με χώρες που έχουν αναπτύξει τεχνολογίες κυβερνοπολέμου, όπως ΗΠΑ και Ισραήλ. Από γεωγραφικής άποψης, ανάπτυξης τεχνολογίας και διπλωματικών δεσμών, αυτή τη στιγμή το Ισραήλ προσφέρεται ως η προτιμότερη επιλογή. Επίσης προτείνεται η ενίσχυση της παρουσίας της χώρας στο Κέντρο Αριστείας Κυβερνοάμυνας του ΝΑΤΟ, στο Ταλίν της Εσθονίας.

ιστ. Το χρονικό διάστημα που τα στελέχη υπηρετούν στη ΓΕΕΘΑ/ΔΙΚΥΒ, προτείνεται να υπολογίζεται ως χρόνος Δκσεως. Έτσι τα εν λόγω στελέχη, τα οποία έχουν επιλεγεί με συγκεκριμένα κριτήρια, προκειμένου να στελεχώσουν τη Δνση, δεν θα χρειαστεί να μετατεθούν για να εξελιχθούν σταδιοδρομικά. Σε ανάλογα ‘’τεχνικά’’ αντικείμενα απαιτείται εμπειρία αρκετών ετών ώστε το προσωπικό να θεωρείται πλήρως αξιοποιήσιμο και αποδοτικό.

ιζ. Η ειδικότητα «Ασφάλεια Πληροφορικής» θα πρέπει να αποδίδεται από όλους τους κλάδους και να προβλέπονται εκπαιδεύσεις είτε μέσω ΠΜΣ στην Ελλάδα και το εξωτερικό, είτε μέσω ειδικών σεμιναρίων από εξειδικευμένους καθηγητές.

ιη. Η κυβερνοασφάλεια είναι μια αναδυόμενη περιοχή εμπειρογνωμοσύνης που βασίζεται σε μια πολυεπιστημονική προσέγγιση. Ως εκ τούτου, πρέπει να δημιουργηθούν νέα εκπαιδευτικά προγράμματα για την Ελληνική

δομή ασφαλείας, τα οποία θα επεκταθούν με την αποτελεσματική συνεργασία μεταξύ ακαδημαϊκών κύκλων και ιδιωτικού τομέα.

Κεφάλαιο Ένατο
Επίλογος

Ο σύγχρονος συμβατικός πόλεμος έχει πλέον πολλά στοιχεία πληροφορικής. Η τεχνολογία έχει εξελιχθεί με απίστευτους ρυθμούς, οι ηλεκτρονικοί υπολογιστές θεωρούνται πλέον απαραίτητα εργαλεία και η πληροφορία παίζει ρόλο κλειδί στη λειτουργία του παγκόσμιου συστήματος. Κυκλοφορεί ευρέως πλέον η άποψη ότι «μερικά γραμμάρια πυριτίου σ' έναν υπολογιστή είναι πιο αποτελεσματικά από έναν τόνο ουρανίου στο πεδίο της μάχης». Όποιος από τους αντιπάλους χειρίζεται με τον καλύτερο τρόπο ''το πληκτρολόγιο'' έχει μεγάλο πλεονέκτημα πρόσβασης σε κρίσιμες υποδομές και ως εκ τούτου μπορεί να επηρεάσει σε μεγάλο βαθμό την έκβαση μιας σύγκρουσης.

Οι σύγχρονοι χειριστές του κυβερνοπολέμου διαθέτουν πολλά εργαλεία με τα οποία μπορούν είτε να αποτρέψουν είτε να πειθαναγκάσουν ενέργειες του αντιπάλου. Τα κυβερνοόπλα είναι πιο γρήγορα και πιο οικονομικά σε σχέση με τα όπλα του συμβατικού πολέμου ενώ τα αποτελέσματά τους είναι το ίδιο ή και περισσότερο ισχυρά.

Ανάλογα με τις δυνατότητες της κάθε εποχής εξελίσσονται και μαζί με αυτά και οι τρόποι αντιμετώπισής τους. Η τεχνολογία έχει προχωρήσει και η προστασία των κρατών απαιτεί όλο και πιο ισχυρά τεχνολογικά μέσα για να μπορεί να ανταπεξέλθει.

Οι πρόσφατες αυτές εξελίξεις ενδέχεται να θέτουν σε κίνδυνο όλες τις κρίσιμες υποδομές της χώρας, τόσο στον ιδιωτικό τομέα, όσο και στο χώρο των ενόπλων δυνάμεων. Θα πρέπει λοιπόν η Ελλάδα να είναι έτοιμη να αμυνθεί των σύγχρονων κυβερνοεπιθέσεων ώστε να διασφαλιστούν τα εθνικά μας συμφέροντα.

Κλείνοντας θα ήθελα να τονίσω ότι οι δυνατότητες κυβερνοπολέμου κάθε έθνους αποτελούν επτασφράγιστο μυστικό, με αποτέλεσμα η συγκεκριμένη διατριβή, προκειμένου να παραμείνει αδιαβάθμητη, να χρησιμοποιεί πληροφορίες που διατίθενται μόνο μέσω ευρέως δημοσιοποιημένων έντυπων και ηλεκτρονικού υλικού. Η αλήθεια όμως είναι, όπως έχω ήδη αναφέρει, ότι την περίοδο αυτή διαδραματίζονται σημαντικές διαδικασίες στο χώρο του κυβερνοπολέμου σε εθνικό επίπεδο.

Σελίδα σκόπιμα κενή

Βιβλιογραφία

Ελληνόγλωσση Βιβλιογραφία

Καζαντζόγλου Αβραάμ, Διπλωματική Εργασία του Τμήματος Διεθνών Σχέσεων του Πανεπιστημίου Μακεδονία, *Σύγχρονα τεχνολογικά μέσα και η έννοια της επίθεσης στο διεθνές δίκαιο. Ο Κυβερνοπόλεμος, υπό το πρίσμα του ΝΑΤΟ, της ΕΕ και των ελληνικών ενόπλων δυνάμεων του 21ου αιώνα.*

Καψοκόλη Ελένη, Διάλεξη, *ΝΑΤΟ και Κυβερνοάμυνα,* 6ο Συνέδριο Ελληνικής Υψηλής Στρατηγικής, ΛΑΕΔ, 27 Μαρτίου 2019.

Λέκκου Δάντου Ρένα, Sun Tzu, *The Art of War*, Αθήνα, Περίπλους, 2007.

Μαυρόπουλος Παναγιώτης, *Κυβερνοπόλεμος και Εθνική Στρατηγική*.

Μαυρόπουλος, Παναγιώτης, *Κυβερνοπόλεμος,* Διάλεξη ΣΕΘΑ, 25 Ιαν 17

Σίμου Φλώρα, Διπλωματική Εργασία του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, *Κυβερνοπόλεμος και επιθέσεις στο διαδίκτυο,* Οκτ 2016

Χατζηκωνσταντίνου Κώστας και Χαράλαμπος, Αποστολίδης και Μιλτιάδης, Σαρηγιάννης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο,* Αθήνα, Σάκκουλα, 2014.

Κατευθυντήριο Πλαίσιο Ανάπτυξης Κυβερνοάμυνας στις ΕΔ, ΓΕΕΘΑ/ΔΙΚΥΒ, Αυγ 2013.

Πολιτική Κυβερνοάμυνας στις ΕΔ, ΓΕΕΘΑ/ΔΙΚΥΒ, Φεβ 2014.

ΥΦΕΘΑ της Λιθουανίας, ομιλία, παρουσίαση στη ΣΕΘΑ, 13 Φεβ 2019

ΦΕΚ 199, ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4577, *Ενσωμάτωση στην ελληνική νομοθεσία της οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις*, 3 Δεκ 2018.

ΠαΔ 1-26/2019 περί *Διαχείρισης Ασφαλείας Πληροφοριακών Συστημάτων και Τοπικών Δικτύων Δεδομένων*

Ξενόγλωσση Βιβλιογραφία

Assange Julian and others, *Cypherpunks, Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των WikiLeaks,* Αθήνα, Ποιότητα, 2013.

Luke Timothy W, *Cyberspace as Meta Nation: The Net Effects of Online E Publicanism*, Alternatives: Global, Local, Political 26, 2001.

Randall Dipert, *The Ethics Of Cyberwarfare: Journal Of Military Ethics: Vol 9, No 4*, Journal of Military Ethics, 2016

Reich Pauline, *Cyber Warfare: A Review Of Theories, Law, Policies, Actual Incidents–And The Dilemma Of Anonymity,* European Journal of Law and Technology 1.2, 2010.

Ηλεκτρονικός Τύπος

Γιαννόπουλος Βασίλειος, «Κυβερνοπόλεμος. Υπαρκτή παγκόσμια ασύμμετρη απειλή», *Ελεύθερη Ζώνη,*3 Ιανουαρίου 2011, http://www.elzoni.gr/html/ent/321/ent.5321.asp, (έγινε πρόσβαση στις 6 Μαρ 2019)

Παπαδόπουλος Γιάννης, «Η μεγάλη διεθνής σύναξη των χάκερ», K*αθημερινή,* 20 Αυγούστου 2018, http://www.kathimerini.gr/980573/gallery/texnologia/diadiktyo/h-megalh-die8nhs-syna3h-twn-xaker, (έγινε πρόσβαση στις 3 Απρ 19)

Παρθενοπούλου Νίνα, «Ο ιός Stuxnet και το πυρηνικό πρόγραμμα του Ιράν», *Κέντρο Διεθνών Στρατηγικών Αναλύσεων,* https://kedisa.gr/o-ιός-stuxnet-και-το-πυρηνικό-πρόγραμμα-του-ι/, (έγινε πρόσβαση στις 14 Μαρ 2019)

Fayutkin Dan, «The American and Russian Approaches to Cyber Challenges», *Journal of Defence Management,* 2012, https://www.omicsonline.org/open-access/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (έγινε πρόσβαση στις 16 Μαρ 2019)

Hall Eleanor, «Former White House security advisor warns og cyber war», *The World today*,7 September 2010, http://www.abc.net.au/worldtoday/content/2010/s3086792.htm, (έγινε πρόσβαση στις 15 Μαρ 2019)

https://help.f-secure.com/product.html?home/internet-security/latest/el/concept_AD66CB676C2749B8A235B6D7E63BB4C2-internet-security-latest-el, (έγινε πρόσβαση στις 14 Μαρ 2019)

http://ebackspace.blogspot.com/2013/04/blog-post_9252.html, (έγινε πρόσβαση στις 14 Μαρ 2019)

https://www.ip.gr/el/dictionary/215-Spoofing, (έγινε πρόσβαση στις 14 Μαρ 2019)

https://www.pandasecurity.com/homeusers/downloads/docs/product/help/ap/2013/el/675.htm, (έγινε πρόσβαση στις 14 Μαρ 2019)

https://www.dhs.gov/topic/cybersecurity, (έγινε πρόσβαση στις 16 Μαρ 2019)

https://ccdcoe.org/about-us/, (έγινε πρόσβαση στις 28 Μαρ 2019)

https://www.nato.int/cps/en/natohq/topics_78170.htm, (έγινε πρόσβαση στις 28 Μαρ 2019)
https://www.nato.int/cps/en/natohq/news_163358.htm?selectedLocale=en, (έγινε πρόσβαση στις 28 Μαρ 2019)
http://www.geetha.mil.gr/el/briefing-el/press-el/6640-askhsh-«panopths-2018».html, (έγινε πρόσβαση στις 23 Μαρ 2019)
https://www.dogana-project.eu/, (έγινε πρόσβαση στις 22 Μαρ 2019)
https://www.certcoop.eu/, (έγινε πρόσβαση στις 22 Μαρ 2019)
https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, (έγινε πρόσβαση στις 22 Μαρ 2019)
https://www.consilium.europa.eu/media/32079/pesco-overview-of-first-collaborative-of-projects-for-press.pdf, (έγινε πρόσβαση στις 23 Μαρ 2019)
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, (έγινε πρόσβαση στις 23 Μαρ 2019)
http://rt.com/news/248073-islamic-state-hackers-french-tv/ (έγινε πρόσβαση στις 20 Οκτ 2019)
http://rt.com/usa/221927-central-command-hackedcybercaliphate/ (έγινε πρόσβαση στις 20 Οκτ 2019
https://en.wikipedia.org/wiki/Unit_8200, (έγινε πρόσβαση στις 3 Απρ 19)
https://el.wikipedia.org/wiki/Μπλέτσλεϊ_Παρκ, (έγινε πρόσβαση στις 3 Απρ 19)