ΑΔΙΑΒΑΘΜΗΤΟ

ΣΧΟΛΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

71η ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

ΚΑΝΟΝΙΚΗΣ ΦΟΙΤΗΣΗΣ

ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ

«Η ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΩΣ ΝΕΑ ΠΑΓΚΟΣΜΙΑ ΑΠΕΙΛΗ. ΟΙ ΕΥΡΩΠΑΙΚΕΣ ΑΠΑΝΤΗΣΕΙΣ»

ΑΠΟ ΤΟΝ

ΣΧΗ (ΔΒ) ΠΑΝΑΓΙΩΤΗ ΝΙΑΚΑΡΗ

ΑΠΡΙΛΙΟΣ 2019

ΑΔΙΑΒΑΘΜΗΤΟ

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΕΛΙΔΑ

ΣΕΛΙΔΑ

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματεύεται την κυβερνοεπίθεση ως μια νέα παγκόσμια απειλή και τις απαντήσεις της Ευρωπαϊκής Ένωσης (ΕΕ). Αρχικά, στο πρώτο κεφάλαιο γίνεται μία εισαγωγή στους όρους κυβερνοχώρος και κυβερνοεπίθεση, δίνονται οι αντίστοιχοι ορισμοί και αποσαφηνίζονται οι συγκεκριμένες έννοιες. Αναλύεται ακόμα η φύση του κυβερνοπολέμου, ως ένα αναπόσπαστο στοιχείο των υβριδικών επιχειρήσεων και ως μια ασύμμετρη απειλή, που στοχεύει τόσο στη συνολική ψυχολογική αποδυνάμωση των μελών της κοινωνίας στόχου όσο και στην οργανωτική αποσύνθεση του κράτους. Το κεφάλαιο καταλήγει με την περιγραφή των ειδών των κυβερνοεπιθέσεων και αναλύει τους παράγοντες που ευνοούν τη διεξαγωγή τους.

Το δεύτερο κεφάλαιο επικεντρώνεται αρχικά στη διερεύνηση των λόγων για τους οποίους μια κυβερνοεπίθεση δύναται να θεωρηθεί ως μια παγκόσμια απειλή. Στη συνέχεια, προσδιορίζονται οι κύριοι στόχοι των κυβερνοεπιθέσεων, δίνεται ο ορισμός των κρίσιμων υποδομών σύμφωνα με τις διατάξεις της ΕΕ και αναλύονται οι κατηγορίες αυτών. Το κεφάλαιο κλείνει με την παράθεση τεσσάρων ιστορικών περιστατικών κυβερνοπολέμου από το πρόσφατο παρελθόν, ώστε ο αναγνώστης ν' αντιληφθεί το μέγεθος της νέας αυτής απειλής και τις διαστάσεις των καταστροφικών της συνεπειών.

Στο τρίτο κεφάλαιο γίνεται μία σύντομη αναφορά στους υπεύθυνους ευρωπαϊκούς φορείς για την κυβερνοασφάλεια και ακολουθεί μια συνοπτική αναφορά στις στρατηγικές της ΕΕ για τη δημιουργία ενός ασφαλή κυβερνοχώρου. Στη συνέχεια, επιχειρείται η ανάλυση των σημαντικότερων πολιτικών πρωτοβουλιών και νομοθετικών ρυθμίσεων της ΕΕ στο τομέα της κυβερνοασφάλειας και το κεφάλαιο καταλήγει με τις τελευταίες εξελίξεις της χρηματοδότησης των ευρωπαϊκών φορέων και δαπανών για την υλοποίηση των στόχων της στρατηγικής.

Στο τέταρτο κεφάλαιο αναφέρονται αρχικά, οι δράσεις της ΕΕ για την ενίσχυση της αποτροπής των κυβερνοεπιθέσεων. Τονίζεται η σπουδαιότητα της εμβάθυνσης και ενίσχυσης της συνεργασίας μεταξύ της ΕΕ και του ΝΑΤΟ και εντοπίζονται οι νέες προκλήσεις για την ενίσχυση της ευρωπαϊκής αποτροπής στις κυβερνοεπιθέσεις. Ακολουθεί μία σύντομη περιγραφή στις προσπάθειες της ΕΕ για την ενίσχυση της κοινωνικής ανθεκτικότητας σε περιστατικά κυβερνοεπιθέσεων και δηλώνεται η αναγκαιότητα της ανάπτυξης των δεξιοτήτων και της εκπαίδευσης του ανθρώπινου δυναμικού καθώς και της ενημέρωσης και ευαισθητοποίησης του κοινού.

Τέλος, καταγράφονται συμπεράσματα που προέκυψαν από τη συγγραφή του παρόντος πονήματος και παρουσιάζονται ρεαλιστικές προτάσεις για την αντιμετώπιση των προκλήσεων της ΕΕ στο νομοθετικό πλαίσιο και την ενίσχυση της αποτροπής και της ανθεκτικότητας στις απειλές των κυβερνοεπιθέσεων.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Σχης (ΔΒ)
Παναγιώτης Νιάκαρης
του Νικολάου (ΑΜ:50187)
Σπουδαστής 71ης ΕΣ
Αθήνα, 23 Απρ 19

ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ

ΘΕΜΑ: «Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή. Οι ευρωπαϊκές απαντήσεις»

ΕΙΣΑΓΩΓΗ

«Στον κυβερνοχώρο οι άνθρωποι δρουν υπό το καθεστώς σχετικής ατιμωρησίας και από την προστασία της ανωνυμίας. Οι απειλές μπορούν, μεταξύ άλλων, να προέρχονται εξίσου από κράτη, εξτρεμιστικές ή τρομοκρατικές ομάδες, μεμονωμένους χάκερ (hacker) ή από οργανωμένους επαγγελματίες, οι οποίοι ασκούν την ισχύ τους δυσανάλογα περισσότερο από την ισχύ που θα μπορούσαν να ασκήσουν στον πραγματικό κόσμο, με την ίδια προσπάθεια και τα ίδια μέσα[1]».

Στο πέρασμα του χρόνου, τα μέσα και τα πεδία πραγματοποίησης μιας σύγκρουσης αλλάζουν όσο προοδεύουν οι επιστήμες και η τεχνολογία. Οι στόχοι όμως των συγκρούσεων παραμένουν ίδιοι και δεν είναι άλλοι από την καταστροφή του αντιπάλου. Η διαφορά σήμερα είναι ότι σε ελάχιστο χρονικό διάστημα, μόλις μέσα σε λίγες ώρες, είναι δυνατό να συντελεστούν καταστροφές, που να οδηγήσουν σε κατάρρευση μια ολόκληρη χώρα, ενώ άλλοτε θα απαιτούνταν μακροχρόνιες προσπάθειες με κόστος τις ανθρώπινες απώλειες.

Με την τεχνολογία να μας συνοδεύει σε κάθε μας βήμα σήμερα, τις ηλεκτρονικές συσκευές να αποτελούν προέκταση του εαυτού μας και την διαδικτυακή σύνδεση να αποτελεί το ψηφιακό μας «οξυγόνο», πλέον βρισκόμαστε ευάλωτοι σε νέες μορφές απειλών, τις κυβερνοεπιθέσεις, που λαμβάνουν χώρα σ' ένα νέο και χαοτικό «πεδίο μάχης», τον κυβερνοχώρο.

Παρά το γεγονός ότι οι κυβερνοεπιθέσεις αφορούν τον ψηφιακό και όχι τον υλικό κόσμο μπορούν να επιφέρουν πολυποίκιλες επιζήμιες επιδράσεις σε πρόσωπα,

[1] Claire Yorke, ''Cybersecurity and Society'', December 2010, Vol.66, No 12, p.19.

οργανισμούς, επιχειρήσεις, κοινότητες και κράτη. Η κυβερνοεπίθεση, ως αναπόσπαστο μέρος των ευρύτερων υβριδικών επιχειρήσεων , συνιστά μια ασύμμετρη απειλή, που στόχος της είναι να προκαλέσει τη διατάραξη της κανονικότητας, να σπείρει το φόβο και την αβεβαιότητα, να πλήξει τους δημοκρατικούς θεσμούς ακόμα και με παρεμβάσεις σε εκλογικές διαδικασίες, και κάποιες φορές να προκαλέσει, σε συνδυασμό με προπαγάνδα και παραπληροφόρηση, την κρατική παράλυση απειλώντας ακόμα και την εδαφική κυριαρχία ανεξάρτητων κρατών.

Τα εργαλεία και οι τακτικές που χρησιμοποιούν οι σύγχρονες αυτές ηλεκτρονικές «βόμβες», συχνά καθιστούν δυσχερή τον εντοπισμό του δράστη. Σ' έναν τέτοιο κόσμο γεμάτο απειλές, οι πολίτες νιώθουν όλο και πιο ανοχύρωτοι ενώ κράτη και διεθνείς οργανισμοί κινητοποιούνται για να αμυνθούν. Είναι προφανές ότι ανατέλλει μια νέα εποχή όπου, κράτη, πανεπιστήμια, κοινωνικοί, πολιτικοί και στρατιωτικοί φορείς βρίσκονται σε ετοιμότητα για ν' αντιμετωπίσουν τη νέα «αόρατη» παγκόσμια απειλή, την κυβερνοεπίθεση.[2]

ΣΚΟΠΟΣ

Σκοπός της παρούσης διατριβής είναι να διερευνηθούν οι απειλές που παρουσιάζονται σ' ένα όχι και τόσο διακριτό πεδίο επιχειρήσεων, όπως αυτό του Κυβερνοχώρου, μέσω της ολοένα αυξανόμενης διεξαγωγής κυβερνοεπιθέσεων από κρατικούς και μη κρατικούς δρώντες, να τεκμηριωθούν οι λόγοι για τους οποίους οι κυβερνοεπιθέσεις θεωρούνται ως παράγοντες που απειλούν την ελευθερία του ατόμου αλλά και την παγκόσμια ασφάλεια, και τέλος να αναλυθούν οι πολιτικές και στρατηγικές που έχουν υιοθετηθεί τα τελευταία χρόνια από την Ευρωπαϊκή Ένωση (ΕΕ) για την αποτελεσματική αντιμετώπιση των απειλών αυτών στο πλαίσιο προάσπισης των αρχών της δημοκρατίας, των ανθρωπίνων αξιών και των δικαιωμάτων που η Ευρώπη πρεσβεύει.

ΠΡΟΫΠΟΘΕΣΕΙΣ

Για τη σύνταξη της διατριβής τέθηκαν οι παρακάτω προϋποθέσεις:

- Το πρωτόκολλο επικοινωνίας TCP/IP[3] θα εξακολουθήσει να έχει δομή πλέγματος.

- Οι παρεχόμενες υπηρεσίες του διαδικτύου (Internet) θα εξακολουθούν να

[2]Σωτήρης Σιδέρης, ''Κυβερνοπόλεμος ο νέος παγκόσμιος εφιάλτης και ποια είναι η νέα δύναμη πυρός", διαθέσιμο στο διαδίκτυο: https://www.militaire.gr/.
[3] Όλοι οι υπολογιστές που είναι συνδεδεμένοι στα χιλιάδες μικρότερα δίκτυα του Internet τρέχουν το πρωτόκολλο TCP/IP κι έτσι μιλούν μια κοινή γλώσσα.

βασίζονται στο μοντέλο «client/server» (καταναλωτής/παραγωγός) και δεν θα διαφοροποιηθούν σημαντικά ως προς την αρχική φιλοσοφία ανάπτυξής τους.

- Η κακόβουλη χρήση του διαδικτύου από εθνικούς φορείς και μη κρατικούς δρώντες θα εξακολουθήσει να υφίσταται και μάλιστα με εντονότερους ρυθμούς καθιστώντας την προστασία των ανεξάρτητων δικτύων και των ψηφιακών συστημάτων - υποδομών όλο και δυσκολότερο επίτευγμα.

- Η ψηφιακή δικτύωση που έχει αναπτυχθεί, τόσο στις κρίσιμες υποδομές της σύγχρονης κοινωνίας, όσο και στις ένοπλες δυνάμεις των ευρωπαϊκών κρατών, θα συνεχίσει να αυξάνεται.

- Η ΕΕ θα συνεχίσει να υποστηρίζει το σχεδιασμό, την ανάπτυξη και την εφαρμογή της Κοινής Πολιτικής Άμυνας και Ασφάλειας (ΚΠΑΑ) και οι πολιτικές της πεποιθήσεις θα παραμείνουν πιστές στους δημοκρατικούς θεσμούς και ενάντια στις εθνικιστικές προκαταλήψεις

ΚΕΦΑΛΑΙΟ 1ο

ΚΥΒΕΡΝΟΧΩΡΟΣ ΚΑΙ ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

1. Η έννοια του κυβερνοχώρου

Ο όρος «κυβερνοχώρος», γνωστός στην αγγλική γλώσσα ως «cyberspace», χρησιμοποιείται για να περιγράψει εκείνο το πλασματικό-εικονικό περιβάλλον μέσα στο οποίο λαμβάνουν χώρα ηλεκτρονικές επικοινωνίες, όπως το διαδίκτυο και η ανταλλαγή ηλεκτρονικών μηνυμάτων[4]. Σύμφωνα δε με άλλον ορισμό αποτελεί ένα παγκόσμια διασυνδεδεμένο δίκτυο ψηφιακών πληροφοριών και επικοινωνιακών υποδομών[5]. Η λέξη έγινε δημοφιλής στη δεκαετία του 1990, όταν οι χρήσεις του διαδικτύου, της δικτύωσης και της ψηφιακής επικοινωνίας αυξανόταν δραματικά και ο όρος «κυβερνοχώρος» μπόρεσε να αντιπροσωπεύσει τις πολλές νέες ιδέες και φαινόμενα που εμφανίστηκαν.

Οι προσπάθειες προσδιορισμού της έννοιάς του ήταν κατά το παρελθόν και συνεχίζουν να είναι μέχρι και σήμερα αρκετές. Σύμφωνα λοιπόν με τον Erik M. Mudrinich και σχετική ανάλυσή του, κυβερνοχώρος είναι *«ένας επιχειρησιακός τομέας βρισκόμενος ταυτόχρονα σε λογικά αλλά και υλικά στρώματα, του οποίου η μοναδική αρχιτεκτονική διαμορφώνεται από τη χρήση της ηλεκτρονικής και του ηλεκτρομαγνητικού φάσματος, για να δημιουργήσει, αποθηκεύσει, τροποποιήσει, ανταλλάξει και εκμεταλλευτεί πληροφορίες μέσω διασυνδεδεμένων δικτύων, τα οποία τέμνουν απρόσκοπτα άλλους τομείς, όπως επίσης και γεωγραφικά και αναγνωρισμένα πολιτικά σύνορα»*[6].

Ο κυβερνοχώρος θεωρείται στις ημέρες μας ο πέμπτος τομέας των πολεμικών επιχειρήσεων μετά την ξηρά, τον αέρα, τη θάλασσα και το διάστημα, με τη διαφορά ότι είναι ο μόνος που έχει δημιουργηθεί εξ ολοκλήρου από τον άνθρωπο[7]. Το χαρακτηριστικό αυτό είναι κομβικό με την έννοια ότι επιτρέπει τη γρήγορη μετάλλαξη και ανάπτυξή του, δεδομένης της γεωμετρικής προόδου με την οποία εξελίσσεται η τεχνολογία[8]. Το γεγονός ότι προσφέρει ένα περιβάλλον που αποτελείται από πολλούς συμμετέχοντες με την ικανότητα να επηρεάζονται και να επηρεάζουν ο ένας τον άλλον, τον καθιστά κρίσιμο για την εθνική και την ασφάλεια[9].

---

[4] Gaul Allison, “Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare”, (2013) Syracuse J. Sci. & Tech. L. Rep. 51.
[5] Geiss Robin, “Cyber Warfare: Implications for Non-International Armed Conflicts” (2013) Int’l L. Stud. 627.
[6] Gervais Michael, “Cyber Attacks and the Laws of War”, (2012) Berkeley J. Int'l Law 525.
[7] Grosswald Levi, “Cyberattack Attribution Matters Under Article 51 of the U.N. Charter”, (2011) 36 Brook. J. Int’l L. 1151.
[8] Halberstam Manny, “Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks”, (2013) 46 Geo. Wash. Int’l L. Rev. 199.
[9] Handler Gosnell Stephanie, “The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare”, (2012) 48 Stan. J. Int'l L. 209.

Η τεράστια σημασία του αποτυπώνεται με τον πλέον ξεκάθαρο τρόπο, όταν διαπιστώνεται πως σε περίπτωση απενεργοποίησης - διακοπής των δυνατοτήτων του, η μετάπτωση από μια ψηφιακή σε μια «σκοτεινή εποχή» θα ήταν απλά θέμα χρόνου[10].

2. **Κυβερνοπόλεμος και Κυβερνοτρομοκρατία**

Ο κυβερνοπόλεμος, γνωστός στην διεθνή ορολογία ως «cyber warfare», είναι μια μορφή επιχειρήσεων του ευρύτερου Πληροφοριακού Πολέμου που αναλαμβάνεται στον κυβερνοχώρο όχι μόνο από κράτη αλλά και από μη κρατικούς δρώντες με σκοπό να διακόψει, να αλλοιώσει, υποκλέψει και να καταστρέψει πληροφορίες ευρισκόμενες σε υπολογιστές ή υπολογιστικά δίκτυα[11]. Ακριβώς σε αυτού του είδους τις επιχειρήσεις έχει αποδοθεί ο όρος «επιθέσεις υπολογιστικών δικτύων» (Computer Network Attacks - CNA)[12].

Το είδος αυτό του «πολέμου» παρουσιάζει σαφείς διαφορές από τον παραδοσιακό πόλεμο καθώς δεν προσδιορίζεται γεωγραφικά, απαιτεί ελάχιστο κόστος και διεξάγεται ταχύτατα.[13] Χρησιμοποιεί τεχνικές υπεράσπισης (κυβερνοάμυνα) και επίθεσης (κυβερνοεπίθεση) πληροφοριών και δικτύων υπολογιστών που υπάρχουν στον κυβερνοχώρο, συχνά μέσω μιας παρατεταμένης εκστρατείας στον κυβερνοχώρο ή μιας σειράς σχετικών εκστρατειών.

Από την άλλη, η κυβερνοτρομοκρατία είναι η χρήση δικτύων ηλεκτρονικών υπολογιστών για τον τερματισμό κρίσιμων εθνικών υποδομών (όπως η ενέργεια, οι μεταφορές, οι κυβερνητικές επιχειρήσεις) ή για τον εξαναγκασμό ή τον εκφοβισμό κυβερνήσεων ή πολιτών[14]. Αυτό σημαίνει ότι το τελικό αποτέλεσμα τόσο του κυβερνοπολέμου όσο και της κυβερνοτρομοκρατίας είναι το ίδιο, να καταστρέψει τις κρίσιμες υποδομές και τα συστήματα ηλεκτρονικών υπολογιστών που συνδέονται μεταξύ τους μέσα στα όρια του κυβερνοχώρου.

3. **Η φύση και τα χαρακτηριστικά του Κυβερνοπολέμου – Πόλεμος ή Ειρήνη;**

Ο κυβερνοπόλεμος είναι μια εκτεταμένη κατάσταση δικτυακών συγκρούσεων με αντιπάλους οι οποίοι είναι διατεθειμένοι να εξουθενώσουν ο ένας τον άλλο, ακριβώς όπως και στην περίπτωση του πραγματικού πολέμου. Αποτελεί μια μορφή

[10] Augustine P. Zachary, «Cyber Neutrality: A Textual Analysis of Traditional Jus in. Bello Neutrality Rules through a Purpose - Based Lens», (2014) 71 A.F.L. Rev. 69

[11] Hoisington Matthew, «Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense», (2009) 32 B.C. Int'l & Comp. L. Rev. 439.

[12] International Law Association Study Group on the Conduct of Hostilities in the 21st Century, 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 93 Int'l L. Stud. 322.

[13] Ιωάννη Σακκά, «Ο Κυβερνοπόλεμος», 04 Οκτ 2018, διαδικτυακή πηγή: https://www.ilioupoligiaolous.gr/article.php?id=22426.

[14] Kim, A., Wampler, B., Goppert, J., Hwang, I., & Aldridge, H. (2012). Cyber-attack vulnerabilities analysis for unmanned aerial vehicles. In Infotech Aerospace 2012 (p. 2438).

επιχειρήσεων που δεν επηρεάζεται από αυτή την κανονικότητα που μέχρι σήμερα προσδιοριζόταν με ακρίβεια και ήταν ευρέως γνωστή με τη λέξη «ειρήνη».

Διεξάγεται χωρίς να επηρεάζεται από αποστάσεις σε όλα τα πλάτη και μήκη του πλανήτη μας και θέτει νέα ζητήματα νομιμότητας και ηθικής. Δεν έχει καθορισμένο πεδίο μάχης και μετακινείται συνεχώς για να αποφύγει την ανίχνευση και να στοχεύσει τον αντίπαλο στις ευπάθειές του[15].

Οι στόχοι επιλέγονται όχι τόσο για τη φυσική καταστροφή, αλλά περισσότερο για την ψυχική και ηθική επίπτωση στον αντίπαλο. Προκαλείται με αυτόν τον τρόπο μια κατάσταση παράλυσης των συνεκτικών δομών της κοινωνίας – κράτους, και ο «πόλεμος» κερδίζεται χωρίς να απαιτείται η παρουσία αεροπλανοφόρων, σύγχρονων αρμάτων και γενικά συμβατικών όπλων της τελευταίας τεχνολογικής αιχμής.

Δικαίως λοιπόν, ο κυβερνοπόλεμος έχει χαρακτηριστεί ως ένας βασικός πυλώνας του «υβριδικού πολέμου», ως μια μορφή «ασύμμετρης απειλής» που στοχεύει τόσο στη συνολική ψυχολογική αποδυνάμωση των μελών της κοινωνίας όσο και στην οργανωτική αποσύνθεση του κράτους.

Το γεγονός ότι στην περίπτωση των κυβερνοεπιθέσεων δε χρειάζεται να περάσει κανείς τα σύνορα για να επιτεθεί, και τα κυβερνοόπλα μπορούν να κάνουν ακαριαία προβολή ισχύος σε παγκόσμια κλίμακα χωρίς να χρειάζονται βάσεις σε εδάφη συμμάχων[16], τείνει να θολώσει τις γραμμές μεταξύ του πολέμου και της πολιτικής, των συγκρούσεων και της ειρήνης. Απειλεί θα λέγαμε να ταυτίσει την ειρήνη με τον πόλεμο ενισχύοντας και εγκαθιστώντας μια νέα ζώνη μεταξύ αυτών των δύο. Έτσι, διαμορφώνεται μια «γκρίζα ζώνη», όπου μέσα σε αυτήν δεν βασιλεύει ούτε η «ειρήνη» ούτε ο παραδοσιακός «συμβατικός» πόλεμος. Αντιθέτως, κυριαρχεί ένας αόρατος και διακριτικός πόλεμος, ο σύγχρονος πόλεμος του 21ου αιώνα, γνωστός ως κυβερνοπόλεμος.

Σε αυτό το νέο περιβάλλον προκλήσεων ή κατά πολλούς «πεδίο μάχης», η ασφάλεια και η προστασία τόσο των πολιτών όσο και των κρατών προϋποθέτει τη δημιουργία μιας ισχυρής **κυβερνοασφάλειας**, η οποία περιλαμβάνει όλες τις ασφαλιστικές δικλείδες και τις δράσεις που μπορούν να χρησιμοποιηθούν για τη προστασία του κυβερνοχώρου, τόσο στο στρατιωτικό όσο και στο μη στρατιωτικό πεδίο από εκείνες τις απειλές που μπορούν να βλάψουν τα ανεξάρτητα δίκτυα και τις υποδομές πληροφόρησης[17].

---

[15] Williamson, C.S.C From fourth generation warfare to Hybrid war, Strategy research project, Carlisle Barracks, US Army College.
[16] Ανδρέας Λιαρόπουλος, Κυβερνοπόλεμος: «Το νέο στρατηγικό όπλο», διαθέσιμο στο διαδίκτυο: https://www.onalert.gr/uncategorized/kubernopolemos-to-neo-strathgiko-oplo/128648.
[17] Μαριλένα Κοππά, «Η Κοινή Πολιτική Άμυνας και Ασφάλειας – Η Ιστορία, οι θεσμοί, οι στρατηγικές», Εκδόσεις Πατάκη, Ιούνιος 2017, σελ. 193.

4. Η έννοια της Κυβερνοεπίθεσης

Μία κυβερνοεπίθεση είναι οποιοσδήποτε τύπος προσβλητικού ελιγμού που στοχεύει συστήματα πληροφορικής, υποδομές, δίκτυα υπολογιστών ή συσκευές προσωπικών υπολογιστών. Ο εισβολέας είναι ένα πρόσωπο ή μια διαδικασία που προσπαθεί να αποκτήσει πρόσβαση σε δεδομένα, λειτουργίες ή σε άλλες απαγορευμένες περιοχές του συστήματος χωρίς εξουσιοδότηση, ενδεχομένως με κακόβουλη πρόθεση[18]. Ανάλογα με το πλαίσιο, οι κυβερνοεπιθέσεις μπορούν να αποτελούν μέρος του κυβερνοπολέμου ή της κυβερνοτρομοκρατίας ενώ μπορούν να χρησιμοποιηθούν από έθνη-κράτη, άτομα, ομάδες, κοινωνίες ή οργανώσεις.

5. Τα είδη των κυβερνοεπιθέσεων και το κυβερνοέγκλημα

Πρέπει να σημειωθεί ότι έχουν επιχειρηθεί ως σήμερα πολλές κατηγοριοποιήσεις των κυβερνοεπιθέσεων, άλλες αναλυτικότερες και άλλες πιο συγκεντρωτικές, η καθεμιά με τα δικά της κριτήρια και στόχους, και ως εκ τούτου δεν είναι δυνατή η λεπτομερής απαρίθμησή τους.

Προσπαθώντας να καταλήξουμε σε μια ευρύτερη ταξινόμηση των κυβερνοεπιθέσεων, κυρίως με κριτήριο το σκοπό για τον οποίο διεξάγονται αυτές, ως πρώτη κατηγορία διακρίνουμε τις κυβερνοεπιθέσεις για **υποκλοπή** πληροφοριών. Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας ήταν η κυβερνοεπίθεση που συνέβη για την υποκλοπή των κωδικών χιλιάδων λογαριασμών ηλεκτρονικού ταχυδρομείου της εταιρείας Google τον Ιούνιο του 2011, κάποιοι από τους οποίους ανήκαν σε υψηλόβαθμα στελέχη της κυβέρνησης των ΗΠΑ, σε Κινέζους ακτιβιστές και σε δημοσιογράφους. Υπεύθυνη θεωρήθηκε η Κίνα, όπως και τον Ιανουάριο του 2010 όταν και σημειώθηκαν ανάλογες παραβιάσεις[19].

Συνηθισμένη μορφή κυβερνοεπιθέσεων είναι επίσης **η κατανεμημένη άρνηση υπηρεσιών** (Distributed Denial of Service / DDoS). Πρόκειται για κυβερνοεπιθέσεις που αποσκοπούν στο να καταστήσουν μη διαθέσιμη μια πηγή ηλεκτρονικού υπολογιστικού συστήματος στους εξουσιοδοτημένους ή δυνητικούς χρήστες της διακόπτοντας την λειτουργία της[20].

Πραγματοποιείται συνήθως από περισσότερα του ενός άτομα με τη χρησιμοποίηση, μετά από εξασφάλιση του ελέγχου, πολλών ηλεκτρονικών υπολογιστών από διάφορα μέρη του πλανήτη και τη μαζική αποστολή δεδομένων με στόχο την παρεμπόδιση της αποτελεσματικής και φυσιολογικής λειτουργίας μιας

[18] Denning, P. J., & Denning, D. (2010). The Profession of IT, Discussing Cyber Attack.
[19] Sui-Lee Wee, Alexei Oreskovic, «Google reveals Gmail hacking, says likely from China» Reuters, διαθέσιμο στην Ιστοσελίδα: http://www.reuters.com/article/us-google-hacking-idUSTRE7506U320110602, 06 Μαρ 2019.
[20] Shaun Roberts, «Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors», (2014) 41 N. Ky. L. Rev. 535, p.541.

ιστοσελίδας, μιας υπηρεσίας κ.λπ. και την προσωρινή ή μη κατάρρευσή της[21]. Τέτοιας μορφής κυβερνοεπιθέσεις ήταν αυτές στην Εσθονία το 2007 και στη Γεωργία το 2008.

Οι κυβερνοεπιθέσεις της μορφής DDoS συνιστούν επί της ουσίας μια πιο ισχυρή κατηγορία κυβερνοεπιθέσεων συγκριτικά με τις **απλές επιθέσεις άρνησης υπηρεσιών** (Denial of Service / DoS), οι οποίες αποσκοπούν στο να αποκόψουν τους νόμιμους χρήστες συγκεκριμένων δικτύων ή Η/Υ από την πρόσβαση σε πληροφορίες ή υπηρεσίες και διενεργούνται από μεμονωμένους hackers ή επιτιθέμενους[22].

Επόμενη εξίσου σημαντική κατηγορία είναι οι **επιθέσεις ελέγχου συστήματος** (Control System Attacks), που αποσκοπούν κυρίως στο να εκθέσουν τα λειτουργικά συστήματα και να μετατρέψουν τα δεδομένα τους. Αυτού του είδους οι επιθέσεις χωρίζονται σε δύο κατηγορίες· τις **συντακτικές** (Syntactic Attacks) και τις **σημασιολογικές** (Semantic Attacks)[23].

Οι πρώτες χρησιμοποιούν συνήθως **κακόβουλο λογισμικό** (Viruses, Worms, Trojan Horses)[24] για να εκθέσουν τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών, ενώ οι δεύτερες δρουν **παραπλανητικά** και παρακολουθώντας το λογισμικό ενός συστήματος ή δικτύου μετατρέπουν τα αναπαραγόμενα δεδομένα την ίδια στιγμή που φαίνεται πως η συνολική τους λειτουργία συνεχίζεται απρόσκοπτη.

Κλασικό παράδειγμα «Semantic Attack» ήταν ο ιός «Stuxnet» που δημιουργήθηκε το 2008 με την συνεργασία των ΗΠΑ-Ισραήλ (CIA-Mossad) με στόχο να στερήσουν από το Ιράν την δυνατότητα εξέλιξης του πυρηνικού του προγράμματος. Τα δύο αυτά είδη κυβερνοεπιθέσεων συναντά κανείς και με το χαρακτηρισμό **«επιθέσεις εισχώρησης»** (Penetration Attacks)[25], όρος με τον οποίο τονίζεται η δυνατότητα εισβολής στο σύστημα είτε μέσω τοπικής πρόσβασης είτε απομακρυσμένα μέσω ενός ασύρματου δικτύου.

Αξίζει να αναφέρουμε ότι κυβερνοεπίθεση και κυβερνοέγκλημα (cyber crime) είναι κατά βάση δύο διαφορετικές έννοιες αν και θεωρείται ότι υπό προϋποθέσεις και σε συγκεκριμένες περιπτώσεις αλληλεπικαλύπτονται[26].

Κυβερνοέγκλημα σε μια προσπάθεια γενικής προσέγγισης της έννοιας θεωρείται η χρήση μεθόδων βασισμένων σε ηλεκτρονικούς υπολογιστές και σχετικά δίκτυα, προκειμένου να διαπραχθεί μια παράνομη πράξη. Βασικά χαρακτηριστικά του

---

[21] Peter Z. Stockburger, «Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum» (2016) 31 Am. U. Int'l L. Rev. 545, p.554.

[22] Christopher D. DeLuca, «The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors», (2013) 3 No. 9 Pace Int'l L. Rev. Online Companion 278, p.282-283.

[23] Peter Z. Stockburger, «Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum» (2016) 31 Am. U. Int'l L. Rev. 545, p.558-560.

[24] Christopher D. DeLuca, «The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors», (2013) 3 No. 9 Pace Int'l L. Rev. Online Companion 278, p.284-286.

[25] Reese Nguyen, «Navigating Jus Ad Bellum in the Age of Cyber Warfare» (2013) 101 Cal. L. Rev. 1079, p. 1093-1095.

[26] Oona A. Hathaway, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, «The Law of Cyber-Attack» (2012) 100 Calif. L. Rev.817, p. 836.

είναι ότι διαπράττεται από ιδιώτες και όχι από κράτη, ότι ως επί το πλείστον οι δράστες του δεν έχουν πολιτικούς σκοπούς και δεν επιδιώκουν να πλήξουν την εθνική ασφάλεια ενός κράτους. Τέλος, η διαπραχθείσα ενέργεια ποινικοποιείται με βάση το εσωτερικό/εθνικό; ή το διεθνές δίκαιο[27].

6. Μέσα εκδήλωσης Κυβερνοεπιθέσεων

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 (Cyber weapons) και είναι:

α. Υπολογιστής

Ο υπολογιστής αποτελεί σήμερα το βασικό εργαλείο με το οποίο σχεδιάζονται και από το οποίο εκδηλώνονται οι κυβερνοεπιθέσεις. Στο πλαίσιο αυτό του ρόλου του, ο υπολογιστής μπορεί να χαρακτηριστεί ως όπλο διεξαγωγής κυβερνοπολέμου (κυβερνοόπλο). Μία συνηθισμένη περίπτωση χρήσης του υπολογιστή σήμερα είναι αυτή στην οποία ο έλεγχός του έχει αναληφθεί από άγνωστο άτομο με την εγκατάσταση κατάλληλου λογισμικού, έτσι ώστε να χρησιμοποιηθεί για την εκτόξευση επιθέσεων τύπου DDoS, εν αγνοία του χειριστή του, για λόγους απόκρυψης της ταυτότητας του δράστη. Στην ορολογία του κυβερνοπολέμου ένας τέτοιος υπολογιστής ονομάζεται **zombie ή bot**[28].

β. 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 σε έναν υπολογιστή ή πρόγραμμα, χωρίς να το γνωρίζει ο ιδιοκτήτης του. Στο Παράρτημα «Β» απεικονίζεται η εκθετική αύξηση των κακόβουλων λογισμικών. Ο χαρακτηρισμός «κακόβουλο» αναφέρεται στην πρόθεση του δημιουργού του λογισμικού.

7. Τα όπλα που χρησιμοποιούνται στον κυβερνοχώρο

Τα συνηθέστερα «όπλα» για την πραγματοποίηση μιας επίθεσης μέσω του κυβερνοχώρου, τα οποία μπορούν να χρησιμοποιηθούν είτε μεμονωμένα, είτε και

[27] Oona A. Hathaway, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, «The Law of Cyber-Attack» (2012) 100 Calif. L. Rev.817, p. 833-835.
[28] Υπτγου ε.α Παναγιώτη Μαυρόπουλου, «Κυβερνοπόλεμος και Εθνική Στρατηγική», σελ. 6, διαθέσιμο στην ιστοσελίδα: http://www.geetha.mil.gr/media/1.vima-ell-strat-skepsis/kuvernopolemos.pdf.

συνδυαστικά μεταξύ τους για να επιφέρουν εκτεταμένες δυσλειτουργίες ή και την πλήρη απενεργοποίηση του στόχου, είναι τα παρακάτω:

α. **Ιός (Virus)**

Κακόβουλο λογισμικό το οποίο έχει τη δυνατότητα να εξαπλώνεται εύκολα σε χρήσιμα προγράμματα ενός ξένου υπολογιστή με αποτέλεσμα να βλάψει χρήσιμα αρχεία ενός χρήστη. Ο ιός μπορεί να κρυφτεί σε απίθανες τοποθεσίες στη μνήμη ενός συστήματος υπολογιστών και να συνδεθεί σε οποιοδήποτε αρχείο θεωρεί κατάλληλο για να εκτελέσει τον κώδικα του. Μπορεί επίσης να αλλάξει το ψηφιακό αποτύπωμα κάθε φορά που αναπαράγεται καθιστώντας πιο δύσκολο τον εντοπισμό στον υπολογιστή[29].

β. **«Σκουλήκι» (Worm)**

«Κυκλοφορεί» σε κάποιο δίκτυο και μολύνει άλλους υπολογιστές και συστήματα που είναι συνδεμένα σε αυτό. Σε πολύ μεγαλύτερη κλίμακα, τα σκουλήκια μπορούν να σχεδιαστούν για βιομηχανική κατασκοπία για να παρακολουθούν και να συλλέγουν δραστηριότητες διακομιστή και κυκλοφορίας και στη συνέχεια να τις μεταδίδουν πίσω στον δημιουργό τους[30].

γ. **Δούρειος Ίππος (Trojan)**

Ένας «Δούρειος ίππος» έχει σχεδιαστεί για να εκτελεί νόμιμες εργασίες αλλά επίσης εκτελεί άγνωστη και ανεπιθύμητη δραστηριότητα. Μεταμφιέζεται ως κανονικό και ασφαλές λογισμικό που έχει την ικανότητα να μολύνει τη συσκευή. Μπορεί να επιτεθεί σε ένα σύστημα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, προγραμμάτων περιήγησης ιστού, και απομακρυσμένου λογισμικού και ενημερώσεων[31].

δ. **Rootkit**

Ο όρος “rootkit” αποτελεί μια δυνατότητα που επιτυγχάνει την μεγαλύτερη πρόσβαση στο σύστημα. Τα rootkits τροποποιούν και παρεμποδίζουν τις τυπικές λειτουργίες του λογισμικού, μολύνουν την «καρδιά» του λειτουργικού συστήματος και είναι 100% αόρατα στο χρήστη[32].

8. Δρώντες των κυβερνοεπιθέσεων – Είδη εισβολέων

Οι δράστες, οι οποίοι επιδίδονται σε παράνομες δραστηριότητες στον κυβερνο-

[29] Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control, 58(11), p. 2715-2729.
[30] Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2014, July). A cyber-attack evaluation methodology. In Proc. of the 13th European Conference on Cyber Warfare and Security, p. 264-270.
[31] Raiyn, J. (2014). A survey of cyber-attack detection strategies. International Journal of Security and Its Applications, 8(1), p. 247-256.
[32] PC Security, «Τι είναι το κακόβουλο λογισμικό», 4 Φεβ 19, διαθέσιμο στο: https://pcsecurity.gr/kakovoulo-logismiko-malware.

χώρο, ομαδοποιούνται γενικώς σε κατηγορίες, κυρίως με βάση το σκοπό για τον οποίο δραστηριοποιούνται. Το Παράρτημα «Δ» απεικονίζει τα κυριότερα κίνητρα των ατόμων που διεξάγουν κυβερνοεπιθέσεις.

Η διεξαγωγή των κυβερνοεπιθέσεων δύναται να λάβει χώρα ανάμεσα σε διάφορους συνδυασμούς δρώντων της διεθνούς σκηνής. Μπορεί να προκύψει μεταξύ των επίσημων αρχών αντίπαλων κρατών. Να εμφανιστεί μεταξύ ενός κυρίαρχου κράτους και ενός μη κρατικού δρώντος, που χρηματοδοτείται ωστόσο από άλλο κυρίαρχο κράτος. Επίσης, να χρησιμοποιηθεί ενάντια στις πολιτικές μιας συγκεκριμένης κυβέρνησης από μεμονωμένες ομάδες που υποστηρίζουν για παράδειγμα, το περιβάλλον, τα ανθρώπινα δικαιώματα ή άλλα ζητήματα θρησκευτικού ή πολιτιστικού χαρακτήρα.

Οι κυβερνοεπιθέσεις θεωρούνται επίσης μια ιδιαίτερη ελκυστική πρακτική για τις τρομοκρατικές ομάδες, κυρίως εξαιτίας της δυνατότητας που προσφέρουν για ανώνυμη, χωρίς υψηλό κόστος και απομακρυσμένη δράση, ικανή να πλήξει ποικίλους στόχους και να επηρεάσει άμεσα την καθημερινότητα μεγάλου αριθμού ατόμων[33].

Οι κύριες κατηγορίες των οργάνων διεξαγωγής των κυβερνοεπιθέσεων, γνωστών στη διεθνή βιβλιογραφία ως «εισβολέων» στα ψηφιακά συστήματα και δίκτυα, ανάλογα με τα κίνητρα, τις ικανότητές τους καθώς και τον επιδιωκόμενο σκοπό της κυβερνοεπίθεσης, κατατάσσονται στις παρακάτω κατηγορίες:

α. **Οι επαγγελματίες χάκερς (hackers)**

Πρόκειται για άτομα που είτε εργάζονται μόνοι τους είτε απασχολούνται από την κυβέρνηση ή τη στρατιωτική υπηρεσία και μπορούν να βρουν συστήματα υπολογιστών με τρωτά σημεία που δεν διαθέτουν το κατάλληλο λογισμικό ασφαλείας. Μόλις εντοπιστούν αυτά τα τρωτά σημεία, μπορούν να μολύνουν τα συστήματα με κακόβουλο κώδικα και στη συνέχεια να ελέγχουν εξ αποστάσεως το σύστημα ή τον υπολογιστή στέλνοντας εντολές για προβολή περιεχομένου ή διακοπή άλλων υπολογιστών. Πολλοί από αυτούς επεμβαίνουν παράνομα σε υπολογιστές επειδή απλά αντιμετωπίζουν τη διαδικασία της προσβολής της ασφάλειας υπολογιστών και δικτύων σαν πρόκληση και επιβεβαίωση των ικανοτήτων τους στον τομέα του προγραμματισμού των υπολογιστών.

β. **Κατάσκοποι (Spies)**

Στην κατηγορία αυτή ανήκουν άτομα που επιδιώκουν την παράνομη απόκτηση πληροφοριών με απώτερο στόχο το πολιτικό όφελος.

γ. **Τρομοκράτες (Terrorists)**

Πολλοί επαγγελματίες χάκερς προωθούνται στους κυβερνοτρομοκράτες, όπου ένα νέο σύνολο κανόνων ρυθμίζει τις ενέργειές τους. Οι κυβερνοτρομοκράτες

[33] Ahmad Kamal, UN Report: Law of Cyber Space, Council of Foreign Relations, 2015, p.67-68.

έχουν προμελετημένα σχέδια και οι επιθέσεις τους δεν γεννιούνται από οργή. Πρέπει να αναπτύξουν βήμα-βήμα τα σχέδιά τους και να αποκτήσουν το κατάλληλο λογισμικό για να πραγματοποιήσουν μια επίθεση. Οι τρομοκράτες του κυβερνοχώρου είναι χάκερς με πολιτικό κίνητρο και επιτίθενται σε άτομα ή περιουσίες. Επιφέρουν αρκετή ζημιά για να προκαλέσουν φόβο και πανικό[34].

δ. **Βιομηχανικοί κατάσκοποι (Corporate Raiders)**

Επιδιώκουν την απόκτηση πρόσβασης σε πληροφορίες και συστήματα ανταγωνιστικών εταιριών και επιχειρήσεων με σκοπό το οικονομικό όφελος εις βάρος τους.

ε. **Επαγγελματίες εγκληματίες (Professional Criminals)**

Στοχεύουν στην ικανοποίηση προσωπικών οικονομικών οφελών μέσω παράνομης απόκτησης πληροφοριών ή παραποίησής τους.

στ. **Βάνδαλοι (Vandals)**

Έχουν ως μόνο στόχο την πρόκληση ζημιάς με οποιοδήποτε τρόπο και χωρίς κάποιο συγκεκριμένο προσωπικό όφελος.

9. Παράγοντες που ευνοούν την διεξαγωγή κυβερνοεπιθέσεων

Τα στοιχεία που συνθέτουν τον ιδιαίτερο χαρακτήρα και φύση αυτού του νέου είδους συμπεριφοράς των κυβερνοεπιθέσεων, και όχι μόνο επιτρέπουν αλλά παράλληλα ευνοούν τη διεξαγωγή τους, συνοψίζονται ως εξής:

α. Λόγω της ανοιχτής αρχιτεκτονικής του διαδικτύου αλλά και των άλλων ψηφιακών δικτύων, που χρησιμοποιούν τα ίδια πρωτόκολλα επικοινωνίας[35], παρέχεται η δυνατότητα στον επιτιθέμενο να αποκρύψει την ταυτότητα και τις πραγματικές του προθέσεις. Για τους ίδιους λόγους δεν είναι άμεσα εφικτός ο εντοπισμός του τόπου προέλευσης της επίθεσης, ο οποίος άλλωστε ενδέχεται να απέχει γεωγραφικά κατά πολύ από τον στόχο.

β. Τα «όπλα» μέσω των οποίων διεξάγεται μια επίθεση στον κυβερνοχώρο κοστίζουν ελάχιστα, διατίθενται χωρίς ιδιαίτερους περιορισμούς σε κάθε ενδιαφερόμενο και ο χειρισμός τους επιτυγχάνεται σχετικά εύκολα από τον καθένα χωρίς να απαιτούνται εξειδικευμένες γνώσεις ή μακρά και επίπονη εκπαίδευση[36]. Αντιθέτως, ο οικονομικός απολογισμός των ζημιών που υπάρχει δυνατότητα να προκληθούν μπορεί να καταλήγει σε υπέρογκα χρηματικά ποσά.

---

[34] Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber-attack. Industrial Control Systems, p. 22.
[35] Mathew Sklerov, Solving the dilemma of state responses to cyberattacks: A justification for the use of active defences against states who neglect their duty to prevent, Military Law Review, Fall 2009, p. 5-6.
[36] Thompson Trevor, Terrorizing the technological neighborhood watch: The allienation and deterrence of the 'white hats' under the CFFA, Florida, Spring 2009, p. 04.

γ. Οι περισσότεροι στόχοι μιας τέτοιας επίθεσης, δηλαδή τα διάφορα ηλεκτρονικά συστήματα, λειτουργούν βάσει λογισμικού, που παράγεται μαζικά από επιχειρήσεις του ιδιωτικού τομέα και περιορίζεται επίσης για μαζική κατανάλωση. Κατά συνέπεια, τα συστήματα αυτά είναι εγγενώς ευάλωτα καθώς δεν δίνεται ιδιαίτερη έμφαση και προσοχή σε ζητήματα που αφορούν στην ασφάλειά τους και στην προστασία των συστημάτων από κυβερνοεπιθέσεις. Αυτό συμβαίνει διότι μια τέτοια πρόνοια καθίσταται οικονομικά ασύμφορη καθώς προϋποθέτει το σχεδιασμό εξειδικευμένων και πολύπλοκων προγραμμάτων επιφέροντας ανάλογη αύξηση στο κόστος παραγωγής και στη διάθεση του προϊόντος στην αγορά[37].

δ. Οι κυβερνοεπιθέσεις μπορούν να προκαλέσουν σημαντικές καταστροφές με μακροχρόνια δυσμενή αποτελέσματα στις υποδομές ενός κράτους ή ενός διεθνή οργανισμού χωρίς ο επιτιθέμενος να επιβαρύνεται από το κόστος των ανθρώπινων απωλειών, όπως συνήθως συμβαίνει κατά τη διεξαγωγή ενός συμβατικού πολέμου. Επομένως, η προσβολή υποδομών ζωτικής σημασίας άνευ κόστους και απωλειών για τον επιτιθέμενο, εκμηδενίζει την όποια διστακτικότητα των φορέων που διεξάγουν τις προσβολές υποδομών ζωτικής σημασίας και συγχρόνως αυξάνουν την επιθετική και καταστροφική δυναμική της συμπεριφοράς τους[38].

[37] Natasha Solce, The battlefield of Cyberspace: The inevitable new military branch, Albany Law Journal of Science and Technology, 2008, p. 08.
[38] Ahmad Kamal, UN Report: Law of Cyber Space, Council of Foreign Relations, 2015, p.67-69.

ΚΕΦΑΛΑΙΟ 2ο

ΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΩΣ ΑΠΕΙΛΗ ΓΙΑ ΤΗΝ ΠΑΓΚΟΣΜΙΑ ΑΣΦΑΛΕΙΑ – ΣΤΟΧΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΟΙ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ

«Εάν γνωρίζατε πόσα πολλά μπορούμε να μάθουμε για εσάς από τον υπολογιστή σας, δεν θα χρησιμοποιούσατε ποτέ ξανά το διαδίκτυο….μπορούμε να σπάσουμε σχεδόν κάθε κωδικό και να μπούμε στον τραπεζικό λογαριασμό σας. Μπορούμε να διαβάζουμε τα e-mail σας ή να στείλουμε e-mail από τον υπολογιστή σας στο αφεντικό σας τόσο στα αγγλικά όσο και στα κινέζικα[39].»

1. Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή

Η ασφάλεια στον κυβερνοχώρο είναι κρίσιμης σημασίας, τόσο για την ευημερία όσο και για την παγκόσμια ασφάλεια. Τα περιστατικά που αφορούν την ασφάλεια στον κυβερνοχώρο παρουσιάζουν διαφοροποιήσεις τόσο από την άποψη του προσώπου που ευθύνεται για το περιστατικό όσο και ως προς τον επιδιωκόμενο σκοπό.

Τόσο οι μη στρατιωτικές υποδομές όσο και η στρατιωτική ικανότητα βασίζονται σε ασφαλή ψηφιακά συστήματα. Αυτό αναγνωρίστηκε στο Ευρωπαϊκό Συμβούλιο του Ιουνίου 2017[40], καθώς και στη συνολική στρατηγική για την εξωτερική πολιτική και την πολιτική ασφαλείας. Οι κίνδυνοι αυξάνονται εκθετικά. Η αποκάλυψη ότι χάκερς θα μπορούσαν να θέσουν υπό τον έλεγχό τους τηλεπικοινωνιακούς δορυφόρους και να χρησιμοποιήσουν τις κεραίες τους για να εξαπολύσουν επιθέσεις μικροκυμάτων σε πλοία, αεροπλάνα, στρατιωτικές και άλλες εγκαταστάσεις δείχνει καταφανέστατα ότι, **«η απειλή δεν είναι πια θεωρητική»**.[41]

Καθώς οι οικονομίες εξαρτώνται ολοένα και περισσότερο από τις ψηφιακές τεχνολογίες, αυξάνεται αντιστοίχως και η έκθεσή τους στον σχετικό κίνδυνο. Ο οικονομικός αντίκτυπος της κυβερνοεγκληματικότητας πενταπλασιάστηκε μεταξύ του 2013 και του 2017[42],πλήττοντας κυβερνήσεις και επιχειρήσεις, ανεξαρτήτως μεγέθους. Ενδεικτική της τάσης αυτής είναι η πρόβλεψη για αύξηση των κυβερνοασφαλίστρων από 3 δισεκατομμύρια ευρώ το 2018 σε 8,9 δισεκατομμύρια ευρώ το 2020.

Η εγκληματική απειλή εντείνεται λόγω των ασαφών ορίων μεταξύ του εγκλήματος στον κυβερνοχώρο και του «παραδοσιακού» εγκλήματος, δεδομένου ότι οι

---

[39] Michael Sheridan, ‘‘China’s Net Warriors Take on West’’, Sunday Times, 01 September 2001, p. 24.

[40] Συμπεράσματα του Ευρωπαϊκού Συμβουλίου, διαθέσιμο στο διαδίκτυο: https://www.consilium.europa.eu/media/23968/22-23-euco-final-conclusions-el.pdf, 23 Μαρ. 2017.

[41] Αρθρο της Εφημερίδας Καθημερινή, Τα νέα «όπλα» στα χέρια των χάκερ, 13 Αυγούστου 2018, διαθέσιμο στο διαδίκτυο: http://www.kathimerini.gr/979742/article/texnologia/diadiktyo/ta-nea-opla-sta-xeria-twn-xaker.

[42] Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου, «Η Επιτροπή αναβαθμίζει την απόκριση της ΕΕ στις κυβερνοεπιθέσεις», 19 Σεπτεμβρίου 2019, διαθέσιμο στο διαδίκτυο: http://europa.eu/rapid/press-release_IP-17-3193_el.htm.

δράστες χρησιμοποιούν το διαδίκτυο τόσο ως μέσο για την επέκταση των δραστηριοτήτων τους όσο και ως πηγή για την εξεύρεση νέων μεθόδων και εργαλείων τέλεσης εγκλημάτων[43]. Ωστόσο, στη συντριπτική πλειονότητα των περιπτώσεων, οι πιθανότητες εντοπισμού των εγκληματιών είναι ελάχιστες και οι πιθανότητες δίωξης ακόμη λιγότερες.

Ταυτόχρονα, κρατικοί παράγοντες επιτυγχάνουν όλο και περισσότερο τους γεωπολιτικούς τους στόχους κάνοντας χρήση όχι μόνο παραδοσιακών εργαλείων, όπως οι στρατιωτικές δυνάμεις, αλλά και περισσότερο διακριτικών εργαλείων του κυβερνοχώρου, μεταξύ άλλων παρεμβαίνοντας σε εσωτερικές υποθέσεις κυρίαρχων κρατών και προκαλώντας την αποσάθρωση των δομών τους. Το πρόσφατο παράδειγμα της επέμβασης της Ρωσίας στην Κριμαία με την χρησιμοποίηση υβριδικών επιχειρήσεων, στις οποίες ο κυβερνοπόλεμος είχε πρωταγωνιστικό ρόλο, δεν αφήνει καμιά αμφιβολία ότι η απειλή εξαπλώνεται και στα θεμέλια της εθνικής κυριαρχίας ανεξάρτητων κρατών ανά την υφήλιο.

Η χρήση του κυβερνοχώρου ως πεδίου πολεμικών επιχειρήσεων, είτε αυτόνομα είτε στο πλαίσιο υβριδικής προσέγγισης, αναγνωρίζεται πλέον ευρέως. Τα φαινόμενα των εκστρατειών παραπληροφόρησης, των ψευδών ειδήσεων και των δραστηριοτήτων στον κυβερνοχώρο που έχουν ως στόχο υποδομές ζωτικής σημασίας αυξάνονται συνεχώς και πρέπει να αντιμετωπιστούν.

Μία πιθανή κυβερνοεπίθεση σε ψηφιακούς κόμβους που ελέγχουν τα ηλεκτρικά δίκτυα, τα δίκτυα μεταφορών, τα εργοστάσια, τις οικονομικές συναλλαγές, τα νοσοκομεία και τα σπίτια θα μπορούσε να έχει καταστροφικές συνέπειες στον κοινωνικό ιστό. Η παραβίαση των ανθρωπίνων δικαιωμάτων και των προσωπικών δεδομένων προκαλούν αισθήματα ανασφάλειας, φόβου και σε ορισμένες περιπτώσεις ακόμα και πανικού που μπορεί να προκαλέσει τις απώλειες ανθρώπων.

Δύο ερευνητές έκαναν επίδειξη πώς είναι δυνατό να απενεργοποιηθεί από μακριά μια εμφυτευμένη αντλία ινσουλίνης για διαβητικούς και πώς είναι εξίσου εφικτό να παραβιασθεί πλήρως ένας βηματοδότης καρδιάς, με συνέπεια να εισαχθεί σε αυτόν κακόβουλο λογισμικό, το οποίο πλέον θα περιέχει εντολές δυνητικά θανατηφόρες για τον καρδιοπαθή[44].

Ο κίνδυνος επιθέσεων με πολιτικά κίνητρα σε στρατιωτικούς στόχους εξακολουθεί να ταλανίζει τις στρατιωτικές και πολιτικές ηγεσίες. Για παράδειγμα, η ανάληψη του ελέγχου του λογισμικού πτήσεως ενός Τηλεκατευθυνόμενου Μη Επανδρωμένου Εναέριου Συστήματος (Remotely Piloted Aircraft System – RPAS) από

[43] Europol's Serious and Organised Crime Threat Assessment 2017, διαθέσιμο στο διαδίκτυο: https://www.europol.europa.eu/-activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.
[44] Αρθρο της Εφημερίδας Καθημερινή, Τα νέα «όπλα» στα χέρια των χάκερ, 13 Αυγούστου 2018, διαθέσιμο στο διαδίκτυο: http://www.kathimerini.gr/979742/article/texnologia/diadiktyo/ta-nea-opla-sta-xeria-twn-xaker.

έναν κυβερνοτρομοκράτη, θα μπορούσε εύκολα να προκαλέσει εφιαλτικές συνέπειες στα θεμέλια της άμυνας μιας χώρας με κίνδυνο ακόμη και τις ανθρώπινες απώλειες[45].

2. <u>Στόχοι των κυβερνοεπιθέσεων οι κρίσιμες υποδομές</u>

Εκτός από την απειλή προς τις πληροφορίες, δηλαδή τα «χασκαρίσματα», την υποκλοπή στοιχείων, τις παρακολουθήσεις και τα αμιγώς «ψηφιακά», υπάρχει το φλέγον ζήτημα της κυβερνοαπειλής προς τις κρίσιμες υποδομές. Στο παράδειγμα «Γ» απεικονίζονται, οι επιθέσεις που έλαβαν χώρα κατά των κρίσιμων επιδομών καθώς και τα καταστροφικά αποτελέσματά τους.

Κατά το παρελθόν, τα στοιχεία που συνέθεταν τις βασικές υποδομές ενός κράτους, αποτελούσαν μόνιμους στρατιωτικούς στόχους, διότι η καταστροφή τους μπορούσε εύκολα να οδηγήσει στην αποδυνάμωση του αντίπαλου κράτους και στην σχεδόν βέβαιη επικράτηση στο πεδίο της μάχης[46].

Στις ανεπτυγμένες κοινωνίες του σύγχρονου δυτικού κόσμου, οι ίδιες αυτές υποδομές, από τις οποίες εξαρτάται η οικονομική σταθερότητα, η κοινωνική συνοχή και η εθνική ασφάλεια ενός κράτους, δεν χρειάζεται πλέον να προσβληθούν με το παραδοσιακό οπλοστάσιο του συμβατικού πολέμου, ώστε να επιτευχθεί η «παράλυση» ενός κράτους, διότι οι περισσότερες, αν όχι όλες, είναι πλέον άμεσα εξαρτημένες από την ομαλή λειτουργία ηλεκτρονικών συστημάτων και ψηφιακών δικτύων. Επομένως, συνδέονται με το πεδίο του κυβερνοχώρου και μπορούν εύκολα να πληγούν με τη μεθόδευση μιας κυβερνοεπίθεσης σ' αυτό το πεδίο μάχης.

Τι θεωρούμε και ορίζουμε όμως ως κρίσιμες υποδομές;

Σύμφωνα με την Ευρωπαϊκή Επιτροπή οι κρίσιμες υποδομές διακρίνονται στις υποδομές «ζωτικής σημασίας» και στις «ευρωπαϊκές υποδομές ζωτικής σημασίας». Συγκεκριμένα:

α. «Υποδομές ζωτικής σημασίας» νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για **ένα κράτος μέλος**, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών.

β. «Ευρωπαϊκές υποδομές ζωτικής σημασίας» νοούνται οι υποδομές ζωτικής σημασίας που βρίσκονται εντός των κρατών μελών και των οποίων η διακοπή

[45] Μαριλένα Κοππά, «Η Κοινή Πολιτική Άμυνας και Ασφάλειας – Η Ιστορία, οι θεσμοί, οι στρατηγικές», Εκδόσεις Πατάκη, Ιούνιος 2017, σελ. 197.
[46] Ahmad Kamal, UN Report: Law of Cyber Space, Council of Foreign Relations, 2015, p. 76.

λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο σε **δύο τουλάχιστον κράτη μέλη**[47].

3. Κατηγορίες κρίσιμων υποδομών

Τηλεπικοινωνιακά, ενεργειακά και χρηματοπιστωτικά συστήματα αποτελούν ζωτικής σημασίας υπηρεσίες για τους πολίτες και επομένως θεωρούνται οι πλέον πιθανοί στόχοι. Η αδρανοποίηση ή η καταστροφή τους μπορεί να εγείρει αισθήματα φόβου και ανασφάλειας στον τοπικό πληθυσμό και ως εκ τούτου να πλήξουν το ηθικό του, να αποσταθεροποιήσουν πλήρως την οικονομία, να προκαλέσουν ακόμα τραυματισμούς ή και θανάτους αθώων ανθρώπων και συνεπώς να οδηγήσουν με μαθηματική ακρίβεια στην αποσάθρωση των δομών ενός κράτους[48].

Τον Ιούνιο του 2017, η επίθεση του ιού με το όνομα «NotPetya», αφού έπληξε χρηματοπιστωτικά και ενεργειακά ιδρύματα της Ουκρανίας, εξαπλώθηκε σε χιλιάδες ευρωπαϊκές επιχειρήσεις σταματώντας τις δραστηριότητες σε κρίσιμους τομείς, όπως οι μεταφορές, οι τραπεζικές συναλλαγές, η ενέργεια και το σύστημα υγείας. Στόχος της επίθεσης ήταν κυρίως να προκληθεί αναστάτωση και να πληγεί ο ουκρανικός οικονομικός, ενεργειακός και κυβερνητικός τομέας. Ωστόσο, ο ιός εξαπλώθηκε χωρίς να κάνει διακρίσεις σε όλη την Ευρώπη επηρεάζοντας κι άλλες ευρωπαϊκές επιχειρήσεις.

Φυσικά από τις κρίσιμες υποδομές δεν θα μπορούσαμε να παραλείψουμε τα συστήματα υδροδότησης και υγειονομικής περίθαλψης, τις εγκαταστάσεις αμυντικών βάσεων, πυρηνικών εργοστασίων[49], και τα δίκτυα μεταφορών και εμπορίου[50]. Το νερό ως υποδομή μπορεί να είναι μία από τις πλέον κρίσιμες υποδομές που μπορεί να πληγεί . Θεωρείται ως ένας από τους μεγαλύτερους κινδύνους ασφαλείας μεταξύ όλων των συστημάτων που ελέγχονται από υπολογιστή. Υπάρχει η δυνατότητα να εξαπλωθούν τεράστιες ποσότητες νερού σε μια περιοχή προκαλώντας απώλειες ζωών και υλικές ζημιές. Το εκτιμώμενο κόστος για την αντικατάσταση των κρίσιμων συστημάτων ύδρευσης θα μπορούσε να ανέλθει σε εκατοντάδες δισεκατομμύρια δολάρια[51].

Επίσης, ιδιαίτερη ανησυχία προκαλεί η έκθεση που συνέταξε ο ερευνητικός οργανισμός Chatham House, σύμφωνα με την οποία, ο κίνδυνος μιας «σοβαρής κυβερνοεπίθεσης» σε εργοστάσια πυρηνικής ενέργειας ολοένα και αυξάνεται, καθώς

---

[47] Οδηγία 2008/114/ΕΚ σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους, 08 Δεκ 2008, άρθρο 2 παρ.(α) & (β).

[48] Mathew Sklerov, Solving the dilemma of state responses to cyberattacks: A justification for the use of active defences against states who neglect their duty to prevent, Military Law Review, Fall 2009, p. 7.

[49] Duncan Hollis, ''Why States need an International Law for Information Operations'', Lewis and Clark Law Review, Winter 2007, p. 4.

[50] Natasha Solce, The battlefield of Cyberspace: The inevitable new military branch, Albany Law Journal of Science and Technology, 2008, p. 06.

[51] Kundur, D., Feng, X., Liu, S., Zourntos, T., & Butler-Purry, K. L. (2010, October). Towards a framework for cyber-attack impact analysis of the electric smart grid. In 2010 First IEEE International Conference on Smart Grid Communications (pp. 244-249). IEEE.

στις περισσότερες χώρες τα μέτρα ασφαλείας δεν είναι επαρκή ώστε να ανταπεξέλθουν σε μια τέτοιου είδους επίθεση[52].

4. Ιστορικά περιστατικά κυβερνοεπιθέσεων

α. Εσθονία

Στις 27 Απριλίου του 2007 και με αφορμή απόφαση της εσθονικής κυβέρνησης για τη μεταφορά ενός σοβιετικού μνημείου του Β' Παγκοσμίου Πολέμου από κεντρικό σημείο της πρωτεύουσας της χώρας σε ένα στρατιωτικό νεκροταφείο στα προάστια του Ταλίν, έλαβε χώρα σειρά κυβερνοεπιθέσεων συνολικής διάρκειας τριών εβδομάδων.

Οι μέθοδοι που επιλέχθηκαν ήταν, μεταξύ άλλων, η κατανεμημένη άρνηση υπηρεσιών, η καταστροφή ιστοσελίδων και η μαζική αποστολή ηλεκτρονικών μηνυμάτων με ανεπιθύμητο περιεχόμενο (spam mails). Επλήγησαν πολιτικοί και κυβερνητικοί στόχοι (κοινοβούλιο, υπουργεία, κρατικές υπηρεσίες, πολιτικά κόμματα κ.α.), υπηρεσίες ενημέρωσης, τράπεζες, σχολεία, και διακομιστές για την υποδομή του διαδικτύου[53].

Αναμφίβολα οι κυβερνοεπιθέσεις αυτές επηρέασαν την Εσθονία, μια χώρα που στηριζόταν και στηρίζεται στο διαδίκτυο και τις ηλεκτρονικές υπηρεσίες (χρήση e-banking, ηλεκτρονική πληρωμή φόρων, ηλεκτρονική ψήφος, σχεδόν οικουμενική πρόσβαση στο διαδίκτυο κ.λπ.). Αναφέρεται χαρακτηριστικά ότι η συνολική ζημία εκτιμήθηκε στο 5% του συνόλου της οικονομικής δραστηριότητας της χώρας[54]. Ίχνη των δραστών των ανωτέρω κυβερνοεπιθέσεων βρέθηκαν σε 178 χώρες, ενώ αρκετά από αυτά ανήκαν σε ιδιώτες και πολίτες της Ρωσίας. Η Ρωσία κατηγορήθηκε από τη διεθνή κοινότητα ως υπεύθυνη του χάους που προκλήθηκε στην Εσθονία. Ωστόσο, ουδέποτε οι επίσημες ρωσικές αρχές παραδέχτηκαν την οποιαδήποτε ανάμιξή τους[55].

β. Γεωργία

Περίπου ένα χρόνο αργότερα, τον Ιούλιο του 2008 και λίγο πριν την ένοπλη σύρραξη μεταξύ Ρωσίας και Γεωργίας, η διαδικτυακή υποδομή της τελευταίας δέχτηκε καταιγίδα κυβερνοεπιθέσεων.

Έκπληκτοι υπάλληλοι πολλών Υπουργείων της Γεωργίας διαπίστωναν ότι λίγο πριν την έναρξη των εχθροπραξιών δεν μπορούσαν να ανταλλάξουν μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου. Σχεδόν όλοι οι δικτυακοί τόποι των υπουργείων και

---

[52] Ηλεκτρονικός τύπος «ΤΟ ΒΗΜΑ», ''Τα πυρηνικά εργοστάσια «ευάλωτα σε χάκινγκ'', Πρατικάκης Βαγγέλης, διαθέσιμο στο διαδίκτυο: https://www.tovima.gr/2015/10/05/science/ta-pyrinika-ergostasia-eyalwta-se-xakingk/

[53] Eneken Tikk, Kadri Kaska, Liis Vihul, International Cyber Incidents: Legal Considerations (Cooperative Cyber Defense Centre of Excellence 2010), p. 33.

[54] Shaun Roberts, 'Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors' (2014) 41 N. Ky. L. Rev, p. 535, 535.

[55] Eneken Tikk, Kadri Kaska, Liis Vihul, International Cyber Incidents: Legal Considerations (Cooperative Cyber Defense Centre of Excellence 2010), p. 34.

άλλων κυβερνητικών υπηρεσιών είχαν «νεκρωθεί». Οι εγκαταστάσεις τους είχαν πληγεί από τις ψηφιακές ομοβροντίες των Ρώσων «κομάντος του κυβερνοχώρου» με αποτέλεσμα να υπερφορτωθούν και να απενεργοποιηθούν αρκετοί διακομιστές. Ως εκ τούτου, η κυβέρνηση της χώρας αδυνατούσε τόσο να έρθει σε επικοινωνία με τον υπόλοιπο κόσμο μέσω διαδικτύου[56], όσο και να ενημερώσει αποτελεσματικά και αξιόπιστα τον πληθυσμό της[57] τη στιγμή που οι ρωσικές δυνάμεις εισέβαλαν στη Βόρεια Οσετία.

Η Μόσχα όχι μόνο αρνήθηκε τις κατηγορίες για κυβερνοεπίθεση ενάντια στη Γεωργία, αλλά υποστήριξε ότι πολλοί ρωσικοί δικτυακοί τόποι είχαν υποστεί παρόμοιες επιθέσεις. Ταυτοχρόνως, σύμφωνα με διαπιστώσεις εμπειρογνωμόνων, αποκλείστηκε η πρόσβαση των Γεωργιανών σε όλους τους δικτυακούς τόπους της ρωσικής επικράτειας.

Είχε εκτιμηθεί τότε, ότι το κόστος ενός γενικευμένου μακρόχρονου κυβερνοπολέμου ανάμεσα στις δύο χώρες δεν θα υπέρβαινε το κόστος ενός τεθωρακισμένου οχήματος! Αυτό και μόνο το γεγονός τον έκανε ιδιαίτερα ελκυστικό, αλλά και αναπόφευκτο[58].

γ. **<u>Ιράν</u>**

Το 2010, ο ιός υπολογιστών «Stuxnet Worm», έπληξε το Ιράν λαμβάνοντας τον έλεγχο των μηχανημάτων φυγοκέντρησης (centrifuges) στην πόλη Natanz και καταφέρνοντας να θέσει εκτός λειτουργίας και να οδηγήσει στην αυτοκαταστροφή αρκετά από αυτά.

Ο αποδιδόμενος στις ΗΠΑ και το Ισραήλ αυτός ιός σήμανε σημαντικότατη καθυστέρηση στο πρόγραμμα ανάπτυξης πυρηνικών όπλων της χώρας και ανάλογου μεγέθους οικονομική ζημία. Είχε τη δυνατότητα αφενός να μεταβάλει και να αυξομειώνει την ταχύτητα των ανωτέρω μηχανημάτων και αφετέρου να εισάγει ψευδή δεδομένα αποκρύπτοντας έτσι τη δράση του[59].

Μάλιστα μόλις το Φεβρουάριο του 2016 αποκαλύφθηκε ότι ο ιός «Stuxnet» αποτελούσε μέρος ενός ευρύτερου σχεδίου των ΗΠΑ, βάσει του οποίου σε περίπτωση αρνητικής έκβασης των διαπραγματεύσεων με το Ιράν αναφορικά με το πυρηνικό

---

[56] Shaun Roberts, 'Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors' (2014) 41 N. Ky. L. Rev, p. 544.
[57] Matthew J. Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses Against States Who Neglect Their Duty to Prevent' (2009) 201 Mil. L. Rev. 1, p. 4-5.
[58] Ηλεκτρονικός τύπος «Το ΒΗΜΑ», ''Και κυβερνοπόλεμος στην περιοχή του Καυκάσου'', άρθρο του Γ. Γιανναράκη, διαθέσιμο στο διαδίκτυο: https://www.tovima.gr/2008/08/14/archive/kai-kybernopolemos-stin-perioxi-toy-kaykasoy/
[59] Major Erik M. Mudrinich, 'Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem' (2012) Air Force Law Review 68 A.F. L. Rev, p. 167, 169.

πρόγραμμα του τελευταίου, θα πλήττονταν τα επικοινωνιακά δίκτυα, το ενεργειακό δίκτυο και τα συστήματα αεράμυνας της χώρας[60].

δ. **Ουκρανία (Κριμαία)**

Η επέμβαση της Ρωσίας στην Ουκρανία το 2014 αποτέλεσε την επιτομή του υβριδικού πολέμου και προκάλεσε τον απόλυτο αιφνιδιασμό στις τάξεις της βορειοατλαντικής συμμαχίας. Οι ρωσικές υβριδικές επιχειρήσεις εμπεριείχαν κυβερνοεπιθέσεις, παραπλανητικές ενέργειες, προπαγάνδα, χρησιμοποίηση παραστρατιωτικών οργανώσεων και αποτέλεσαν ένα πρωτοφανές γεγονός στην ιστορία της μεταπολεμικής Ευρώπης.

Η παραπληροφόρηση ήταν συστηματική και εξελισσόταν από το τακτικό μέχρι το στρατηγικό επίπεδο. Ο αντικειμενικός σκοπός των ρωσικών επιχειρήσεων στον κυβερνοχώρο ήταν η διακοπή της επικοινωνίας μεταξύ της εκτελεστικής εξουσίας και των ενόπλων δυνάμεων που επιτηρούσαν εγκαταστάσεις και σύνορα.

Δίκτυα υπολογιστών σε κυβερνητικές υπηρεσίες, υπέστησαν προσβολή από τον ιό ‘’Snake’’. Ο ιός αυτός επέτρεπε στις ρωσικές υπηρεσίες να έχουν πρόσβαση από απόσταση στους προσβαλλόμενους υπολογιστές, να παραποιούν και να αλλοιώνουν τα δεδομένα τους, προκαλώντας σύγχυση και αποσταθεροποίηση στο ουκρανικό σύστημα ελέγχου και διοικήσεως[61].

Τελικά, τα γεγονότα που έλαβαν χώρα στην Κριμαία και είχαν ως αποτέλεσμα την προσάρτησή της και την de facto αλλαγή των συνόρων της, καταδεικνύουν ότι η διεξαγωγή των κυβερνοεπιθέσεων, ως τμήμα των ευρύτερων υβριδικών επιχειρήσεων, απειλεί ακόμη και την εδαφική ακεραιότητα κυρίαρχων κρατών και δύναται να προέρχεται όχι μόνο από μη κρατικούς αλλά και από κρατικούς δρώντες.

[60] Peter Z. Stockburger, ‘Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum’ (2016) 31 Am. U. Int’l L. Rev, p. 545, 548.
[61] Ηλεκτρονικός τύπος «ΤΟ ΒΗΜΑ», Gordon Michael R, «Η νέα, τριπλή στρατηγική Πούτιν στην Ουκρανία», Απρ 2014, διαθέσιμο στο διαδίκτυο: https://www.tovima.gr/2014/04/22/world/i-nea-tripli-stratigiki-poytin-stin-oykrania/.

ΚΕΦΑΛΑΙΟ 3ο

ΟΙ ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΝΟΜΟΘΕΤΙΚΕΣ ΔΡΑΣΕΙΣ ΤΗΣ ΕΕ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ – ΧΡΗΜΑΤΟΔΟΤΗΣΗ ΚΑΙ ΔΑΠΑΝΕΣ

1. Υπεύθυνοι φορείς της ΕΕ για την κυβερνοασφάλεια

Η Ευρωπαϊκή Επιτροπή έχει ως στόχο την ενίσχυση των ικανοτήτων και της συνεργασίας στον τομέα της κυβερνοασφάλειας, καθώς και την ενσωμάτωση της διάστασης αυτής σε άλλες πολιτικές και δραστηριότητες της ΕΕ.

Οι γενικές διευθύνσεις (ΓΔ), που είναι κυρίως αρμόδιες για την πολιτική κυβερνοασφάλειας, είναι η ΓΔ Επικοινωνιακών Δικτύων (κυβερνοασφάλεια) και η ΓΔ Μετανάστευσης και Εσωτερικών Υποθέσεων (κυβερνοεγκληματικότητα). Αυτές οι προαναφερόμενες ΓΔ είναι αρμόδιες για την ψηφιακή ενιαία αγορά και την ένωση ασφάλειας αντίστοιχα.

Η ΓΔ Επικοινωνιακών Δικτύων είναι αρμόδια για την ασφάλεια των ψηφιακών συστημάτων της ίδιας της Επιτροπής. Η Επιτροπή υποστηρίζεται από πλήθος οργανισμών, ιδίως τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών, γνωστός ως ENISA (European Union Agency for Network and Information Security), και τον οργανισμό της ΕΕ για την κυβερνοασφάλεια, ο οποίος αποτελεί συμβουλευτικό κυρίως όργανο που στηρίζει την ανάπτυξη πολιτικής, την ανάπτυξη ικανοτήτων και την ενημέρωση και ευαισθητοποίηση για τα σχετικά θέματα[62].

Το ευρωπαϊκό κέντρο EC3 (European Cyber Crime Centre) της Ευρωπαϊκής Αστυνομίας (Europol) για τα εγκλήματα στον κυβερνοχώρο δημιουργήθηκε με σκοπό να ενισχύσει τις προσπάθειες επιβολής της νομοθεσίας της ΕΕ για την πάταξη της κυβερνοεγκληματικότητας. Η Επιτροπή φιλοξενεί μια ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (Computer Emergency Response Tea / CERT-EU), η οποία υποστηρίζει το σύνολο των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) ηγείται των προσπαθειών στους τομείς της κυβερνοάμυνας, της διπλωματίας στον κυβερνοχώρο και της στρατηγικής επικοινωνίας, και φιλοξενεί κέντρα συλλογής και ανάλυσης πληροφοριών.

[62] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ‘’Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια’’, σελ. 12, Μαρ 2019.

Επίσης, ο Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ) επιδιώκει την ανάπτυξη ικανοτήτων κυβερνοάμυνας.

Τα κράτη μέλη φέρουν την κύρια ευθύνη για την κυβερνοασφάλειά τους και, σε επίπεδο ΕΕ, ενεργούν μέσω του Συμβουλίου, το οποίο διαθέτει πληθώρα οργάνων συντονισμού και ανταλλαγής πληροφοριών.

Οργανώσεις του ιδιωτικού τομέα, συμπεριλαμβανομένων οργανώσεων της βιομηχανίας, φορέων διακυβέρνησης του διαδικτύου, και της πανεπιστημιακής κοινότητας, είναι τόσο εταίροι όσο και συμβάλλοντες στη χάραξη και την εφαρμογή πολιτικών.

2. <u>Πολιτική της ΕΕ για την κυβερνοασφάλεια</u>

Ακρογωνιαίος λίθος της πολιτικής της ΕΕ είναι η στρατηγική για την κυβερνοασφάλεια του 2013[63]. Άμεση προτεραιότητα της στρατηγικής είναι το ψηφιακό περιβάλλον της ΕΕ να καταστεί το ασφαλέστερο παγκοσμίως, με παράλληλη προάσπιση των θεμελιωδών ανθρώπινων αξιών και ελευθεριών. Έχει πέντε βασικούς στόχους: (i)την ενίσχυση της κυβερνοανθεκτικότητας (ii) τη μείωση της κυβερνοεγκληματικότητας·(iii) την ανάπτυξη πολιτικών και ικανοτήτων κυβερνοάμυνας (iv) την ανάπτυξη βιομηχανικών και τεχνολογικών πόρων κυβερνοασφάλειας·και (v) τη θέσπιση διεθνούς πολιτικής για τον κυβερνοχώρο, σύμφωνη με τις θεμελιώδεις αξίες της ΕΕ.

Η στρατηγική για την κυβερνοασφάλεια είναι άρρηκτα συνδεδεμένη με τρεις στρατηγικές που ακολούθησαν και εγκρίθηκαν μεταγενέστερα:

α. **Το Ευρωπαϊκό Θεματολόγιο** για την ασφάλεια (2015), όπου η Ευρωπαϊκή Επιτροπή καθορίζει τη στρατηγική της Ένωσης για την αντιμετώπιση απειλών στον τομέα της ασφάλειας κατά την περίοδο 2015-2020. Κύριος στόχος του είναι η βελτίωση της επιβολής του νόμου και της δικαστικής αντιμετώπισης της κυβερνοεγκληματικότητας. Επιδίωξή του είναι επίσης ο προσδιορισμός των εμποδίων που παρακωλύουν τις ποινικές έρευνες στον τομέα του κυβερνοεγκλήματος και η ανάπτυξη των σχετικών ικανοτήτων για την δραστική καταπολέμησή του[64].

β. Η στρατηγική για την **Ψηφιακή Ενιαία Αγορά** (2015) έχει ως στόχο τη βελτίωση της πρόσβασης σε ψηφιακά προϊόντα και υπηρεσίες[65]. Η επίτευξη της ψηφιακής ενιαίας αγοράς θα επιτρέψει στην Ευρώπη να διατηρήσει τη θέση της ως παγκόσμιου ηγέτη στην ψηφιακή οικονομία, καθώς θα βοηθήσει τις ευρωπαϊκές επιχειρήσεις να αναπτύξουν τις δραστηριότητές τους σε παγκόσμιο επίπεδο.

---

[63] Cybersecurity “Strategy of the European Union”, σελ. 3-4, JOIN (2013) 1 final, Brussels, 7.2.2013.
[64] European Commission, “The European Agenda on Security”, COM (2015) 185 final, Strasbourg, 28.4.2015.
[65] European Commission, “A Digital Single Market Strategy for Europe”, COM (2015) 192 final, Brussels, 6.5.2015

γ. Η **Συνολική Στρατηγική** (2016) επιδιώκει την ενίσχυση του ρόλου της ΕΕ στην παγκόσμια ασφάλεια μέσω της δέσμευσης για ενίσχυση των προσπαθειών σε θέματα κυβερνοχώρου, της συνεργασίας με βασικούς εταίρους και της αποφασιστικότητας για την αντιμετώπιση των απειλών του κυβερνοχώρου σε όλους τους τομείς πολιτικής, συμπεριλαμβανομένης της αντιμετώπισης της παραπληροφόρησης μέσω στρατηγικής επικοινωνίας[66].

Το 2014 εγκρίθηκε το ευρωπαϊκό **Πλαίσιο Πολιτικής για την Κυβερνοάμυνα** (EU Cyber Defence Policy Framework) το οποίο τονίζει ότι ο κυβερνοχώρος είναι το πέμπτο πεδίο στρατιωτικής δραστηριότητας μαζί με την ξηρά, τη θάλασσα, τον αέρα και το διάστημα, και συμπληρώνει ότι η επιτυχής εφαρμογή της ΚΠΑΑ εξαρτάται από έναν ασφαλή κυβερνοχώρο[67].

Το πλαίσιο αυτό, το οποίο **επικαιροποιήθηκε** τον Νοέμβριο του 2018 από το Ευρωπαϊκό Συμβούλιο, δίνει ιδιαίτερη έμφαση στη προστασία των δικτύων επικοινωνιών και πληροφοριών της ΚΠΑΑ και στόχος του είναι να αναπτυχθεί περαιτέρω η πολιτική της ΕΕ για την κυβερνοάμυνα λαμβάνοντας υπόψη σχετικές εξελίξεις σε άλλα φόρουμ και τομείς πολιτικής που έλαβαν χώρα από το 2014 μέχρι το 2018.

Το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα στηρίζει την ανάπτυξη ικανοτήτων κυβερνοάμυνας των κρατών μελών της ΕΕ καθώς και την ενίσχυση της κυβερνοπροστασίας των υποδομών της ΕΕ για την ασφάλεια και την άμυνα, με την επιφύλαξη της εθνικής νομοθεσίας των κρατών μελών και της νομοθεσίας της ΕΕ, συμπεριλαμβανομένου του πεδίου εφαρμογής της κυβερνοάμυνας, όπου αυτό ορίζεται.

Προσδιορίζονται ως τομείς προτεραιότητας για την κυβερνοάμυνα η κατάρτιση και οι ασκήσεις, η έρευνα, η τεχνολογία, η συνεργασία με πολιτικούς φορείς και διεθνείς οργανισμούς ώστε να βελτιωθεί η ικανότητα αντίδρασης της ΕΕ στις κυβερνοκρίσεις και στις υβριδικές επιχειρήσεις μέσω της βελτίωσης των διαδικασιών λήψης αποφάσεων και της διαθεσιμότητας των πληροφοριών. Παράλληλα βέβαια, διευκρινίζονται οι ρόλοι των διαφόρων ευρωπαϊκών φορέων με πλήρη σεβασμό των αρμοδιοτήτων και ευθυνών των φορέων της Ένωσης και των κρατών μελών καθώς και του θεσμικού πλαισίου της ΕΕ και της αυτονομίας της κατά τη λήψη αποφάσεων[68].

Στο πλαίσιο της αποτελεσματικής αντιμετώπισης των κυβερνοαπειλών κατά των ψηφιακών υποδομών ζωτικής σημασίας της ΕΕ αλλά και των ιδιωτών χρηστών εγκρίνεται το 2016 το **Κοινό Πλαίσιο για την Αντιμετώπιση Υβριδικών Απειλών**. Το κείμενο αυτό υπογραμμίζει ότι οι κυβερνοεπιθέσεις μπορούν να εκδηλωθούν με τη

[66] European Union, “A Global Strategy for the European Union’s Foreign and Security Policy”, σελ. 14-17, June 2016
[67] Μαριλένα Κοππά, «Η Κοινή Πολιτική Άμυνας και Ασφάλειας», σελ. 199, Εκδόσεις Πατάκη, Αθήνα 2016.
[68] Συμβούλιο της ΕΕ, ‘’Πλαίσιο της Πολιτικής της ΕΕ για την κυβερνοάμυνα’’ (όπως επικαιροποίηθηκε το 2018), 14413/18, Βρυξέλλες, 19 Νοεμβρίου 2018, σελ 208.

μορφή εκστρατειών παραπληροφόρησης στα μέσα κοινωνικής δικτύωσης με στόχο την κοινωνική αναταραχή και τη διατάραξη της κοινωνικής συνοχής. Επιπλέον, επισημαίνει την ανάγκη καλύτερης ενημέρωσης και ευαισθητοποίησης των ευρωπαίων πολιτών για τις αναδυόμενες απειλές στον κυβερνοχώρο αλλά και της ενίσχυσης της συνεργασίας μεταξύ της ΕΕ και του ΝΑΤΟ[69].

Μια νέα **δέσμη μέτρων** παρουσιάστηκε για την κυβερνοασφάλεια το 2017[70], στην οποία γινόταν σαφής αναφορά στην αναγκαιότητα επικαιροποίησης της στρατηγικής για την κυβερνοασφάλεια του 2013 ώστε αυτή να ανταποκρίνεται αποτελεσματικά στις νέες μορφές κυβερνοαπειλών που αναδύονται ραγδαία. Η δέσμη μέτρων αφορούσε επίσης σε μια σειρά νομοθετικών προτάσεων καθώς και σ' ένα προσχέδιο για ταχεία και συντονισμένη αντίδραση σε περίπτωση μεγάλης κλίμακας κυβερνοεπίθεσης κατά των ψηφιακών και επικοινωνιακών συστημάτων της ΕΕ.

Στο πλαίσιο αυτό προτάθηκε και η αναβάθμιση του οργανισμού της ΕΕ για την Κυβερνοασφάλεια ENISA. Σύμφωνα με την πρόταση, ο «νέος» οργανισμός θα είχε ως μόνιμη εντολή να συνδράμει τα κράτη μέλη στην αποτελεσματική αποτροπή και αντιμετώπιση κυβερνοεπιθέσεων ενώ θα ενίσχυε την ετοιμότητα αντίδρασης της ΕΕ μέσω της διοργάνωσης ετήσιων πανευρωπαϊκών ασκήσεων με αντικείμενο την κυβερνοασφάλεια, καθώς και μέσω της διασφάλισης της καλύτερης ανταλλαγής πληροφοριών και γνώσεων σχετικά με απειλές.

3. <u>Ενέργειες της ΕΕ για την κυβερνοασφάλεια στο νομοθετικό Πλαίσιο</u>

Από το 2002 έχουν εγκριθεί διάφορες νομοθετικές διατάξεις με στόχο την ενίσχυση της κυβερνοασφάλειας στους κόλπους της ΕΕ. Η σπουδαιότερη νομοθετική πράξη είναι η οδηγία του 2016 για την ασφάλεια δικτύων και πληροφοριών (Network Information Systems / NIS). Χάρη σ' αυτή την νομοθετική πράξη της ΕΕ για την κυβερνοασφάλεια, τα κράτη μέλη έχουν ενισχύσει τη συνεργασία τους για την κυβερνοασφάλεια και συντονίζουν τις προσπάθειές τους για την ανάπτυξη των ικανοτήτων απόκρισής τους. Η Επιτροπή συνεργάζεται στενά με τα κράτη μέλη για να τα συνδράμει στη μεταφορά της οδηγίας στο εθνικό τους δίκαιο.

Για να μπορέσουν τα κράτη μέλη να μεταφέρουν γρήγορα την οδηγία NIS στο εθνικό τους δίκαιο και να αναπτύξουν τις ικανότητές τους, το πρόγραμμα του μηχανισμού **«Συνδέοντας την Ευρώπη»** χορηγεί χρηματοδότηση 38 εκατ. ευρώ έως το 2020 για τη στήριξη των εθνικών ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές Computer Security Incident Response Team (CSIRT), καθώς και άλλων ενδιαφερόμενων μερών στο πλαίσιο της οδηγίας NIS, προκειμένου να εφοδιάσει

[69] European Commission, ''Joint Framework on Countering Hybrid Threats'', σελ. 3-4, 6.4.2016 JOIN (2016) 18 final, Brussels.
[70] Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου, ''Κατάσταση της Ένωσης 2017 – Κυβερνοασφάλεια: Η Επιτροπή αναβαθμίζει την απόκριση της ΕΕ στις κυβερνοεπιθέσεις'', Βρυξέλλες, 19 Σεπτεμβρίου 2017.

την Ευρώπη με τα κατάλληλα εργαλεία και μηχανισμούς για την αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων.

Μια άλλη νομοθετική πράξη σπουδαίας σημασίας αποτελεί ο **Γενικός Κανονισμός για την Προστασία των Δεδομένων** (ΓΚΠΔ) που τέθηκε σε ισχύ το 2016 και σε εφαρμογή τον Μάιο του 2018 αντικαθιστώντας ν. 2472/1997. Ο νέος Γενικός Κανονισμός επιχειρεί να δημιουργήσει ένα αυστηρότερο θεσμικό πλαίσιο επεξεργασίας και προστασίας των προσωπικών δεδομένων. Χαρακτηρίζεται ιδίως από την ριζική αλλαγή του συστήματος ευθύνης για τήρηση της νομοθεσίας εισάγοντας **την αρχή της Λογοδοσίας (Accountability Principle)**, σύμφωνα με τον οποίο οι εταιρείες που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα οφείλουν να διαμορφώσουν τις διαδικασίες και τα τεχνικά και οργανωτικά συστήματα τους κατά τέτοιο τρόπο ώστε να είναι πλήρως συμμορφωμένες με όσα προβλέπει ο νέος Κανονισμός[71].

Με το νέο Κανονισμό εκτοξεύεται το ύψος των επαπειλούμενων διοικητικών προστίμων σε περίπτωση διαπίστωσης παράβασης των διατάξεών του, εφόσον δεν λαμβάνονται άλλα μέτρα. Έτσι, συγκεκριμένες παραβάσεις των υποχρεώσεων των υπευθύνων και εκτελούντων επεξεργασία επισύρουν πρόστιμα έως 10.000.000 € ή σε περίπτωση επιχειρήσεων έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο είναι υψηλότερο).

Τα μέλη της Ολομέλειας του Ευρωπαϊκού Κοινοβουλίου (ΕΚ) ενέκριναν τον Μάρτιο του 2019, **την πράξη για την ασφάλεια στον κυβερνοχώρο**. Για πρώτη φορά δημιουργείται πανευρωπαϊκό **σύστημα πιστοποίησης** κυβερνοασφάλειας που διασφαλίζει ότι τα προϊόντα, οι διαδικασίες και οι υπηρεσίες που αποτελούν αντικείμενα εμπορικής συναλλαγής στην ΕΕ πληρούν συγκεκριμένα κριτήρια ασφάλειας του κυβερνοχώρου. Επίσης, το ΕΚ υιοθέτησε ψήφισμα με το οποίο υπογραμμίζει τις απειλές για την ασφάλεια που συνδέονται με την ολοένα αυξανόμενη τεχνολογική παρουσία της Κίνας στην ΕΕ, ενώ καλεί επίσης την Ευρωπαϊκή Επιτροπή να αναθέσει στον ENISA, την επεξεργασία ενός συστήματος που να διασφαλίζει ότι η ανάπτυξη της τεχνολογίας 5G στην Ευρώπη είναι σύμφωνη με τα υψηλότερα πρότυπα ασφαλείας.

Τον Μάρτιο του 2019, η Επιτροπή των Μόνιμων Αντιπροσώπων του Συμβουλίου έδωσε στη ρουμανική Προεδρία **εντολή να ξεκινήσει συζητήσεις** με το ΕΚ για τη θέσπιση του **Ευρωπαϊκού Βιομηχανικού, Τεχνολογικού και Ερευνητικού Κέντρου Κυβερνοασφάλειας** και ενός **Δικτύου Εθνικών Κέντρων Συντονισμού**. Από κοινού οι δύο αυτές δομές θα βοηθήσουν ώστε να θωρακιστεί η ψηφιακή ενιαία αγορά και να αυξηθεί η αυτονομία της ΕΕ στον τομέα της κυβερνοασφάλειας. Ειδικότερα, το βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο κυβερνοασφάλειας θα

[71] Διαδικτυακή Πηγή: https://www.taxheaven.gr/laws/circular/view/id/28194, «Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα», 09 Μαρ 2018.

συμβάλλει στον καλύτερο συντονισμό της έρευνας και καινοτομίας στον τομέα της κυβερνοασφάλειας[72].

Το **δίκτυο ικανοτήτων κυβερνοασφάλειας** θα αποτελείται από τα **εθνικά κέντρα συντονισμού** που έχουν ορίσει τα κράτη μέλη. Τα εθνικά κέντρα είτε θα κατέχουν είτε θα έχουν πρόσβαση σε τεχνολογική εμπειρογνωσία στον τομέα της κυβερνοασφάλειας, για παράδειγμα σε τομείς όπως η κρυπτογραφία, η ανίχνευση εισβολών ή οι ανθρώπινες πτυχές της ασφάλειας. Η χρηματοδότηση για τα κέντρα αυτά θα παρέχεται κυρίως από τα προγράμματα «Ψηφιακή Ευρώπη» και «Ορίζων Ευρώπη», ενώ θα υπάρχει και δυνατότητα οικειοθελών συνεισφορών των κρατών μελών.

Σε αυτό το πλαίσιο δράσης, προτείνεται επίσης η δημιουργία μιας τρίτης δομής, η **κοινότητα ικανοτήτων κυβερνοασφάλειας**, που θα φέρνει σε επαφή τους βασικούς ενδιαφερόμενους φορείς ώστε να ενισχυθεί και να διαδοθεί η εμπειρογνωσία της κυβερνοασφάλειας σε όλη την ΕΕ. Μέλη της θα είναι μεταξύ άλλων, φορείς του κλάδου, πανεπιστημιακοί και μη κερδοσκοπικοί ερευνητικοί οργανισμοί, δημόσιες οντότητες που ασχολούνται με επιχειρησιακά και τεχνικά ζητήματα και κατά περίπτωση, παράγοντες από άλλους τομείς που αντιμετωπίζουν προκλήσεις σχετικές με την κυβερνοασφάλεια.

4. <u>Νέες προκλήσεις – Αποτελεσματικότητα της ΕΕ στο πολιτικό και στο νομοθετικό πλαίσιο για την κυβερνοασφάλεια.</u>

Είναι αναμφισβήτητο γεγονός ότι κατά την δεύτερη δεκαετία του 21ου αιώνα έχουν πραγματοποιηθεί σημαντικά βήματα προόδου στο χώρο της κυβερνοασφάλειας με τη θέσπιση νομοθετικών ρυθμίσεων και δημιουργία φορέων με στόχο τη συμπαγή θωράκιση της ευρωπαϊκής ανθεκτικότητας ως μια δυναμική απάντηση στις ολοένα και αυξανόμενες απειλές των κυβερνοεπιθέσεων.

Το 2013, η ΕΕ παρουσίασε μια στρατηγική για την ασφάλεια στον κυβερνοχώρο δρομολογώντας μια σειρά βασικών αξόνων εργασίας για τη βελτίωση της ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο. Οι κύριοι στόχοι και οι βασικές αρχές της, όσον αφορά την προώθηση ενός αξιόπιστου, ασφαλούς και ανοικτού οικοσυστήματος του κυβερνοχώρου, εξακολουθούν να ισχύουν. Ωστόσο, η απουσία ουσιαστικών κριτηρίων αξιολόγησης και μέτρησης του αντικτύπου των εφαρμοζόμενων πολιτικών και νομοθετικών αλλαγών επιδρούν αρνητικά στην εξαγωγή ασφαλών συμπερασμάτων ως προς την αποτελεσματικότητα τους.

Το γεγονός βέβαια αυτό, ως ένα βαθμό, έχει κάποια λογική εξήγηση αν αναλογιστούμε ότι ένα πλήθος πολιτικών και νομοθετικών μέτρων που έχουν

[72] Συμβούλιο της ΕΕ, «Η ΕΕ συγκεντρώνει και δικτυώνει την εμπειρογνωσία της στον τομέα της κυβερνοασφάλειας», Δελτίο Τύπου της 13 Μαρ 2019.

υιοθετηθεί και αφορούν στην ευρωπαϊκή κυβερνοασφάλεια άρχισαν πρόσφατα να εφαρμόζονται, γεγονός που εμποδίζει την πλήρη και εμπεριστατωμένη αξιολόγηση των συνεπειών τους.

Επίσης, δεν πρέπει να μας διαφεύγει το γεγονός ότι, σημαντικό ρόλο στη διαδικασία της αξιολόγησης διαδραματίζουν τα στατιστικά στοιχεία και χρήσιμα δεδομένα για ζητήματα που σχετίζονται με τον κυβερνοχώρο. Μέχρι στιγμής, ελάχιστα κράτη μέλη έχουν την πρόβλεψη να συγκεντρώνουν συστηματικά επίσημα δεδομένα. Πολλά κράτη δεν είναι πρόθυμα να μοιραστούν με άλλα κράτη πληροφορίες τις οποίες τα ίδια θεωρούν ευαίσθητες για την εθνική τους ασφάλεια. Οι παραπάνω διαπιστώσεις έχουν ως αποτέλεσμα να μην υπάρχει η δυνατότητα της σύγκρισης, με προγενέστερα στατιστικά στοιχεία, που θα αποτύπωνε ως ένα μετρήσιμο μέγεθος το βαθμό προόδου και την αποτελεσματικότητα συγκεκριμένων πολιτικών δράσεων και νομοθεσιών στο χώρο της κυβερνοασφάλειας[73].

Οι ταχύτητες με τις οποίες αναδύονται οι νέες ψηφιακές τεχνολογίες και αναβαθμίζονται οι δυνατότητες των κυβερνοαπειλών υπερβαίνουν σε μεγάλο βαθμό τις αντίστοιχες ταχύτητες σχεδιασμού και εφαρμογής της νομοθεσίας της ΕΕ. Το γεγονός αυτό έχει ως αποτέλεσμα προβλέψεις και διατάξεις του νομοθετικού πλαισίου να εμφανίζονται ως παρωχημένες στην αντιμετώπιση και καταστολή κυβερνοεπιθέσεων και κυβερνοεγκλημάτων που βασίζονται και εξαπλώνονται χρησιμοποιώντας νέες τεχνολογικές μεθόδους.

5. **Χρηματοδότηση και δαπάνες στον τομέα της κυβερνο-ασφάλειας**

α. **Γενικά στοιχεία**

Συγκριτικά, οι δαπάνες στην ΕΕ για έναν ασφαλή και ελεύθερο κυβερνοχώρο είναι χαμηλές, κατακερματισμένες και συχνά δεν συνοδεύονται από συντονισμένα κυβερνητικά προγράμματα. Παρότι η εξασφάλιση ακριβών αριθμητικών στοιχείων είναι δυσχερής, οι δημόσιες δαπάνες της ΕΕ στον τομέα της κυβερνοασφάλειας εκτιμάται ότι κυμαίνονται μεταξύ ενός και δύο δισεκατομμυρίων ευρώ ετησίως[74]. Επίσης, σε χαμηλό σχετικά ποσοστό κυμαίνονται οι δαπάνες ορισμένων κρατών μελών στον τομέα της κυβερνοασφάλειας Ενδεικτικά αναφέρεται ότι οι δαπάνες αυτές εκφρασμένες ως ποσοστό του ΑΕΠ τους, αντιστοιχούν περίπου στο ένα δέκατο ή και λιγότερο του αντιστοίχου επιπέδου των ΗΠΑ[75].

---

[73] Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, «Transatlantic Cyber-Insecurity and Cybercrime», PE 603.948, σελ. viii, Δεκέμβριος 2017.

[74] European Commission, '' Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'', σελ. 5, SWD (2018) 305 final, 06-06-2018.

[75] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ''Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια'', σελ. 28, Μαρ 2019.

β. **Δαπάνες για την κυβερνοασφάλεια**

Η ΕΕ φιλοδοξεί το διαδικτυακό περιβάλλον της να καταστεί το ασφαλέστερο στον κόσμο. Αυτό απαιτεί σημαντικές προσπάθειες από πλευράς όλων των ενδιαφερομένων, συμπεριλαμβανομένης μιας στέρεης χρηματοοικονομικής βάσης.

Κατά την περίοδο 2014-2018, η Επιτροπή διέθεσε τουλάχιστον 1,4 δισεκατομμύρια ευρώ για την εφαρμογή της στρατηγικής της στον τομέα της κυβερνοασφάλειας, το μεγαλύτερο μέρος των οποίων διατέθηκε για το πρόγραμμα «Ορίζων 2020»[76]. Η χρηματοδότηση του προγράμματος «Ορίζων 2020» διοχετεύεται κυρίως στο πλαίσιο των κοινωνικών προκλήσεων **«Ασφαλείς κοινωνίες»** και **«Υπεροχή στις ευρείας εφαρμογής και βιομηχανικές τεχνολογίες»**.

Μεταξύ του 2016 και του 2018, διατέθηκαν ετησίως 13 εκατομμύρια ευρώ από τον μηχανισμό **«Συνδέοντας την Ευρώπη»**, στον οποίο τα κράτη μέλη μπορούσαν να υποβάλουν αίτηση προκειμένου να λάβουν χρηματοδότηση για να συμμορφωθούν με τις απαιτήσεις της οδηγίας NIS. Επίσης, κατά την περίοδο 2014-2018, η ΕΕ δαπάνησε περίπου 50 εκατομμύρια ευρώ για την ενίσχυση της κυβερνοασφάλειας εκτός των συνόρων της. Σχεδόν το ήμισυ του ποσού αυτού διατέθηκε για την ανάπτυξη και την εφαρμογή της νομοθεσίας για την κυβερνοεγκληματικότητα και την ενίσχυση της διεθνούς συνεργασίας σε παγκόσμιο επίπεδο.

Στην προσπάθεια αυτή ανήκει και το πρόγραμμα GLACY+ ύψους 13,5 εκατομμυρίων ευρώ[77]. Σε άλλες περιπτώσεις, οι δαπάνες στο πλαίσιο άλλων χρηματοοικονομικών μέσων της ΕΕ επικεντρώθηκαν σε μεγάλο βαθμό στα Δυτικά Βαλκάνια καθώς και στην ευρωπαϊκή γειτονία.

γ. **Μελλοντικές προοπτικές**

Το ποσό των 2 δισεκατομμυρίων ευρώ που προβλέπεται για την κυβερνοασφάλεια στο πλαίσιο του προτεινόμενου νέου προγράμματος «Ψηφιακή Ευρώπη» για την περίοδο 2021-2027 έχει ως στόχο την ενίσχυση της κοινωνικής προστασίας έναντι των απειλών στο κυβερνοχώρο.

Το **δίκτυο κέντρων ικανοτήτων** στον τομέα της κυβερνοασφάλειας και **το ερευνητικό κέντρο ικανοτήτων** που προτείνεται να δημιουργηθούν με στόχο την υιοθέτηση μιας πιο εξορθολογισμένης προσέγγισης, αναμένεται να αποτελέσουν τον κύριο μηχανισμό εκτέλεσης των δαπανών στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη».

[76] Το πρόγραμμα «Ορίζων 2020» είναι το ύψους 80 δισεκατομμυρίων ευρώ πρόγραμμα της ΕΕ για την έρευνα και την καινοτομία που στηρίζει την Ένωση καινοτομίας, στόχος της οποίας είναι η διασφάλιση της παγκόσμιας ανταγωνιστικότητας της ΕΕ.
[77] Το έργο GLACY+ (Global Action on Cybercrime+) υλοποιείται από κοινού με το Συμβούλιο της Ευρώπης. Στηρίζει δώδεκα χώρες στην Αφρική και σε περιοχές της Ασίας-Ειρηνικού, της Λατινικής Αμερικής και της Καραϊβικής, οι οποίες με τη σειρά τους μπορούν να χρησιμεύσουν ως κόμβοι για την ανταλλαγή των αποκομισθεισών εμπειριών με άλλες χώρες της περιοχής τους.

Πρόσφατα, οι αμυντικές δαπάνες από τον προϋπολογισμό της ΕΕ αυξήθηκαν μέσω του ευρωπαϊκού προγράμματος βιομηχανικής ανάπτυξης στον τομέα της άμυνας, για το οποίο πρόκειται να διατεθούν 500 εκατομμύρια ευρώ κατά την περίοδο 2019-2020 . Το πρόγραμμα αυτό θα επικεντρωθεί στη βελτίωση του συντονισμού και της αποδοτικότητας των αμυντικών δαπανών των κρατών μελών μέσω κινήτρων για από κοινού ανάπτυξη.

δ. **Οι ελλείψεις πόρων που αντιμετωπίζουν οι οργανισμοί της ΕΕ**

Οι τρεις βασικοί φορείς (ENISA, EC3 και CERT-EU) που βρίσκονται στο επίκεντρο της πολιτικής της ΕΕ για την κυβερνοασφάλεια αντιμετωπίζουν ελλείψεις πόρων σε μια περίοδο κατά την οποία η σημασία των πολιτικών προτεραιοτήτων που επικεντρώνονται στην ασφάλεια αυξάνεται. Οι ελλείψεις σε ανθρώπινους και οικονομικούς πόρους που αντιμετωπίζουν επί του παρόντος οι οργανισμοί της ΕΕ δεν τους επιτρέπουν πολλές φορές να ανταποκριθούν αποτελεσματικά στην εκπλήρωση των προσδοκιών, των στόχων και των αποστολών τους.

Τα αιτήματα των οργανισμών για πρόσθετους πόρους προκειμένου να ανταποκριθούν στην αυξανόμενη ζήτηση δεν έχουν ικανοποιηθεί πλήρως, γεγονός που μπορεί να υπονομεύσει την έγκαιρη επίτευξη των στόχων πολιτικής. Χαρακτηριστικό παράδειγμα του προβλήματος αυτού αποτελεί αδυναμία του ENISA να επιτύχει πλήρως τους στόχους του το 2017[78].

Η κλιμάκωση των δημόσιων και ιδιωτικών επενδύσεων στις ευρωπαϊκές επιχειρήσεις που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας αποτελεί μια ιδιαίτερη πρόκληση. Δημόσια χρηματοδότηση είναι συχνά διαθέσιμη κατά τα αρχικά στάδια, χωρίς να συμβαίνει συχνά το ίδιο κατά τα στάδια της ανάπτυξης και της επέκτασης. Ταυτόχρονα, πολυάριθμες πρωτοβουλίες χρηματοδότησης της ΕΕ, δεν αξιοποιούνται στον απαραίτητο βαθμό λόγω της γραφειοκρατίας.

Οι εταιρείες που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας στην ΕΕ υστερούν σε σχέση με τις αντίστοιχες εταιρείες σε διεθνές επίπεδο καθώς είναι λιγότερες και η μέση χρηματοδότηση που προσελκύουν είναι σημαντικά χαμηλότερη[79]. Το γεγονός αυτό αναγκάζει την ΕΕ να προμηθεύεται προϊόντα και υπηρεσίες κυβερνασφάλειας από χώρες εκτός της ένωσης με αποτέλεσμα να αυξάνεται γεωμετρικά ο κίνδυνος της τεχνολογικής εξάρτησής της από αυτές και να εμποδίζεται η υλοποίηση του ευρωπαϊκού οράματος για τη δημιουργία μιας ενιαίας ψηφιακής αγοράς.

[78] This study was carried out for the European Commission by Karin Attström, Vanessa Ludden, Franziska Lessmann, ‘‘Study on the Evaluation of the European Union Agency for Network and Information Security’’, p. 106-107, 2017.
[79] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ‘‘Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια’’, σελ. 29, Μαρ 2019.

ΚΕΦΑΛΑΙΟ 4ο

ΟΙ ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΕ ΓΙΑ ΤΗΝ ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΠΟΤΡΟΠΗΣ ΚΑΙ ΤΗΣ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΣΤΙΣ ΑΠΕΙΛΕΣ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

«Οι προκλήσεις που θέτουν οι κυβερνοαπειλές στις μέρες μας καθιστούν επιτακτική την ανάγκη άμεσης λήψης μέτρων από την ΕΕ για την ενίσχυση της κυβερνοασφάλειας και της ψηφιακής αυτονομίας της, με σταθερή προσήλωση, παράλληλα, στις θεμελιώδεις αξίες της».

Baudilio Tomé Muguruza (μέλος του ΕΕΣ)

1. Αποτελεσματική αντίδραση της ΕΕ σε κυβερνοεπιθέσεις

Η αποτελεσματική αντίδραση σε περίπτωση διεξαγωγής κυβερνοεπιθέσεων σε κρίσιμες υποδομές είναι καίριας σημασίας για την ευρωπαϊκή ασφάλεια και προϋποθέτει την επίτευξη υψηλού συντονισμού δράσης και συνεργασίας από όλους τους ευρωπαϊκούς, εθνικούς και ιδιωτικούς φορείς που εμπλέκονται με τα θέματα της κυβερνοασφάλειας.

α. Ανίχνευση και γνωστοποίηση της κυβερνοαπειλής

Τα κοινά εργαλεία ανίχνευσης καθιστούν δυνατή την αντιμετώπιση της συντριπτικής πλειονότητας των επιθέσεων καθημερινά[80]. Εντούτοις, λόγω της ολοένα μεγαλύτερης πολυπλοκότητας των ψηφιακών συστημάτων είναι αδύνατη η αποτροπή όλων των επιθέσεων. Ο βαθμός πολυπλοκότητάς τους σημαίνει ότι συχνά μπορεί να παρέλθει σημαντικό χρονικό διάστημα μέχρι να αποκαλυφθούν οι επιθέσεις. Σύμφωνα με τους εμπειρογνώμονες, πρέπει συνεπώς να δοθεί έμφαση στην ταχεία ανίχνευση και την άμυνα.

Μετά την ανίχνευση και την ανάλυση της παραβίασης, είναι απαραίτητη η ταχεία γνωστοποίηση και αναφορά της, ούτως ώστε και άλλοι δημόσιοι και ιδιωτικοί φορείς να λάβουν προληπτικά μέτρα, και οι αρμόδιες αρχές να παράσχουν στήριξη σε εκείνους που επλήγησαν. Πολλοί οργανισμοί είναι απρόθυμοι να αναγνωρίσουν και να γνωστοποιήσουν κυβερνοπεριστατικά[81]. Μεγάλη είναι επίσης η σημασία της έγκαιρης συμμετοχής των αρχών επιβολής του νόμου στην αρχική αντίδραση σε

[80] ‘’Gaining Ground on the Cyber Attacker’’, State of Cyber Resilience, p. 8, 2018

[81] ‘’Three reasons why cyber threat detection is still ineffective’’, διαθέσιμο στο διαδίκτυο: https://www.itpro.co.uk/-security/29061/three-reasons-why-cyber-threat-detection-is-still-ineffective.

πιθανολογούμενα κυβερνοεγκλήματα, και η προληπτική ανταλλαγή πληροφοριών με τις CSIRT.

β. **Προστασία των κρίσιμων υποδομών**

Μεγάλο μέρος των υποδομών ζωτικής σημασίας της ΕΕ λειτουργεί μέσω βιομηχανικών συστημάτων ελέγχου (IIndustrial Control Systems / ICS)[82]. Πολλά από αυτά σχεδιάστηκαν ως αυτόνομα συστήματα, με περιορισμένη δυνατότητα σύνδεσης με τον έξω κόσμο. Η σύνδεση ορισμένων συνιστωσών των ICS στο διαδίκτυο τα έχει καταστήσει περισσότερο ευάλωτα σε εξωτερικές παρεμβάσεις.

Καθώς η βιομηχανία εξακολουθεί να ψηφιοποιείται (διαδικασία γνωστή ως «τέταρτη βιομηχανική επανάσταση»),ο αντίκτυπος ενός περιστατικού μεγάλης κλίμακας σε έναν κλάδο της βιομηχανίας μπορεί να έχει αλυσιδωτές αντιδράσεις σε άλλους. Ο ENISA επεσήμανε τη σημασία της χαρτογράφησης του αντικτύπου της αμοιβαίας εξάρτησης που υπάρχει μεταξύ κρίσιμων τομέων[83]. Η διαδικασία αυτή είναι απαραίτητη προκειμένου να γίνει κατανοητός ο ρυθμός ενδεχόμενης εξάπλωσης ενός περιστατικού και αποτελεί προϋπόθεση για την οργάνωση καλά συντονισμένων αντιδράσεων.

γ. **Προστασία κρίσιμων κοινωνικών λειτουργιών**

Η οδηγία NIS αποσκοπεί στην ενίσχυση της ετοιμότητας σε βασικούς τομείς, κρίσιμους για τις υποδομές ζωτικής σημασίας. Ωστόσο, δεν καλύπτονται όλοι οι τομείς[84], γεγονός που περιορίζει την αποτελεσματικότητα της στρατηγικής. Μία από τις σημαντικότερες πηγές προβληματισμού εν προκειμένω είναι η προστασία της δημοκρατικής ακεραιότητας των εκλογών από παρεμβάσεις στις εκλογικές υποδομές και από την παραπληροφόρηση.

Η πρόσφατη δέσμη μέτρων της Επιτροπής για τις εκλογές περιλάμβανε κάποια μέτρα για την ενίσχυση της κυβερνοασφάλειας των εκλογών, όπως τον καθορισμό εθνικών σημείων επαφής για τον συντονισμό και την ανταλλαγή πληροφοριών κατά το διάστημα πριν από τη διεξαγωγή των εκλογών[85]. Όμως, πρέπει να γίνουν και άλλα πολλά στον τομέα αυτόν ώστε να θωρακιστεί ο θεσμός της δημοκρατίας από κακόβουλους του κυβερνοχώρου.

δ. **Ενίσχυση της αυτονομίας**

---

[82] Συστήματα πληροφορικής που χρησιμοποιούνται για τον έλεγχο διεργασιών σε διάφορους κλάδους, όπως οι υπηρεσίες κοινής ωφελείας, η χημική και μεταποιητική βιομηχανία, η επεξεργασία τροφίμων, τα συστήματα και οι κόμβοι μεταφορών, και οι υπηρεσίες υλικοτεχνικής υποστήριξης.

[83] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ''Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια'', σελ. 55, Μαρ 2019.

[84] Παραδείγματος χάριν, η δημόσια διοίκηση, η χημική και πυρηνική βιομηχανία και οι τομείς της μεταποίησης, της μεταποίησης τροφίμων, του τουρισμού, της εφοδιαστικής και της πολιτικής προστασίας.

[85] European Political Strategy Level, Election Interference in the Digital Age, ''A Collection of Think Pieces from 35 leading practioners and experts'', p. 8.

Η ΕΕ είναι καθαρός εισαγωγέας προϊόντων και υπηρεσιών κυβερνοασφάλειας, γεγονός που αυξάνει τον κίνδυνο τεχνολογικής εξάρτησης από παρόχους από τρίτες χώρες, καθώς και τον κίνδυνο ευπάθειας[86]. Ειδικότερα, το γεγονός αυτό υπονομεύει την ασφάλεια των υποδομών ζωτικής σημασίας της ΕΕ, η οποία στηρίζεται σε πολύπλοκες παγκόσμιες αλυσίδες εφοδιασμού. Ο κίνδυνος εντείνεται στις περιπτώσεις που οι εν λόγω τρίτοι πάροχοι αποκτούν τον έλεγχο ευρωπαϊκών εταιρειών κυβερνοασφάλειας. Τα κράτη μέλη είναι υπεύθυνα για τον έλεγχο των άμεσων ξένων επενδύσεων (ΑΞΕ), και επί του παρόντος δεν υπάρχει μηχανισμός ελέγχου σε επίπεδο ΕΕ[87]. Η ενίσχυση της στρατηγικής αυτονομίας αποτελεί στόχο της συνολικής στρατηγικής της ΕΕ, καθώς και της ανακοίνωσης του 2017 για την ανθεκτικότητα, την αποτροπή και την άμυνα[88].

ε. **<u>Συνεργασία ΕΕ και ΝΑΤΟ</u>**

Για τη δημιουργία ισχυρής κυβερνοανθεκτικότητας απαιτείται συλλογική συνεργασία, συνέργεια και ευρεία προσέγγιση από όλους τους διεθνείς οργανισμούς και φορείς. Στο πλαίσιο αυτό η ΕΕ και το ΝΑΤΟ καθιέρωσαν τη συνεργασία τους στον τομέα της ασφάλειας πριν από δεκαπέντε περίπου χρόνια. Η συνεργασία αυτή σέβεται πλήρως τις αρχές της δημοσιότητας, της διαφάνειας, της συμμετοχικότητας, της αμοιβαιότητας και της αυτονομίας λήψης αποφάσεων της ΕΕ.

Στις 10 Ιουλίου 2018 η ΕΕ και το ΝΑΤΟ υπέγραψαν **νέα κοινή δήλωση** στην οποία καθορίζουν το πλαίσιο ενίσχυσης της συνεργασίας τους σε τομείς, όπως η στρατιωτική κινητικότητα, η ασφάλεια στον κυβερνοχώρο και οι υβριδικές απειλές, με το οποίο θα δρουν μαζί για την καταπολέμηση κοινών απειλών για την ασφάλεια. Λίγο μετά την υπογραφή της νέας κοινής δήλωσης ο πρόεδρος της Ευρωπαϊκής Επιτροπής Ζ.Κ. Γιούνκερ ανέφερε: *«Η Ευρώπη αποφάσισε να αναλάβει την ευθύνη για τη δική της ασφάλεια. Το ΝΑΤΟ είναι θεμέλιος λίθος αυτής της στρατηγικής και εργαζόμαστε για την υλοποίηση των 74 κοινών δράσεων που εκτείνονται από την αντιμετώπιση των υβριδικών επιθέσεων ως την ασφάλεια στον κυβερνοχώρο, την άμυνα και την έρευνα»*[89].

Παρόμοια δήλωση μεταξύ ΕΕ και ΝΑΤΟ είχε ανακοινωθεί το 2016 με μια δέσμη ενεργειών για την κοινή προσπάθεια των δύο οργανισμών στην ανάπτυξη ικανοτήτων

---

[86] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ''Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια'', σελ. 60, Μαρ 2019.

[87] Η πρόταση κανονισμού (COM(2017) 487 final της 13ης Σεπτεμβρίου 2017) για τον έλεγχο των ΑΞΕ, που υποβλήθηκε τον Σεπτέμβριο του 2017, εξετάζεται επί του παρόντος στο πλαίσιο της νομοθετικής διαδικασίας. Ειδικότερα, καλύπτει τις τεχνολογίες καίριας σημασίας, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, την κυβερνοασφάλεια και τις εφαρμογές διπλής χρήσης.

[88] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ''Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια'', σελ. 60, Μαρ 2019.

[89] Ηλεκτρονικός Τύπος: iefimerida, ''Κοινή δήλωση για συνεργασία ΕΕ με ΝΑΤΟ υπέγραψαν Τουσκ, Γιούνκερ και Στολτμπεργκ', διαθέσιμο στο διαδίκτυο: https://www.iefimerida.gr/news/429766/koini-dilosi-gia-synergasia-ee-me-nato-ypegrapsan-toysk-gioynker-stoltenmpergk-eikones.

κυβερνοάμυνας, έρευνας και τεχνολογίας, κατάρτισης, εκπαίδευσης, ασκήσεων και ενσωμάτωσης της κυβερνοδιάστασης στη διαχείριση κρίσεων.

Η σύναψη Τεχνικής Διευθέτησης (Technical Arrangement) μεταξύ της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-EU) και της ομάδας αντιμετώπισης συμβάντων πληροφορικής NCIRC (NATO Computer Incident Response Capability) του ΝΑΤΟ, που υπεγράφη τον Φεβρουάριο του 2016, διευκολύνει την ανταλλαγή τεχνικών πληροφοριών ώστε να βελτιώνεται η πρόληψη, η ανίχνευση και η αντιμετώπιση κυβερνοσυμβάντων που αφορούν αμφότερους τους οργανισμούς.

Στο πλαίσιο ενίσχυσης και διεύρυνσης της κοινής προσπάθειας σε θέματα ασφάλειας εννέα κράτη-μέλη της ΕΕ και του ΝΑΤΟ υπέγραψαν τον Απρίλιο του 2017 τη σύσταση ενός κέντρου έρευνας για την αντιμετώπιση των σύγχρονων υβριδικών απειλών, όπως οι κυβερνοεπιθέσεις, η προπαγάνδα και η παραπληροφόρηση. Το κέντρο έχει την βάση του στο Ελσίνκι και αποτελεί μια ισχυρή ευρωπαϊκή και διατλαντική ανάσχεση των υβριδικών απειλών που το τελευταίο διάστημα εξαπολύονται κυρίως από πλευράς Ρωσίας.

Στις σχετικές προτεραιότητες της συνεργίας ΕΕ και ΝΑΤΟ στον τομέα της κυβερνασφάλειας περιλαμβάνονται η προώθηση της διαλειτουργικότητας μέσω της θέσπισης συνεκτικών απαιτήσεων και προτύπων για την άμυνα στον κυβερνοχώρο και η βελτίωση της εκπαίδευσης του ανθρώπινου δυναμικού με την από κοινού οργάνωση και εκτέλεση ασκήσεων.

Οι εμβληματικές ασκήσεις «Cyber Europe» (επιχειρησιακή) και «Locked Shields» προσελκύουν περισσότερους από 1.000 συμμετέχοντες από περίπου τριάντα κράτη. Οι ασκήσεις αυτές επικεντρώνονται κυρίως στην προστασία και τη διατήρηση υποδομών ζωτικής σημασίας στο πλαίσιο σεναρίων προσομοίωσης επιθέσεων, ενώ οι συντονισμένες στρατηγικές ασκήσεις PACE έχουν ως στόχο την εξέταση της αλληλεπίδρασης και αντίδρασης σε δοκιμασίες της ΕΕ και του ΝΑΤΟ στο πλαίσιο ενός σεναρίου υβριδικής κρίσης.

2. **Δημιουργία μιας ανθεκτικής ευρωπαϊκής κοινωνίας σε κυβερνοπεριστατικά**

α. **Εκτιμήσεις απειλών και κινδύνων μιας κυβερνοεπίθεσης στην ΕΕ**

Απαραίτητη προϋπόθεση για την αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων συνιστά η έγκαιρη προετοιμασία και η αποφυγή του αιφνιδιασμού και του πανικού. Κατά συνέπεια οι τεκμηριωμένες και συνεχείς εκτιμήσεις απειλών και κινδύνων που προέρχονται από πιθανές κυβερνοεπιθέσεις αποτελούν σημαντικά εργαλεία για τους οργανισμούς τόσο του δημόσιου όσο και του ιδιωτικού τομέα.

Η CERT-EU παρέχει στα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ εκθέσεις και ενημερωτικά σημειώματα σχετικά με τους κινδύνους που προέρχονται από κυβερνοαπειλές καθώς και τους στόχους ζωτικής σημασίας που πρέπει να προστατευτούν.

Ωστόσο, δεν υπάρχει τυποποιημένη προσέγγιση για την ταξινόμηση και τη χαρτογράφηση των κυβερνοαπειλών ή για την εκτίμηση των κινδύνων, με αποτέλεσμα το περιεχόμενο των εκτιμήσεων να ποικίλλει σημαντικά. Το γεγονός αυτό δυσχεραίνει την υιοθέτηση μιας συνεκτικής προσέγγισης σε επίπεδο ΕΕ όσον αφορά την κυβερνοασφάλεια[90].

β. **Ενίσχυση της κατάρτισης και των δεξιοτήτων**

Οι κατάλληλες δεξιότητες και η κατάλληλη κατάρτιση, τόσο σχετικά με την πρόληψη συμβάντων ασφάλειας στον κυβερνοχώρο όσο και με την αντιμετώπιση και τον μετριασμό των επιπτώσεών τους, αποτελούν ορισμένα βασικά ζητήματα για την επίτευξη ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο. Ωστόσο, προβλέπεται ότι, έως το 2022 το έλλειμμα σε επαγγελματίες με δεξιότητες στον τομέα της ασφάλειας στον κυβερνοχώρο θα ανέλθει σε 350.000[91].

Σήμερα, ο ENISA, η Ευρωπαϊκή Ομάδα για την Εκπαίδευση και Κατάρτιση στον τομέα του Κυβερνοεγκλήματος και η Ευρωπαϊκή Αστυνομική Ακαδημία διαδραματίζουν σημαντικό ρόλο στον τομέα της εκπαίδευσης και στη δημιουργία ικανοτήτων στον κυβερνοχώρο, μέσω της έκδοσης σχετικών εγχειριδίων και της διοργάνωσης εκπαιδευτικών σεμιναρίων και ασκήσεων.

Ο ENISA έχει επισημάνει ότι οι χρήστες διαδραματίζουν καίριο ρόλο στην αντιμετώπιση των κυβερνοεπιθέσεων και ότι η ενίσχυση των δεξιοτήτων και η αύξηση της εκπαίδευσης και της ενημέρωσης του ανθρώπινου δυναμικού είναι ουσιώδους σημασίας για τη δημιουργία μιας κυβερνοανθεκτικής κοινωνίας. Είτε στο πλαίσιο της εργασίας τους είτε στην προσωπική τους ζωή, όσοι είναι ικανοί να εντοπίζουν τις προειδοποιητικές ενδείξεις και γνωρίζουν τις κατάλληλες τεχνικές, μπορούν να καθυστερήσουν ή να αποτρέψουν κυβερνοεπιθέσεις[92].

Σε επίπεδο θεσμικών οργάνων της ΕΕ, είναι σημαντικό να διασφαλίζεται η ύπαρξη υπαλλήλων με το σωστό μείγμα δεξιοτήτων. Ο ENISA διοργανώνει ετησίως την άσκηση «Cyber Challenge», ενώ το Σεπτέμβριο του 2017 πραγματοποιήθηκε η πρώτη άσκηση σε επίπεδο υπουργών με την ονομασία «EU CYBRID», η οποία

[90] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ''Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια'', σελ. 40, Μαρ 2019.
[91] Ευρωπαϊκή Επιτροπή, ''Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ'', Join (2017) 450, Βρυξέλλες, 13 Σεπ 2017, σελ. 14.
[92] Ευρωπαϊκό Ελεγκτικό Συμβούλιο, ''Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια'', σελ. 41-42, Μαρ 2019.

επικεντρώθηκε στη λήψη στρατηγικών αποφάσεων από τους συμμετέχοντες σε θέματα κυβερνοαπειλών και κυβερνοεγκλημάτων.

γ. **Ενημέρωση και ευαισθητοποίηση**

Είναι συχνό το φαινόμενο οι πολίτες να χρησιμοποιούνται για την πραγματοποίηση επιθέσεων και να γίνονται φορείς διάδοσης της παραπληροφόρησης, καθώς είναι πιθανό να εκτεθούν εν αγνοία τους σε κενά ασφάλειας χρησιμοποιώντας φθηνές και ευρέως διαδεδομένες συσκευές και λογισμικά. Ως εκ τούτου, η ενημέρωση και η ευαισθητοποίηση είναι καίριας σημασίας για την ανάπτυξη της κυβερνοανθεκτικότητας. Ωστόσο αυτό δεν είναι καθόλου ευκαταφρόνητο, δεδομένου ότι είναι δύσκολο για τους μη ειδικούς να κατανοήσουν την πολυπλοκότητα της κυβερνοασφάλειας και τους συναφείς κινδύνους.

Ο «Ευρωπαϊκός μήνας» για την ασφάλεια στον κυβερνοχώρο «European Cyber Security Awareness Month» (ECSM), που διοργανώνεται ετησίως, η Ημέρα Ασφαλέστερου Διαδικτύου και η εκστρατεία «Say No!» της Europol αποτελούν ενδεικτικές προσπάθειες της ΕΕ για την αύξηση της ενημέρωσης και της ευαισθητοποίησης του κοινωνικού ιστού. Βέβαια, στους κόλπους της Επιτροπής αναγνωρίζεται ότι οι προσπάθειες προς την κατεύθυνση αυτή πρέπει να εντατικοποιηθούν, καθώς η στρατηγική για την κυβερνοασφάλεια στο παρελθόν στους τομείς ενημέρωσης και ευαισθητοποίησης των πολιτών και των επιχειρήσεων υπήρξε μερικώς αποτελεσματική[93]. Στο Παράρτημα «Α» απεικονίζονται οι σχετικές απαντήσεις ευρωπαίων πολιτών στην ερώτηση: «Τι γνωρίζεται για τους κινδύνους του κυβερνοεγκλήματος».

δ. **Συνεργασία και ανταλλαγή πληροφοριών με τον ιδιωτικό τομέα**

Απαραίτητη προϋπόθεση για την ενίσχυση της κυβερνοασφάλειας είναι η συνεργασία μεταξύ του δημόσιου και του ιδιωτικού τομέα, κυρίως όσον αφορά την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών. Η εμπιστοσύνη είναι καίριας σημασίας για τη διασυνοριακή ανταλλαγή ευαίσθητων πληροφοριών. Κατά την αξιολόγηση της στρατηγικής για την ασφάλεια στον κυβερνοχώρο το 2017, η Επιτροπή επισήμανε ότι η ανταλλαγή πληροφοριών μεταξύ ιδιωτικών φορέων και μεταξύ δημόσιου και ιδιωτικού τομέα δεν ήταν ακόμη η βέλτιστη δυνατή, λόγω της απουσίας αξιόπιστων μηχανισμών αναφοράς και κινήτρων.

Μια δυναμική απάντηση της ΕΕ στη κατεύθυνση αυτή είναι η σύσταση των Κέντρων Κοινοχρησίας και Ανάλυσης Πληροφοριών (Information Sharing and Analysis Centers / ISAC)[94]. Οι οργανισμοί αυτοί συστάθηκαν για να παρέχουν πλατφόρμες και πόρους για τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ του δημόσιου και του

[93] Ευρωπαϊκή Επιτροπή, ‘’Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ’’, Join (2017) 450, Βρυξέλλες, 13 Σεπ 2017, σελ. 4.
[94] ENISA, διαθέσιμο στο διαδίκτυο: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

ιδιωτικού τομέα, καθώς και για τη συγκέντρωση πληροφοριών σχετικά με τις κυβερνοαπειλές. Στόχος τους είναι η οικοδόμηση εμπιστοσύνης μέσω της ανταλλαγής εμπειριών, γνώσεων και αναλύσεων, ιδίως όσον αφορά τα βαθύτερα αίτια, τα συμβάντα και τις απειλές. Εθνικά και τομεακά ISAC υπάρχουν ήδη σε πολλά κράτη μέλη, αλλά σε ευρωπαϊκό επίπεδο είναι ακόμη σχετικά περιορισμένα[95].

ΣΥΜΠΕΡΑΣΜΑΤΑ

1. Η τεχνολογική πρόοδος της πληροφορικής και η εκθετική αύξηση της χρήσης και της διάστασης του διαδικτύου τα τελευταία είκοσι χρόνια, έφεραν στην επιφάνεια μια νέα μορφή απειλής, τις επιθέσεις μέσω ή εναντίον του Κυβερνοχώρου. Όλα τα κράτη τα οποία εξαρτώνται σε μεγάλο βαθμό από την πληροφοριακή υποδομή και τα δίκτυα υπολογιστών για τη λειτουργία των κρίσιμων υποδομών τους, όπως ο οικονομικός τομέας, η ενέργεια, οι τηλεπικοινωνίες κ.α, αντιμετωπίζουν αυτή την απειλή. Συνεπώς, οι πιθανές επιπτώσεις των κυβερνοεπιθέσεων είναι σοβαρές και κυμαίνονται από τη διατάραξη της καθημερινότητας των πολιτών, μέχρι την υπονόμευση της εθνικής κυριαρχίας ενός κράτους.

2. Η επιλογή των κυβερνοεπιθέσεων φαντάζει ελκυστική, τόσο για κρατικούς, όσο και για μη κρατικούς δρώντες, αφού δεν περιορίζεται από γεωγραφικά όρια. Ακόμα υπάρχει το στοιχείο της απόκρυψης του επιτιθέμενου, ενώ το κόστος απόκτησης τέτοιων κυβερνοδυνατοτήτων είναι σχετικά χαμηλό. Επίσης, τα απαραίτητα εργαλεία (λογισμικό) και πόροι (πληροφορίες) για τη διεξαγωγή κυβερνοεπιθέσεων είναι ευρέως διαδεδομένα στους δρώντες του διεθνούς συστήματος.

3. Ο κυβερνοχώρος είναι το πέμπτο πεδίο επιχειρήσεων, μαζί με την ξηρά, τη θάλασσα, τον αέρα και το διάστημα. Συνεπώς η επιτυχής υλοποίηση των αποστολών και των επιχειρήσεων της ΕΕ εξαρτάται όλο και περισσότερο από την αδιάλειπτη πρόσβαση σε έναν ασφαλή κυβερνοχώρο και προϋποθέτει, ως εκ τούτου, αξιόπιστες και ανθεκτικές επιχειρησιακές ικανότητες στον κυβερνοχώρο.

4. Το νομοθετικό έργο της ΕΕ στο χώρο της κυβερνοασφάλειας δεν έχει ακόμη ολοκληρωθεί. Η ασυνεπής μεταφορά της ευρωπαϊκής νομοθεσίας στο εθνικό δίκαιο των κρατών μελών δημιουργούν δυσκολίες στην εφαρμογή της. Η απουσία ουσιαστικών κριτηρίων αξιολόγησης και στατιστικών δεδομένων μέτρησης του αντικτύπου, των εφαρμοζόμενων πολιτικών και νομοθετικών διατάξεων που υιοθετούνται από την ΕΕ και σχετίζονται με θέματα και περιστατικά του κυβερνοχώρου, επιδρούν αρνητικά στην εξαγωγή αξιόπιστων συμπερασμάτων, ως προς την αποδοτικότητά τους.

[95] Παραδείγματος χάριν, στο ISAC των ευρωπαϊκών χρηματοπιστωτικών ιδρυμάτων συμμετέχουν εκπρόσωποι του χρηματοπιστωτικού τομέα, εθνικές CERT, υπηρεσίες επιβολής του νόμου, ο ENISA, η Europol, η Ευρωπαϊκή Κεντρική Τράπεζα, το Ευρωπαϊκό Συμβούλιο Πληρωμών και η Ευρωπαϊκή Επιτροπή.

5. Οι ταχύτητες με τις οποίες εξελίσσονται οι νέες ψηφιακές τεχνολογίες και αναβαθμίζονται οι καταστροφικές δυνατότητες των κυβερνοεπιθέσεων υπερβαίνουν σε μεγάλο βαθμό τις αντίστοιχες ταχύτητες σχεδιασμού και εφαρμογής της ευρωπαϊκής νομοθεσίας, με αποτέλεσμα, προβλέψεις και διατάξεις του νομοθετικού πλαισίου για την αντιμετώπιση και καταστολή των κυβερνοεπιθέσεων και των κυβερνοεγκλημάτων που διαπράττονται στον κυβερνοχώρο, να θεωρούνται παρωχημένες.

6. Οι δαπάνες της ΕΕ στον τομέα της κυβερνοασφάλειας είναι χαμηλές συγκριτικά με τις εκθετικά αυξανόμενες προκλήσεις και τις απαιτήσεις που διαμορφώνονται στον κυβερνοχώρο. Πολλές φορές αυτές δεν συνοδεύονται από συντονισμένα κυβερνητικά προγράμματα που να ευθυγραμμίζονται με τους στόχους και τα οράματα της ενιαίας ευρωπαϊκής στρατηγικής για ένα ασφαλή και ελεύθερο κυβερνοχώρο. Οι διαπιστωμένες προς το παρόν ελλείψεις ανθρώπινου δυναμικού και χρηματοδοτήσεων, στους επίσημους υπεύθυνους φορείς της ΕΕ για την κυβερνοασφάλεια, δυσχεραίνουν την καθημερινή τους λειτουργικότητα και κατά συνέπεια, ενδέχεται να μην επιτρέψουν την απρόσκοπτη υλοποίηση των φιλόδοξων στόχων της ΕΕ στον τομέα του κυβερνοχώρου.

7. Η ΕΕ έχει τα τελευταία χρόνια καταβάλει μια τεράστια προσπάθεια να βελτιώσει τις ικανότητές της και τους μηχανισμούς της αντίδρασης στις κυβερνοκρίσεις με την υιοθέτηση και εφαρμογή μιας σειράς ενεργειών, όπως η ενίσχυση της συνεργασίας με άλλους διεθνείς οργανισμούς (π.χ ΝΑΤΟ), η προστασία των κρίσιμων υποδομών που διασυνδέονται με τον κυβερνοχώρο και η έγκαιρη ανίχνευση και γνωστοποίηση των κυβερνοεπιθέσεων σε άλλους δημόσιους και ιδιωτικούς φορείς. Ωστόσο, η απουσία τυποποιημένης χαρτογράφησης των κυβερνοαπειλών, η μη ανταγωνιστικότητα των ευρωπαϊκών επιχειρήσεων κυβερνασφάλειας που στην ουσία καθιστούν την ΕΕ εξαρτώμενη από παρόχους τρίτων χωρών, καθώς και η αδυναμία επίτευξης του μέγιστου βαθμού συνεργασίας και ανταλλαγής πληροφοριών και εμπειρογνωσίας είναι μερικές από τις προκλήσεις που η ΕΕ θα πρέπει να δώσει τις δικές της δυναμικές απαντήσεις σύντομα.

8. Η δημιουργία μιας κυβερνοανθεκτικής κοινωνίας είναι μια από τις κύριες προτεραιότητες της στρατηγικής της ΕΕ και απαιτεί συλλογική κα ευρεία προσέγγιση. Η ασφάλεια στον κυβερνοχώρο έχει μια ισχυρή εκπαιδευτική διάσταση καθώς αυτή βασίζεται σε μεγάλο βαθμό στις δεξιότητες των ενδιαφερόμενων ατόμων. Το έλλειμμα σε επαγγελματίες με δεξιότητες στο τομέα της ασφάλειας του κυβερνοχώρου που δραστηριοποιούνται σε ιδιωτικές επιχειρήσεις είναι άκρως ανησυχητικό.

9. Δεδομένου του διασυνοριακού χαρακτήρα των εγκλημάτων στον κυβερνοχώρο, η εντατικοποίηση της ανταλλαγής πληροφοριών μεταξύ των αστυνομικών και δικαστικών αρχών και η ενίσχυση της συνεργασίας μεταξύ των εμπειρογνωμόνων στον τομέα της εγκληματικότητας στον κυβερνοχώρο έχουν καθοριστική σημασία στη διεξαγωγή ουσιαστικών ερευνών και στη λήψη ηλεκτρονικών αποδεικτικών στοιχείων.

10. Η ευαισθητοποίηση και ενημέρωση του κοινού στα θέματα ασφάλειας του κυβερνοχώρου είναι επίσης μια προτεραιότητα της στρατηγικής της ΕΕ για τη δημιουργία μιας ευρωπαϊκής κοινωνίας με ισχυρά αποτρεπτικά ανακλαστικά στις κυβερνοεπιθέσεις. Ο «Ευρωπαϊκός μήνας» για την ασφάλεια στον κυβερνοχώρο που διοργανώνεται ετησίως, η «Ημέρα Ασφαλέστερου Διαδικτύου» και η εκστρατεία «Say No!» της Europol αποτελούν αισιόδοξα μηνύματα προόδου προς αυτή την κατεύθυνση. Όμως, το γεγονός ότι μεγάλη πλειοψηφία των ευρωπαίων πολιτών εξακολουθεί να έχει άγνοια των στοιχειωδών κανόνων της ασφαλούς πλοήγησης στο διαδίκτυο και των κινδύνων που εγκυμονεί η έκθεση προσωπικών τους δεδομένων σε αυτό, καθιστά επιτακτική τη συνέχιση των προσπαθειών της ΕΕ στον τομέα αυτόν.

11. Η σύσταση του Κέντρου Κοινοχρησίας και Ανάλυσης Πληροφοριών αποτελεί μια δυναμική πρωτοβουλία και απάντηση της ΕΕ για την ενίσχυση της συνεργασίας μεταξύ του ιδιωτικού τομέα στη διαμόρφωση κοινής αντίληψης και αντιμετώπισης των απειλών του κυβερνοχώρου. Η ανταλλαγή πληροφοριών και γνώσεων σε μια στέρεη βάση εμπιστοσύνης είναι βέβαιο ότι θα συμβάλει αποφασιστικά στην δημιουργία μιας πιο κυβερνοανθεκτικής κοινωνίας. Ωστόσο, η προσπάθεια αυτή πρέπει να εντατικοποιηθεί κα από πλευράς των κρατών-μελών δεδομένου ότι η προσπάθεια αυτή σε εθνικό επίπεδο είναι πολύ περιορισμένη στην Ευρώπη.

ΠΡΟΤΑΣΕΙΣ

1. Η ΕΕ, ως προς τις προκλήσεις που αντιμετωπίζει στο πολιτικό και νομοθετικό πλαίσιο, προτείνεται να:

α. Θέσει ως καίρια προτεραιότητα την ανάπτυξη καινοτόμων και ευέλικτων διαδικασιών, προκειμένου να διασφαλιστεί ένα πολιτικό και νομικό πλαίσιο προσαρμοσμένο στις σύγχρονες ανάγκες και απαιτήσεις των προκλήσεων που αναδύονται ραγδαία στον κυβερνοχώρο, με στόχο την καλύτερη πρόβλεψη και διαμόρφωση του μέλλοντος.

β. Θεσπίσει ουσιαστικά κριτήρια αξιολόγησης μέτρησης του αντικτύπου των εφαρμοζόμενων πολιτικών και νομοθετικών ρυθμίσεων που υιοθετούνται και εφαρμόζονται από την ΕΕ και σχετίζονται με θέματα και περιστατικά του κυβερνοχώρου.

γ. Δημιουργήσει κατάλληλους φορείς και διαδικασίες τήρησης στατιστικών δεδομένων που θα έχουν καταλυτικό ρόλο στην εξαγωγή αξιόπιστων συμπερασμάτων ως προς την αποτελεσματικότητα της ευρωπαϊκής νομοθεσίας και των εφαρμοζόμενων πολιτικών για θέματα κυβερνασφάλειας.

2. Στον τομέα των δαπανών και χρηματοδοτήσεως των υπεύθυνων φορέων για την ασφάλεια στο κυβερνοχώρο, προτείνεται να:

α. Αυξηθεί το χρηματικό ύψος των διατιθέμενων δαπανών που σχετίζονται με θέματα κυβερνοασφάλειας.

β. Θεσπιστούν διαδικασίες και μηχανισμοί τήρησης συγκεντρωτικών στατιστικών στοιχείων δαπανών και έγκαιρη ένταξη αυτών σε συγκεκριμένα κυβερνητικά προγράμματα που θα είναι εναρμονισμένα με τις κατευθύνσεις της στρατηγικής της ΕΕ στο τομέα ασφάλειας.

3. Για την αντιμετώπιση των ελλείψεων ανθρώπινου δυναμικού, που έχει διαπιστωθεί στους υπεύθυνους φορείς και υπηρεσίες για την κυβερνασφάλεια, προτείνεται:

α. Η ενίσχυση της χρηματοδότησης για την πλήρωση των κενών οργανικών θέσεων.

β. Η οργάνωση διαφημιστικών και ενημερωτικών εκστρατειών για την προσέλκυση εξειδικευμένου προσωπικού από την αγορά εργασίας.

4. Η ΕΕ, στο πλαίσιο αναβάθμισης της αποτρεπτικής ικανότητάς της στις αναδυόμενες κυβερνοαπειλές, προτείνεται να:

α. Αναβαθμίσει τις δυνατότητες ανίχνευσης εισόδου κακόβουλου λογισμικού στις κρίσιμες ψηφιακές υποδομές της.

β. Ενημερώσει τις επιχειρήσεις του ιδιωτικού τομέα ως προς τη σπουδαιότητα της έγκαιρης ανίχνευσης κακόβουλου λογισμικού στα ψηφιακά τους συστήματα για τον περιορισμό των επιπτώσεων και της εξάπλωσης της προσβολής.

γ. Ενθαρρύνει τις ιδιωτικές επιχειρήσεις στη θέσπιση εσωτερικών διαδικασιών αναφοράς και ανίχνευσης κακόβουλου λογισμικού με σκοπό τη γνωστοποίηση της απειλής στους αρμόδιους εμπλεκόμενους φορείς προκειμένου να ληφθούν από αυτούς όλα τα απαραίτητα μέτρα περιορισμού της περαιτέρω εξάπλωσης του κακόβουλου λογισμικού.

δ. Προβεί στη χαρτογράφηση της αμοιβαίας εξάρτησης των κρίσιμων υποδομών της που βασίζονται σε ψηφιακά και αυτόματα συστήματα ελέγχου προκειμένου να γίνει κατανοητός ο ρυθμός της ενδεχόμενης εξάπλωσης ενός κακόβουλου λογισμικού και να εκτιμηθεί η ενδεχόμενη αλληλεπίδραση του συστήματος που θα δεχθεί μια πιθανή κυβερνοεπίθεση με άλλες κρίσιμες υποδομές.

ε. Συνεχίσει τις προσπάθειες εμβάθυνσης της συνεργασίας με το ΝΑΤΟ στους τομείς έρευνας και τεχνολογίας, συμπεριλαμβανομένης της παράλληλης συμμετοχής σε συντονισμένες ασκήσεις και της ενίσχυσης της διαλειτουργικότητας των προτύπων ασφάλειας στον κυβερνοχώρο.

στ. Ενισχύσει τις διαδικασίες ανταλλαγής πληροφοριών μεταξύ των κύριων υπεύθυνων υπηρεσιών για την επιτάχυνση των διαδικασιών εντοπισμού, ανάλυσης και αναφοράς διάπραξης κυβερνοεγκλημάτων, με την αντίστοιχη διάθεση, του απαραίτητου έμψυχου και υλικοτεχνικού εξοπλισμού, στους εμπλεκομένους.

ζ. Αποτρέψει τις επιθέσεις σε κρίσιμες υποδομές και τις παρεμβάσεις στις δημοκρατικές διαδικασίες.

η. Θεσπίσει νομοθετικά τη νόμιμη πρόσβαση των αρχών επιβολής του νόμου σε σχετικές πληροφορίες ώστε να επιτυγχάνεται η επακριβής ταυτοποίηση του χρήστη μιας διεύθυνσης IP και συνεπώς η απόδοση ευθύνης στη περίπτωση διάπραξης κυβερνοεγκλήματος ή κυβερνοεπίθεσης.

5. Η ΕΕ, στο πλαίσιο διαμόρφωσης μιας κυβερνοανθεκτικής κοινωνίας, προτείνεται να:

α. Υποστηρίξει την ενίσχυση της κατάρτισης και των δεξιοτήτων του ανθρώπινου δυναμικού με:

(1) Τη δημιουργία νέων ειδικών προγραμμάτων σπουδών για την ασφάλεια στον κυβερνοχώρο με στόχο τόσο την τυπική κατάρτιση του εργατικού δυναμικού όσο και την εξειδικευμένη κατάρτιση στους επαγγελματίες

(2) Την καθιέρωση ωρών διδασκαλίας, για θέματα απειλών του κυβερνοχώρου και κανόνες ασφαλούς πλοήγησης στο διαδίκτυο, στα διάφορα εκπαιδευτικά ιδρύματα.

(3) Τη θέσπιση διδασκαλίας και απόκτησης ψηφιακών ικανοτήτων για το διδακτικό προσωπικό και τους μαθητές της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης.

(4) Την οργάνωση εκπαιδευτικών σεμιναρίων για την ενημέρωση της κοινωνίας.

β. Ενισχύσει τις προσπάθειες ενημέρωσης και ευαισθητοποίησης της κοινωνίας για τους κινδύνους που κρύβονται στον κυβερνοχώρο με:

(1) Την παρότρυνση των κρατών μελών να θέσουν ως προτεραιότητα την ευαισθητοποίηση σχετικά με τον κυβερνοχώρο οργανώνοντας εκστρατείες και σεμινάρια που θα απευθύνονται σε σχολεία, πανεπιστήμια, την επιχειρηματική κοινότητα και σε ερευνητικούς φορείς.

(2) Την ενημέρωση του κοινωνικού ιστού των κινδύνων που εγκυμονούν οι διαδικτυακές εκστρατείες παραπληροφόρησης και οι ψευδείς ειδήσεις

στα μέσα κοινωνικής δικτύωσης που αποσκοπούν ειδικά στην υπονόμευση των δημοκρατικών διαδικασιών και των ευρωπαϊκών αξιών.

(3) Την οργάνωση εκπαιδευτικών δραστηριοτήτων με τη συμμετοχή μαθητών, δημόσιων και ιδιωτικών επιχειρήσεων για θέματα που σχετίζονται με τους τρόπους ασφαλούς περιήγησης και χρήσης των διαφόρων μέσων στο διαδίκτυο.

γ. Προάγει συνεργασία και ανταλλαγή πληροφοριών με τον ιδιωτικό τομέα με:

(1) Δημιουργία ομάδων στις οποίες οι επιχειρήσεις και οι καταναλωτές θα μπορούν να αναφέρουν περιστατικά παραβίασης της ασφάλειας στον κυβερνοχώρο.

(2) Παρότρυνση των κρατών μελών να ενδυναμώσουν το θεσμό των Κέντρων Κοινοχρησίας και Ανάλυσης Πληροφοριών (ISAC) στο εσωτερικό τους με στόχο την οικοδόμηση εμπιστοσύνης, μεταξύ του δημόσιου και του ιδιωτικού τομέα, μέσω της ανταλλαγής εμπειριών, γνώσεων και αναλύσεων συμβάντων που σχετίζονται με την κυβερνοασφάλεια.

ΥΠΟΓΡΑΦΗ

Παναγιώτης Νιάκαρης

Σχης (ΔΒ)

ΠΑΡΑΡΤΗΜΑΤΑ

«Α» Στοιχεία Ενημερότητας Πολιτών για το Κυβερνοέγκλημα.

«Β» Αύξηση της Εξάπλωσης Κακόβουλου Λογισμικού.

«Γ» Στατιστικά Κυβερνοεπιθέσεων σε Κρίσιμες Υποδομές.

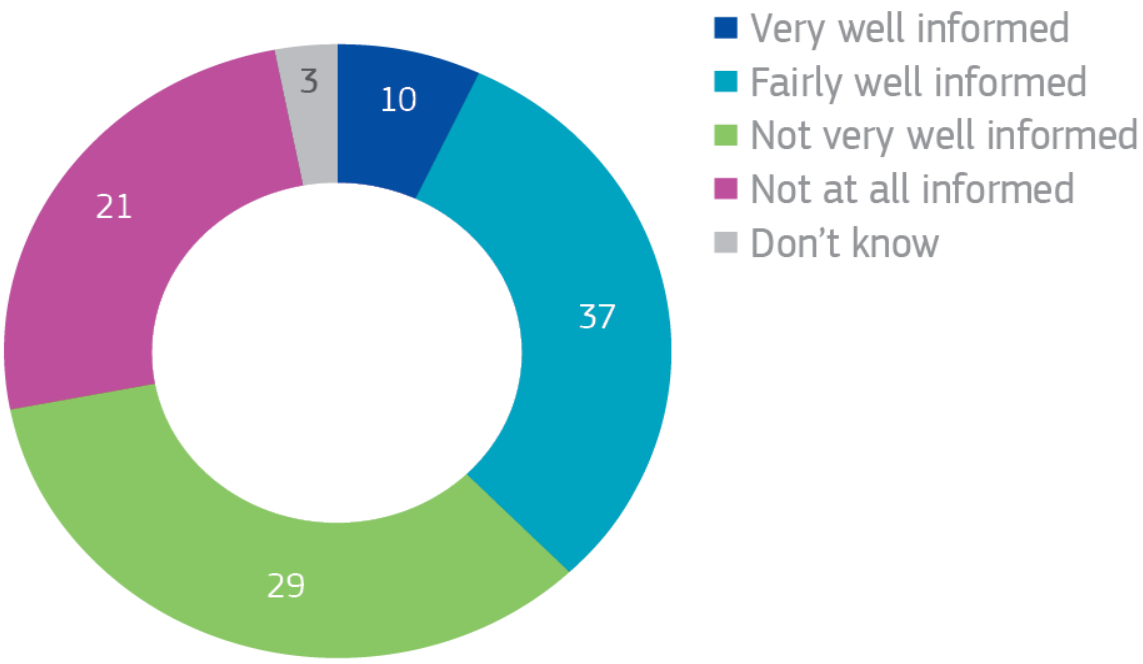
«Δ» Κίνητρα των Επιθέσεων στον Κυβερνοχώρο.

«Ε» Βιβλιογραφία.

ΣΧΟΛΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
71η ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ
ΚΑΝΟΝΙΚΗΣ ΦΟΙΤΗΣΗΣ
Αθήνα, 23 Απρ 2019

ΠΑΡΑΡΤΗΜΑ «Α» ΣΤΗΝ
ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ
ΤΟΥ ΣΧΗ (ΔΒ) ΠΑΝΑΓΙΩΤΗ ΝΙΑΚΑΡΗ

ΣΤΟΙΧΕΙΑ ΕΝΗΜΕΡΟΤΗΤΑΣ ΠΟΛΙΤΩΝ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ



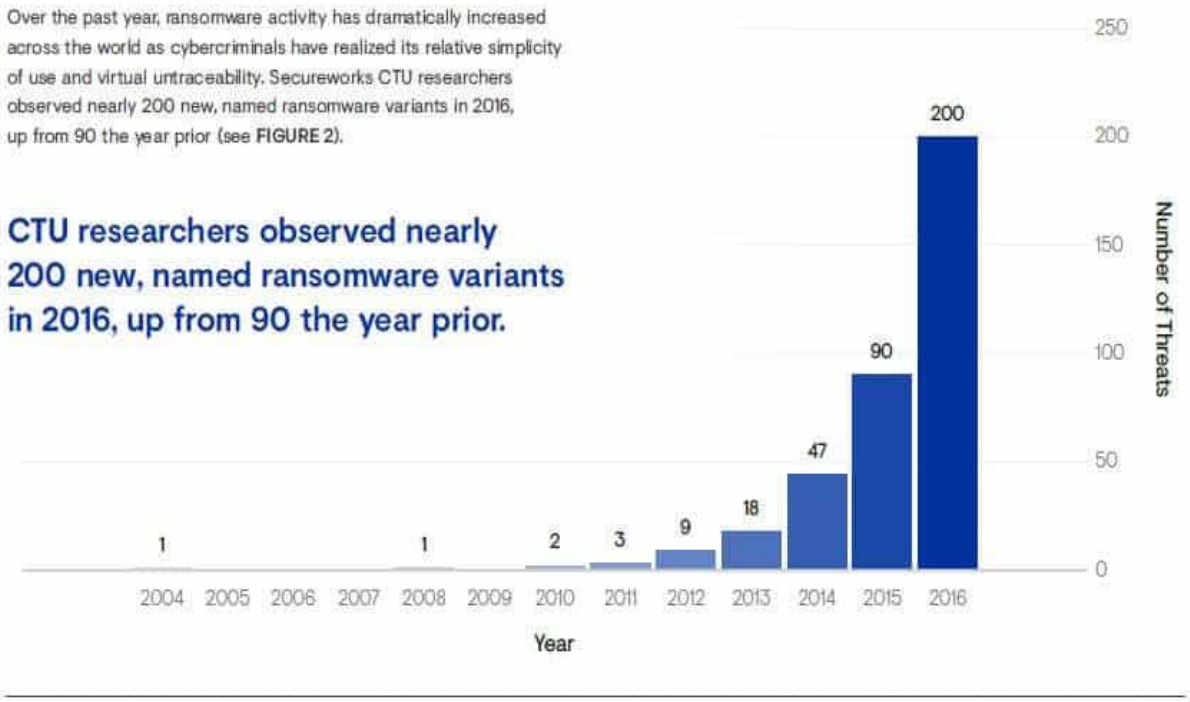
Εικόνα «1» Αφορά τις απαντήσεις ευρωπαίων πολιτών στην ερώτηση σε ποιο βαθμό είναι ενημερωμένοι για το κυβερνοέγκλημα.[96]

[96] Building an effective European Cyber shield, διαθέσιμο στο διαδίκτυο: https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

ΣΧΟΛΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
71η ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ
ΚΑΝΟΝΙΚΗΣ ΦΟΙΤΗΣΗΣ
Αθήνα, 23 Απρ 2019

ΠΑΡΑΡΤΗΜΑ «Β» ΣΤΗΝ
ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ
ΤΟΥ ΣΧΗ (ΔΒ) ΠΑΝΑΓΙΩΤΗ ΝΙΑΚΑΡΗ

ΑΥΞΗΣΗ ΤΗΣ ΕΞΑΠΛΩΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ



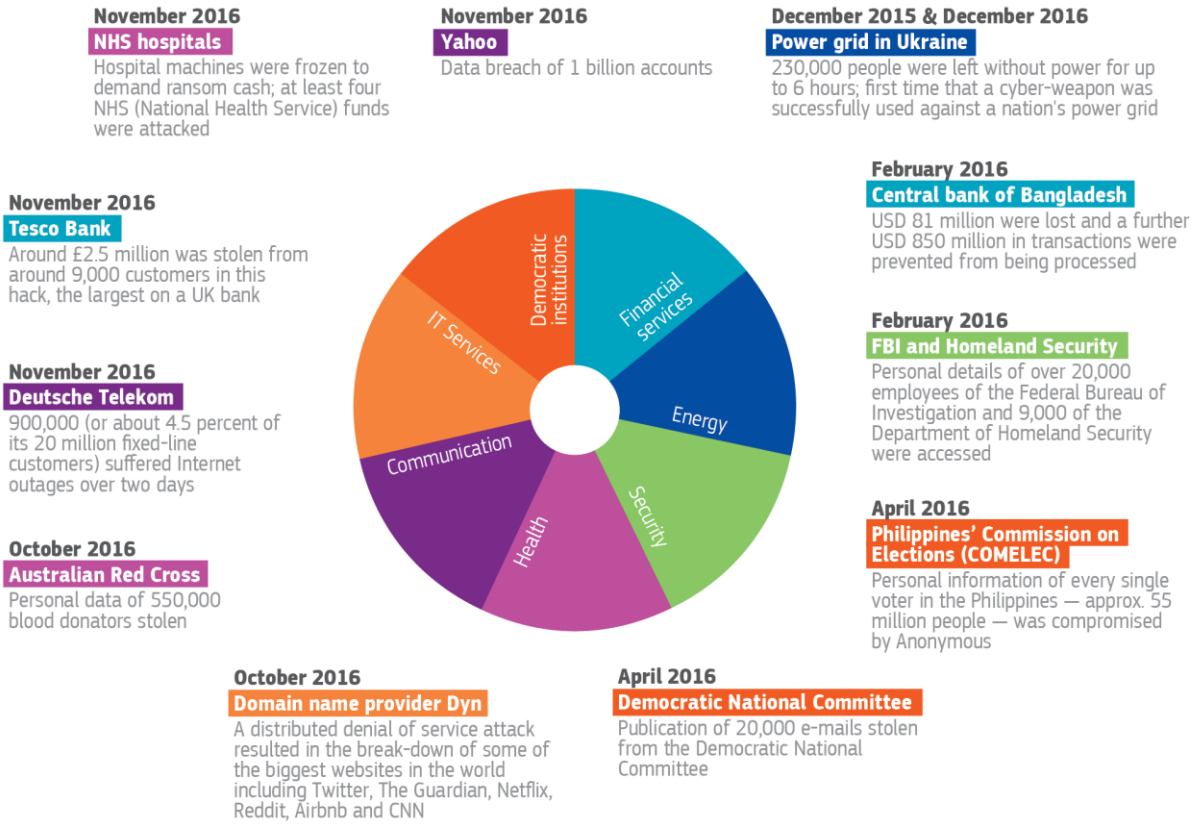
Εικόνα «2» Το διάγραμμα δείχνει την εκθετική αύξηση των κυβερνοόπλων[97].

[97] Cybercrime and Cybersecurity Statistics & Trends, διαθέσιμο στο διαδίκτυο: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

ΣΧΟΛΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
71η ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ
ΚΑΝΟΝΙΚΗΣ ΦΟΙΤΗΣΗΣ
Αθήνα, 23 Απρ 2019

ΠΑΡΑΡΤΗΜΑ «Γ» ΣΤΗΝ
ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ
ΤΟΥ ΣΧΗ (ΔΒ) ΠΑΝΑΓΙΩΤΗ ΝΙΑΚΑΡΗ

ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΣΕ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ



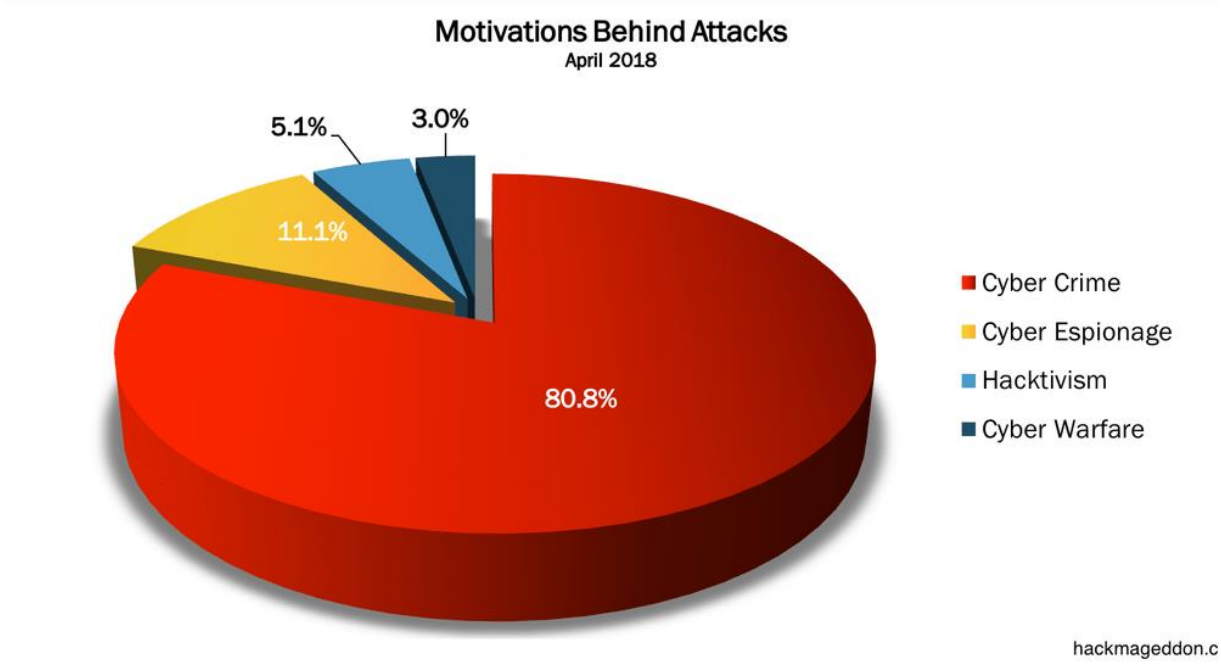
Εικόνα «3» Το σχεδιάγραμμα μας δείχνει τις επιθέσεις κακόβουλου λογισμικού στις κρίσιμες υποδομές[98].

[98] Building an effective European Cyber shield, διαθέσιμο στο διαδίκτυο: https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

ΣΧΟΛΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
71η ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ
ΚΑΝΟΝΙΚΗΣ ΦΟΙΤΗΣΗΣ
Αθήνα, 23 Απρ 2019

ΠΑΡΑΡΤΗΜΑ «Δ» ΣΤΗΝ
ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ
ΤΟΥ ΣΧΗ (ΔΒ) ΠΑΝΑΓΙΩΤΗ ΝΙΑΚΑΡΗ

ΚΙΝΗΤΡΑ ΤΩΝ ΕΠΙΘΕΣΕΩΝ ΚΥΒΕΡΝΟΧΩΡΟ



Εικόνα «4» Τα κίνητρα των κυβερνοεπιθέσεων[99].

[99] Διαθέσιμο στο διαδίκτυο: https://www.hackmageddon.com/2018/05/29/april-2018-cyber-attacks-timeline/.

ΣΧΟΛΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
71η ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ
ΚΑΝΟΝΙΚΗΣ ΦΟΙΤΗΣΗΣ
Αθήνα, 23 Απρ 2019

ΠΑΡΑΡΤΗΜΑ «Ε» ΣΤΗΝ
ΑΤΟΜΙΚΗ ΔΙΑΤΡΙΒΗ
ΤΟΥ ΣΧΗ (ΔΒ) ΠΑΝΑΓΙΩΤΗ ΝΙΑΚΑΡΗ

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

1. Κοππά Μαριλένα, «Η Κοινή Πολιτική Άμυνας και Ασφάλειας – Η Ιστορία, οι θεσμοί, οι στρατηγικές», Εκδόσεις Πατάκη, Ιούνιος 2017, σελ. 193.

ΞΕΝΟΓΛΩΣΣΗ

1. Augustine P. Zachary, «Cyber Neutrality: A Textual Analysis of Traditional Jus in. Bello Neutrality Rules through a Purpose - Based Lens», (2014) 71 A.F.L. Rev.

2. DeLuca Christopher D., «The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors», (2013) 3 No. 9 Pace Int'l L. Rev. Online Companion 278.

3. Denning, P. J., & Denning, D. (2010). The Profession of IT, Discussing Cyber Attack.

4. Gaul Allison, «Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare», (2013) Syracuse J. Sci. & Tech. L. Rep.

5. Geiss Robin, «Cyber Warfare: Implications for Non-International Armed Conflicts» (2013) Int'l L. Stud.

6. Gervais Michael, «Cyber Attacks and the Laws of War», (2012) Berkeley J. Int'l Law.

7. Grosswald Levi, «Cyberattack Attribution Matters Under Article 51 of the U.N. Charter», (2011) 36 Brook. J. Int'l L.

8. Halberstam Manny, «Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks», (2013) 46 Geo. Wash. Int'l L. Rev.

9. Handler Gosnell Stephanie, «The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare», (2012) 48 Stan. J. Int'l L.

10. Hathaway A. Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, «The Law of Cyber-Attack» (2012) 100 Calif. L. Rev.

11. Hoisington Matthew, «Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense», (2009) 32 B.C. Int'l & Comp. L. Rev.

12. Kamal Ahmad, UN Report: «Law of Cyber Space», Council of Foreign Relations, 2015.

13. Kundur, D., Feng, X., Liu, S., Zourntos, T., & Butler-Purry, K. L. (2010, October). «Towards a framework for cyber-attack impact analysis of the electric smart grid». In 2010 First IEEE International Conference on Smart Grid Communications (pp. 244-249). IEEE.

14. Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber-attack. Industrial Control Systems.

Mudrinich Major Erik M., 'Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem (2012) Air Force Law Review 68 A.F. L. Rev.

15. Nguyen Reese, «Navigating Jus Ad Bellum in the Age of Cyber Warfare» (2013) 101 Cal. L. Rev. 1079.

16. Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). «Attack detection and identification in cyber-physical systems», IEEE Transactions on Automatic Control, 58(11).

17. Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2014, July), «A cyber-attack evaluation methodology». In Proc. of the 13th European Conference on Cyber Warfare and Security.

18. Roberts Shaun, «Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors», (2014) 41 N. Ky. L. Rev. 535.

19. Sklerov Mathew, «Solving the dilemma of state responses to cyberattacks: A justification for the use of active defences against states who neglect their duty to prevent», Military Law Review, Fall 2009.

20. Solce Natasha, «The battlefield of Cyberspace: The inevitable new military branch», Albany Law Journal of Science and Technology, 2008.

21. Stockburger Z. Peter, «Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum» (2016) 31 Am. U. Int'l L. Rev. 545.

22. Trevor Thompson, Terrorizing the technological neighborhood watch: The allienation and deterrence of the 'white hats' under the CFFA, Florida, Spring 2009.

23. Wampler A. Kim, B., Goppert, J., Hwang, I., & Aldridge, H. (2012) «Cyber-attack vulnerabilities analysis for unmanned aerial vehicles» in Infotech Aerospace 2012.

24. Williamson, C.S.C From fourth generation warfare to Hybrid war, Strategy research project, Carlisle Barracks, US Army College.

25. Yorke Claire, «Cybersecurity and Society», December 2010, Vol.66, No 12.

ΑΡΘΡΑ - ΚΑΝΟΝΙΣΜΟΙ ΕΕ

ΕΛΛΗΝΙΚΑ

1. Ευρωπαϊκή Επιτροπή, «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ», Join (2017) 450, Βρυξέλλες, 13 Σεπ 2017.

2. Ευρωπαϊκό Ελεγκτικό Συμβούλιο, «Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνασφάλεια», Μαρ 2019.

3. Συμβούλιο της ΕΕ, «Πλαίσιο της Πολιτικής της ΕΕ για την κυβερνοάμυνα» (όπως επικαιροποίηθηκε το 2018, 14413/18, Βρυξέλλες, 19 Νοεμβρίου 2018.

4. Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου, «Κατάσταση της Ένωσης 2017 – Κυβερνοασφάλεια: Η Επιτροπή αναβαθμίζει την απόκριση της ΕΕ στις κυβερνοεπιθέσεις», Βρυξέλλες, 19 Σεπτεμβρίου 2017.

5. Συμβούλιο της ΕΕ, «Η ΕΕ συγκεντρώνει και δικτυώνει την εμπειρογνωσία της στον τομέα της κυβερνοασφάλειας», Δελτίο Τύπου της 13 Μαρ 2019.

6. Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, «Transatlantic Cyber-Insecurity and Cybercrime», PE 603.948, Δεκέμβριος 2017.

ΞΕΝΟΓΛΩΣΣΑ

1. Cybersecurity «Strategy of the European Unio», JOIN (2013) 1 final, Brussels, 7.2.2013.

2. European Commission, «The European Agenda on Securit», COM (2015) 185 final, Strasbourg, 28.4.2015.

3. European Commission, «Joint Framework on Countering Hybrid Threats», 6.4.2016 JOIN (2016) 18 final, Brussels.

4. European Commission, «Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027», SWD (2018) 305 final, 06-06-2018.

5. European Commission, «A Digital Single Market Strategy for Europe», COM (2015) 192 final, Brussels, 6.5.2015

6. European Political Strategy Level, Election Interference in the Digital Age, «A Collection of Think Pieces from 35 leading practioners and experts».

7. European Union, «A Global Strategy for the European Union's Foreign and Security Policy», June 2016.

8. Sheridan Michael, «China's Net Warriors Take on West», Sunday Times, 01 September 2001.

ΜΕΛΕΤΕΣ

1. «Gaining Ground on the Cyber Attacker», State of Cyber Resilience, 2018

2. International Law Association Study Group on the Conduct of Hostilities in the 21st Century, «The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare», (2017) 93 Int'l L. Stud.

3. Raiyn, J. (2014). «A survey of cyber-attack detection strategies», International Journal of Security and Its Applications, 8(1).

4. «Study on the Evaluation of the European Union Agency for Network and Information Security», This study was carried out for the European Commission by Karin Attström, Vanessa Ludden, Franziska Lessmann, 2017.

5. Tikk Eneken, Kadri Kaska, Liis Vihul, «International Cyber Incidents: Legal Considerations» (Cooperative Cyber Defense Centre of Excellence 2010).

ΔΙΑΔΙΚΤΥΟ

1. Λιαρόπουλος Ανδρέας, Κυβερνοπόλεμος: «Το νέο στρατηγικό όπλο», διαθέσιμο στο διαδίκτυο: https://www.onalert.gr/uncategorized/kubernopolemos-to-neo-strathgiko-oplo/128648.

2. Υπτγου ε.α Μαυρόπουλου Παναγιώτη, «Κυβερνοπόλεμος και Εθνική Στρατηγική», διαθέσιμο στην ιστοσελίδα: http://www.geetha.mil.gr/media/1.vima-ell-strat-skepsis/kuvernopolemos.pdf.

3. Σακκά Ιωάννη, «Ο Κυβερνοπόλεμος», 04 Οκτ 2018, διαδικτυακή πηγή: https://www.ilioupoligiaolous.gr/article.php?id=22426.

4. Σιδέρης Σωτήρης, ''Κυβερνοπόλεμος ο νέος παγκόσμιος εφιάλτης και ποια είναι η νέα δύναμη πυρός", διαθέσιμο στο διαδίκτυο: https://www.militaire.gr/.

5. Ηλεκτρονικός τύπος «Το ΒΗΜΑ», ''Και κυβερνοπόλεμος στην περιοχή του Καυκάσου'', άρθρο του Γ. Γιανναράκη, διαθέσιμο στο διαδίκτυο: https://www.-tovima.gr/2008/08/14/archive/kai-kybernopolemos-stin-perioxi-toy-kaykasoy/

6. Ηλεκτρονικός τύπος «ΤΟ ΒΗΜΑ», Gordon Michael R, «Η νέα, τριπλή στρατηγική Πούτιν στην Ουκρανία», Απρ 2014, διαθέσιμο στο διαδίκτυο: https://www.tovima.gr/2014/04/22/world/i-nea-tripli-stratigiki-poytin-stin-oykrania/.

7. Ηλεκτρονικός τύπος «ΤΟ ΒΗΜΑ», ‘’Τα πυρηνικά εργοστάσια «ευάλωτα» σε χάκινγκ’’, Πρατικάκης Βαγγέλης, διαθέσιμο στο διαδίκτυο: https://www.tovima.gr-/2015/10/05/science/ta-pyrinika-ergostasia-eyalwta-se-xakingk/

8. Ηλεκτρονικός Τύπος: iefimerida, ‘’Κοινή δήλωση για συνεργασία ΕΕ με ΝΑΤΟ υπέγραψαν Τουσκ, Γιούνκερ και Στολτμπεργκ’’, διαθέσιμο στο διαδίκτυο: https://www.iefimerida.gr/news/429766/koini-dilosi-gia-synergasia-ee-me-nato-ypegrapsan-toysk-gioynker-stoltenmpergk-eikones.

9. Άρθρο της Εφημερίδας Καθημερινή, Τα νέα «όπλα» στα χέρια των χάκερς, 13 Αυγούστου 2018, διαθέσιμο στο διαδίκτυο: http://www.kathimerini.gr/979742/article-/texnologia/diadiktyo/ta-nea-opla-sta-xeria-twn-xaker.

10. Sui-Lee Wee, Alexei Oreskovic, «Google reveals Gmail hacking, says likely from China» Reuters, διαθέσιμο στην Ιστοσελίδα: http://www.reuters.com/article/us-google-hacking-idUSTRE7506U320110602, 06 Μαρ 2019.

11. PC Security, «Τι είναι το κακόβουλο λογισμικό», 4 Φεβ 19, διαθέσιμο στο: https://pcsecurity.gr/kakovoulo-logismiko-malware.

12. Συμπεράσματα του Ευρωπαϊκού Συμβουλίου, διαθέσιμο στο διαδίκτυο: https://www.consilium.europa.eu/media/23968/22-23-euco-final-conclusions-el.pdf, 23 Μαρ. 2017.

13. Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου, «Η Επιτροπή αναβαθμίζει την απόκριση της ΕΕ στις κυβερνοεπιθέσεις», 19 Σεπτεμβρίου 2019, διαθέσιμο στο διαδίκτυο: http://europa.eu/rapid/press-release_IP-17-3193_el.htm.

14. Europol’s Serious and Organised Crime Threat Assessment 2017, διαθέσιμο στο διαδίκτυο: https://www.europol.europa.eu/-activities-services/main-reports/eu-ropean-union-serious-and-organised-crime-threat-assessment-2017.

15. «Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα», διαθέσιμο στο διαδίκτυο: https://www.taxheaven.gr/laws/circular-/view-/id/28194.

16. ENISA, διαθέσιμο στο διαδίκτυο: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

17. Αρθρο της Εφημερίδας Καθημερινή, Τα νέα «όπλα» στα χέρια των χάκερ, Αυγούστου 2018, διαθέσιμο στο διαδίκτυο: http://www.kathimerini.gr/979742-/article/texnologia/diadiktyo/ta-nea-opla-sta-xeria-twn-xaker.

18. «Three reasons why cyber threat detection is still ineffective», διαθέσιμο στο διαδίκτυο: https://www.itpro.co.uk/-security/29061/three-reasons-why-cyber-threat-detection-is-still-ineffective.

19. Building an effective European Cyber shield, διαθέσιμο στο διαδίκτυο: https://ec.-europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.