ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ & ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΙΣ «ΔΙΕΘΝΕΙΣ & ΕΥΡΩΠΑΪΚΕΣ ΣΠΟΥΔΕΣ»

«Σύγχρονες προκλήσεις ασφάλειας στον κυβερνοχώρο. Οι Ευρωπαϊκές πολιτικές αντιμετώπισης».

Ασαρίδου Νικολέτα

(ΑΜ:17901)

Μεταπτυχιακή Διπλωματική εργασία που κατατίθεται ως μέρος των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών στις Διεθνείς & Ευρωπαϊκές Σπουδές

Επιβλέπων Καθηγητής: κ. Τσάκωνας Παναγιώτης

Αθήνα

ΣΕΠΤΕΜΒΡΙΟΣ 2018

Ευχαριστίες.

Η συγγραφή μίας μεγάλης έκτασης εργασίας απαιτεί συστηματική μελέτη για την εξεύρεση, ανάγνωση, ανάλυση και αξιοποίηση πρωτογενών και δευτερογενών πηγών. Αποτελεί, όμως, και μία μοναδική ευκαιρία για τον φοιτητή να επιχειρήσει να συνθέσει δεδομένα και να εφαρμόσει τη θεωρία που διδάχτηκε σε πρακτικό επίπεδο.

Η παρούσα εργασία είχε αρκετές απαιτήσεις, καθώς μέσω αυτής μου δόθηκε η ευκαιρία να κατανοήσω το περιεχόμενο και τη σπουδαιότητα του εν λόγω επίκαιρου και μη εξαντλητικού θέματος, δίδοντάς μου τη δυνατότητα για περαιτέρω έρευνα και μελέτη πάνω στα σύγχρονα ζητήματα κυβερνοασφάλειας. Παράλληλα, υπήρξε η δυνατότητα εκ μέρους της συντάκτριας να αποτιμήσει το αν και σε ποιο βαθμό κατείχε τις απαραίτητες γνώσεις και ικανότητες ώστε φέρει εις πέρας το έργο που ανέλαβε.

Κατά συνέπεια, η παρούσα μελέτη αποδείχθηκε μία εξαιρετική ευκαιρία διεύρυνσης των γνωστικών οριζόντων, μέσω του εμπλουτισμού των υφισταμένων γνώσεων με δημιουργικές ιδέες στον τομέα των σύγχρονων ζητημάτων ασφαλείας.

Η διαδικασία συλλογής υλικού αποδείχθηκε μία σύνθετη διαδικασία. Παρότι υπήρχε ποικίλο υλικό διαθέσιμο στη βιβλιοθήκη, απαιτήθηκε περαιτέρω έρευνα στο διαδίκτυο, καθώς οι πηγές έπρεπε να είναι σύγχρονες και οι πληροφορίες να αφορούν τις τελευταίες εξελίξεις στον τομέα. Άλλωστε, επιθυμητός στόχος της συντάκτριας αποτέλεσε η συνεισφορά στην επιστήμη με νέες οπτικές, μέσω της προσωπικής εκτίμησης και όχι η απλή παράθεση και περιγραφή έργων τρίτων.

Αξίζει να επισημανθεί ότι η υποστήριξη του επιβλέποντος της εργασίας αποδείχθηκε καίρια, από την απλή καθοδήγηση στα πρώτα βήματα του σχεδιασμού της δομής της παρούσας μελέτης, μέχρι την παρότρυνση να εκφραστεί η προσωπική άποψη της γράφουσας.

ΠΕΡΙΛΗΨΗ

Η ασφάλεια στον κυβερνοχώρο και η κυβερνοισχύς αποτελούν από τα πιο σύγχρονα αντικείμενα μελέτης των ανθρωπιστικών και όχι μόνο επιστημών. Η διεθνής πολιτική πλέον, δεν ασκείται μόνο σε κλειστές αίθουσες και η θεωρία θα πρέπει να είναι σε θέση να συλλέγει και επεξεργάζεται τα δεδομένα και τις πληροφορίες, προκειμένου να ερμηνεύει τα σύγχρονα φαινόμενα. Οι σύγχρονες προκλήσεις που καλούνται να διαχειριστούν τα κράτη, εκδηλώνονται τόσο στο «φυσικό» περιβάλλον τους, όσο και στον κυβερνοχώρο, ως άμεση απόρροια της παγκοσμιοποιημένης κοινωνίας, γεγονός που επιβάλλει την πολύπλευρη προσέγγισή τους.

Η παρούσα μελέτη επιχειρεί να εξετάσει τα πλέον καίρια ζητήματα στον τομέα της διεθνούς πολιτικής και των διεθνών σχέσεων, εστιάζοντας σε μία όσο το δυνατόν πιο διεξοδική ανάλυση του ζητήματος των κυβερνοαπειλών και της κυβερνοτρομοκρατίας στην Ευρωπαϊκή Ένωση. Επιπροσθέτως, αντικείμενο επεξεργασίας θα αποτελέσει και η επίδραση των προαναφερθεισών απειλών στην κυβερνοισχύ της τελευταίας. Θα εξεταστούν βασικές έννοιες, ενώ παράλληλα θα αναλυθεί η έννοια της κυβερνοαπειλής και ο τρόπος με τον οποίο αυτή εκδηλώνεται στο σκοτεινό δίκτυο, ενώ τέλος, θα περιγραφεί το υφιστάμενο δικαιικό πλαίσιο σχετικά με την πρόληψη και αντιμετώπιση του κυβερνοεγκλήματος.

Λέξεις κλειδιά:

Διαδίκτυο, κυβερνοισχύς, κυβερνοαπειλές, κυβερνοασφάλεια, darkweb, ΕΕ.

ABSTRACT

Cyber security and cybercrime are among the most modern subjects of study of humanities, and not only, science. International politics is no longer practiced only in closed rooms, and theory should be able to collect and process the available data and information to explain the contemporary phenomena. The modern challenges facing states are manifested both in their "physical" state of and in cyberspace, as a direct result of globalized society, which imposes a multi-faceted approach.

This study attempts to address the most crucial issues in the field of international politics and international relations by focusing on a thorough analysis of the issue of cyber-threats and cyber-terrorism in the European Union. In addition, the effect of the aforementioned threats on cyberpower of the European Union will be studied. Key concepts will be examined, and the analysis will emphasize on what cyber threats and how they appear in the dark network and how the legal framework is developed to prevent and tackle cybercrime.

Keywords:

Internet, cybercrime, cyber threats, cyber-security, dark web, EU.

Περιεχόμενα

Ευχαριστίες. ... 2
ΠΕΡΙΛΗΨΗ ... 3
ABSTRACT ... 4
Κυριότεροι όροι και αντιστοιχία με αγγλική ορολογία ... 7
ΕΙΣΑΓΩΓΗ ... 8
ΚΕΦΑΛΑΙΟ 1 ... 10
ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΘΕΩΡΗΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ... 10
1.1. Βασικές έννοιες και ορισμοί. ... 10
1.2. Θεωρητική προσέγγιση. ... 12
ΚΕΦΑΛΑΙΟ 2 ... 15
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΕΙΛΕΣ ... 15
2.1. Dark web και κυβερνοασφάλεια. ... 15
2.2. «Κυβερνοτρομοκρατία»- μία διεθνής απειλή. ... 17
ΚΕΦΑΛΑΙΟ 3 ... 20
ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ... 20
3.1. Η νομική διάσταση του προβλήματος. ... 20
3.2. ΕΕ και κυβερνοασφάλεια. ... 21
3.3. Συνεργασίες και συνέργειες της ΕΕ. ... 27
3.4. Κυβερνοασφάλεια στην Ελλάδα. ... 31
ΚΕΦΑΛΑΙΟ 4 ... 34
ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΚΡΙΤΙΚΗ ... 34
4.1. Αποτίμηση της ερευνητικής διαδικασίας. ... 34
4.2. Αξιολόγηση της στρατηγικής της ΕΕ. ... 35
ΒΙΒΛΙΟΓΡΑΦΙΑ ΚΑΙ ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ ... 43

Πίνακας συντομεύσεων και ακρωνυμίων

BEREC	Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες
CIA	Central Intelligence Agency
IoT	Internet of Things
Δλδ.	Δηλαδή
ΕΑΑ	Οργανισμός της Ευρωπαϊκής Ένωσης για την Κατάρτιση στον Τομέα της Επιβολής του Νόμου
EASA	Ευρωπαϊκός Οργανισμό Ασφάλειας της Αεροπορίας –
ΕΕ	Ευρωπαϊκή Ένωση
EU Lisa	Ευρωπαϊκός Οργανισμό για τη Λειτουργική Διαχείριση Μεγάλων Πληροφοριακών Συστημάτων στον Χώρο της Ελευθερίας, Ασφάλειας και Δικαιοσύνης
ENISA	Ευρωπαϊκός Οργανισμός για την Ασφάλεια των Δικτύων
ΕΟΚ	Ευρωπαϊκή Οικονομική Ένωση
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΚΕΠΠΑ	Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας
Κλπ.	Και λοιπά
Λ.χ.	Λόγου χάρη
ΝΑΤΟ	Οργανισμός Βορειοατλαντικού Συμφώνου
ΟΑΣΕ	Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη

Κυριότεροι όροι και αντιστοιχία με αγγλική ορολογία

Διαδίκτυο	Internet
Διαδίκτυο των πραγμάτων (δεν μεταφράζεται πλήρως στα ελληνικά/δεν υπάρχει συμφωνία ως προς την απόδοση του όρου)	Internet of things
Ισχύς	Power
Κυβερνό-	Cyber-
Κυβερνοαπειλή	Cyberthreat
Κυβερνοασφάλεια	Cybersecurity
Κυβερνοισχύς	Cyberpower
Κυβερνοτρομοκρατία	Cyberterrorism
Κυβερνοχώρος	Cyberspace
Ρητορική μίσους	Hate speech
Σκοτεινό δίκτυο	Dark web
Φονταμενταλισμός	Fundamentalism
Ψηφιακός	Digital

ΕΙΣΑΓΩΓΗ

Η ραγδαία τεχνολογική εξέλιξη οδήγησε στην ανάδειξη της κυβερνοασφάλειας ως ένα σύγχρονο, δυναμικό και διαρκώς εξελισσόμενο αντικείμενο μελέτης. Ταυτόχρονα, η ασφάλεια στο διαδικτυακό περιβάλλον είναι απαραίτητη προϋπόθεση για την καλή λειτουργία των θεσμών και την προστασία της οικονομίας, της κοινωνίας και του πολιτισμού ενός κράτους.

Οι λόγοι για τους οποίους η κυβερνοασφάλεια αποτελεί, πλέον, προτεραιότητα είναι πολλοί. Συγκεκριμένα, μεγάλο μέρος των συναλλαγών στις μέρες μας λαμβάνει χώρα μέσω της χρήσης διαδικτυακών υπηρεσιών, ενώ πληθώρα φορέων χρησιμοποιούν το διαδίκτυο για τις καθημερινές λειτουργίες τους. Εκτός αυτού, οι καθημερινές επικοινωνίες πραγματοποιούνται μέσω της χρήσης κινητών τηλεφώνων και ηλεκτρονικών υπολογιστών (Cashell, Jackson, Jickling, &Webel, 2004).

Συνεπώς, γίνονται εύκολα κατανοητοί οι λόγοι για τους οποίους, οι διεθνείς και περιφερειακοί οργανισμοί, καθώς επίσης και τα κράτη, ασχολούνται σε τόσο μεγάλο βαθμό με την αντιμετώπιση των προβλημάτων που διαπιστώνονται και των απειλών που λαμβάνουν χώρα στον κυβερνοχώρο. Εστιάζοντας στην περίπτωση της Ευρωπαϊκής Ένωσης, εντοπίζουμε την συχνή εφαρμογή περίπλοκων στρατηγικών, προκειμένου να αντιμετωπιστούν επιτυχώς οι κίνδυνοι στους διαδικτυακούς της τόπους και να προληφθούν πιθανές μελλοντικές κρίσεις τόσο σε ενωσιακό όσο και σε εθνικό επίπεδο. Εξάλλου, η άμεση σύνδεση της κυβερνοασφάλειας με τον πόλεμο κατά της τρομοκρατίας συνεπάγεται την συμπερίληψή της στις κύριες επιδιώξεις της Ένωσης, η οποία την έχει αναγάγει, μάλιστα, σε βασική προτεραιότητά της, καθώς δεν αποτελεί απλά άλλον έναν εξωτερικό κίνδυνο, αλλά ένα ζήτημα με σοβαρότερες προεκτάσεις (Vries, 2005).

Στη παρούσα μελέτη γίνεται μια προσπάθεια ανάδειξης των κύριων ζητημάτων που σχετίζονται με την αντιμετώπιση των απειλών σε διαδικτυακό περιβάλλον τόσο για τους ευρωπαϊκούς θεσμούς, όσο και τα κράτη μέλη της ΕΕ και τους πολίτες τους. Αναγνωρίζοντας την ανάγκη συνεργασίας με διεθνείς οργανισμούς και τρίτα κράτη, η έρευνα δεν θα περιοριστεί σε μία απλή περίληψη και αναφορά δευτερογενών πηγών. Αντίθετα, θα γίνει μία αποτίμηση των υπαρχουσών δράσεων και στρατηγικών της

Ένωσης και θα αναπτυχθούν οι προοπτικές και οι προκλήσεις που συνεπάγεται η διεθνής συνεργασία στον τομέα της κυβερνοασφάλειας. Έμφαση θα δοθεί, επομένως, στο ρόλο του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) και άλλων διεθνών οργανισμών για την αντιμετώπιση των «υβριδικών» απειλών (Bachman, 2011).

Υπό το πρίσμα των ανωτέρω και εστιάζοντας στην δομή της παρούσας μελέτης, στο 1^{ο} Κεφάλαιο επιχειρείται η θεωρητική εισαγωγή και επεξήγηση των βασικών εννοιών που διέπουν το κύριο σώμα της έρευνας. Ειδικότερα, θα αναδειχθούν οι έννοιες της κυβερνητικής ισχύος και του κυβερνοχώρου, με έμφαση στα βασικά χαρακτηριστικά τους και το υφιστάμενο νομικό καθεστώς.

Στο 2^{ο} Κεφάλαιο, η μελέτη εμβαθύνει στους κινδύνους και τις προκλήσεις που σχετίζονται με την κυβερνοασφάλεια. Πιο αναλυτικά, παρατίθενται οι ορισμοί των διακριτών μορφών απειλών και προκλήσεων στον κυβερνοχώρο, ενώ για την καλύτερη κατανόηση επισημαίνονται τα βασικά χαρακτηριστικά που δύνανται να καταστήσουν το διαδίκτυο ιδανικό «εργαλείο» τρομοκρατίας για τη διεξαγωγή κυβερνοεπιθέσεων.

Το «νομικό καθεστώς» και η Στρατηγική κυβερνοασφάλειας είναι οι δύο κυρίαρχες συνιστώσες της Ένωσης που θα πραγματευτεί το 3^{ο} Κεφάλαιο, με ιδιαίτερη έμφαση στους διαθέσιμους φορείς και δράσεις.

Το 4^{ο} Κεφάλαιο είναι το καταληκτικό κεφάλαιο συμπερασμάτων της παρούσας εργασίας, όπου θα γίνει αντιληπτό ότι βασικός γνώμονας για την αποτίμηση της αποτελεσματικότητας των δράσεων της ΕΕ στον τομέα της κυβερνοασφάλειας αποτελεί η αξιολόγηση της στρατηγικής και των πολιτικών της ΕΕ.

ΚΕΦΑΛΑΙΟ 1

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΘΕΩΡΗΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

1.1. Βασικές έννοιες και ορισμοί.

Ξεκινώντας από το πρώτο συνθετικό των βασικών όρων που θα χρησιμοποιηθούν στη μελέτη συνολικά, με το πρόθεμα «κυβερνό-» (cyber) περιγράφονται οι όροι που σχετίζονται με το διαδίκτυο και τους υπολογιστές (Ottis&Lorrents, 2010, σ. 267). Τη διαρκή εξέλιξη του διαδικτύου ακολουθούν και οι θεωρητικές προσεγγίσεις του. Είναι γεγονός άλλωστε, ότι στην ακαδημαϊκή κοινότητα δεν είναι εφικτή η επίτευξη πλήρους συμφωνίας αναφορικά με την σημασία των εννοιών, με απόρροια την ύπαρξη εναλλακτικών προσεγγίσεων (Kuehl, 2009).

Ο όρος «κυβερνοχώρος» χρησιμοποιείται για την εννοιολογική οριοθέτηση του νοητού χώρου που δημιουργείται με τη χρήση του διαδικτύου και των ηλεκτρονικών υπολογιστών (Merriam-webster, 2018). Ωστόσο ο ορισμός αυτός είναι σχετικά περιορισμένος, χρήζοντας αναγκαία την περαιτέρω διεύρυνσή του. Κατά συνέπεια, επιλέγονται περισσότερο περιγραφικοί ορισμοί και, ανάλογα με τον τομέα, γίνεται μία διαφορετική προσέγγιση. Η διατύπωση πως ο «κυβερνοχώρος» είναι το περιβάλλον στο οποίο πραγματοποιείται δραστηριότητα με τη χρήση του διαδικτύου δύναται να αποτελέσει έναν ακριβέστερο και πιο οικείο, στο ευρύ κοινό, ορισμό. Η δραστηριότητα αυτή μπορεί να περιλαμβάνει επικοινωνίες, αγοραπωλησίες, συναλλαγές, έρευνα κλπ. (Ottis&Lorrents, 2010, p. 267).

Το διαδίκτυο ως «χώρος» αποτελεί ένα περίπλοκο περιβάλλον. Ο κυβερνοχώρος δεν οριοθετείται και δεν περιορίζεται, με το μέγεθος του να είναι πρακτικά άπειρο και το μεγαλύτερο μέρος του να παραμένει άγνωστο στο ευρύ κοινό. Κατά συνέπεια, η δυνατότητα πρόσβασης από έναν ιδιώτη σε όλο το σύνολό του καθίσταται αδύνατη, χωρίς αυτός να διαθέτει εξειδικευμένες γνώσεις και ένα πολυδύναμο μηχάνημα. Αυτό ονομάζεται «σκοτεινό δίκτυο» ή, στην αγγλική “dark web” (Provos, Rajab, &Mavrommatis, 2009).

Στον κυβερνοχώρο, τα εγκλήματα που λαμβάνουν χώρα είναι, σε μεγάλο βαθμό, υβριδικά, δηλαδή δύναται να ξεκινούν στον άυλο χώρο του διαδικτύου, συνδέονται, ωστόσο,στενά και με τον «πραγματικό» κόσμο. Επεξηγηματικά, οι εγκληματικές οργανώσεις που απειλούν την εθνική και διεθνή ασφάλεια μέσω των δραστηριοτήτων τους στον κυβερνοχώρο μπορεί να ασχολούνται με το «χακάρισμα», δηλαδή την παραβίαση των συστημάτων ασφαλείας φορέων ή ιδιωτών, τη διαρροή πληροφοριών ή την πρόσβαση σε τραπεζικά συστήματα μέσω του διαδικτύου. Στην καθημερινότητα, στο διαδίκτυο λαμβάνουν χώρα ύποπτες δραστηριότητες και απειλές που περιλαμβάνουν την εκτέλεση παράνομων συναλλαγών και αγοραπωλησιών σε ψηφιακό περιβάλλον, το παραεμπόριο, τις απειλές κοκ (Gordon&Ford, 2006).

Παράνομες δραστηριότητες, με τα χαρακτηριστικά που προαναφέραμε, οι οποίες λαμβάνουν χώρα στο διαδικτυακό περιβάλλον εντάσσονται στην κατηγορία των «κυβερνοεπιθέσεων». Η ιδιαιτερότητα των επιθέσεων αυτών έγκειται στην δυσκολία εντοπισμού και αντιμετώπισής τους, καθώς, πολύ συχνά, λαμβάνουν χώρα σε ταυτόχρονη βάση από διαφορετικά σημεία ανά τον κόσμο, δυσχεραίνοντας κατά συνέπεια την εύρεση του αρχικού χρήστη και του τελικού αποδέκτη (Ottis&Lorrents, 2010). Η πλειοψηφία των προαναφερθέντων επιθέσεων έχει σκοπό το οικονομικό κέρδος ή την πρόκληση χάους. Το έγκλημα, σε αυτήν την περίπτωση, μπορεί να οδηγήσει σε μία γενικευμένη κρίση. Οι πιθανότητες, μάλιστα, πρόκλησης κρίσεων μεγάλου εύρους, ικανές να πλήξουν την πολιτική και την οικονομία μιας χώρας, πολλαπλασιάζονται στις περιπτώσεις παραβίασης συστημάτων ασφαλείας ενός φορέα ή μίας επιχείρησης, με σκοπό τη μεταπώληση πληροφοριών ή την αμφισβήτηση της ικανότητας του φορέα ή της εταιρείας να προστατεύσει τους πελάτες του ή τις βάσεις δεδομένων της (Eriksson&Giacomello, 2006).

Αποτελεί πραγματικότητα το γεγονός πως ισχυρά κράτη και ομάδες που εμπλέκονται στο οργανωμένο έγκλημα βρίσκονται συχνά πίσω από κυβερνοεπιθέσεις. Ορισμένοι «χάκερς», έχουν τόσο εξελιγμένη τεχνογνωσία, ώστε το επίπεδο διείσδυσης που επιτυγχάνουν, προκειμένου διαταραχθεί η παγκόσμια ισορροπία και οι αγορές, είναι ανέφικτο για έναν απλό χρήστη του διαδικτύου (Betz, 2012).

Τέλος, η κυβερνοισχύς αποτελεί μία ακόμη έννοια με ιδιαίτερο ενδιαφέρον. Η κυβερνοασφάλεια σχετίζεται σε κάθε περίπτωση με την πολιτική και την κυβερνοισχύ. Η ισχύς, στη διεθνή πολιτική, εκφράζεται σε επίπεδο διεθνούς συστήματος με

διαφορετικές, ανά περίπτωση, μορφές. Ενδέχεται να είναι ήπια, δηλαδή να διαμορφώνεται με μέσα όπως η διπλωματία και η πολιτιστική ανταλλαγή, ή σκληρή, δηλαδή να σχετίζεται με τις ένοπλες δυνάμεις. Η ισχύς είναι καθοριστικής σημασίας για τα κράτη, με τον κυβερνοχώρο, ως ένα αβέβαιο περιβάλλον, να αποτελεί ένα σύστημα στο οποίο δεν ισχύουν οι «παραδοσιακοί» κανόνες που εφαρμόζονται στο διεθνές σύστημα. Μικρότερα κράτη μπορούν να είναι εξίσου ανταγωνιστικά με μεγαλύτερα, εφόσον διαθέτουν τις υποδομές για να διεκδικήσουν μεγαλύτερο μερίδιο κυβερνοισχύος (Kramer, Starr, &Wentz, 2009).

Ανάλογα με το πλαίσιο στο οποίο γίνεται αναφορά του όρου, η κυβερνοισχύς μπορεί να θεωρηθεί είτε σκληρή (hardpower), είτε ήπια (softpower) μορφή ισχύος (Kuehl, 2009).

1.2. Θεωρητική προσέγγιση.

Η παραδοσιακή θεωρία του ρεαλισμού δεν είναι σε θέση να επεξηγήσει τον τρόπο διαμόρφωσης των σχέσεων εντός του ηλεκτρονικού περιβάλλοντος. Ωστόσο, διαφορετικές και πιο σύγχρονες προσεγγίσεις φαίνεται να είναι ικανές να ερμηνεύσουν, έως ένα βαθμό, τη νέα πραγματικότητα. Άλλωστε, οι τάσεις εντός του κυβερνοχώρου ακολουθούν την πορεία του «πραγματικού κόσμου». Εξάλλου δεν είναι τυχαίο γεγονός πως όμοια προβλήματα που απασχολούν τα φυσικά και νομικά πρόσωπα στο περιβάλλον της κοινωνίας των πολιτών εκφράζονται και στα μέσα κοινωνικής δικτύωσης στο διαδίκτυο. Εκτενής αναφορά, επιπροσθέτως, πρέπει να γίνει και για τα αδικήματα που τελούνται εντός του κυβερνοχώρου, τα οποία θεωρούνται εγκλήματα υβριδικού χαρακτήρα, καθώς ξεκινούν στο «φυσικό» και ολοκληρώνονται στο ψηφιακό περιβάλλον και αντίστροφα (Biener, Eling, &Wirfs, 2015).

Στις διεθνείς σχέσεις δεν τίθεται ζήτημα δεοντολογίας και τα εγκλήματα αντιμετωπίζονται ως απειλές για τη διεθνή ασφάλεια και την ειρήνη όταν υφίσταται ενδείξεις σύνδεσης μίας παράβασης ή εγκληματικής ενέργειας με την τρομοκρατία ή επίθεση στο «φυσικό» χώρο του κράτους. Κατά γενική ομολογία, μία κυβερνοεπίθεση

νοείται ως απειλή για τη διεθνή ασφάλεια όταν οι στόχοι της είναι ανάλογοι με των τρομοκρατικών επιθέσεων, ήτοι η αμφισβήτηση των θεσμών ή η κατάρρευση και απορρύθμιση του συστήματος. Επιπροσθέτως, για να καταστεί δυνατή η απαγγελία κατηγοριών σε έναν εγκληματία που δραστηριοποιείται στο διαδίκτυο, προκειμένου αυτός να δικασθεί ως «τρομοκράτης» θα πρέπει να έχουν απειληθεί, κινδυνεύσει ή πληγεί ανθρώπινες ζωές ή να έχουν προκληθεί υλικές ζημιές (Raboin, 2011)

Η κυβερνοασφάλεια αποτελεί, πράγματι, ένα σύνθετο πρόβλημα, γεγονός που επιβάλλει την προηγούμενη αποσαφήνιση των κύριων εννοιών που την συνθέτουν, ώστε μέσω μίας πλήρους ανάλυσης κόστους και κινδύνου στις στρατηγικές να επιτευχθεί η ενίσχυσή της. Μόνο έτσι θα καταστεί εφικτή η λεπτομερής εξέταση του συνόλου των επιμέρους ζητημάτων που σχετίζονται με αυτήν. Τονίζεται πως σε παγκόσμιο επίπεδο ποικίλουν οι θεωρίες που εξετάζουν το θέμα αυτό με αποτέλεσμα, ανάλογα με την εκάστοτε προσέγγιση δύναται να εντοπισθούν διαφορές στην απόδοση των όρων. Ομοίως και στην περίπτωση της έννοιας του κυβερνοχώρου, τα μέτρα και οι πολιτικές για την επίτευξη της μεγιστοποίησής της ποικίλλουν, ανάλογα με το κράτος, το σύστημά του και τις προκλήσεις που καλείται αυτό να αντιμετωπίσει (Hathaway, και συν., 2012).

Στην παρούσα μελέτη θα χρησιμοποιηθούν εργαλεία και προσεγγίσεις που εμπίπτουν στο επιστημονικό πεδίο των διεθνών σχέσεων και την φιλελεύθερη θεώρηση. Έμφαση , πρωτίστως, δίδεται στο ρόλο των θεσμών και της κοινής αγοράς, επιδιώκοντας να αποτιμηθεί η επίδραση της παγκοσμιοποίησης στην πορεία της εξέλιξης της κυβερνοασφάλειας και των κυβερνοεπιθέσεων για τα ευρωπαϊκά κράτη. Παράλληλα, θα τονιστεί και η σημασία των πολιτών και της δημόσιας-ιδιωτικής πρωτοβουλίας για την πάταξη του εγκλήματος, καθώς και ο ρόλος των διεθνών οργανισμών και του διεθνούς δικαίου (Yost, 2010).

Δεδομένου πως οι διεθνείς σχέσεις δεν περιορίζονται σε ένα πεδίο αλλά εμπεριέχουν στοιχεία από την πολιτική θεωρία, τις ανθρωπιστικές επιστήμες γενικά, τη νομική, την στρατηγική και την ψυχολογία, η επιλογή της συγκεκριμένης θεωρητικής προσέγγισης αποτέλεσε λογική απόρροια. Συνεπώς, τα εργαλεία που προσφέρει η διεθνής θεωρία δύνανται να καλύψουν πλήρως τις ερευνητικές ανάγκες

της μελέτης, επιτρέποντας τη συγκριτική ανάλυση δεδομένων με σκοπό την συνθετική αποτίμηση των πραγματικών στοιχείων και την κριτική (Eriksson&Giacomello, 2006).

ΚΕΦΑΛΑΙΟ 2

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΕΙΛΕΣ

2.1. Dark web και κυβερνοασφάλεια.

Το διαδίκτυο δεν αποτελεί έναν ενιαίο χώρο. Για λόγους ανάλυσης, θεωρείται πως χωρίζεται σε τρία τμήματα (Fu, Abbasi, & Chen, 2010):

- Το διαδίκτυο που χρησιμοποιεί η πλειοψηφία των πολιτών, στο οποίο περιέχονται πληροφορίες που μπορεί κανείς να ανακτήσει εύκολα μέσω των ειδικών μηχανών αναζήτησης, όπως το Google και το Bing.
- Στο deep web, το οποίο περιέχει πληροφορίες που δεν είναι καταχωρημένες στις δημοφιλείς πλατφόρμες αναζήτησης και, θεωρητικά, αποτελεί το μεγαλύτερο μέρος αυτού.
- Στο σκοτεινό δίκτυο (dark web), όπου λαμβάνει χώρα το μεγαλύτερο μέρος των παράνομων αγοραπωλησιών, διατίθεται υλικό που δεν μπορεί να δημοσιευθεί ή να διαμοιραστεί σε νόμιμες ιστοσελίδες, όπως φωτογραφίες παιδικής πορνογραφίας. Συχνά, επιπλέον, λαμβάνουν χώρα επικοινωνίες που δεν δύναται να υλοποιηθούν επίσημα, καθώς σε περίπτωση που πραγματοποιούνταν στο φυσικό ή «πραγματικό» περιβάλλον θα θεωρούνταν κακουργήματα, όπως, λ.χ. συμφωνίες μεταξύ εγκληματικών οργανώσεων.

Παρά τις συντονισμένες προσπάθειες των κρατών, το σκοτεινό δίκτυο ακόμη παραμένει ένα ανασφαλές περιβάλλον, το οποίο δύσκολα παρακολουθείται και ελέγχεται, ενώ, ταυτόχρονα, εξελίσσεται διαρκώς. Άλλωστε είναι γεγονός πως η αδυναμία πλήρους ταξινόμησης των πληροφοριών που περιέχονται στο deep web και το dark web, καθιστά την εξασφάλιση του ελέγχου αυτών δύσκολα πραγματοποιήσιμη (Fu, Abbasi, &Chen, 2010).

Παραπάνω, ορίστηκε η έννοια του σκοτεινού δικτύου ή dark web. Πιο αναλυτικά, οι κύριες εγκληματικές δραστηριότητες που λαμβάνουν χώρα στο σκοτεινό

δίκτυο και απειλούν την ασφάλεια του κυβερνοχώρου περιλαμβάνουν, μεταξύ άλλων (βάσει της μελέτης των Chertoff&Simon, 2015, σελ. 2-5):

1) Διαφορετικών μορφών και τύπων παράνομες ή παράτυπες αγοραπωλησίες και συναλλαγές, οι οποίες θα αναγνωρίζονταν ως εγκληματικές ενέργειες στο κράτος στο οποίο λαμβάνουν χώρα ή που ορίζονται ως «εγκλήματα» στο διεθνές δίκαιο. Στην κατηγορία αυτή δύναται να συμπεριληφθούν η αγορά ή η πώληση αγαθών, των οποίων η κατοχή συνιστά παράβαση. Τέτοιου είδους αγαθά είναι τα εξωτικά ζώα, τα ναρκωτικά, τα όπλα και άλλες ουσίες (λ.χ. φάρμακα). Τέλος, το εμπόριο λευκής σαρκός και η εμπορία βρεφών συγκαταλέγονται στην εν λόγω κατηγορία.
2) Η ανταλλαγή και πώληση κλοπιμαίων και παρανόμως αποκτημένων πληροφοριών. Ειδικότερα, τα αγαθά αυτά μπορεί να είναι υλικά ή άυλα εμπεριέχοντας αρχαιότητες, φορτία ή και τηλεφωνικούς αριθμούς, επαφές πελατών, πορνογραφικό υλικό και φωτογραφίες.
3) Τις δραστηριότητες υποστήριξης και υποκίνησης της μαφίας και της τρομοκρατίας, όπως οργάνωση εγκληματικών δράσεων. Επισημαίνεται ότι στην συγκεκριμένη κατηγορία συγκαταλέγεται και η εύρεση νέων μελών που θα στελεχώσουν τις εν λόγω ομάδες.
4) Τον παράνομο διαμοιρασμό μουσικής, βίντεο και άλλου υλικού μέσω του διαδικτύου, κοινώς «πειρατεία», του οποίου τα πνευματικά δικαιώματα είναι κατοχυρωμένα.
5) Η χαρτοπαιγνία και το παράνομο στοίχημα. Εξαιρούνται οι περιπτώσεις πληρωμής στο κράτος των ανάλογων εισφορών από τις νόμιμες στοιχηματικές εταιρείες, μέσω των οποίων εξασφαλίζεται η προστασία του χρήστη.
6) Δολοφονίες και επιθέσεις που αποσκοπούν στον εκφοβισμό υψηλών προσώπων συχνά οργανώνονται στο περιβάλλον του dark web.

Συχνά υφίσταται η λανθασμένη εντύπωση πως οι δράστες σε περιπτώσεις κυβερνοεπιθέσεων είναι μεμονωμένα άτομα ή ομάδες ατόμων με εγκληματικό χαρακτήρα. Μάλιστα, πολλάκις, στο υποσυνείδητο των πολιτών έχει εντυπωθεί η εικόνα μίας στερεοτυπικής φυσιογνωμίας, η οποία δρα όπως παρουσιάζεται στην έβδομη τέχνη. Στην πραγματικότητα, δεν είναι σπάνιο πίσω από κυβερνοεπιθέσεις να βρίσκονται πολυεθνικές εταιρείες που έχουν ως στόχο τους να καπηλευθούν τη θέση

τους για να αποκτήσουν πρόσβαση σε βάσεις δεδομένων εταιριών με ανταγωνιστικά συμφέροντα ή και κράτη. Επί της ουσίας, η λειτουργία των ομάδων στο σκοτεινό δίκτυο παρομοιάζει με αυτήν της μαφίας στον «φυσικό κόσμο» (Funk, 2008).

Η ύπαρξη και μόνο του σκοτεινού δικτύου συνιστά μελανό σημείο για τις κυβερνήσεις, θέτοντας σε κίνδυνο τη διεθνή ασφάλεια. Για τα κράτη τα οποία αποτελούν βάση των εγκληματικών οργανώσεων, η έλλειψη ικανότητάς τους να αντιμετωπίσουν τις απειλές και να συλλάβουν τους παραβάτες μεταφράζεται ως αδυναμία. Συχνά, λοιπόν, τίθεται ο προβληματισμός ως προς τον προσδιορισμό του τρόπου εντοπισμού και σύλληψης των εγκληματιών, δεδομένου πως μπορεί, μεν, ο κυβερνοχώρος να είναι ένας νοητός χώρος, ωστόσο, η σύλληψη θα πρέπει να λάβει χώρα σε πραγματικό περιβάλλον (Chertoff&Simon, 2015).

Πέραν των επιπτώσεων που έχει η ίδια η πράξη της τέλεσης μίας παράνομης δραστηριότητας στον κυβερνοχώρο, η εγκληματική δραστηριότητα μπορεί να επιβαρύνει, συνολικά, τους πολίτες και εμμέσως. Η παραοικονομία και η «μαύρη αγορά», οδηγούν σε προβλήματα στην οικονομία και την παραγωγικότητα της χώρας και θέτουν σε κίνδυνο την ομαλή λειτουργία των θεσμών. Εξαιτίας της μη απόδοσης των ανάλογων εισφορών, δεν καθίσταται δυνατή και η υλοποίηση των κατάλληλων ελέγχων. Συνεπώς, τα αγαθά που πωλούνται, ακόμη κι αν έχουν αποκτηθεί με νόμιμους τρόπους, δεν είναι βέβαιο πως θα πληρούν τις απαραίτητες απαιτήσεις ασφαλείας και πως η ποιότητά τους θα είναι ανάλογη των απαιτήσεων του αγοραστή (Funk, 2008).

2.2. «Κυβερνοτρομοκρατία» - μία διεθνής απειλή.

Η κυβερνοτρομοκρατία αποτελεί μία σύγχρονη πρόκληση για τη διεθνή κοινότητα. Οι τρομοκράτες δεν επιθυμούν απαραίτητα το θάνατο ανθρώπων. Απεναντίας, έχει γίνει, πλέον, σαφές πως η τρομοκρατία αποσκοπεί στην αμφισβήτηση της διεθνούς τάξης και ασφάλειας, καθώς και της δυνατότητας των φορέων να τις εγγυηθούν, μέσω της προκαλούμενης αταξίας. Η αγοραπωλησία όπλων και χημικών ουσιών εμπίπτει, συχνά, στην κατηγορία της τρομοκρατίας, στις περιπτώσεις που τα

όπλα δύναται να χρησιμοποιηθούν για πρόκληση μαζικών καταστροφών ή τα χημικά μπορούν να αποτελέσουν πρώτη ύλη για την κατασκευή βιολογικών όπλων. Η αδυναμία ελέγχου δρα πολλαπλασιαστικά για το υφιστάμενο κλίμα ανασφάλειας, ενώ συγχρόνως επιτυγχάνεται ευκολότερα ο στόχος της αποδυνάμωσης και αποδιοργάνωσης της εξουσίας με ευρείες πολιτικές και κοινωνικές συνέπειες (AlRowaily, Abulaish, Haldar, &AlRubaian, 2015).

Η τρομοκρατική απειλή είναι διαρκώς παρούσα. Η ισχύς των τρομοκρατών προέρχεται από τη δυνατότητά τους να παραμένουν αόρατοι, αλλά πάντα παρόντες, με την ταυτότητα των μελών τους και το εύρος της εξουσίας τους να μένουν ασαφή (Al Rowaily, Abulaish, Haldar, & Al Rubaian, 2015). Με δεδομένο το παραπάνω, δεν εκπλήσσει το γεγονός πως οι περισσότερες τρομοκρατικές οργανώσεις εδρεύουν σε διάφορες χώρες, διαθέτουν ένα πολύπλοκο σύστημα ιεραρχίας, χρησιμοποιούν υβριδικά δίκτυα επικοινωνίας, δύνανται να παραβιάζουν σε ανύποπτο χρόνο τα συστήματα ασφαλείας, κοινοποιούν γραπτές διακηρύξεις και προβαίνουν σε απειλές. Τέλος, σε πολλές περιπτώσεις, η εξεύρεση και ο «προσηλυτισμός» μπορεί να λαμβάνουν χώρα στα μέσα κοινωνικής δικτύωσης με έμμεσο τρόπο και με τη χρήση προπαγάνδας ή πειθούς (Chen, 2012).

Οι τρομοκρατικές οργανώσεις στον κυβερνοχώρο, όπως άλλωστε συμβαίνει και στον φυσικό κόσμο, τείνουν να αδράττουν την κατάλληλη στιγμή για να δράσουν. Σε χώρες που πλήττονται, λ.χ. από ευρείες κρίσεις ή που αποτελούν συχνή βάση για την τέλεση επιχειρηματικών δραστηριοτήτων ή που έχουν σημαντικό στρατηγικό ενδιαφέρον, η πιθανότητα του να επιχειρηθεί μία κυβερνοεπίθεση είναι μεγαλύτερη. Η διαφορά, ωστόσο, έγκειται στην ικανότητα αντιμετώπισης και θωράκισης του κυβερνοχώρου από τους αρμόδιους φορείς σε αυτές τις χώρες (Chertoff & Simon, 2015).

Τα αίτια της κυβερνοτρομοκρατίας εμφανίζουν άμεση σύνδεση με τα φαινόμενα που εκδηλώνονται στο εσωτερικό της κοινωνίας. Τα προβλήματα που αντιμετωπίζουν οι σύγχρονοι άνθρωποι δεν είναι ανεξάρτητα μεταξύ τους. Απεναντίας, λόγω της αλληλεξάρτησης των κρατών στην παγκοσμιοποιημένη κοινωνία στις μέρες μας, παρατηρούνται συχνά τριβές και συγκρούσεις που λαμβάνουν χώρα σε όλα τα επίπεδα. Η διάκριση μεταξύ αναπτυγμένου και «τρίτου»

κόσμου δεν έχει εξαλειφθεί, με βαθιά ριζωμένα στερεότυπα και συντηρητικές αντιλήψεις να κλονίζουν ακόμη το διεθνές σύστημα (Giacomello, 2014).

Πολλές από τις κυβερνοαπειλές έχουν ως αίτιο τα προβλήματα που εκδηλώνονται σε επίπεδο κοινωνίας. Η διαρκής αμφισβήτηση, λ.χ. των δικαιωμάτων των μειονοτήτων σε αυτό-αποκαλούμενες «αναπτυγμένες χώρες», το φαινόμενο του θρησκευτικού φονταμενταλισμού και ο άκρατος κρατοκεντρισμός ορισμένων χωρών, οδηγούν σε εκδηλώσεις φαινομένων ρατσισμού. Οι μειονοτικές ομάδες εκφράζονται ευχερέστερα στο διαδίκτυο, καθώς η παρεχόμενη από αυτό ανωνυμία και προστασία της ταυτότητάς τους δεν εξαναγκάζει τα πρόσωπα να έρχονται σε άμεσο κίνδυνο, μιας και μπορούν να είναι ακτιβιστές από την ασφάλεια του σπιτιού τους (Brauchler, 2007).

Στο διαδίκτυο συχνά λαμβάνουν χώρα επιθέσεις οι οποίες δε δύνανται να θεωρηθούν ποινικά εγκλήματα, perse, διότι αποτελούν έμμεσες απειλές για την ασφάλεια, όπως για παράδειγμα το «χάκινγκ» μίας ομάδας σε ιστοσελίδα με σκοπό την δημοσίευση υλικού και χιουμοριστικών εικόνων (Hongthong, 2017). Ωστόσο, με τις πρόσφατες νομικές μεταρρυθμίσεις στην ΕΕ και την αναγόρευση της ρητορικής μίσους σε έγκλημα, οποιαδήποτε υποκίνηση σε ρατσιστική βία λαμβάνει χώρα σε ψηφιακό περιβάλλον θεωρείται ως έμμεση ή άμεση απειλή κατά της ζωής, της αξιοπρέπειας και της ασφάλειας των πολιτών και λαμβάνονται μέτρα για τον περιορισμό και την καταπολέμησή της (Betz, 2012).

Παρόλα αυτά, ακόμη και στην ΕΕ, δεν έχει βρεθεί ακόμη τρόπος να συντονιστούν πλήρως τα νομικά συστήματα και οι δρώντες, ούτως ώστε το ρατσιστικό έγκλημα και η ρητορική μίσους στον κυβερνοχώρο να αντιμετωπιστούν εξ ολοκλήρου από κοινού. Οι προσπάθειες ακόμη επικεντρώνονται στην εξεύρεση ενός κοινώς αποδεκτού ορισμού παρά στην πάταξη του εγκλήματος. Συνεπώς, γίνεται ακόμη πιο ξεκάθαρο το γιατί η συνεργασία σε ευρωπαϊκό επίπεδο είναι επιβεβλημένη, καθώς σε αντίθετη περίπτωση, δυσχεραίνεται σημαντικά η εφαρμογή του δικαίου (Betz, 2012).

ΚΕΦΑΛΑΙΟ 3

ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

3.1. Η νομική διάσταση του προβλήματος.

Η πλειοψηφία των σύγχρονων πολιτών προβαίνει –σχεδόν καθημερινά- σε χρήση του διαδικτύου. Από τις καθημερινές επικοινωνίες και αγοραπωλησίες, μέχρι τον συντονισμό μεταξύ κυβερνήσεων και τον διαμοιρασμό εγγράφων, που περιέχουν πληροφορίες που αφορούν την ασφάλεια των πολιτών από πλευράς κράτους, είναι θεμελιώδης η ύπαρξη πλήρους έλεγχου των δεδομένων που ανταλλάσσονται και διαμοιράζονται μέσω διαδικτύου. Ωστόσο, τόσο λόγω του τεράστιου όγκου των πληροφοριών, όσο και της πολυπλοκότητας του διαδικτύου, αλλά και της ιδιαιτερότητας του κυβερνοχώρου, η επίτευξη ενός απόλυτου επιπέδου ασφάλειας και ελέγχου αποτελεί στόχο δύσκολα επιτεύξιμο. Η ύπαρξη και μόνο σύνθετων νομοθεσιών και δράσεων δεν συνεπάγεται την μείωση των κινδύνων στον κυβερνοχώρο ή την δυνατότητα αντιμετώπισης κρίσεων που σχετίζονται με απειλές κυβερνοασφάλειας (Hathaway, etal., 2012).

Νομικά, οι επιθέσεις στον κυβερνοχώρο θεωρούνται ποινικό αδίκημα και διώκονται βάσει των όσων προβλέπονται από την ισχύουσα νομοθεσία. Τα εγκλήματα που λαμβάνουν χώρα σε διαδικτυακό περιβάλλον, επηρεάζοντας πάνω από ένα κράτη και τους πολίτες αυτών θεωρούνται διεθνούς χαρακτήρα. Αρμόδιοι για την σύλληψη των διεθνών εγκληματιών ή εγκληματικών οργανώσεων που δραστηριοποιούνται στον κυβερνοχώρο είναι οι θεσμοί του κράτους στο οποίο τελείται το έγκλημα. Στο εσωτερικό, ωστόσο, της ΕΕ και, εφόσον η απειλή είναι δυνατόν να πλήξει την ασφάλεια ή να θέσει σε κίνδυνο την ευημερία και την ανάπτυξη της κοινής αγοράς, υφίσταται δυνατότητα έκδοσης ευρωπαϊκού εντάλματος σύλληψης, καθώς επιβάλλεται η αντιμετώπισή του σε ενωσιακό επίπεδο (Biener, Eling, &Wirfs, 2015).

Τουναντίον, μέσω της κοινής αντιμετώπισης των απειλών γίνεται σαφές πως η νομοθεσία δεν καλύπτει πλήρως και πάντα τις ανάγκες της κοινωνίας. Το διαδίκτυο εξελίσσεται και διευρύνεται συνεχώς, καθιστώντας επιτακτική την ανάγκη διαρκούς

επικαιροποίησης και αναδιαμόρφωσης των υφιστάμενων πολιτικών με στόχο την παρεμπόδιση κατάχρησης του διαδικτύου και τον περιορισμό της εγκληματικής δραστηριότητας εντός του κυβερνοχώρου. Η ανωνυμία του χρήστη, η δυνατότητα παρεμβολής του σήματος και η αλλοίωση των δεδομένων αποτελούν μερικά από τα σημαντικότερα «εμπόδια» στην επαρκή και κατάλληλη εφαρμογή του δικαίου για την αντιμετώπιση των υφιστάμενων απειλών, που σχετίζονται με το deep ή το dark web και την κυβερνοασφάλεια (Tikk, 2011).

3.2. ΕΕ και κυβερνοασφάλεια.

Η Ευρωπαϊκή Ένωση, ως γνωστόν, αποτελεί μία πολιτική οντότητα "sui generis" που τοποθετείται μεταξύ διακυβερνητικής συνεργασίας και υπερεθνικής ολοκλήρωσης. Αν και ξεκίνησε ως μία κυρίως εμπορική ένωση, σήμερα έχει εξελιχθεί σε πολιτική και οικονομική, με τα κράτη μέλη της να είναι υποχρεωμένα να συνεργάζονται σε πολλούς τομείς, παραχωρώντας εκούσια μέρος των κυριαρχικών τους δικαιωμάτων στους θεσμούς της. Η κυβερνοασφάλεια και η από κοινού αντιμετώπιση των κυβερνοαπειλών συμπεριλαμβάνονται στις βασικές υποχρεώσεις των θεσμικών οργάνων της Ένωσης, καθώς αποτελούν συνιστώσα της κοινής πολιτικής ασφαλείας της. Για το σκοπό αυτό, τα θεσμικά όργανα της ΕΕ συνεργάζονται στενά με τα κράτη μέλη (Wessel, 2015).

Η Ευρωπαϊκή Ένωση δίδει σημαντικές εξουσίες σε ένα από τα βασικά θεσμικά της όργανα: την Ευρωπαϊκή Επιτροπή. Η επιτροπή κατέχει την υψηλή επίβλεψη των έργων, την καθοδήγηση και υποβοήθηση τόσο των κρατών μελών όσο και των λοιπών θεσμικών οργάνων, μέσω της προσφοράς τεχνογνωσίας και πόρων. Επιπλέον, επιβλέπει και συντονίζει τις στρατηγικές και τα διάφορα προγράμματα της ΕΕ στον τομέα της κυβερνοασφάλειας, διασφαλίζοντας στο σύνολο των δράσεων την εφαρμογή του Ευρωπαϊκού Δικαίου (ΔΒΜ, 2013).

Με αφετηρία τα όσα ορίζει η Ψηφιακή Στρατηγική της ΕΕ, τα κράτη μέλη και τα θεσμικά όργανα της Ένωσης έχουν αναλάβει τις κάτωθι υποχρεώσεις (Petrovic, Bojkovic, Anic, Stamenkovic, &Tarle, 2014):

1) να λαμβάνουν μέτρα για να εξασφαλίζουν πλήρως πως τα κράτη μέλη διαθέτουν τα απαραίτητα μέσα για να επιτυγχάνουν μία χρηματοπιστωτική σταθερότητα μέσω των δομών της ψηφιακής οικονομίας. Σε αυτήν την προτεραιότητα, μεγάλο ρόλο παίζει η προστασία του ηλεκτρονικού εμπορίου και των ηλεκτρονικών συναλλαγών στον κυβερνοχώρο,
2) να υποστηρίζουν τις μικρομεσαίες επιχειρήσεις και τις πολυεθνικές, εξίσου, στην διαδικασία προστασίας των δεδομένων τους και να λαμβάνουν μέτρα για τη σταθεροποίηση του οικονομικού περιβάλλοντος σε ψηφιακούς χώρους. Στην εν λόγω υποχρέωση, συμπεριλαμβάνονται και η παρακολούθηση των συναλλαγών, η προστασία των χρηστών, ο έλεγχος εφαρμογής της νομοθεσίας κοκ,
3) να προωθούν και να υποστηρίζουν πρωτοβουλίες που περιλαμβάνουν το Internet of Things (IoT), δηλαδή δράσεις που αφορούν την ανάπτυξη υποδομών και τεχνολογιών που θα εστιάζουν στην ψηφιοποίηση, την αυτοματοποίηση και τον συντονισμό δράσεων με τη χρήση ίντερνετ, το ψηφιακό εμπόριο, την διατομεακή συνεργασία με τη χρήση του διαδικτύου κοκ.

Το υφιστάμενο νομικό πλαίσιο της ΕΕ αναφορικά με την αντιμετώπιση των κυβερνοαπειλών είναι πλούσιο και σύνθετο, ταυτόχρονα. Τα κράτη μέλη της Ευρωπαϊκής Ένωσης έχουν προβεί στην ανάπτυξη ενός συστήματος, ικανού να εφαρμοστεί και να αξιοποιηθεί από οποιοδήποτε εθνικό σύστημα των μελών της Ένωσης. Οι κρατικοί φορείς, σε συνεργασία με τα θεσμικά όργανα της Ένωσης, την τελευταία εικοσαετία, πράγματι, έχουν προβεί στην λήψη μέτρων, επιτυχαίνοντας σημαντικές βελτιώσεις στο επίπεδο και τις μεθόδους προστασίας του διαδικτύου. Αποσκοπώντας στης ενσωμάτωση του ευρωπαϊκού στο εθνικό δίκαιο, όπως επίσης και στην εξέλιξη του εκάστοτε εθνικού κώδικα και συστημάτων, τα κράτη μέλη υποχρεούνται, μεταξύ άλλων, να εναρμονιστούν με τις επιταγές των ευρωπαϊκών προτύπων. Η νομοθεσία της ΕΕ, επί του παρόντος, περιλαμβάνει κώδικες δεοντολογίας, νόμους, διατάξεις, κατευθυντήριες γραμμές, κανονισμούς και δράσεις για την πάταξη του ηλεκτρονικού εγκλήματος και την προστασία των δικαιωμάτων των πολιτών (Klimburg, 2010).

Στη διαμόρφωση του τρόπου αντιμετώπισης των κυβερνοαπειλών, σημαντικότατο ρόλο διαδραματίζουν δύο θεμελιώδεις αρχές του ευρωπαϊκού δικαίου, αυτή της αναλογικότητας και της επικουρικότητας. Υπό το πρίσμα των ανωτέρω, εύκολα γίνεται αντιληπτό το γεγονός πως, οι δράσεις που προγραμματίζονται και οι επιλεγμένες μέθοδοι αντιμετώπισης μίας κρίσης θα πρέπει, σε κάθε περίπτωση, να είναι ανάλογες της βαρύτητας και της σημασίας της παράβασης. Ταυτόχρονα, σύμφωνα με τα όσα προβλέπονται από την αρχή της επικουρικότητας, τα θεσμικά όργανα αναλαμβάνουν δράση μόνο στο βαθμό εκείνο στον οποίο το κράτος μέλος το οποίο εμπλέκεται δεν είναι σε θέση να αντιμετωπίσει με τις δικές του «δυνάμεις» το πρόβλημα που ανέκυψε (Γιάννης, 2014).

Οι κυριότερες νομικές και διατομεακές πρωτοβουλίες που λαμβάνει η Ένωση για την κυβερνοασφάλεια αποβλέπουν στην πρόληψη της εγκληματικότητας στον κυβερνοχώρο και της τρομοκρατίας. Ειδικότερα, με σκοπό την επίτευξη του ανωτέρω στόχου, εφαρμόζεται η Οδηγία 2016/1148/ΕΕ για την ασφάλεια των Δικτύων, αποσκοπώντας στην προστασία της κοινής αγοράς και των δικαιωμάτων των πολιτών της Ένωσης. Στα πλαίσια της εφαρμογής της εν λόγω Οδηγίας, τα κράτη μέλη καλούνται να συστήνουν ομάδες αντιμετώπισης κυβερνοαπειλών, να επιτρέπουν τη χωρίς περιορισμό πρόσβαση στην πληροφορία και το διαδίκτυο στο σύνολο των πολιτών τους, να παρέχουν υψηλού επιπέδου ψηφιακές υπηρεσίες και να προλαμβάνουν, αντιμετωπίζουν και αποκαθιστούν κρίσεις που προέρχονται από ή εκδηλώνονται σε ψηφιακούς χώρους (ΕΕ, Οδηγία 2016/1148, 2016).

Στην διεκπεραίωση των στόχων της ΕΕ στον τομέα της κυβερνοασφάλειας σημαντική αναδεικνύεται και η δράση του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών, ENISA, αποτελώντας ένα κέντρο «εμπειρογνωμοσύνης» μέσω της παροχής των αναγκαίων πληροφοριών στα κράτη μέλη, αναφορικά με ζητήματα που άπτονται του τομέα της κυβερνοασφάλειας. Από το 2004, μέχρι σήμερα, ο ENISA (ΕΕ, 2018):

- παρέχει συμβουλές,
- προτείνει λύσεις,
- καθοδηγεί τόσο δημόσιους όσο και ιδιωτικούς φορείς στην ΕΕ,
- αναπτύσσει ασκήσεις αντιμετώπισης κρίσεων σε ευρωπαϊκό επίπεδο,

- ενισχύει τις εθνικές δομές και πρωτοβουλίες αντιμετώπισης των προβλημάτων στον τομέα της ασφάλειας στο διαδίκτυο,
- εκπονεί μελέτες,
- ενώ, τέλος, συνεργάζεται με τα θεσμικά όργανα της ΕΕ.

Η λειτουργία του ENISA βασίζεται στις προβλέψεις του Κανονισμού 469/2004 της ΕΕ, ο οποίος ενισχύθηκε από τον Κανονισμό 526/2013 της ΕΕ, με τον τελευταίο να αναφέρεται σε θέματα ασφάλειας στο διαδίκτυο και την πληροφορική (ENISAA, 2018).

Αξιοσημείωτη για την ενίσχυση του περιβάλλοντος ασφάλειας της Ένωσης είναι η επιτυχής πρωτοβουλία για την αντιμετώπιση των προβλημάτων στην κυβερνοασφάλεια που φέρει το τίτλο Μόνιμη Δομημένη Συνεργασία ή Permanent Structured Cooperation (PESCO). Η PESCO αποτελεί τμήμα της Παγκόσμιας Στρατηγικής της ΕΕ για την πολιτική ασφαλείας της και εμπίπτει, συνεπώς, στον τομέα της εξωτερικής πολιτικής της (EU, 2018).Ο στόχος της ανάπτυξης μίας Μόνιμης Διαρθρωμένης Συνεργασίας για την Ασφάλεια και την Άμυνα (PESCO), περιλαμβάνεται στη ΣΛΕΕ και καλύπτεται από τα όσα προβλέπονται στα άρθρα 42 παρ. 6 και 46, καθώς και στο Πρωτόκολλο 10 της Συνθήκης. Παράλληλα, στα πλαίσια της PESCO, η ΕΕ δρα ως ένας διεθνής οργανισμός και τα κράτη μέλη της κατορθώνουν να υλοποιήσουν το στόχο μίας από κοινού πορείας ανάπτυξης χωρίς περιορισμούς. Το όφελος, επομένως, για τα κράτη μέλη και τους πολίτες τους, τα οποία συμμετέχουν σε αυτήν εθελοντικά από το 2017, είναι αξιοπρόσεκτο και διαρκές (EU, 2018).

Τα κράτη μέλη της ΕΕ έχουν επενδύσει στην PESCO με στόχο να εντείνουν και να επεκτείνουν τις προσπάθειες κοινής άμυνας της Ένωσης απέναντι στους εξωτερικούς κινδύνους. Άμεσο απότοκο του τελευταίου, αποτελεί η ενίσχυση των δομών εξωτερικής ασφάλειας, τις οποίες προσάρμοσαν στις ισχύουσες δομές, αυξάνοντας παράλληλα τις επενδύσεις τους στην άμυνα και αναπτύσσοντας συνεργασίες στον τομέα των αμυντικών συστημάτων, γεγονός που μεγιστοποιεί την αποτελεσματικότητα των προσπαθειών τους, μειώνοντας το συνεπαγόμενο κόστος (Fiott, 2017).

Τονίζεται πως η PESCO είναι ένα μόνιμο πλαίσιο συνεργασίας και λαμβάνει υπόψη τα συμφέροντα του εκάστοτε κράτους μέλους, σύμφωνα και με τα όσα

προβλέπουν η ΚΕΠΠΑ και η ΣΛΕΕ. Κατά αυτό τον τρόπο, δημιουργείται ένα κοινό αμυντικό μέτωπο ενάντια στις εξωτερικές απειλές, μαζί με το ΝΑΤΟ και τις δυνάμεις των κρατών μελών. Για την κυβερνοασφάλεια, όπως και για το σύνολο των απειλών, αξιοποιείται το ισχύον νομικό πλαίσιο, το οποίο και συμπληρώνεται από πρόσθετα μέσα και δράσεις ανάλογα με τις ανάγκες της Ένωσης και των κρατών μελών (Biscop, 2017). Η διαφορά, ωστόσο, μεταξύ της PESCO και έτερων μορφών συνεργασίας έγκειται στο ότι η πρώτη είναι δεσμευτικού χαρακτήρα για τα κράτη μέλη, κάτι που δεν εντοπίζεται στην πλειοψηφία των λοιπών πρωτοβουλιών της Ένωσης (EU, 2018).

Ξεχωριστός λόγος θα πρέπει να γίνει για την πλατφόρμα NIS, για την κυβερνοασφάλεια στην Ευρώπη. Η NIS δημιουργήθηκε στα πλαίσια της εφαρμογής της Οδηγίας 2016/1148/ΕΕ, καθώς η τελευταία θεωρήθηκε επιτακτικής σημασίας για την ασφάλεια της Ένωσης. Πιο αναλυτικά, μέσω της εν λόγω πλατφόρμας επιτυγχάνεται και ενθαρρύνεται η δικτύωση μεταξύ φυσικών και νομικών προσώπων και η σύναψη εταιρικών σχέσεων. Παράλληλα, επιτρέπεται η συνεργασία μεταξύ του δημόσιου τομέα και των ιδιωτικών εταιρειών αποσκοπώντας στην αντιμετώπιση των κυβερνοαπειλών και της κυβερνοτρομοκρατίας (Weber&Studer, 2016).

Συμπληρωματικά στα ανωτέρω, επισημαίνεται ότι η πλατφόρμα NIS επιτρέπει την επίτευξη ενός υψηλού επιπέδου προστασίας με σειρά δράσεων όπως (ENISAA, 2018):

- την αντιμετώπιση κρίσεων (ομάδα εργασίας 1)
- την ανταλλαγή πληροφοριών (ομάδα εργασίας 2)
- την προστασία του κυβερνοχώρου (ομάδα εργασίας 3).

Τα κράτη μέλη προέβησαν στην ψήφιση της Οδηγίας για την Κυβερνοασφάλεια αναγνωρίζοντας ότι, πλέον, αποτελεί πρόκληση για την ασφάλεια και την ευημερία των πολιτών και την λειτουργία της κοινής αγοράς. Η διεύρυνση της Ένωσης έκανε εντονότερη την ανάγκη ψήφισης αυτής. Ωστόσο η πλήρης υιοθέτησή της ακόμη δεν έχει επιτευχθεί (Carrapico & Barrinha, 2017). Σε μεγάλο βαθμό, η εφαρμογή της εν λόγω Οδηγίας αποτέλεσε σημείο τριβής μεταξύ της Ένωσης και των κρατών μελών, κατά κύριο λόγο στα ακόλουθα ζητήματα (ΚΕΗΔ, 2018):

- στην υποχρεωτική κοινοποίηση δεδομένων και πληροφοριών,
- στην ενσωμάτωση της Οδηγίας στο εθνικό δίκαιο,
- στο κόστος της εφαρμογής της Οδηγίας,

- στη μη συμμόρφωση των κρατών και στις συνέπειες αυτής.

Σημαίνοντα ρόλο για την προστασία των δραστηριοτήτων στον κυβερνοχώρο διαδραματίζει η Europol, συνεργαζόμενη με τις ένοπλες δυνάμεις των κρατών μελών και των εταίρων της ΕΕ. Ως μερικές από τις βασικότερες επιδιώξεις της αναγνωρίζονται η προστασία των συναλλαγών, η υποβοήθηση των θεσμικών οργάνων, η εξασφάλιση συνεργασίας με φορείς και οργανισμούς αντίστοιχου χαρακτήρα, λ.χ. τη CIA (Central Intelligence Agency) στις ΗΠΑ, καθώς και η παροχή αυξημένου βαθμού προστασίας για το σύνολο της Ένωσης και των κρατών μελών της. Πιο αναλυτικά, οι στόχοι της περιλαμβάνουν μεταξύ άλλων (Europol, 2018):

- Τον αποκλεισμό κακόβουλου λογισμικού τύπου "trojan".
- Τον εντοπισμό αυτόματων συστημάτων διασύνδεσης με ηλεκτρονικούς υπολογιστές μέσω ενός κοινού κέντρου, τύπου "botnet" ή "rootkit".
- Τον καθορισμό των βασικών απειλών κατά προσωπικών ή δημοσίων ηλεκτρονικών υπολογιστών και συσκευών, όπως ταμπλέτες και έξυπνα τηλέφωνα που επιτρέπουν την πρόσβαση στο διαδίκτυο.
- Την προστασία των ψηφιακών τους χώρων παρέχοντας εμπειρογνωμοσύνη και εξειδικευμένες πληροφορίες για κακόβουλο λογισμικό, botnet κλπ.
- Την λήψη μέτρων για τον έγκαιρο και αποτελεσματικό εντοπισμό και τη σύλληψη των εγκληματιών και καταδίκη τους.

Για την επίτευξη των προαναφερθέντων στόχων ως καθοριστική αξιολογείται και η συνδρομή των κάτωθι οργανισμών (ΕΕ, 2018):

- ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κατάρτιση στον Τομέα της Επιβολής του Νόμου (ΕΑΑ), που εδρεύει στη Βουδαπέστη και ασχολείται με την γνωμοδότηση, την έρευνα και την εκπαίδευση στον τομέα της κυβερνοασφάλειας.

- ο Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), που εδρεύει στη Λετονία και προσφέρει υπηρεσίες που στοχεύουν «στην ανάπτυξη και την καλύτερη λειτουργία της εσωτερικής αγοράς δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών».

- ο Ευρωπαϊκός Οργανισμός για τη Λειτουργική Διαχείριση Μεγάλων Πληροφοριακών Συστημάτων στον Χώρο της Ελευθερίας, Ασφάλειας και Δικαιοσύνης (eu-LISA), που επικουρεί μεγάλου εύρους εταιρείες και δραστηριότητες στον τομέα της πληροφορικής,

- ο Ευρωπαϊκός Οργανισμός Ασφάλειας της Αεροπορίας – EASA, που μαζί με τους υπόλοιπους θεσμούς και οργανισμούς της ΕΕ συνεισφέρουν στη μεγιστοποίηση του επιπέδου ασφάλειας στην Ένωση.

3.3. Συνεργασίες και συνέργειες της ΕΕ.

Ο κυβερνοχώρος δεν διαθέτει συγκεκριμένα γεωγραφικά σύνορα και, συνεπώς, παρέχει τη δυνατότητα πραγματοποίησης παράνομων δραστηριοτήτων σε περισσότερα από ένα κράτη. Έτσι, καθίσταται προφανής η αναγκαιότητα διακρατικής αντιμετώπισης του φαινομένου και διατομεακής συνεργασίας.

Η εύρεση εναλλακτικών λύσεων αναγνωρίζεται ως επιτακτική ανάγκη, άμεσο απότοκο τόσο της έλλειψης μιας «ευρωπαϊκής αστυνομίας», όσο και της διατήρησης, από την πλευρά των κρατών μελών της Ένωσης, των κυριαρχικών τους δικαιωμάτων στο τομέα της εξωτερικής ασφάλειας. Η ευρωπαϊκή ολοκλήρωση συχνά αξιολογείται ως βέλτιστη επιλογή για την επίλυση παρόμοιων ζωτικής σημασίας ζητημάτων της Ένωσης. Η ενωσιακή ολοκλήρωση σαν όραμα υπήρχε ήδη από την αρχή του 20^{ου} αιώνα, με την σύναψη των πρώτων διεθνών συνθηκών. Στην επαύριο των δύο παγκοσμίων πολέμων, συνέπεια των οποίων αποτέλεσε η κρίση αξιών στην Ευρώπη, μίας μορφής διακρατική συνεργασία ανάμεσα στα κυρίαρχα κράτη του τότε ανεξάρτητου κόσμου, μεταξύ των οποίων οι μεγάλες ευρωπαϊκές δυνάμεις, προτάθηκε ως επικρατέστερη λύση. Ωστόσο, η ιδέα της ολοκλήρωσης παρέμεινε ουτοπική μέχρι και τα μέσα της δεκαετίας του 1960 (Sliwinski, 2014).

Οραματιστές, όπως ο Ντελόρ, θεώρησαν την Ευρωπαϊκή Οικονομική Ένωση (ΕΟΚ), τον προπομπό της ΕΕ, ως μία προοπτική για μία μόνιμη συνεργασία μεταξύ των ευρωπαϊκών κρατών. Οι πολιτικοί που στήριζαν στρατηγικές αυτού του περιεχομένου, αναφέρονταν σε μιάς μορφής «ομοσπονδιοποίηση» της Ένωσης με

σκοπό την μείωση των τριβών, την καλύτερη συνεργασία και την από κοινού πρόοδο και ανάπτυξη. Ωστόσο, τα εσωτερικά προβλήματα μεταξύ των ευρωπαϊκών κρατών, οι εθνικοί ανταγωνισμοί, οι διαφορές στη γλώσσα, την ανάπτυξη κοκ εμποδίζουν τα κράτη από το να παραχωρήσουν, πλήρως και εκούσια, τα κυριαρχικά τους δικαιώματα. Παρόλο που η Συνθήκη της Λισαβόνας προέβαλλε μία νέα διάσταση, φέρνοντας τα κράτη μέλη της ΕΕ πιο κοντά στην ιδέα της ολοκλήρωσης -ακόμη και σήμερα- τα κράτη απορρίπτουν την δημιουργία ενός ευρωπαϊκού συντάγματος, ως προοπτική και, αντ' αυτού, εστιάζουν στην οικονομική ολοκλήρωση. Επιλέγεται, επομένως, η συνεργασία από την εκχώρηση δικαιωμάτων παρότι, πράγματι, με την Συνθήκη της Λισαβόνας (2009) εντάθηκαν οι προσπάθειες για τη δημιουργία οργάνων που θα αναλαμβάνουν την εξωτερική εκπροσώπηση της Ένωσης, όπως η ΚΕΠΠΑ (Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας) που υφίσταται από το 1993 και ενισχύεται με την ΕΥΕΔ (Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης) (Ευρωπαϊκό Κοινοβούλιο, 2018).

Η ΕΕ συνεργάζεται πλέον ενεργά με εταίρους σε παγκόσμιο επίπεδο, τόσο στα πλαίσια των διεθνών οργανισμών όσο και με διακρατικές συνεργασίες (ENISAA, 2018). Ειδικότερα, η Ευρωπαϊκή Ένωση συνεργάζεται συστηματικά με (Petrovic, Bojkovic, Anic, Stamenkovic, & Tarle, 2014):

1) Τον Οργανισμό Ηνωμένων Εθνών (Ο.Η.Ε.).
2) Το ΝΑΤΟ και τους συμμάχους του και, πιο συγκεκριμένα, τις ΗΠΑ και τις υπηρεσίες τους.
3) Τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ).
4) Τον Οργανισμό για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ).
5) Τα κράτη που λαμβάνουν μέρος στην Παγκόσμια Διάσκεψη Κορυφής για την Κοινωνία της Πληροφορίας (WSIS) .

Το δίκαιο της ΕΕ δύναται να καλύψει σε ικανοποιητικό βαθμό θέματα τα οποία υπάγονται σε εσωτερικά ζητήματα της Ένωσης ή των κρατών μελών. Ωστόσο, μέσω της συνεργασίας με άλλους περιφερειακούς οργανισμούς, η Ένωση έχει επιτύχει την διεύρυνση του πεδίου εφαρμογής των συνθηκών της (Bachman, 2011).

Για την ΕΕ, η επίλυση προβλημάτων πρέπει να λαμβάνει χώρα ως μία συνολική προσπάθεια, χωρίς αυτό, ωστόσο, να σημαίνει πως τα κράτη μέλη δεν

μπορούν να προβούν στην εφαρμογή επιπρόσθετων διατάξεων, βάσει των διακριτικών αναγκών τους, των επιταγών της νομικής και θεσμικής τους παράδοσης, όπως επίσης και των εθνικών προτεραιοτήτων τους. Κατά συνέπεια, τα κράτη μέλη που εκτίθενται σε κίνδυνο κυβερνοεπιθέσεων και τα οποία αναγνωρίζουν την ύπαρξη προβλημάτων στην κυβερνοασφάλειά τους που, δυνητικά, θα επηρεάσουν το επίπεδο κυβερνοισχύος αυτών και της Ένωσης συνολικά, μπορούν να διευρύνουν το πεδίο ισχύος των συνθηκών, προτείνοντας επιπρόσθετα μέτρα και, εφόσον το ευρωπαϊκό δίκαιο τηρείται πλήρως, να εφαρμόσουν αυστηρότερους ελέγχους και διατάξεις (Bendiek, 2014).

Με την συνέργεια και την εγκαθίδρυση εταιρικών σχέσεων, η Ένωση αντιμετωπίζει διακρατικές απειλές και ρυθμίζει τις δράσεις της με σκοπό την μείωση του ρίσκου και των κινδύνων που άπτονται του πεδίου της συλλογής, αξιολόγησης και χρήσης δεδομένων. Παράλληλα, μειώνεται στο ελάχιστο ο κίνδυνος παραλείψεων, λαθών, εσφαλμένων εκτιμήσεων και παρανοήσεων και αυξημένης έκθεσης των πολιτών σε κινδύνους από διαδικτυακούς χρήστες. Η συνεργασία με τον ΟΑΣΕ αποτελεί χαρακτηριστικό παράδειγμα από κοινού αντιμετώπισης εξωτερικών κινδύνων στον κυβερνοχώρο. Τα θετικά αποτελέσματα που έχει επιφέρει η ως άνω συνεργασία αποδεικνύονται επίσης και με τη σημαντική μείωση του εμπορίου λευκής σαρκός, της τρομοκρατίας και της διακίνησης ναρκωτικών, περιορίζοντας ταυτόχρονα κάθε μορφής ασυδοσία (Hughes, 2014).

Αποσκοπώντας στην καταπολέμηση των βασικών προβλημάτων της κυβερνοισχύος, ο ΟΑΣΕ έχει προβεί, επιπλέον, στην εφαρμογή σύνθετων νομικών διατάξεων. Με την υπ' αριθ. 1202 απόφαση ενισχύει την προσπάθεια εγκαθίδρυσης δράσεων για την οικοδόμηση μέτρων εμπιστοσύνης και την αντιμετώπιση των κινδύνων συγκρούσεων που δύναται να προκύψουν από τη χρήση πληροφοριών. Ως στόχοι της εν λόγω απόφασης, σύμφωνα με το πλήρες κείμενο της, επισημαίνονται οι ακόλουθοι (ΟΑΣΕ, 2012):

- η ρύθμιση των σχέσεων για την καλύτερη ανταλλαγή τεχνογνωσίας, τεχνολογίας, πληροφοριών και δεδομένων,
- η ενθάρρυνση του διεθνούς διαλόγου και δικτύωσης για την αντιμετώπιση των κυβερνοαπειλών,
- η ενημέρωση των πολιτών,
- η λήψη περαιτέρω δράσεων και πρωτοβουλιών.

Ξεχωριστός λόγος θα πρέπει να γίνει και για τις προσπάθειες συνεργασίας του ΝΑΤΟ, της ΕΕ και του Συμβουλίου της Ευρώπης (ΣτΕ). Με την εφαρμογή της απόφασης 3/04 με στόχο την «καταπολέμηση της παράνομης χρήσης του Διαδικτύου και μετά την προσχώρησή του στη Μονάδα Δράσης κατά της Τρομοκρατίας (ΑΤΟ) που λειτουργεί στο Γραφείο για τα Ναρκωτικά και το Έγκλημα των Ηνωμένων Εθνών (UNODC)», οι στόχοι της ΕΕ για μία ευρωπαϊκή κοινή ατζέντα κατά της τρομοκρατίας ευθυγραμμίστηκαν με αυτές της διεθνούς κοινότητας (Pisano, Berger, Endl, & Sedlacko, 2011).

Η συχνότητα των κυβερνοεπιθέσεων τα τελευταία χρόνια αυξάνεται διαρκώς, όπως αποδεικνύεται και από τα δεδομένα της Europol για το 2015. Προς επίρρωση των ανωτέρω, επισημαίνεται πως κατά μέσο όρο, ανά δευτερόλεπτο, στην ΕΕ εκδηλώνονται δώδεκα (12) κυβερνοεγκλήματα στον κυβερνοχώρο (KPMG, 2015, σ. 2). Πάνω από το ογδόντα τοις εκατό (80%) αυτών καταπολεμούνται πριν προκαλέσουν πρόβλημα ασφαλείας. Συμπληρωματικά, σύμφωνα με την KPMG (2015, σ. 2-6), πάνω από το 45% των χρηστών τραπεζικών υπηρεσιών μέσω διαδικτύου έχουν πέσει θύματα τραπεζικών απατών ή επιθέσεων παρότι, στην πλειοψηφία τους, οι κυβερνοεπιθέσεις αντιμετωπίστηκαν εγκαίρως (KPMG, 2015).

Εξετάζοντας τα πληροφοριακά δεδομένα για το 2017, το διάστημα 2016-2017, η ΕΕ αντιμετώπισε, εκατόν δέκα (110) συνολικά κυβερνοεπιθέσεις που, στην πλειοψηφία τους, αντιμετωπίστηκαν εγκαίρως από τις υπηρεσίες με αντίστοιχα καθήκοντα, σε συνεργασία με τα γραφεία πληροφοριών των ΗΠΑ. Πολλές από αυτές τις επιθέσεις αποδίδονται σε οργανώσεις συντονισμένες ή υποστηριζόμενες από την ρωσική κυβέρνηση. Οι πληροφορίες αυτές διατάραξαν σημαντικά τις ρωσο-ευρωπαϊκές και ρωσο-αμερικανικές σχέσεις, αναδεικνύοντας τον διαρκή «χαρακτήρα» των απειλών, οι οποίες δύναται να προέρχονται από ποικίλες, επίσημες ή μη, πηγές, αναδεικνύοντας ως επιτακτική την αναγκαιότητα λήψης ακόμη πιο συντονισμένων πολιτικών (Kirby, 2017).

Ο αγώνας, συμπερασματικά, κατά της κυβερνοτρομοκρατίας και του κυβερνοεγκλήματος δεν διεξάγεται με συμβατικά μέσα. Απεναντίας, οι εγκληματίες χρησιμοποιούν εναλλακτικούς διαύλους, αποσκοπώντας στην κατάρριψη της άμυνας στον κυβερνοχώρο, όχι επιτιθέμενοι σε κεντρικές βάσεις πληροφοριών, αλλά με μαζικές επιθέσεις σε πιο «αδύναμους» δρώντες. Κατά συνέπεια, περισσότερο

ευάλωτες σε επιθέσεις καθίστανται οι μικρομεσαίες επιχειρήσεις που συνεργάζονται με δημόσιους φορείς και οι ιδιώτες (Prichard&MacDonald, 2004).Το ζήτημα, άλλωστε, της ασφάλειας του ηλεκτρονικού εμπορίου και, ειδικότερα, η προστασία των επιχειρήσεων και των οικονομικών δραστηριοτήτων αποτελεί έναν από τους σημαντικότερους στόχους και πρωτεύουσα προτεραιότητα της Ένωσης. Η τελευταία συνεργαζόμενη στενά με τα κράτη μέλη, αποσκοπεί στην ελαχιστοποίηση των οικονομικών κινδύνων και του στοιχείου της απειλής στο πεδίο των ηλεκτρονικών πληρωμών (Bendiek, 2014).

Στο πλαίσιο της ΕΕ η απειλή των κυβερνοεπιθέσεων στρέφεται, πρωτίστως, προς τους θεσμούς αλλά και τα κράτη μέλη της Ένωσης. Παρότι ορισμένα από τα κράτη μέλη είναι περισσότερο εκτεθειμένα σε απειλές, ειδικά τα ισχυρότερα σε διεθνές επίπεδο, όπως η Γαλλία και η Γερμανία, κάθε ένα διατηρεί αμοιβαία ευθύνη για το συντονισμό των πολιτικών και των ενεργειών του. Κύριοι κοινοί στόχοι, επομένως, αποτελούν η εξασφάλιση της λειτουργίας της κοινής αγοράς, η προστασία της ίδιας της Ένωσης, η διασφάλισης ενός καλού επιπέδου ασφάλειας και ευημερίας και η προάσπιση των δικαιωμάτων των πολιτών (ENISAA, 2018). Μία αντίστοιχη δέσμη προτεραιοτήτων, που εστιάζει, όμως, στην ασφάλεια και στην αντιμετώπιση της τρομοκρατίας και δεν περιλαμβάνει, σε τόσο μεγάλο βαθμό, την κοινή αγορά, πρεσβεύει και το NATO (Ziolkowski, 2013).

3.4. Κυβερνοασφάλεια στην Ελλάδα.

Δεδομένης της πρωτοκαθεδρίας του δικαίου της ΕΕ για τα κράτη μέλη της, το εθνικό πλαίσιο υποχρεούται να προσαρμόζεται στο ενωσιακό και, ως εκ τούτου και η χώρα μας υπόκειται σε συγκεκριμένες υποχρεώσεις (Carrapico & Barrinha, 2017). Παράλληλα, όμως, διατηρεί το δικαίωμα να διαμορφώσει το εθνικό της πλαίσιο αποσκοπώντας στην εξυπηρέτηση των συμφερόντων της και την κάλυψη των αναγκών της.

Στο πλαίσιο αυτό, η Ελλάδα έχει διαμορφώσει μία Εθνική Στρατηγική για την αντιμετώπιση των απειλών στον τομέα της κυβερνοασφάλειας, η οποία καλύπτει τους

ακόλουθους στόχους (Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης, 2018):

- Τη συνεργασία και την συνέργεια,
- Την εφαρμογή των ευρωπαϊκών στρατηγικών,
- Την καταγραφή και την αποτίμηση των ελληνικών πόρων και υποδομών,
- Την πλήρη εφαρμογή του εθνικού πλαισίου και την ανανέωσή του, εφόσον αυτό κριθεί αναγκαίο,
- Την καθοδήγηση και υποστήριξη των αρμόδιων φορέων,
- Την υποβοήθηση της εκπαίδευσης των αρμόδιων,
- Την ενημέρωση του κοινού,
- Την ανταλλαγή εμπειρογνωμοσύνης, τεχνογνωσίας και βέλτιστων πρακτικών.

Η Εθνική Στρατηγική Κυβερνοασφάλειας αποτελεί βασικό εργαλείο για τον συντονισμό των φορέων. Στα πλαίσια εφαρμογής της Οδηγίας 2016/1148 της ΕΕ, η προαναφερθείσα στρατηγική εγκρίθηκε το 2018 αποβλέποντας στην αναβάθμιση της ικανότητας αντιμετώπισης των προκλήσεων στον τομέα της κυβερνοασφάλειας (Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης, 2018). Οι φορείς που, κατεξοχήν, ασχολούνται με τον συγκεκριμένο τομέα είναι οι εξής (Μαυραγάνης, 2017):

- το Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, Υποδομών και Μεταφορών,
- η Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.),
- η Διεύθυνση Κυβερνοάμυνας, που ασχολείται με την άμυνα των ελληνικών ενόπλων δυνάμεων και εφαρμόζει τη Στρατιωτική Στρατηγική Κυβερνοάμυνας, το Δόγμα Επιχειρήσεων Κυβερνοχώρου, πολιτικής και Κυβερνοάμυνας, τα τεχνικά σχεδία δράσεως ανάπτυξης κυβερνοάμυνας στις Ένοπλες Δυνάμεις, και οργανώνει εθνικές ασκήσεις κυβερνοάμυνας, όπως ο «ΠΑΝΟΠΤΗΣ», ενώ συμμετέχει και σε διεθνείς ασκήσεις,
- η Δίωξη Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, η οποία είναι επιφορτισμένη με τον εντοπισμό και την αντιμετώπιση των απειλών στον κυβερνοχώρο, συνεργαζόμενη στενά με το Υπουργείο Προστασίας του Πολίτη, στη χάραξη στρατηγικών και τον συντονισμό δράσεων,

- η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεριμνά για την ασφάλεια των συναλλαγών και των δεδομένων που ανταλλάσσονται με τη χρήση του διαδικτύου.

Αν και η Ελλάδα δεν μπορεί να θεωρηθεί εξίσου εκτεθειμένη με άλλα κράτη μέλη της Ένωσης σε κυβερνοαπειλές, όπως και εξίσου ικανή να διαχειριστεί προβλήματα στον κυβερνοχώρο της, η συνεργασία της επιτρέπει -όντας λιγότερο ισχυρή οικονομικά και στρατιωτικά- να αντιμετωπίσει τις απειλές αποτελεσματικά (Biscop, 2017). Το θεσμικό πλαίσιο που ισχύει στη χώρα μας είναι αρκετά πλούσιο και καλύπτει διαφορετικές πτυχές του ζητήματος. Ως χαρακτηριστικά παραδείγματα βασικών νομικών διατάξεων επισημαίνονται τα άρθρα 5 και 9 του Ελληνικού Συντάγματος (Δικαίωμα στην πληροφόρηση και την ενημέρωση), το άρθρο 6 του Ποινικού Κώδικα (ΚΕΗΔ, 2018), η συμπληρωματική εθνική νομοθεσία για την αντιμετώπιση της παιδικής πορνογραφίας, ο Ν. 4411/2016 κοκ. Η αποτελεσματικότητα, ωστόσο, των νομοθετικών ρυθμίσεων παραμένει αμφιλεγόμενη (Biener, Eling, & Wirfs, 2015).

ΚΕΦΑΛΑΙΟ 4

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΚΡΙΤΙΚΗ

4.1. Αποτίμηση της ερευνητικής διαδικασίας.

Όσο ενθαρρυντική και αν είναι σήμερα ραγδαία εξέλιξη των μέσων αντιμετώπισης των κυβερνοεπιθέσεων, παρ' όλα αυτά, είναι εξαιρετικά δύσκολο να προβλεφθεί ο τρόπος με τον οποίο θα διασφαλιστεί η απόλυτη και έγκαιρη προστασία του κυβερνοχώρου, απέναντι στη γεωμετρικά εξελισσόμενη ακτίνα δράσης της κυβερνοτρομοκρατίας.

Το μόνο το οποίο είμαστε σε θέση να συμπεράνουμε με ασφάλεια, αποτελεί η διαπίστωση πως σε διεθνές επίπεδο, οι ανωτέρω προκλήσεις παρουσιάζουν πλήθος κοινών στοιχείων, χωρίς ωστόσο να μπορούν να χαρακτηριστούν ως όμοιες. Ως εκ τούτου, το υπό συζήτηση φαινόμενο, όντας διαρκώς υπό εξέλιξη, θα πρέπει να εξετάζεται συστηματικά και με ιδιαίτερη προσοχή, καθώς οι συνέπειες της κυβερνοτρομοκρατίας δεν περιορίζονται μόνο σε μία χώρα ή μία ομάδα πολιτών, όπως άλλωστε παρουσιάστηκε λεπτομερώς σε προηγούμενο κεφάλαιο. Γίνεται επομένως εμφανής η σπουδαιότητα της συνεχούς ενημέρωσης και η αποφυγή λήψης μέτρων αποκλειστικά σε επίπεδο κράτους, καθώς οι προκλήσεις έχουν ευρείες συνέπειες που ξεπερνούν τα εθνικά σύνορα.

Με γνώμονα λοιπόν την ανωτέρω διαπίστωση, αξιολογώντας την διαδικασία έρευνας για την συγγραφή της μελέτης και επιχειρώντας μία κριτική αποτίμηση των δεδομένων της, συνολικά, καθίσταται αναγκαία η επισήμανση ορισμένων διευκρινιστικών παρατηρήσεων.

Παρότι η ανάλυση έδωσε έμφαση στην αποτίμηση και την κριτική σύνθεση πληροφοριών από πρωτογενείς και δευτερογενείς πηγές, η χρήση αξιόπιστων δεδομένων ήταν δυσχερής, καθώς η εύρεση διαφορετικών στοιχείων από τις πηγές που αξιοποιήθηκαν αποτέλεσε συχνό φαινόμενο. Παρόλα αυτά, τα στοιχεία που χρησιμοποιήθηκαν καθ' όλη την έκταση της εργασίας έχουν διασταυρωθεί. Ωστόσο, κρίνεται αναγκαία η επισήμανση πως, κατά το παρελθόν, υπήρξε πληθώρα

κατηγοριών για αλλοίωση δεδομένων, με χαρακτηριστικότερα παραδείγματα το NATO και τη CIA. Επομένως, και λόγω της στρατηγικής σημασίας της κυβερνοασφάλειας και της κυβερνοισχύος, η ως άνω επιφύλαξη αποτέλεσε βασικό γνώμονα κατά την εξαγωγή των συμπερασμάτων της παρούσας μελέτης.

Ολοκληρώνοντας, υπογραμμίζεται πως ήταν ιδιαίτερα δύσκολη η εύρεση αξιοποιήσιμης και αξιόπιστης βιβλιογραφίας στην ελληνική γλώσσα. Με το ως άνω δεδομένο, ήταν απαραίτητη η χρήση και ανάλυση πηγών στην αγγλική, κυρίως, γλώσσα. Δεδομένου του γεγονότος ότι η πληθώρα του υλικού που εντοπίστηκε αποτελούσε αναδημοσιεύσεις, σημαντική ποσότητα πληροφοριών αποκλείστηκε και διατηρήθηκαν μόνο επίσημες πηγές ώστε να μην υπάρξει κίνδυνος ακούσιας παραπληροφόρησης.

4.2. Αξιολόγηση της στρατηγικής της ΕΕ.

Οι κυβερνοεπιθέσεις αποτελούν σοβαρές απειλές, με αντίκτυπο σε περισσότερες από μία χώρες, υποδεικνύοντας την αναγκαιότητα επικέντρωσης του ενδιαφέροντος στον ανθρώπινο παράγοντα. Η κυβερνοισχύς και ο «κυβερνο-πόλεμος» που διεξάγεται, μέσω της χρήσης του deep και του dark web σε διαδικτυακό περιβάλλον, δύνανται να επηρεάσουν την ποιότητα ζωής των πολιτών. Εντούτοις, το ερώτημα που γεννιέται είναι κατά πόσο το κοινό γνωρίζει, πράγματι, τους κινδύνους που αντιμετωπίζει κατά την καθημερινή χρήση του διαδικτύου.

Παράλληλα, η εξέλιξη των αμυντικών συστημάτων με τη χρήση ηλεκτρονικών υπολογιστών, δορυφορικών συστημάτων κοκ πολλαπλασίασε εν τέλει την τρωτότητά τους. Ειδικότερα, πολλά από τα μηχανήματα και μέρος του εξοπλισμού που περιλαμβάνονται στις στρατιωτικές επιχειρήσεις επιβλέπονται, εξ αποστάσεως. Συνεπώς, μία ενδεχόμενη κυβερνοεπίθεση θα μπορούσε να αλλάξει την έκβαση μίας επίθεσης σε πραγματικό χρόνο. Πέραν τούτου, η τεχνητή νοημοσύνη εξελίσσεται διαρκώς, με τα ρομποτικά συστήματα να χρησιμοποιούνται όλο και περισσότερο και στο πεδίο των μαχών (Chen, 2012).

Οι επιτυχίες της ΕΕ στην αντιμετώπιση των κυβερνοαπειλών είναι αξιοσημείωτες, καλύπτοντας διαφορετικές προτεραιότητες της. Ιδιαίτερη έμφαση δίδεται, επιπροσθέτως, και στην τάση για ευθυγράμμιση των εθνικών και ευρωπαϊκών επιχειρησιακών δράσεων για την καταπολέμηση του ηλεκτρονικού εγκλήματος, μέσω και της καλύτερης αξιοποίησης των διαθέσιμων πληροφοριακών συστημάτων (ENISAA, 2018).

Ένας εκ των βασικών λόγων χάρη στον οποίο οι ευρωπαϊκές πολιτικές έχουν αποδειχθεί μέχρι σήμερα αρκετά επιτυχείς, αποτελεί το γεγονός πως τα θεσμικά όργανα της ΕΕ, ιδίως η Ευρωπαϊκή Επιτροπή και το Ευρωπαϊκό Συμβούλιο, ανέπτυξαν και εφαρμόζουν μια "στρατηγική ασφαλείας", αποφεύγοντας παράλληλα τη μεμονωμένη αντιμετώπιση του φαινομένου εκ μέρους των κρατών μελών της Ένωσης. Όπως αναλύθηκε ανωτέρω, η ύπαρξη λεπτομερών διατάξεων για την πρόληψη κυβερνοεπιθέσεων και την προστασία των συστημάτων πληροφορικής των κρατών μελών, οδηγεί στην εξασφάλιση της δημιουργίας ενός «δικτύου προστασίας» που ελέγχεται σε ευρωπαϊκό επίπεδο. Δεδομένου ότι η παρέμβαση των ενωσιακών Οργάνων λαμβάνει χώρα άμεσα, τα κράτη μέλη συνεργάζονται σε ικανοποιητικό επίπεδο, με την διαδικασία ελέγχου να είναι αυτοματοποιημένη, γεγονός που οδηγεί στην αποφυγή άσκοπων καθυστερήσεων (Vries, 2005).

Η κριτική για την αποτελεσματικότητα της Ένωσης δεν θα πρέπει να εστιάζει μόνο στο θεσμικό επίπεδο, αλλά να περιλαμβάνει και μία εκτενή συζήτηση για τα κράτη μέλη. Σε εθνικό επίπεδο, η έρευνα έχει αποδείξει ότι οι περιοχές από τις οποίες προέρχεται η εγκληματική δραστηριότητα, εντοπίζονται στα κράτη που εμφανίζουν υψηλότερα επίπεδα διαφθοράς. Τέτοιου είδους δραστηριότητες παρατηρούνται συχνότερα στα κράτη μέλη που έχουν ενταχθεί πρόσφατα στην Ένωση, με χαρακτηριστικά παραδείγματα αυτά της Βουλγαρίας, της Ρουμανίας και της Κροατίας. Αντίθετα, τα οικονομικά ισχυρότερα κράτη μέλη της Ένωσης, όπως η Γαλλία, το Βέλγιο και η Γερμανία αποτελούν βασικούς στόχους κυβερνοεπιθέσεων. Ως εκ τούτου η Ευρωπαϊκή Ένωση θα πρέπει να δημιουργήσει μία συνεκτική πολιτική απέναντι στο φαινόμενο, με διττό στόχο, αφενός στην ενίσχυση της διαφάνειας στους αδύναμους πόλους της και αφετέρου στην προστασία των πολιτών τόσο στις οικονομικά εύρωστες, όσο και στις ασθενέστερες συγκριτικά χώρες (Dimitrova, Stoykov, &Marinov, 2018).

Η παγκοσμιοποίηση διαδραματίζει σημαντικότερο ρόλο στο σύγχρονο διεθνές σύστημα, λόγω της εντονότερης αλληλεξάρτησης μεταξύ των κρατικών δρώντων ως απότοκο κυρίως της τεχνολογικής προόδου. Η εν λόγω εξέλιξη καθιστά αυτούς τους δρώντες ιδιαίτερα επιρρεπείς σε κυβερνοαπειλές, αν και όχι απαραιτήτως στον ίδιο βαθμό. Είναι γεγονός, άλλωστε, πως τα κράτη που έχουν, όντως, τις υποδομές για να αντιμετωπίσουν μία ευρεία απειλή στον κυβερνοχώρο τους αναδεικνύονται, σε πολλές περιπτώσεις, ταυτόχρονα και δημοφιλής στόχοι τρομοκρατών και κυβερνοαπειλών (Chertoff & Simon, 2015).

Συμπληρωματικά, το επίπεδο ασφάλειας απέναντι στις κυβερνοαπειλές έχει ενισχυθεί μέσω της ανάπτυξης δικτύων συνεργασίας, όπως είναι η ΕΕ και το ΝΑΤΟ, τα οποία απέδειξαν ότι η κοινή απόκριση είναι εφικτή, απαραίτητη και επωφελής όταν διακυβεύονται εθνικά συμφέροντα, ακόμη και μεταξύ πάλαι ποτέ ανταγωνιστικών κρατικών δρώντων. Στις περιπτώσεις αυτές που τα κράτη έχουν δράσει από κοινού και έχουν ενεργοποιήσει τους μηχανισμούς ασφαλείας τους, για την αντιμετώπιση απειλών στον κυβερνοχώρο, παρατηρείται ενίσχυση της αποτελεσματικότητας των δράσεων (Bendiek, 2014).

Σημειώνεται, δε, πως η Ένωση απολαμβάνει σε θεσμικό επίπεδο ένα υψηλό βαθμό προστασίας των ατομικών δικαιωμάτων, ήτοι της ελευθερίας του λόγου και της έκφρασης, αποσκοπώντας στην διατήρηση ισορροπίας μεταξύ προστασίας και ελευθερίας. Από την άλλη πλευρά, τα κυριαρχικά δικαιώματα των κρατών μελών δεν θα πρέπει να παραγκωνίζονται σε ενωσιακό επίπεδο, παρόλο που η ανάληψη, εκ μέρους της Ένωσης, προκαταρκτικών μέτρων για την αποφυγή ενδεχόμενης εγκληματικής δραστηριότητας στον κυβερνοχώρο καθίσταται μία απαιτητική και ταυτόχρονα αναγκαία ενέργεια (Carrapico & Barrinha, 2017).

Η κυβερνοτρομοκρατία, όπως και το ηλεκτρονικό έγκλημα, έχουν αναδειχθεί σε πόλο μείζονος ενδιαφέροντος για τον ακαδημαϊκό και τον πολιτικό χώρο, αποτελώντας ένα νέο και, για πολλούς, άγνωστο τύπο εγκληματικής δραστηριότητας που δύναται να επηρεάσει τόσο την καθημερινότητά του απλού πολίτη όσο και την εν γένει οικονομική δραστηριότητα του επιχειρηματικού κόσμου. Η ραγδαία εξέλιξη τόσο των εξοπλισμών, όσο και γενικότερα, της τεχνολογίας, η οποία χρησιμοποιείται από τις διάφορες εγκληματικές και τρομοκρατικές ομάδες που δραστηριοποιούνται στον κυβερνοχώρο, καθιστά αναγκαία την προσαρμογή των αρχών επιβολής του

νόμου στη διαρκώς μεταβαλλόμενη πραγματικότητα. Μόνο έτσι θα καταστεί εφικτή η παρακολούθηση των εξελίξεων και μέσω αυτής η αντιμετώπιση των κυβερνοαπειλών με αξιόπιστο και διαρκή τρόπο (Biener, Eling, & Wirfs, 2015).

Σε προηγούμενο κεφάλαιο αναλύθηκαν εκτενώς οι λόγοι για τους οποίους οι κρατικές δράσεις αποτυγχάνουν στο εν λόγω τομέα. Ως χαρακτηριστικό παράδειγμα θα μπορούσε να αναφερθεί η έννοια της ρητορικής μίσους, για την οποία δεν υφίσταται επαρκής εννοιολογική οριοθέτηση από τον ευρωπαίο νομοθέτη. Άμεση απόρροια αποτελεί η αδυναμία ύπαρξης πλήρους σύμπνοιας μεταξύ των κρατών μελών, γεγονός το οποίο με τη σειρά του συνεπάγεται την αδυναμία εφαρμογής των υφιστάμενων κανόνων δικαίου, και ως εκ τούτου την αδυναμία οριστικής επίλυσης των προβλημάτων που έχουν ανακύψει (Biener, Eling, & Wirfs, 2015).

Τα φαινόμενα της ξενοφοβίας και της μισαλλοδοξίας που εκδηλώνονται στο διαδίκτυο δεν μπορούν να ρυθμιστούν και να αντιμετωπιστούν αποκλειστικά και μόνο μέσω δράσεων για τον περιορισμό της ρητορικής μίσους που εκδηλώνεται σε διαδικτυακό περιβάλλον. Αντιθέτως, λαμβάνοντας υπόψη και τον υβριδικό χαρακτήρα πολλών απειλών, οι κυβερνήσεις θα πρέπει να εφαρμόσουν μεικτού και σύνθετου χαρακτήρα δραστηριότητες. Η προσπάθεια αποκατάστασης των στερεοτυπικών αντιλήψεων και ο περιορισμός της εκδήλωσης ρατσιστικών φαινομένων στο περιβάλλον της κοινωνίας, θα πρέπει να αποτελέσει το εναρκτήριο έναυσμα των κρατών μελών της ΕΕ, διευρύνοντας, στη συνέχεια, τις προσπάθειές τους και στο ψηφιακό περιβάλλον (Betz, 2012).

Εάν τα φαινόμενα της τρομοκρατίας και της κυβερνοτρομοκρατίας, των κυβερνοαπειλών και της ξενοφοβίας που εκδηλώνονται στο διαδίκτυο εξεταστούν πολύπλευρα, εύκολα συνάγεται το συμπέρασμα πως πρόκειται για αλληλένδετα προβλήματα, με συγγενή αίτια. Οι κρίσεις που απορρέουν από τα προαναφερθέντα φαινόμενα οδηγούν τους κρατικούς δρώντες σε καθεστώς συνεχούς ανασφάλειας, προκαλώντας ενίοτε ανταγωνισμό ισχύος, που μπορεί να διαταράξει τις σχέσεις σε πολιτικό και οικονομικό επίπεδο (Eriksson&Giacomello, 2006).

Η δημιουργία σύγχρονων συστημάτων αντιμετώπισης κυβερνοαπειλών αποτελεί ένδειξη του γεγονότος πως η Ένωση έχει αναδειχθεί στον αποτελεσματικότερο οργανισμό σε διεθνές επίπεδο, στον εν λόγω τομέα. Προς αυτή την κατεύθυνση, η «επένδυση» της Ένωσης σε εταιρικές σχέσεις με τρίτες χώρες και

συνεργασίες μεταξύ των μελών της, δρα πολλαπλασιαστικά, ενισχύοντας την θωράκισής της σε τέτοιου είδους επιθέσεις (Carrapico&Barrinha, 2017).

Ο κυβερνοχώρος μη διαθέτοντας συγκεκριμένα σύνορα και, συνεπώς, παρέχοντας τη δυνατότητα πραγματοποίησης παράνομων δραστηριοτήτων σε περισσότερα από ένα κράτη, αναδεικνύει την αναγκαιότητα της από κοινού αντιμετώπισης του φαινομένου και της συνεργασίας μεταξύ θεσμών. Ένα πρώτο παράδειγμα είναι η συνεργασία που αναπτύσσεται μεταξύ ΕΕ και ΝΑΤΟ. Πριν να υπάρξει αυτή η συνέργεια, μία ενδεχόμενη επέμβαση μίας ευρωπαϊκής δύναμης σε μία επίθεση προερχόμενη από αμερικανικό έδαφος να δημιουργούσε μία διπλωματική κρίση μεταξύ ΗΠΑ και της εν λόγω χώρας.[1] Εν έτει 2018, ο κίνδυνος αυτός έχει ελαχιστοποιηθεί ως απότοκο της προαναφερθείσας συνεργασίας, ενώ συγχρόνως εξασφαλίζεται η αμοιβαία ανταλλαγή τεχνογνωσίας και τεχνολογίας (Carrapico&Barrinha, 2017).

Η Europol συνιστά το επίσημο «εργαλείο» της Ευρωπαϊκής Ένωσης για την καταστολή αυτών των διεθνών εγκληματικών δραστηριοτήτων. Μια εκ των επιδιώξεων αυτής της ευρωπαϊκής υπηρεσίας είναι και η εξασφάλιση συνεργασίας με έναν φορέα συλλογής και επεξεργασίας πληροφοριών, όπως είναι η CIA, προκειμένου να λειτουργήσουν ως έναν σημαντικό διεθνή παράγοντα επιβολής του νόμου (ENISAA, 2018). Ωστόσο, μέχρι σήμερα, η αδυναμία επίτευξης του επιθυμητού επίπεδου συνεργασίας μεταξύ των ανωτέρω Οργανισμών, στερεί την αναβάθμιση της ευελιξίας τους, γεγονός που καθιστά δυσχερή την δυνατότητα να συμβαδίσουν με τη συνεχή ανάπτυξη και εξέλιξη του κυβερνοχώρου.

Εντός ενός έθνους κράτους το οποίο διαθέτει εποπτεία επί των αποφάσεων που λαμβάνουν τα όργανά του, είναι δυνατή η άμεση ανταπόκριση στις «παραδοσιακές» εγκληματικές δραστηριότητες. Παρόλα αυτά, οι κυβερνοεπιθέσεις δεν είναι εξίσου απλές στην αντιμετώπισή τους με το παραδοσιακό έγκλημα. Κατά συνέπεια, προκειμένου να καταστεί εφικτή η επίτευξη σταθερότητας και η διατήρηση της τάξης στο εσωτερικό του κράτους, χρήζει αναγκαία η πλήρης εποπτεία κάθε δραστηριότητας εντός του κυβερνοχώρου. Βεβαίως, κάτι τέτοιο είναι αδύνατο σε κρατικό επίπεδο,

[1]Λαμβάνουμε εδώ ως δεδομένο ότι η κυρίαρχη χώρα στο πλαίσιο του ΝΑΤΟ είναι οι ΗΠΑ, λόγω της οικονομικής στήριξης που παρέχει στον Οργανισμό του Βορειοατλαντικού Συμφώνου και των πολιτικών κατευθύνσεων που υποδεικνύει σε αυτόν.

δεδομένου του όγκου και της ταχύτητας ανταλλαγής πληροφοριών που λαμβάνει στο διαδικτυακό περιβάλλον (Biener, Eling, &Wirfs, 2015). Αυτή η αβεβαιότητα λόγω της αδυναμίας πλήρους εποπτείας αποτελεί το πρωτεύον στοιχείο, το οποίο επιδιώκουν να εκμεταλλευτούν οι τρομοκρατικές οργανώσεις και οι εγκληματίες που αποσκοπούν στην πρόκληση «πλήγματος» στην κυβερνοισχύ των κρατών.

Υπό το πρίσμα των ανωτέρω, καθίσταται αντιληπτό ότι είναι απαραίτητη η συμβολή της Ένωσης και των εργαλείων της. Ωστόσο, το γεγονός ότι δεν έχει επιταχυνθεί η ολοκλήρωση εντός αυτής, σε συνδυασμό με την πρωτοτυπία των προκλήσεων που καλείται να αντιμετωπίσει, περιπλέκει την κατάσταση ακόμη περισσότερο. Αναδεικνύονται κατ΄ αυτό τον τρόπο οι βασικές αδυναμίες του ενωσιακού οικοδομήματος, με τις κάτωθι να αναγνωρίζονται ως σημαντικότερες:

Καταρχήν, η Ένωση βασίζεται στις δυνατότητες του ΝΑΤΟ για την εξασφάλιση της εξωτερικής ασφάλειας. Παρότι με την ΚΕΠΠΑ, έως ένα σημείο, αυτό περιορίζεται, στην πραγματικότητα χωρίς έναν οργανωμένο ευρωπαϊκό στρατό, άμεση επέμβαση είναι αδύνατο να υπάρξει (Pisano, Berger, Endl, &Sedlacko, 2011).

Δεύτερον, λόγω του διεθνούς ανταγωνισμού ισχύος στο διεθνές σύστημα, η ΕΕ καθίσταται εκ των βασικών στόχων κυβερνοεπιθέσεων, οι οποίες αποσκοπούν στην αποδιοργάνωση των θεσμικών της οργάνων και κατ΄ επέκταση την αποσταθεροποίηση της ίδιας της Ένωσης (Biener, Eling, &Wirfs, 2015).

Τρίτον, παρότι η ΕΕ είναι σε θέση να αντιμετωπίσει μία «ευρωπαϊκή απειλή», πολλά από τα πιο «αδύναμα» κράτη μέλη της, όπως η Βουλγαρία και η Κύπρος, δεν διαθέτουν εξίσου ισχυρούς προληπτικούς μηχανισμούς, με αποτέλεσμα να εκτίθενται σε υψηλότερο κίνδυνο. Το παράδειγμα της Εσθονίας που υπέστη διεθνή διασυρμό λόγω των κυβερνοεπιθέσεων που έπληξαν την κυβερνοισχύ της το 2007 είναι χαρακτηριστικό (Euronews, 2017).

Η βαθύτερη ευρωπαϊκή ολοκλήρωση, πράγματι, θα επέλυε ορισμένα βασικά ζητήματα που αντιμετωπίζει η Ένωση, αναδεικνύοντάς την σε ισχυρό δρώντα ικανό να αντεπεξέλθει στην πλειοψηφία των εξωτερικών απειλών. Ωστόσο, κάτι τέτοιο ενδεχομένως να σήμαινε και την ανάδειξη περισσότερων ανταγωνιστικών τάσεων απέναντι στις ΗΠΑ και, πιθανόν, θα έθετε σε αμφισβήτηση τη χρησιμότητα του ΝΑΤΟ. Έτσι, θα υπήρχε πιθανό ρίσκο τριβής τόσο με τις Ηνωμένες Πολιτείες Αμερικής όσο και με άλλες μεγάλες δυνάμεις, όπως η Ρωσία και η Κίνα, με συνέπειες

στην εξωτερική πολιτική όσο και την παγκόσμια οικονομία. Δεδομένης της αδυναμίας ταύτισης απόψεων, τα τελευταία χρόνια, των κρατών μελών της Ένωσης, η ολοκλήρωση δεν έχει επιτευχθεί στον επιθυμητό βαθμό, γεγονός όμως που ενόψει των ανωτέρω μπορεί να διαθέτει και θετικές διαστάσεις (Klimburg, 2010).

Σταχυολογώντας τα βασικότερα στοιχεία της ως άνω αξιολόγησης, το κάτωθι αντικείμενο μελέτης εγείρει το ερευνητικό μου ενδιαφέρον για μελλοντική ενασχόληση:

Μία ενδεχόμενη κατάρρευση του έθνους κράτους ως απόρροια κυβερνοαπειλής, φαντάζει απίθανη. Οι χώρες οργανώνουν τις στρατηγικές τους με στόχο να εξελίξουν τα συστήματα προστασίας τους σε διαδικτυακό περιβάλλον, εκμεταλλευόμενες το ρόλο του ηλεκτρονικού υπολογιστή και του διαδικτύου στην ενίσχυση της εξωτερικής τους ασφάλειας. Παράλληλα, οι διακρατικές σχέσεις λαμβάνουν πλέον χώρα σε ένα νέο είδος συστήματος, όπου εφαρμόζεται ένα μείγμα εθνικών πολιτικών και υπερεθνικών δράσεων εντός των διεθνών και περιφερειακών οργανισμών. Θα είχε λοιπόν ενδιαφέρον να εστιάσει κανείς στο πώς και εάν αυτή η αντίληψη του διεθνούς συστήματος αναδεικνύει μία νέα τάση στις διεθνείς σχέσεις.

Με γνώμονα το σύνολο των ανωτέρω παρατηρήσεων είναι αναγκαίο να διευκρινιστεί αν τελικά ο κυβερνοχώρος, για τα κράτη μέλη της ΕΕ και τα θεσμικά της όργανα, αποτελεί ένα εργαλείο ή τελικό σκοπό (Bachman, 2011).

Σύμφωνα με τα όσα επισημαίνονται στα κείμενα Στρατηγικών της Ένωσης, η διαχείριση των προβλημάτων στον τομέα της κυβερνοασφάλειας αναγνωρίζεται ως μία πρόκληση και μία προοπτική για την ΕΕ. Η πλήρης συνεργασία των κρατών μελών για την εκπλήρωση των στόχων της Ένωσης στον τομέα αυτό, αποτελεί δείγμα της ικανότητας και πρόθεσής τους να συνεργαστούν σε ζητήματα υψηλής πολιτικής, επικαλούμενα τις πραγματικές απειλές που εντοπίζονται στον κυβερνοχώρο (Carrapico & Barrinha, 2017).

Η συνέργεια και η επίτευξη συμβιβασμών την επίτευξη σύγκλισης στρατηγικών, καθώς και η «επένδυση» των κρατών σε ιδίες πρωτοβουλίες, οι οποίες με τη σειρά τους διευρύνουν το ευρωπαϊκό θεσμικό πλαίσιο, με τρόπους που όχι μόνον δεν παρεμποδίζουν το έργο της Ένωσης, αλλά, αντίθετα, το ενισχύουν, αποδεικνύουν πως η ευρωπαϊκή ολοκλήρωση ίσως να μην αποτελεί ένα ουτοπικό όραμα, αλλά μία

μελλοντική προοπτική (Bachman, 2011). Επιπροσθέτως, η υποστήριξη του ΝΑΤΟ και η συνεργασία με τις ΗΠΑ αποδεικνύουν πως η ασφάλεια στον κυβερνοχώρο είναι μάλλον περισσότερο σκοπός σε ό,τι αφορά τις εξωτερικές σχέσεις της ΕΕ και εργαλείο στον τομέα της ευρωπαϊκής διακυβέρνησης.

Επομένως, είναι ίσως καλύτερο να υποθέσει κανείς πως ο κυβερνοχώρος είναι ένας «νοητός» χώρος που, για τα κράτη μέλη, πρέπει να προστατεύεται και να εξελίσσεται διαρκώς. Ωστόσο, ερωτηματικό παραμένει το αν η Ένωση θα κατορθώσει να ανταπεξέλθει στις νέες προκλήσεις που αναδύονται στον κυβερνοχώρο και αν θα παραμείνει ένας ισχυρός παίκτης στο διεθνές σύστημα.

ΒΙΒΛΙΟΓΡΑΦΙΑ ΚΑΙ ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. Al Rowaily, K., Abulaish, M., Haldar, N., & Al Rubaian, M. (2015). BiSAL–A bilingual sentiment analysis lexicon to analyze Dark Web forums for cyber security. *Digital Investigation, 14*, σσ. 53-62.
2. Bachman, S. (2011). Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management. *Amicus Curiae, 88*, σσ. 24-26. Ανάκτηση Αύγουστος 17, 2018, από http://sas-space.sas.ac.uk/4562/1/1671-2132-1-SM.pdf
3. Bendiek, A. (2014). Tests of partnership: transatlantic cooperation in cyber security, internet governance, and data protection. *SSOAR Publications, GESIS, Leibniz Institut fur Sozialwissenschaften*, σσ. https://www.ssoar.info/ssoar/bitstream/handle/document/38557/ssoar-2014-bendiek-Tests_of_partnership_transatlantic_cooperation.pdf?sequence=1.
4. Betz, D. (2012). Cyberpower in strategic affairs: neither unthinkable nor blessed. *Journal of Strategic Studies, 35(5)*, σσ. 689-711.
5. Biener, C., Eling, M., & Wirfs, J. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1)*, σσ. 131-158.
6. Biscop, S. (2017). *Differentiated integration in defence: a plea for PESCO.* Instituto Affari Internazionali.
7. Brauchler, B. (2007). Religious conflicts in cyberage. *Citizenship Studies, 11(4)*, σσ. 329-347.
8. Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? *JCMS: Journal of Common Market Studies, 55(6)*, σσ. 1254-1272.
9. Cashell, B., Jackson, W., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC). *Congressional Research Service Documents, CRS RL32331.* Washington DC: http://www.au.af.mil/au/awc/awcgate/crs/rl32331.pdf.

10. Chen, H. (2012). Intelligence and Security Informatics (ISI): Research Framework. Στο *Dark Web* (σσ. 19-30). New York: Springer.
11. Chertoff, M., & Simon, T. (2015). The impact of the Dark Web on Internet governance and cyber security. *Global Commission on Internet Governance*. (Gigi, Μεταγλωττιστής) Gigionline. Ανάκτηση Αύγουστος 19, 2018, από https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf
12. Dimitrova, S., Stoykov, S., & Marinov, R. (2018, June). Black Sea Region and European Security Policy. *International conference, "Knowledge Based Organizations", Vol. 24, No. 1. Sciendo*, σσ. 65-70.
13. ENISAA. (2018). NIS Platform. *Resilience and security of communication infrastructure, networks and services*. Ανάκτηση Αύγουστος 15, 2018, από https://resilience.enisa.europa.eu/nis-platform
14. Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory? *International political science review, 27(3)*, σσ. 221-244.
15. EU. (2018). *Fact sheet PESCO.* https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en.
16. Euronews. (2017, Σεπτέμβριος 29). ΕΕ: η κυβερνοασφάλεια στο Επίκεντρο. *http://gr.euronews.com/2017/09/29/ee-i-kyvernoasfaleia-sto-epikentro*.
17. Europol. (2018). *Cybercrime.* https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime .
18. Fiott, D. (2017). *The CARD on the EU defence table.* European Union Institute for Security Studies.
19. Fu, T., Abbasi, A., & Chen, H. (2010). A focused crawler for Dark Web forums. *Journal of the American Society for Information Science and Technology, 61(6)*, σσ. 1213-1231.
20. Funk, T. (2008). *Web 2.0 and beyond: Understanding the new online business models, trends, and technologies.* Praeger Publishers.
21. Giacomello, G. (2014). Close to the edge: Cyberterrorism today. Στο *Understanding Terrorism* (σσ. 217-236). Emerald Group Publishing Limited.

22. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2(1)*, σσ. 13-20.
23. Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, σσ. 817-885.
24. Hongthong, W. (2017). Preventative Measures against On-line Hate Speech: A Case Study of Thailand Political Conflict, 2005-2014. *International Journal of Crime, Law and Social Issues, 4(1)*, σσ. 17-27.
25. Hughes, D. M. (2014). Trafficking in human beings in the European Union: Gender, sexual exploitation, and digital communication technologies. *Sage Open, 4(4)*.
26. Jenses, E. (2009). Cyber warfare and precautions against the effects of attacks. *Tex. L. Rev., 88*, σ. 1533.
27. Kirby, W. (2017, Ιανουάριος 8). EU MELTDOWN: Number of cyber attacks on Brussels servers SURGE amid Russian hacking fears. *Express Co.* https://www.express.co.uk/news/world/751773/EU-Brussels-Russia-cyber-hacking-increase-Russia-Julian-King-France-Germany-elections-nato.
28. Klimburg, A., & Tirmaa Klaar, H. (2011). *Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU.* Βρυξέλλες: European Parliament, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO-SEDE_ET(2011)433828.
29. Klimburg, A. (2010). The Whole of Nation of Cyberpower. *Geo. J. Int'l Aff., 11*, σ. 171.
30. KPMG. (2015). The cybersecurity Challenge. *KPMG online*, σσ. https://home.kpmg.com/xx/en/home/insights/2018/06/if-recognizing-the-problem-is-half-the-battle-then-ceos-are-ready-for-the-cyber-security-challenge.html.
31. Kuehl, D. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, σ. 30.
32. Merriam-webster. (2018, Αύγουστος 21). https://www.merriam-webster.com/dictionary/cyberspace.

33. Ottis, R., & Lorrents, P. (2010). Cyberspace: Definition and implications. *In International Conference on Cyber Warfare and Security* (σ. 267). Academic Conferences International Limited.
34. Petrovic, M., Bojkovic, N., Anic, I., Stamenkovic, M., & Tarle, S. (2014). An ELECTRE-based decision aid tool for stepwise benchmarking: An application over EU Digital Agenda targets. *Decision Support Systems, 59*, σσ. 230-241.
35. Pisano, U., Berger, G., Endl, A., & Sedlacko, M. (2011). *Sustainable development governance and policies in the light of major EU policy strategies and international developments.* Vienna: ESDN Quarterly Report, European Sustainability Network (ESDN). Ανάκτηση Αύγουστος 15, 2018, από http://www.sd-network.eu/quarterly%20reports/report%20files/pdf/2011-September-SD_governance_and_policies.pdf
36. Prichard, J., & Mac Donald, L. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks. *Journal of Information Technology Education: Research, 3*, σσ. 279-289.
37. Provos, N., Rajab, M., & Mavrommatis, P. (2009). Cybercrime 2.0: when the cloud turns dark. *Queue, 7(2)*, σσ. 46-47.
38. Raboin, B. (2011). Corresponding evolution: international law and the emergence of cyber warfare. *J. Nat'l Ass'n Admin. L. Judiciary, 31*, σ. 602.
39. Sliwinski, K. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy, 35(3)*, σσ. 468-486.
40. Tikk, E. (2011). Global cybersecurity–Thinking about the niche for NATO. *SAIS Review of International Affairs, 30(2)*, σσ. 105-109.
41. Vries, G. D. (2005). The European Union's Role in the Fight Against Terrorism:[Opening Address-The Role of the EU in the Fight Against Terrorism]. *Irish studies in international affairs, 16*, σσ. 3-9.
42. Weber, R., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review, 32(5)*, σσ. 715-728.
43. Wessel, R. (2015). Towards EU cybersecurity law: Regulating a new policy field. *Chapters*, σσ. 403-425.
44. Yost, D. S. (2010). NATO's evolving purposes and the next Strategic Concept. *International affairs, 86(2)*, σσ. 489-522.

45. Ziolkowski, K. (2013). *Peacetime regime for state activities in cyberspace.* Tallinn: CCDCOE NATO: NATO Cooperative Cyber Defence Center of Excellence, http://www.academia.edu/download/40986873/Peacetime-Regime_for_state_activities_in_cyberspace.pdf.
46. Γιάννης, Ν. (2014). *Αρχή της Επικουρικότητας, Αρχή της Ελευθερίας, Συμμετοχής και Ευθύνης.* Αθήνα: ΚΕΦΙΜ. Ανάκτηση από https://www.kefim.org/images/pdf/20140829_subsidiarity1.pdf
47. ΔΒΜ. (2013). *Στρατηγική Ευρώπη 2020.* ΥΠΕΘ, Γενική Γραμματεία Δια Βίου Μάθησης. Αθήνα: Ελληνική Δημοκρατία. Ανάκτηση Αύγουστος 19, 2018, από http://www.gsae.edu.gr/el/european-union/europe-2020-strategy/812-2020
48. ΕΕ. (2018). *ENISA.* https://europa.eu/european-union/about-eu/agencies/enisa_el.
49. Ευρωπαϊκό Κοινοβούλιο. (2018). Εξωτερική πολιτική- στόχοι, μέσα και επιτεύγματα. http://www.europarl.europa.eu/factsheets/el/sheet/158/%CE%B5%CE%BE%CF%89%CF%84%CE%B5%CF%81%CE%B9%CE%BA%CE%B7-%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%B7-%CF%83%CF%84%CE%BF%CF%87%CE%BF%CE%B9-%CE%BC%CE%B5%CF%83%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%B5%CF%80%CE%.
50. ΚΕΗΔ. (2018). *Προειδοποίηση της ΕΕ στα κράτη μέλη για την κυβερνοασφάλεια.* Αθήνα: http://www.dgrc.gr/blog/proidopiisi-tis-ee-sta-krati-meli-gia-tin-kyvernoasfalia/, Κέντρο Έρευνας για την Ηλεκτρονική Διακυβέρνηση.
51. Μαυραγάνης, Κ. (2017). *Κυβερνοεπιθέσεις και Κυβερνοασφάλεια στην Ελλάδα.* Αθήνα: https://www.huffingtonpost.gr/2017/05/06/eidhseis-politikh-tech-kyvernoepi8eseis-kai-kyvernoasfaleia-sthn-ellada-_n_15683960.html, Huffington Post.
52. Νόμος 4411/2016. (2016). Αθήνα: https://www.taxheaven.gr/laws/law/index/law/766.
53. ΟΑΣΕ. (2012). Cyber / ICT Security.

http://www.osce.org/secretariat/256071?download=true.

54. Πανελλήνιο σχολικό δίκτυο. (2017). *Παιδική πορνογραφία.* Αθήνα: https://blogs.sch.gr/internet-safety/archives/1052.
55. Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης. (2018). *Εθνική Στρατηγική Κυβερνοασφάλειας.* Αθήνα: http://www.mindigital.gr/index.php/kyvernoasfaleia/2055-ethniki-stratigiki-kyvernoasfaleias.