ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ: ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΜΣ: ΕΘΝΙΚΗ ΚΑΙ ΕΝΩΣΙΑΚΗ ΔΙΟΙΚΗΣΗ

Έτος: 2018-2019

Διπλωματική Εργασία με θέμα:

Κυβερνοασφάλεια και Συγκρούσεις στον Κυβερνοχώρο.

Εικόνα 1 https://www.enisa.europa.eu/news/enisa-news/regional-cybersecurity-forum-for-europe

Ενωσιακές δράσεις κατά των κυβερνοεπιθέσεων.

Επιβλέπων Καθηγητής: Δονάτος Παπαγιάννης

Ονοματεπώνυμο: Αλεξάνδρα Κοσκινά

A.M.: 7118M006

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον κ. Μάρκο Παπακωνσταντή για τις πολύτιμες συμβουλές και την καθοδήγηση καθ' όλη τη διάρκεια εκπόνησης της παρούσας εργασίας. Ακόμη, θερμές ευχαριστίες στον κ. Δονάτο Παπαγιάννη, Διευθυντή του Μεταπτυχιακού Προγράμματος Σπουδών για την αμέριστη στήριξη που επέδειξε αλλά και την έμπνευση που παρείχε. Τέλος θα ήθελα να εκδηλώσω τις ευχαριστίες μου σε όλους τους διδάσκοντες του τμήματος και ιδιαιτέρως στην κ. Πολυξένη Παπαδάκη για την αδιάκοπη ενασχόληση και την έμπρακτη βοήθεια της σε αυτό το ακαδημαϊκό ταξίδι.

Τριμελής Επιτροπή

Επιβλέπων καθηγητής: Δονάτος Παπαγιάννης

Μέλη: Πολυξένη Παπαδάκη, Μάρκος Παπακωνσταντής

Περίληψη

Η παρούσα εργασία έχει ως σκοπό την ανάλυση των βασικών εννοιών που συνθέτουν τον κυβερνοχώρο και τις συγκρούσεις που αναπτύσσονται στους κόλπους του έτσι ώστε ο αναγνώστης να κατανοήσει εις βάθος την έννοια της κυβερνοασφάλειας αλλά και την ανάγκη θεσμοθέτησης στρατηγικών για την θωράκιση της τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο. Σε αυτή τη βάση περιγράφεται η νέα πραγματικότητα των επιθέσεων την οποία πρέπει να διαχειριστούν όχι μόνο τα κράτη αλλά και οι πολίτες σε ατομική βάση.

Αφότου ο αναγνώστης έχει αποκτήσει μια σφαιρική εικόνα σχετικά με τις έννοιες που συνθέτουν την κυβερνοασφάλεια, αναλύονται οι Οργανισμοί οι οποίοι επιφορτίζονται την εφαρμογή των μέτρων που θέτει στο επόμενο επίπεδο η νομοπαραγωγική δράση της Ένωσης σχετικά με την καταπολέμηση των κυβερνοεπιθέσεων από το 2002 έως και σήμερα.

Έχοντας αναλύσει εις βάθος το νομοθετικό πλαίσιο της κυβερνοασφάλειας στην Ένωση, στη συνέχεια θίγονται οι διεθνείς συνεργασίες της Ένωσης στην προσπάθεια να θεσπιστούν παγκόσμιοι κοινοί κανόνες αντιμετώπισης των κυβερνοαπειλών ώστε να πραγματοποιηθεί ουσιαστική σύμπλευση σε διεθνές επίπεδο.

Τέλος, ο αναγνώστης λαμβάνει γνώση των προοπτικών που υπάρχουν για την επίτευξη του υψηλότερου δυνατού επιπέδου ασφαλείας και των ευκαιριών εξέλιξης που διαθέτει η Ένωση ώστε να δημιουργήσει την πλέον αποτελεσματική στρατηγική κυβερνοασφαλείας.

Μετά το πέρας της ανάγνωσης αναμένεται να έχει αποσαφηνιστεί η πολυπλοκότητα του κυβερνοχώρου και των απειλών που αυτή επιφέρει σε συνδυασμό με τις δράσεις που αναλαμβάνει η Ένωση στο πλαίσιο του Χώρου Ελευθερίας Ασφάλειας και Δικαιοσύνης για τη δημιουργία ασφαλούς χώρου δράσης για τους πολίτες της.

Λέξεις – Κλειδιά

Ασφάλεια

Διαδίκτυο

Διεθνείς συνεργασίες

Ενωσιακή στρατηγική

Επιτροπή

Κυβερνοασφάλεια

Κυβερνοεπίθεση

Κυβερνοπόλεμος

Κυβερνοχώρος

Νομοθετική πράξη

Προκλήσεις

Κράτη-μέλη

Συμβούλιο

Hackers

Συντομογραφίες

ΕΕ: Ευρωπαϊκή Ένωση

ΧΕΑΔ: Χώρος Ελευθερίας Ασφάλειας και Δικαιοσύνης

ENISA: Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια

CSIRT: Ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών

CDPF: Cyber Defence Policy Framework

DDoS: Distributed Denial of service Attacks

N.A.T.O.: North Atlantic Treaty Organization

JOIN: Joint proposals, communications, reports, white papers and green papers adopted by the Commission and the High Representative

COM: Other documents: communications, recommendations, reports, white papers, green papers

ΤΠΕ: Τεχνολογία Πληροφοριών και Επικοινωνιών

ΕΕΠ: Ενιαία Ευρωπαϊκή Πράξη

ΔΕΥ: Δικαιοσύνη και Εσωτερικές Υποθέσεις

ΣΕΕ: Συνθήκη για την Ευρωπαϊκή Ένωση

ΣΛΕΕ: Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης

ΜΜΕ: Μικρές και Μεσαίες Επιχειρήσεις

CERT-EU: Computer Emergency Response Teams

EC3: European Cybercrime Center

IOCTA: Internet Organized Crime Treat Assessment

ΕΥΖΣ: Ευρωπαϊκές Υποδομές Ζωτικής Σημασίας

CIFP: Critical Information Infrastructure Protection

ΕΟΠΙΚ: Ευρωπαϊκή Ομάδα Πιστοποίησης της Κυβερνοασφάλειας

CCDCOE: Cooperative Cyber Defense Centre of Excellence

CEPOL: European Union Agency for Law Enforcement Training

ΕΑΑ: Ευρωπαϊκή Αστυνομική Ακαδημία

ΚΠΑΑ: Κοινή Πολιτική Ασφάλειας και Άμυνας

ΕΥΕΔ: Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης

PESCO: Permanent Structure Operation

ΕΟΑ: Ευρωπαϊκός Οργανισμός Άμυνας

EUMS: European Union Military Staff

CMPD: Crisis Management and Planning Directoratekαι τη Μη Στρατιωτική

CPCC: Civilian Planning and Conduct Capability

ECSM: European Cyber Security Awareness

Περιεχόμενα

Εισαγωγή

Ο 21ος αιώνας χαρακτηρίζεται από άκρατη τεχνολογική εξέλιξη στον τομέα των επικοινωνιών, των μεταφορών, της οικονομίας, της πολιτικής, της διακυβέρνησης, των καθημερινών δραστηριοτήτων και της συνδεσιμότητας. Η 4η βιομηχανική επανάσταση, η επανάσταση των πληροφοριακών συστημάτων, όπως πολλοί την χαρακτηρίζουν, έχει μεταλλάξει τον κόσμο όπως τον γνωρίζαμε πριν την εμφάνιση του διαδικτύου. Η διάδοση του διαδικτύου και η μετέπειτα εγκαθίδρυση του ως βασικό εργαλείο στην πλειοψηφία των κοινωνικών, οικονομικών και πολιτικών αλληλεπιδράσεων έχει μεταλλάξει την πραγματικότητα των διακρατικών σχέσεων-πέραν των ατομικών- σε τέτοιο βαθμό ώστε οι διαταραχές οι οποίες έχουν δημιουργηθεί και συνεχίζουν να δημιουργούνται χρήζουν τέτοιας αντιμετώπισης για την οποία δεν υφίσταται ούτε νομικό ούτε πρακτικό προηγούμενο.

Η πολυπλοκότητα του διαδικτύου και η άνευ ορίων διάθεση του, το καθιστά το πλέον διαχειρίσιμο μέσο για την ανάπτυξη εγκληματικών ενεργειών οι οποίες υπερβαίνουν τα διακρατικά σύνορα και πολλές φορές λαμβάνουν τη μορφή σύρραξης χωρίς όμως αυτή να συνοδεύεται από τη χρήση όπλων και επίσης, δίχως τη συνέπεια της ανθρώπινης απώλειας. Οι νέες αυτές συγκρούσεις, οι λεγόμενες κυβερνοεπιθέσεις, αποτελούν μια νέα μορφή πολέμου η οποία ίσως να φαίνεται ηπιότερη λόγω της μη ύπαρξης ανθρώπινης απώλειας, όμως ο τρόπος διεξαγωγής της και τα πλήγματα που εν τέλει δύναται να επιφέρει, την κατατάσσουν στις πλέον επικίνδυνες και στις πλέον δύσκολα αντιμετωπίσιμες. Η δυσκολία στα μέτρα απόκρουσης των κυβερνοεπιθέσεων έγκειται στο χαοτικό περιβάλλον του κυβερνοχώρου, στην ευκολία απόκρυψης των στοιχείων του δράστη και στην ταχέως αναπτυσσόμενη τεχνολογία της πληροφορίας η οποία με την εξέλιξη της δεν δημιουργεί μόνον καινοτομίες θετικού αντίκτυπου, αλλά διανοίγει και νέους δρόμους επιθετικών δράσεων σε σημαντικά δίκτυα και πληροφορίες υψηλής κρατικής σημασίας.

Το ζήτημα της κυβερνοασφάλειας, όπως γίνεται αντιληπτό, αποτελεί πλέον καίριο ζήτημα τόσο σε διεθνές όσο και σε ευρωπαϊκό επίπεδο καθώς τόσο οι κυβερνήσεις όσο και οι ιδιωτικοί οικονομικοί φορείς ασφυκτιούν κάτω από την ανεξέλεγκτη μορφή μέσω της οποίας λαμβάνουν χώρα οι κυβερνοεπιθέσεις. Η αδυναμία των κρατών μελών να οριοθετήσουν το χώρο του διαδικτύου ώστε να προασπιστούν τα κυριαρχικά τους δικαιώματα αλλά και την ασφάλεια των πολιτών τους αποδεικνύει πως η εφαρμογή υψηλού επιπέδου κυβερνοασφάλειας πρέπει και δύναται να επιτευχθεί αποτελεσματικότερα σε επίπεδο Ένωσης, η οποία αναλαμβάνει το ρόλο του συντονιστή στην προσπάθεια εναρμόνισης μέτρων και κανόνων των εθνικών στρατηγικών κυβερνοασφάλειας υπό τη σκέπη της ενωσιακής στρατηγικής.

1. Κυβερνοχώρος και Κυβερνοασφάλεια

1.1 Η έννοια του κυβερνοχώρου

Ο κυβερνοχώρος σαν έννοια εμφανίστηκε για πρώτη φορά με την προσέγγιση του Γερμανοαμερικανού μαθηματικού Νόρμπετ Βίνερ στο έργο του «*Κυβερνητική*[1]*: ή Έλεγχος και Επικοινωνία στο Ζώο και τη Μηχανή* » -που αφορούσε το τότε επιστημονικό πεδίο της κυβερνητικής- στο οποίο και θεμελιώνεται. Το επιστέγασμα, όμως της έννοιας επήλθε από δύο άρθρα του Γουόρεν ΜακΚάλλοχ (δημοσιευθέντα το 1943 και 1944) στα οποία εξάγεται το συμπέρασμα πως «*η τυπική περιγραφή του νευρικού συστήματος δεν είναι δυνατή με τα εργαλεία της κλασικής δυαδικής λογικής*» αλλά με την έννοια της ετεραρχίας[2], δηλαδή της συνεργατικής και συνδυασμένης δράσης[3]. Η τελική πρόταση του όρου εισήχθη από το μυθιστόρημα του Γουίλιαμ Γκίμπσον (Νευρομάντης,1984) , στο πλαίσιο της περιγραφής κυβερνοπολέμων του μέλλοντος και εικονικών περιβάλλοντων. Η ακριβής χροιά του όρου δόθηκε από τον δημοσιογράφο και φιλόσοφο των ΜΜΕ Τζον Πέρρυ Μπάρλοου, ο οποίος για πρώτη φορά χρησιμοποίησε τον όρο του κυβερνοχώρου με σκοπό να περιγράψει το συνδυασμό της τεχνολογίας, των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιών προσδίδοντας του πλήρως την έννοια με την οποία τον χρησιμοποιούμε έως σήμερα.

Ο όρος κυβερνοχώρος επικράτησε του όρου «*κυβερνοδιαστήματος*» και σύμφωνα με τη Λενιώ Μυριβήλη (PhD) *«ο κυβερνοχώρος αναφέρεται ως ψηφιακός τόπος της τεχνοεπιστήμης, για άλλους είναι ένας ιδιαίτερος χώρος διεπαφής υποκειμένων, πρακτικών και τεχνολογιών. Μερικές φορές ο κυβερνοχώρος παρουσιάζεται ως χώρος διαφυγής από την «πραγματικότητα», αφού σε αυτόν μπορούμε να μεταμορφωνόμαστε κατά βούληση. Άλλες φορές*

[1] Κυβερνητικό σύστημα ονομάζεται ένα αναδραστικό πολύπλοκο σύστημα. Κυβερνητική (cybernetics) είναι ένα υποσύνολο της επιστήμης συστημάτων το οποίο επικεντρώνεται στη μελέτη κυβερνητικών συστημάτων. Η κυβερνητική προέκυψε μετά το Β' Παγκόσμιο Πόλεμο από μία μείξη της θεωρίας πληροφοριών, η οποία μελετούσε τη μαθηματική έννοια της πληροφορίας από τη σκοπιά των τηλεπικοινωνιών, και της θεωρίας ελέγχου, η οποία μελετούσε πρακτικούς συνθετικούς μηχανισμούς ανάδρασης από τη σκοπιά των μηχανικών. Χωρίς ακόμη να έχει διαμορφωθεί τότε η επιστήμη συστημάτων και η ολιστική μεθοδολογία, η κυβερνητική υιοθέτησε εξ αρχής μία συστημική προσέγγιση και μία έμφαση στην αυτοοργάνωση και στην αυτονομία, αποτελώντας έτσι σημαντική πηγή ερεθισμάτων για την ανάπτυξη της σύγχρονης επιστήμης συστημάτων αλλά και κλάδων όπως η τεχνητή νοημοσύνη. Ιστορικά, κεντρική ιδέα πίσω από την κυβερνητική υπήρξε η ομοιότητα μεταξύ ζωντανών οργανισμών και τεχνολογικών μηχανισμών, μία ομοιότητα που μοντελοποιήθηκε με τις έννοιες του συστήματος, της ομοιόστασης και της ανάδρασης. Σε σχέση με τη θεωρία συστημάτων η κυβερνητική επικεντρώνεται περισσότερο στη λειτουργία των πολύπλοκων συστημάτων, δηλαδή στον τρόπο που ελέγχουν τη δράση τους, επικοινωνούν μεταξύ τους, αλληλοεπιδρούν τα μέρη τους κλπ., παρά στη δομή τους. https://el.wikipedia.org/wiki/Επιστήμη_συστημάτων (είσοδος 2/11/2019)

[2] **ντετερμινισμός,** ή **αιτιοκρατία,** ή **ετεραρχία** [determinism]. Η θεωρία ότι ο κόσμος ή η φύση υπόκειται παντού σε αιτιώδεις νόμους (βλ. ΑΙΤΙΟΤΗΤΑ), ότι όλα τα γεγονότα σε αυτόν έχουν μια αιτία. Αν αυτό αληθεύει, τότε κάθε γεγονός που συμβαίνει πραγματικά πρέπει να συμβεί, εφόσον το ότι συμβαίνει απορρέει λογικά από μια περιγραφή των προϋποθέσεων της εκδήλωσής του σε συνδυασμό με τους σχετικούς νόμους της φύσης. Παρομοίως, κάθε γεγονός που δε συμβαίνει δε θα μπορούσε να συμβεί.

[3] Ulysses goes CyberSpace... Warren St. McCulloch, A Heterarchy of Values Determined by the Topology of Nervous Nets, Abdruck in: Embodiments of Mind, Warren St. McCulloch, MIT Press, Cambridge Mass. 1970, σελ. 20

πάλι φαντάζει ως υβριδικός χώρος μέσα στον οποίο συμφιλιώνονται και μετουσιώνονται πολιτισμικοί πόλοι».

Ο ορισμός της έννοιας του κυβερνοχώρου δεν απαντάται ακόμη σε ολοκληρωμένη μορφή, παρά την αλματώδη εξέλιξη της τεχνολογίας τον προηγούμενο και τον παρόντα αιώνα. Παρότι το διαδίκτυο αποτελεί μια παράλληλη πραγματικότητα κατά πολλούς και παρά το γεγονός πως η τεχνολογία έχει ενταχθεί πλήρως στην ιδιωτική και εργασιακή καθημερινότητα σχεδόν ολόκληρης της υφηλίου, η έννοια του κυβερνοχώρου βρίθει αναλύσεων αλλά αποτελεί ακόμη και σήμερα ένα πεδίο διαρκούς έρευνας και επεξηγήσεων καθώς οι νέοι πόλοι και διακλαδώσεις που συνεχώς δημιουργούνται φαίνεται να ξεπερνούν την κοινή ανθρώπινη λογική. Η επιστημονική κοινότητα ακόμη αμφιταλαντεύεται στο να ορίσει επακριβώς την έννοια του χώρου αυτού -παρά την ενδελεχή έρευνα στην οποία υποβάλλεται- καθώς φαίνεται πως ακόμη, μόνο επιφανειακά μπορούμε να ψηλαφίσουμε τις δυνατότητες του τόσο κοινωνικά όσο και πολιτικά αλλά κυρίως σε επίπεδο διπλωματίας και διακρατικών σχέσεων.

Ένας βασικός ορισμός ο οποίος δύναται να αποδώσει σφαιρικά την έννοια του κυβερνοχώρου έγκειται στον προσδιορισμό του ως ένα περιβάλλον άυλο, το οποίο εκτείνεται χωρικά σε παγκόσμιο επίπεδο και εντός του πλαισίου του πραγματοποιείται διαδικτυακή επικοινωνία μεταξύ προσώπων, λογισμικού και υπηρεσιών, δια μέσου δικτύων ηλεκτρονικών υπολογιστών και τεχνολογικών συσκευών.[4] Παραδείγματα τέτοιων δικτύων, αποτελούν τα τοπικά δίκτυα (LANs) –στα οποία ορισμένοι ηλεκτρονικοί υπολογιστές είναι συνδεδεμένοι μεταξύ τους, μέσα στο ίδιο δωμάτιο ή στο ίδιο κτήριο για να εξυπηρετείται η δίοδος των πληροφοριών, για να μοιράζεται η επεξεργασία ή για την διευκόλυνση των επικοινωνιών– και τα ευρείας εμβέλειας δίκτυα (WANs) όπως το σύστημα του Internet (το διεθνές δίκτυο των δικτύων για ακαδημαϊκούς και ερευνητές), για τις ίδιες δραστηριότητες σε εθνικά και παγκόσμια δίκτυα.[5] Σύμφωνα με τον Erik M. Mudrinich «*κυβερνοχώρος είναι ένας επιχειρησιακός τομέας ευρισκόμενος 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*».

Ο κυβερνοχώρος πέραν της συνδυαστικής άυλης και υλικής εφαρμογής του γίνεται περισσότερο κατανοητός μέσω της κατανόησης των επιμέρους ιδιοτήτων του.

Α. Αποκρύπτει την ταυτότητα και τη θέση των δρώντων εξαιτίας της φυσικής αρχιτεκτονικής και των πρωτόκολλων λογισμικού, τα οποία επιτρέπουν τη

[4] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 75

[5] Βλ. σχετικές πληροφορίες: Βικιπαιδεία, Κυβερνοχώρος, Διαθέσιμο στο: https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82, (πρόσβαση 06.10.2019)

σχετικά εύκολη χρήση των ψευδωνύμων και των πληρεξουσίων με αποτέλεσμα να είναι και σχετικά δύσκολη η διείσδυση και η αποκάλυψη τους.

Β. Αυξάνει ριζικά την ταχύτητα, την ένταση και την εμβέλεια στις επικοινωνίες, όχι μόνο ισχυρών κρατών και εταιρειών, αλλά και μεμονωμένων πολιτών που μπορούν να τον χρησιμοποιήσουν ώστε να επικοινωνούν παγκοσμίως και σχεδόν στιγμιαία, με ασφάλεια, χρησιμοποιώντας μια ποικιλία μέσων. Αν και είναι άνισα κατανεμημένος- δηλαδή, πανταχού παρών σε μερικά μέρη αλλά ανύπαρκτος σε άλλα- η πρόσβαση σε αυτόν έχει ανοδική πορεία σε όλο τον κόσμο, συμπεριλαμβανομένων και των φτωχότερων περιοχών όπου ο τομέας των τηλεπικοινωνιών τείνει να είναι ο ταχύτερα αναπτυσσόμενος τομέας της οικονομίας.

Γ. Τα εμπόδια εισόδου στον κυβερνοχώρο, μειώνονται περαιτέρω με την εξάπλωση των χαμηλού κόστους συσκευών που συνδυάζουν τηλεπικοινωνίες, πρόσβαση στο διαδίκτυο και καταγραφικές δυνατότητες φωτογραφιών και βίντεο. Οι βασικές προϋποθέσεις πρόσβασης είναι μόνον η ύπαρξη υπολογιστή και διαδικτύου[6].

Στο πλαίσιο της 4ης Βιομηχανικής Επανάστασης[7] με την ταχύτατη εξέλιξη της τεχνολογίας που αυτή επιφέρει, ο κυβερνοχώρος αποτελεί πλέον μία άυλη μεν, πραγματικότητα δε, υπό τη σκέπη της οποίας λαμβάνει χώρα μία νέα αρένα διαδραστικότητας η οποία επεκτείνεται σε πολιτικό και διπλωματικό επίπεδο δημιουργώντας ευκαιρίες αλλά και κινδύνους επεκτεινόμενους σε όλες τις διακυβερνητικές και διακρατικές βαθμίδες. Εξαιτίας του διάχυτου της φύσης του κυβερνοχώρου η νομοθετική οριοθέτηση του τόσο σε ενωσιακό όσο και εθνικό επίπεδο κρίνεται τόσο δυσχερής όσο και αναγκαία, δεδομένων των απειλών που δημιουργούνται θέτοντας ζητήματα όχι μόνο στη βάση της προάσπισης της κυβερνοασφάλειας αλλά και των δημοκρατικών θεσμών.

[6] David J. Betz and Tim Stevens, Cybersecurity and the State, IISS, UK, σελ.5

[7] Προκόπης Παυλόπουλος, Ομιλία, 28.02.2019, 4ο Οικονομικό Forum των Δελφών, Διαθέσιμο στο: https://sputniknews.gr/politiki/201902282432706-oikonomiko-forum-delfon-pavlopoulos/

1.2 Η έννοια της κυβερνοασφάλειας

Αν ο ορισμός της έννοιας του κυβερνοχώρου εγείρει προβληματισμό στις επιστημονικές και επιχειρηματικές κοινότητες, ο ορισμός της έννοιας της κυβερνοασφαλείας συναντά την ίδια ίσως και μεγαλύτερη πολυφωνία. Προτού προβούμε στην προσπάθεια αποσαφήνισης του όρου θα πρέπει να τον διαχωρίσουμε από έννοιες με τις οποίες συχνά συγχέεται όπως αυτή της ασφάλειας πληροφοριακών συστημάτων και αυτή της ασφάλειας πληροφοριακών και επικοινωνιακών τεχνολογιών.

Η μεν πρώτη αφορά την ασφάλεια των υπολογιστών ή/και των υπολογιστικών συστημάτων και συνδέεται άμεσα τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές, προφυλάσσοντας από κάθε είδους απειλή τυχαία ή σκόπιμη αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση[8]. Αφορά κατά βάση την διατήρηση της ακεραιότητας, του απορρήτου και της προσβασιμότητας των πληροφοριών, οι οποίες μπορούν να έχουν πολλές μορφές όμως κατά κύριο λόγο ευρίσκονται σε ηλεκτρονική μορφή.

Η δε δεύτερη αφορά την προστασία των τεχνολογικών συστημάτων, των οποίων η πληροφορία είναι αποθηκευμένη ή/και μεταδιδόμενη. Το διεθνές πρότυπο ISO/IEC 13335-1, 2004, ορίζει την ασφάλεια πληροφοριακών και επικοινωνιακών τεχνολογιών ως όλες τις εκείνες πτυχές, που σχετίζονται με τον καθορισμό, την επίτευξη και τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας, της προσβασιμότητας, της μη αποποίησης, της ευθύνης, της αυθεντικότητας και της αξιοπιστίας των πηγών της πληροφορίας.

Παρατηρείται πως οι ανωτέρω όροι πραγματεύονται ναι μεν το ζήτημα της ασφάλειας, όμως, επικεντρώνονται σε πρακτικό και τεχνικό επίπεδο, σε αντίθεση με την έννοια της κυβερνοασφάλειας η οποία προσεγγίζει και αυτή το ίδιο ζήτημα όμως μέσω ενός πρίσματος του οποίου η βάση χωρεί την ανάπτυξη νομοθετικών πλαισίων και κυβερνητικών πολιτικών στρατηγικής. Αυτός είναι και ο κύριος λόγος που ο ορισμός της διατρέχεται από οπτικές πολλών τομέων καθώς αγγίζει το οικονομικό, το κοινωνικό, το πολιτικό και φυσικά το ανθρωπιστικό πλαίσιο και όλα αυτά υπό τη σκέπη του τεχνολογικού. Επόμενο λοιπόν αποτελεί γεγονός πως δεν υπάρχει τυποποιημένος ορισμός για την κυβερνοασφάλεια. Μια αρκετά τεχνική προσέγγιση του όρου περιλαμβάνει τη μείωση του κινδύνου κακόβουλης επίθεσης σε λογισμικά, υπολογιστές και δίκτυα, δηλαδή τα εργαλεία που χρησιμοποιούνται για την ανίχνευση εισβολέων, ιών, ώστε να αποκλείεται η κακόβουλη πρόσβαση, να επιβάλλεται έλεγχος ταυτότητας και να ενεργοποιούνται οι κρυπτογραφημένες επικοινωνίες[9].

---

[8] Βλ. σχετικές πληροφορίες: Βικιπαίδεια, Ασφάλεια Πληροφοριακών Συστημάτων, Διαθέσιμο στο: https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8E%CE%BD_%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%AC%CF%84%CF%89%CE%BD (πρόσβαση 6.11.2019)

[9] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity, Technology Innovation Management Review, October 2014, σελ. 14

Η πλήρης γραμματική ανάλυση του όρου βασίζεται στον όρο «κυβερνητικός» που αναφέρεται στο πεδίο της θεωρίας ελέγχου και επικοινωνίας και στον όρο «ασφάλεια» που εμπεριεκλείει τα εξής: από ποιόν τίθεται, από τι προστατεύει (απειλές) και γιατί [10].

Στη σύγχρονη, τεχνολογικά αναπτυγμένη και πλήρως διασυνδεδεμένη πραγματικότητα ο όρος της κυβερνοασφάλειας δεν θα μπορούσε παρά να συνδυάζει τόσο τεχνικά όσο και κοινωνιολογικά χαρακτηριστικά. Βάσει αυτής της συλλογιστικής μπορούμε να καταλήξουμε στον εξής ορισμό: η κυβερνοασφάλεια αφορά το σύνολο των διασφαλίσεων και μέτρων που υιοθετούνται για την προστασία των συστημάτων πληροφοριών και των χρηστών τους έναντι μη εξουσιοδοτημένης πρόσβασης, επιθέσεων και ζημίας, ώστε να εξασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων. Η κυβερνοασφάλεια καλύπτει την πρόληψη και την ανίχνευση κυβερνοπεριστατικών, την αντίδραση σε αυτά και την ανάκαμψη από αυτά. Τα περιστατικά μπορεί να είναι εσκεμμένα ή μη και να κυμαίνονται, ενδεικτικά, από την τυχαία κοινοποίηση πληροφοριών, έως τις επιθέσεις κατά επιχειρήσεων και υποδομών ζωτικής σημασίας και την κλοπή δεδομένων προσωπικού χαρακτήρα, ή ακόμη και έως την παρεμβολή σε δημοκρατικές διαδικασίες. Όλα αυτά τα συμβάντα μπορούν να έχουν πολυποίκιλες επιδράσεις σε πρόσωπα, οργανισμούς και κοινότητες. Όπως χρησιμοποιείται στους πολιτικούς κύκλους της Ευρωπαϊκής Ένωσης, ο όρος «κυβερνοασφάλεια» δεν καλύπτει μόνο την ασφάλεια δικτύων και πληροφοριών, αλλά και κάθε παράνομη δραστηριότητα με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο. Ως εκ τούτου, μπορεί να περιλαμβάνει κυβερνοεγκλήματα όπως την εξαπόλυση επιθέσεων με ιούς υπολογιστών ή την απάτη με μέσα πληρωμής πλην των μετρητών και να αφορά τόσο τα συστήματα όσο και το περιεχόμενο. Μπορεί επίσης να καλύπτει εκστρατείες παραπληροφόρησης για την άσκηση επιρροής στον διαδικτυακό διάλογο και υπόνοιες για παρέμβαση σε εκλογικές διαδικασίες. Επιπλέον, σύμφωνα με την Europol θεωρείται ότι υπάρχει σύγκλιση μεταξύ κυβερνοεγκλήματος και τρομοκρατίας[11].

Το πλαίσιο της κυβερνοασφάλειας, λοιπόν προσεγγίζεται τόσο πολύπλευρα όσο πολύπλευρες είναι και οι διαστάσεις οι οποίες δύναται να λάβει. Πολλοί αναλυτές υποστηρίζουν πως ο κυβερνοχώρος αποτελεί μία νέα διάσταση η οποία δεν μπορεί να προσδιοριστεί χωρικά, διαθέτει όμως τις ιδιότητες της χωρικής και της χρονικής διάστασης και ενώ είναι κατασκευασμένος από τον άνθρωπο, την ίδια στιγμή ο τελευταίος φαίνεται να μετατρέπεται σε αποδέκτη των ίδιων του των ενεργειών παρά σε κυρίαρχο[12]. Οι νέες απειλές που γεννιούνται στον τομέα της κυβερνοασφάλειας επιτάσσουν την αναθεώρηση των ήδη υφιστάμενων νομικών πλαισίων ενώ πολλοί μιλούν για ένα νέο είδος αντισυμβατικού πολέμου, αυτού που λαμβάνει χώρα μέσω των κυβερνοεπιθέσεων.

[10] Βλ. 9.
[11] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 9
[12] David J. Betz and Tim Steven, Cybersecurity and the space, IISS, UK

1.3 Η έννοια του κυβερνοπολέμου

Στο πλαίσιο του αναδυόμενου και επεκτεινόμενου φαινομένου του κυβερνοπολέμου, η νέα πραγματικότητα των απειλών λαμβάνει χώρα μέσω της έννοιας της κυβερνοεπίθεσης, μία κατάσταση η οποία απασχολεί όλο και περισσότερο τις κυβερνήσεις διεθνώς καθώς δεν προκαλεί υλικές ζημιές όπως ο συμβατικός πόλεμος, όμως οι συνέπειες της ανάγονται σε πολύ περισσότερους τομείς, ίσως και πιο σημαντικούς από αυτόν της ύλης.

Ένας ακριβής και τυποποιημένος ορισμός του κυβερνοπολέμου και πάλι κρίνεται δυσχερής να εξαχθεί. Σε γενικό επίπεδό μπορεί να λεχθεί πως αφορά τη σύγκρουση που λαμβάνει χώρα στον κυβερνοχώρο με αντίστοιχα μέσα και μεθόδους, ενώ έχει διατυπωθεί και ως κάθε δράση που διακόπτει, αλλοιώνει, παρακρατεί ή καταστρέφει πληροφορίες ευρισκόμενες σε υπολογιστές ή υπολογιστικά δίκτυα[13].

Το φαινόμενο του κυβερνοπολέμου διεξάγεται μέσω των κυβερνοεπιθέσεων, απόπειρων, δηλαδή υπονόμευσης ή καταστροφής του απορρήτου, της ακεραιότητας και της διαθεσιμότητας δεδομένων ή συστημάτων πληροφορικής, οι οποίες υπάγονται στην ευρύτερη έννοια των κυβερνοπεριστατικών, περιστατικά τα οποία, άμεσα ή έμμεσα, βλάπτουν ή απειλούν την ανθεκτικότητα και την ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων που αυτά επεξεργάζονται ή τα οποία είναι αποθηκευμένα σε αυτά ή διαβιβάζονται από αυτά. Διακρίνεται από την έννοια του κυβερνοεγκλήματος, δηλαδή τις διάφορες εγκληματικές δραστηριότητες που διεξάγονται μέσω των ηλεκτρονικών υπολογιστών. Στις δραστηριότητες αυτές περιλαμβάνονται τα εξής: παραδοσιακά αδικήματα (π.χ. απάτη, πλαστογραφία και κλοπή ταυτότητας), αδικήματα σχετικά με το περιεχόμενο (π.χ. διανομή υλικού παιδικής πορνογραφίας ή υποκίνηση φυλετικού μίσους) και αδικήματα που αφορούν ειδικά τους ηλεκτρονικούς υπολογιστές και τα συστήματα πληροφοριών (π.χ. επιθέσεις κατά συστημάτων πληροφοριών, επιθέσεις άρνησης υπηρεσίας και επιθέσεις με κακόβουλο λογισμικό)[14]. Η μεγαλύτερή τους διαφορά έγκειται στον σκοπό της παράνομης δράσης, στο δρώντα αλλά και στον αποδέκτη. Οι κυβερνοεπιθέσεις στο επίπεδο του κυβερνοπολέμου ξεκινούν κατά βάση με ιδεολογικά ή/και πλήρως στρατιωτικά κίνητρα και απευθύνονται στην ευρύτερη κοινή γνώμη ενώ τα κυβερνοεγκλήματα ξεκινούν με ιδιωτικά κίνητρα και απευθύνονται σε μεμονωμένου ενδιαφέροντος κοινό.

Ως απαρχή των κυβερνοεπιθέσεων, ιστορικά, μπορεί να τεθεί το 1991, όταν η NSA[15] παγίδευσε δορυφορικά συνομιλίες Ιρακινών κατά τη διάρκεια του πολέμου με τον Saddam Hussein, ή/και στα τέλη της δεκαετίας του ’90, όταν οι Ηνωμένες Πολιτείες έκλεισαν μέσω δορυφόρων τους πομπούς σήματος στις τηλεοράσεις της Βοσνίας-Ερζεγοβίνης, για να αποθαρρύνουν τους Σέρβους της χώρας από

[13] Nils Melzer, Cyberwarfare and International Law, Unidir Resources, 2011, σελ. 5
[14] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 74
[15] Βλ. σχετικές πληροφορίες: National Security Agency, Διαθέσιμο στο: https://www.nsa.gov/ (Πρόσβαση 6.11.2019)

το να βλέπουν συγκεκριμένα κανάλια που τους παρακινούσαν να διαδηλώσουν κατά του Ν.Α.Τ.Ο και της συμφωνίας του Dayton, που είχε σημάνει τη λήξη του πολέμου στην περιοχή. Ωστόσο, αναντίρρητα, η πρώτη φορά που σημειώθηκε «κυβερνοεπίθεση» -με τη σύγχρονη μορφή της-, ήταν το 2006, όπου θύμα ήταν το Ιράν και το πυρηνικό του πρόγραμμα. Η NSA έθεσε ως στόχο τον πυρηνικό αντιδραστήρα Natanz, εισβάλλοντας στο λειτουργικό του σύστημα και, εγκαθιστώντας κακόβουλο λογισμικό (Stuxnet worm) που αύξησε υπέρμετρα τη ροή ουρανίου και προκάλεσε εκρήξεις, καταστρέφοντας τμήματα του αντιδραστήρα. Μέχρι το 2010, οπότε και έγινε αντιληπτή η εισβολή, οι ΗΠΑ είχαν ήδη προκαλέσει τεράστιες ζημιές στο πυρηνικό πρόγραμμα του Ιράν[16].

Είναι πλέον κάτι παραπάνω από ξεκάθαρο πως οι συγκρούσεις στον κυβερνοχώρο τις οποίες θα αναλύσουμε διεξοδικότερα εν συνεχεία, τον καθιστούν τον πέμπτο τομέα εμπόλεμης δραστηριότητας μετά τη ξηρά, τη θάλασσα, τον αέρα και το διάστημα. Ο πρώην πρόεδρος των Ηνωμένων Πολιτειών της Αμερικής Μπάρακ Ομπάμα είχε δηλώσει πως η ψηφιακή υποδομή αποτελεί ένα εθνικό στρατηγικό περιουσιακό στοιχείο για τη χώρα του[17]. Προς την ίδια κατεύθυνση τείνουν τόσο η Ευρωπαϊκή Ένωση όσο και η Διεθνής κοινότητα, καθώς γίνεται όλο και πιο ξεκάθαρο πως η ανάπτυξη στρατηγικών πολιτικών κυβερνοασφάλειας πρέπει να αποτελέσει πρωταρχικό στόχο κυβερνητικών και μη δρώντων.

[16] Βλ. σχετικές πληροφορίες: Power Politics, Διαθέσιμο στο: https://powerpolitics.eu/, (Πρόσβαση 08.11.2019)

[17] Βλ. σχετικές πληροφορίες: The Economist (2010), War in the fifth domain, Διαθέσιμο στο: http://www.economist.com/node/16478792 (Πρόσβαση 08.11.2019)

2. Κυβερνοεπιθέσεις

2.1 Είδη κυβερνοεπιθέσεων

Το φαινόμενο των κυβερνοεπιθέσεων παρά τις προσπάθειες αντιμετώπισης του που λαμβάνονται σε διάφορα επίπεδα εξελίσσεται κλιμακούμενο. Σύμφωνα με μελέτη που εκδόθηκε από τη Hiscox στην οποία συμμετείχαν πάνω από 5.300 επαγγελματίες του χώρου της κυβερνοασφάλειας από τις Ηνωμένες Πολιτείες, το Ηνωμένο Βασίλειο, το Βέλγιο, τη Γαλλία, τη Γερμανία και την Ισπανία[18], ο ρυθμός των κυβερνοεπιθέσεων έχει αποκτήσει αρκετά εντονότερους ρυθμούς. Το 61% των επιχειρήσεων έχουν δηλώσει πως έχουν δεχτεί κυβερνοεπίθεση κατά το έτος 2018 συγκριτικά με το 45% του προηγούμενου έτους.

Οι κυβερνοεπιθέσεις δύνανται να διεξαχθούν σε μεγάλη κλίμακα και υπάγονται στις ακόλουθες κατηγορίες:

Βανδαλισμός στον Κυβερνοχώρο (Cyber Vandalism) [19]

Αποτελεί μία πολύ διαδεδομένη και σχετικά ακίνδυνη πρακτική κυβερνοεπίθεσης. Η κύρια μορφή της είναι η τροποποίηση ή η καταστροφή περιεχομένου στον κυβερνοχώρο, όπως ανεξέλεγκτες αλλαγές στο περιεχόμενο μιας ιστοσελίδας χωρίς έγκριση του υπεύθυνου χειρισμού της. Οι πλέον διαδεδομένες μορφές που έχουν καταγραφεί είναι οι εικονικές καταλήψεις, η ακατάσχετη αποστολή ηλεκτρονικών μηνυμάτων, η προσβολή συστημάτων μέσω ιών και το hacking[20] σε ιστοσελίδες.

Κυβερνοκατασκοπεία (Cyber Espionage)[21]

Η κυβερνοκατασκοπεία αφορά τη συλλογή κρίσιμων πληροφορίων με τη χρήση μέσων ψηφιακής τεχνολογίας. Ο βασικός στόχος αυτής της πρακτικής είναι διττός και αφορά την ανώτερη κρατική λειτουργία. Η μορφή αυτού του είδους της κατασκοπείας αφορά τη συλλογή κρατικών μυστικών πληροφοριών τόσο πολιτικής όσο και οικονομικής σημασίας. Η δράση της κυβερνητικής κατασκοπείας συχνά προσομοιάζεται με την επιχείρηση ενός βομβαρδιστικού. Όπως το επιτιθέμενο βομβαρδιστικό εισβάλει στον αμυνόμενο και στη συνέχεια επιχειρεί να μειώσει το επιβλαβές ωφέλιμο φορτίο του, με τον ίδιο τρόπο

[18] Βλ. σχετικές πληροφορίες: PrivSec Report, Διαθέσιμο στο: https://gdpr.report/news/2019/04/29/cyber-attacks-reported-by-61-of-us-and-european-firms-over-past-year/ (Πρόσβαση 8.11.2019)

[19] Τατσούλης Περικλής, Ο κυβερνοπόλεμος ως πολυδιάστατο στρατηγικό εργαλείο και η εφαρμογή του σε κρίσιμες στρατιωτικές και μη υποδομές, Μάιος 2019, Μεταπτυχιακή Διατριβή, Διιδρυματικό Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών, Εφαρμοσμένη Επιχειρησιακή Έρευνα και Ανάλυση, Στρατιωτική Σχολή Ευελπίδων, Πολυτεχνείο Κρήτης, σελ. 16

[20] Εισβολή σε υπολογιστικά συστήματα από τους λεγόμενους χάκερς οι οποίοι έχουν τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζονται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως οι χάκερς είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες αποκαλούνται κράκερς. https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81
(Πρόσβαση 10.11.2019)

[21] Βλ. σχετικές πληροφορίες: Rathenau Instituut, Διαθέσιμο στο: https://www.rathenau.nl/en/digital-society/cyberspace-without-conflict/cyber-attacks-cyber-espionage (Πρόσβαση 10.11.2019)

λαμβάνει χώρα και η κυβερνοκατασκοπεία. Ο σκοπός βέβαια των δύο επιθέσεων διαφέρει εκ διαμέτρου.

Κυβερνοτρομοκρατία (Cyber Terrorism)

Σύμφωνα με το Ομοσπονδιακό Γραφείο Διερεύνησης των ΗΠΑ, η κυβερνο-τρομοκρατία είναι οποιαδήποτε «προμελετημένη, πολιτικά παρακινούμενη επίθεση κατά των πληροφοριών, των υπολογιστικών συστημάτων, των προγραμμάτων ηλεκτρονικών υπολογιστών και των δεδομένων, που οδηγεί σε επίθεση κατά μη-μαχητικών στόχων από υποεθνικές ομάδες ή παράνομους πράκτορες». Μια κυβερνοεπίθεση υπάγεται στο καθεστώς της κυβερνοτρομοκρατίας όταν ασκεί βία κατά ατόμων ή περιουσιών, ή όταν προκαλεί τέτοια ζημιά που επιφέρει τον τρόμο. Η κυβερνοτρομοκρατία περιλαμβάνει προμελετημένες και πολιτικά υποκινούμενες κυβερνοεπιθέσεις, ενώ πιθανοί της στόχοι είναι τα κυβερνητικά δίκτυα Η/Υ, τα οικονομικά δίκτυα, τα εργοστάσια παραγωγής ενέργειας και τα πληροφοριακά δίκτυα ελέγχου της εναέριας κυκλοφορίας[22].

Σε μία πιο εξειδικευμένη και τεχνική ανάλυση οι κυβερνοεπιθέσεις μπορούν να διαχωριστούν ως εξής:

1. Κυβερνοεπιθέσεις με σκοπό τη συλλογή δεδομένων και την απόσπαση πληροφοριών. Ένα παράδειγμα αυτής της κατηγορίας είναι η προσπάθεια υποκλοπής των κωδικών εκατοντάδων λογαριασμών ηλεκτρονικού ταχυδρομείου της εταιρείας Google τον Ιούνιο του 2011, κάποιοι από τους οποίους ανήκαν σε υψηλόβαθμα στελέχη της κυβέρνησης των ΗΠΑ και σε Κινέζους ακτιβιστές και δημοσιογράφους. Υπεύθυνη θεωρήθηκε η Κίνα, όπως και τον Ιανουάριο του 2010 όταν και σημειώθηκαν ανάλογες παραβιάσεις[23].

2. Οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών (Distributed Denial of service Attacks - DDoS) οι οποίες αποτελούν ένα από τα σημαντικότερα προβλήματα στο πεδίο της ασφάλειας δικτύων. Σκοπός των επιθέσεων είναι να προκληθεί στο σύστημα-στόχο (θύμα) αδυναμία να προσφέρει τις υπηρεσίες του, λόγω της υψηλής εισροής δεδομένων και του υπολογιστικού φόρτου που προκαλείται από την επίθεση. Αυτή η σωρευμένη δικτυακή ροή δημιουργείται από εκατοντάδες χιλιάδες δικτυακά συστήματα που βρίσκονται υπό τον έλεγχο του χρήστη, ο οποίος είναι υπεύθυνος για τις κατανεμημένες αυτές επιθέσεις άρνησης υπηρεσιών (θύτης)[24].

3. Οι επιθέσεις ελέγχου συστήματος (control system attacks), αποσκοπούν κυρίως στο να εκθέσουν τα λειτουργικά συστήματα και να μετατρέψουν τα δεδομένα τους. Αυτού του είδους οι επιθέσεις χωρίζονται σε δύο κατηγορίες· τις

[22] Τατσούλης Περικλής, Ο κυβερνοπόλεμος ως πολυδιάστατο στρατηγικό εργαλείο και η εφαρμογή του σε κρίσιμες στρατιωτικές και μη υποδομές, Μάιος 2019, Μεταπτυχιακή Διατριβή, Διιδρυματικό Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών, Εφαρμοσμένη Επιχειρησιακή Έρευνα και Ανάλυση, Στρατιωτική Σχολή Ευελπίδων, Πολυτεχνείο Κρήτης, σελ. 17

[23] Αλέξανδρος Λιούτας, Η Έννοια της Ένοπλης Επίθεσης στον Κυβερνοχώρο, Μάιος 2019, Διπλωματική Εργασία, Δημόσιο Διεθνές Δίκαιο, Νομική Σχολή Α.Π.Θ., σελ. 11

[24] Κυριάκος Στεφανίδης, Προστασία Συστημάτων από Κατανεμημένες Επιθέσεις στο Διαδίκτυο, Νοέμβριος 2013, Διδακτορική Διατριβή, Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, σελ. 40

συντακτικές (syntactic attacks) και τις σημασιολογικές (semantic attacks). Οι πρώτες χρησιμοποιούν συνήθως κακόβουλο λογισμικό 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[25].

Στο σημείο αυτό αξίζει να σημειωθεί πως η κυβερνοεπίθεση με όποια μορφή και αν διεξαχθεί δεν πρέπει να συγχέεται με την έννοια του κυβερνοεγκλήματος αν και κατά πολλούς θεωρούνται έννοιες που αλληλοκαλύπτονται. 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 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 και ότι η διαπραχθείσα ενέργεια ποινικοποιείται με βάση το εκάστοτε εθνικό ή το διεθνές δίκαιο[26]. Επί της ουσίας οι δύο δράσεις διαφέρουν τόσο στη στοχοποίηση όσο και στις συνέπειες που επιδιώκουν να επιφέρουν.

[25] Αλέξανδρος Λιούτας, Η Έννοια της Ένοπλης Επίθεσης στον Κυβερνοχώρο, Μάιος 2019, Διπλωματική Εργασία, Δημόσιο Διεθνές Δίκαιο, Νομική Σχολή Α.Π.Θ., σελ. 12
[26] Βλ. 25

2.2 Ιστορικά περιστατικά κυβερνοεπιθέσεων

Είναι γεγονός πως ιστορικά η ανάπτυξη νέων τεχνολογιών συμβάδιζε με την επανάσταση στα πολεμικά μέσα. Το ίδιο ακριβώς επιβεβαιώνεται και σήμερα με τη συνεχή ανάπτυξη της τεχνολογίας πληροφοριών και δικτύων. Με την τεχνολογική επανάσταση δεν έχει μεταβληθεί μόνο το παγκόσμιο οικονομικό στερέωμα αλλά και η ισχύς των στρατών, οι οποίοι τώρα μπορούν να στέλνουν μη επανδρωμένα αεροσκάφη για να συλλέγουν πληροφορίες ή για να βομβαρδίζουν. Ο κυβερνοχώρος είναι ο πέμπτος τομέας, όπως προελέχθη, στον οποίο μπορεί να εκδηλωθεί πόλεμος, μετά την ξηρά, τη θάλασσα, τον αέρα και το διάστημα. Αν αρχίσουν να καταρρέουν τα δίκτυα των υπολογιστών, θα εκδηλωθούν εκρήξεις σε χημικά και άλλα εργοστάσια, θα τεθούν εκτός ελέγχου δορυφόροι και θα καταρρεύσουν δίκτυα ισχύος και ολόκληρα οικονομικά συστήματα. Το να διεισδύσει κάποιος σε ένα δίκτυο και να το αλώσει είναι πλέον πολύ εύκολο. Οι ειδικοί προειδοποιούν για τον κίνδυνο και οι κυβερνήσεις τους κατανοούν, όμως οι ίδιες αποτελούν «τους πιο ενθουσιώδεις hackers», οπότε διστάζουν να θέσουν περιοριστικούς κανόνες[27].

Ο κυβερνοπόλεμος και οι διαστάσεις οι οποίες δύνανται να εκδηλωθούν από τις επιχειρήσεις κυβερνοεπιθέσεων δεν άργησαν να γίνουν αντιληπτές επί του πρακτέου μόλις εκδηλώθηκαν οι πρώτες διασυνοριακές κυβερνοεπιθέσεις. Οι αιτίες, οι σκοποί και ο τρόπος διεξαγωγής των κυβερνοεπιθέσεων επιβεβαίωσαν τις μέχρι τότε θεωρητικές ανησυχίες των ειδικών πως ο κυβερνοχώρος δεν θα αργούσε να μετατραπεί σε ένα νέο πεδίο διπλωματίας και μάχης με τα ίδια ακριβώς χαρακτηριστικά των ένοπλων συγκρούσεων και όλα τα χαρακτηριστικά του παραδοσιακού πολέμου πλην του παράγοντα της ανθρώπινης απώλειας, τουλάχιστον όχι τόσο άμεσα όσο στο συμβατικό πόλεμο.

2.2.1 Εσθονία 2007

Στις 27 Απριλίου 2007, η Εσθονία βίωσε κυβερνοεπιθέσεις διάρκειας τριών εβδομάδων, οι οποίες θεωρείται ότι συνιστούν την πρώτη ιστορικά έκφραση κυβερνοπολέμου παγκοσμίως.

Η κυβερνοεπίθεση που δέχτηκε η Εσθονία αποδίδεται στη Ρωσική κυβέρνηση της οποίας ο «κυβερνοστρατός» εξαπέλυσε δύο κύματα επιθέσεων το δεύτερο πιο εξελιγμένο από το πρώτο καταφέρνοντας σχεδόν να αποκλείσει τελείως την Εσθονία από το διαδίκτυο. Πιο συγκεκριμένα οι επιθέσεις (Distributed Denial of service Attacks - DDoS) στόχευαν σε κυβερνητικούς οργανισμούς (πολιτικούς, οικονομικούς,) και άλλα websites και e-services. Προφανώς οι επιθέσεις αποτέλεσαν τη ρωσική απάντηση στην πρόθεση της εσθονικής κυβέρνησης να μεταφέρει ένα μνημείο πολέμου της σοβιετικής εποχής (ο χάλκινος στρατιώτης και ο τόπος ταφής του Τάλλιν).

Οι αρχικές επιθέσεις άρχισαν στις 26 Απριλίου, την ημέρα εκκίνησης των ανασκαφών, ακολουθούμενες από μία πολύ πιο σύνθετη και καλά συντονισμένη επίθεση που ξεκίνησε στις 4 Μαΐου και κορυφώθηκε στις 9 Μαΐου (Ημέρα Νίκης,

[27] Βλ. σχετικές πληροφορίες: Ο κυβερνοπόλεμος άρχισε, 8 Ιουλίου 2010, Ελευθεροτυπία, Διαθέσιμο στο: http://www.enet.gr/?i=news.el.article&id=181298 (Πρόσβαση 13.11.2019)

εθνική εορτή στη Ρωσική Ομοσπονδία, η οποία μνημονεύει τη νίκη επί της Ναζιστικής Γερμανίας στο «Μεγάλο Πατριωτικό Πόλεμο»). Οι επιθέσεις ήταν δυναμικές, και έπαψαν να ισχύουν σε συγκεκριμένο χρονικό διάστημα όταν συγχρονίστηκαν και με άλλες ενέργειες της Ρωσίας που ήταν εχθρικές προς την Εσθονία, όπως η αποκοπή εμπορικών σιδηροδρομικών συνδέσεων, χωρίς προειδοποίηση, για υποτιθέμενες «επισκευές»[28].

Η Εσθονία αντιμετώπισε την απώλεια παραγωγικότητας, με την αποκατάσταση και την απόκτηση εναλλακτικής φιλοξενίας ιστοσελίδων σε περίπτωση έκτακτης ανάγκης που εκτιμάται ότι ανέρχεται σε δισεκατομμύρια ευρώ. Η επίθεση θα μπορούσε να είχε ως αποτέλεσμα την αποδυνάμωση της εμπιστοσύνης των Εσθονών πολιτών στην ικανότητα της κυβέρνησης να υπερασπιστεί τη χώρα από τις αντισυμβατικές επιθέσεις αλλά η γρήγορη αντίδραση της κυβέρνησης, σε συνδυασμό με την υποστήριξη του ΝΑΤΟ και πολλών κρατών μελών, εμπόδισε τη γενικευμένη δυσπιστία του κοινού.

Εκτιμάται ότι οι επιθέσεις στον κυβερνοχώρο δεν είχαν σημαντική επίπτωση σε τυχόν εσωτερικές διαιρέσεις μεταξύ Εσθονών πολιτών διαφορετικής γλωσσικής και εθνοτικής κληρονομιάς[29].

2.2.2. Γεωργία 2008

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[30].

Ο επίσημος ιστότοπος του Γεωργιανού Προέδρου Μιχαήλ Σαακασβίλι, ο κεντρικός κυβερνητικός χώρος, καθώς και οι αρχικές σελίδες για το Υπουργείο Εξωτερικών και το Υπουργείο Άμυνας, βγήκαν εκτός λειτουργίας ενώ ορισμένοι εμπορικοί ιστότοποι επίσης καταστρατηγήθηκαν.

Η γεωργιανή κυβέρνηση δήλωσε ότι η διαταραχή προκλήθηκε από επιθέσεις που διεξήγαγε η Ρωσία στο πλαίσιο της συνεχιζόμενης σύγκρουσης μεταξύ των δύο κρατών για τη γεωργιανή επαρχία της Νότιας Οσετίας.

Σε μια δήλωση που δημοσιεύθηκε μέσω ενός ιστότοπου αντικατάστασης που βασίστηκε στην υπηρεσία φιλοξενίας ιστολόγιων της Google, το γεωργιανό υπουργείο Εξωτερικών δήλωσε: «Μια εκστρατεία κυρώσεων στον κυβερνοχώρο από τη Ρωσία διαταράσσει σοβαρά πολλούς ιστότοπους της Γεωργίας, συμπεριλαμβανομένου του Υπουργείου Εξωτερικών»[31].

Η Μόσχα όχι μόνο αρνήθηκε τις κατηγορίες για εμπλοκή ενάντια στη Γεωργία, αλλά υποστήριξε ότι πολλοί ρωσικοί δικτυακοί τόποι είχαν υποστεί παρόμοιες επιθέσεις. Ταυτοχρόνως, σύμφωνα με διαπιστώσεις εμπειρογνωμόνων,

[28] 2007 Cyber Attacks on Estonia, Cyber Operations, 2007, NATO, StratCom, COE, σελ. 53
[29] Βλ. 28
[30] Παναγιώτης Νιάκαρης, Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή, οι ευρωπαϊκές απαντήσεις, Απρίλιος 2019, Ατομική διατριβή, Σχολή Εθνικής Άμυνας, σελ. 25
[31] Βλ. σχετικές πληροφορίες: Georgia: Russia 'conducting cyber war', Διαθέσιμο στο: https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html (Πρόσβαση 15.11.2019)

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[32].

Όπως αποδείχθηκε εν συνεχεία, η επίθεση αυτή μπορεί να ήταν μια πρόβα για έναν εκτενή κυβερνοπόλεμο, όταν άρχισαν οι συγκρούσεις μεταξύ Γεωργίας και Ρωσίας. Σύμφωνα με τους τεχνικούς εμπειρογνώμονες του Διαδικτύου, ήταν η πρώτη φορά που μία γνωστή κυβερνοεπίθεση συνέπεσε με έναν πόλεμο συμβατικών μέσων[33].

2.2.3 Ουκρανία 2014

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[34].

Για την παρέμβασή τους στην Κριμαία οι Ρώσοι χρησιμοποίησαν μια έκτακτη στρατιωτική άσκηση για να αποσπάσουν την προσοχή και να αποκρύψουν τις προετοιμασίες τους. Στη συνέχεια ειδικά εκπαιδευμένοι στρατιώτες, χωρίς διακριτικά, κινήθηκαν γρήγορα για να εξασφαλίσουν βασικές εγκαταστάσεις. Μόλις τέθηκε σε εφαρμογή η επιχείρηση, η ρωσική δύναμη μπλόκαρε τις επικοινωνίες και χρησιμοποίησε εργαλεία κυβερνοπολέμου για να απομονώσει τις ουκρανικές στρατιωτικές δυνάμεις που βρίσκονταν στη χερσόνησο[35]. 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[36].

---

[32] Παναγιώτης Νιάκαρης, Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή, οι ευρωπαϊκές απαντήσεις, Απρίλιος 2019, Ατομική διατριβή, Σχολή Εθνικής Άμυνας, σελ. 26

[33] Βλ. σχετικές πληροφορίες: Before the Gunfire, Cyberattacks, John Markoff, 12.8.2018, Διαθέσιμο στο: https://www.nytimes.com/2008/08/13/technology/13cyber.html (Πρόσβαση 15.11.2019)

[34] Παναγιώτης Νιάκαρης, Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή, οι ευρωπαϊκές απαντήσεις, Απρίλιος 2019, Ατομική διατριβή, Σχολή Εθνικής Άμυνας, σελ. 20

[35] Βλ. σχετικές πληροφορίες: Η νέα, τριπλή στρατηγική Πούτιν στην Ουκρανία, 22 Απριλίου 2014, Το Βήμα, Διαθέσιμο στο: https://www.tovima.gr/2014/04/22/world/i-nea-tripli-stratigiki-poytin-stin-oykrania/ (Πρόσβαση 15.11.2019)

[36] Παναγιώτης Νιάκαρης, Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή, οι ευρωπαϊκές απαντήσεις, Απρίλιος 2019, Ατομική διατριβή, Σχολή Εθνικής Άμυνας, σελ. 20

2.2.4 Τα σημαντικότερα περιστατικά κυβερνοεπιθέσεων 2018-2019[37]

Νοέμβριος 2019. Ένας υποτιθέμενος μη κρατικός δρών στόχευσε στο κόμμα του Εργατικού Κόμματος του Ηνωμένου Βασιλείου μέσω επίθεσης που έθεσε προσωρινά τα ηλεκτρονικά συστήματα του κόμματος εκτός σύνδεσης.

Οκτώβριος 2019. Μια εκστρατεία υπό κρατική χρηματοδότηση επιτέθηκε σε περισσότερους από 2.000 ιστότοπους σε όλη τη Γεωργία, συμπεριλαμβανομένων κυβερνητικών διαδικτυακών τόπων και ιστότοπων δικαστηρίων που περιείχαν υλικό υποθέσεων και προσωπικά δεδομένα θέτοντας τους εκτός σύνδεσης.

Σεπτέμβριος 2019. Hackers φίλα προσκείμενοι στη ρωσική κυβέρνηση διενήργησαν μια εκστρατεία κατά των πρεσβειών και των υπουργείων Εξωτερικών των χωρών της Ανατολικής Ευρώπης και της Κεντρικής Ασίας.

Αύγουστος 2019. Η Τσεχική Δημοκρατία ανακοίνωσε ότι το υπουργείο Εξωτερικών της χώρας υπήρξε θύμα κυβερνοεπίθεσης από άγνωστης ταυτότητας ξένο κράτος. Η επίθεση αποδόθηκε αργότερα στη Ρωσία.

Ιούλιος 2019. Αρκετές μεγάλες γερμανικές βιομηχανικές επιχειρήσεις, όπως η BASF, η Siemens και η Henkel ανακοίνωσαν ότι υπήρξαν θύματα μιας κρατικά επιχορηγούμενης εκστρατείας κυβερνοεπιθέσεων που αναφέρθηκε ότι συνδέεται με την κινεζική κυβέρνηση.

Μάρτιος 2019. Ρώσοι hackers στόχευσαν σε ένα μεγάλο αριθμό ευρωπαϊκών κυβερνητικών φορέων πριν από τις εκλογές για το Ευρωπαϊκό Κοινοβούλιο τον Μάιο 2019.

Φεβρουάριος 2019. Η ευρωπαϊκή αεροδιαστημική εταιρεία Airbus αποκαλύπτει ότι δέχθηκε επίθεση από Κινέζους hackers οι οποίοι υπέκλεψαν τις προσωπικές πληροφορίες και τις πληροφορίες αναγνώρισης πληροφορικής ορισμένων ευρωπαίων εργαζομένων.

Ιανουάριος 2019. Hackers υπέκλεψαν τα προσωπικά στοιχεία, τις ιδιωτικές επικοινωνίες και τις οικονομικές πληροφορίες εκατοντάδων Γερμανών πολιτικών, που αντιπροσώπευαν κάθε πολιτικό κόμμα εκτός από αυτό της άκρας δεξιάς AfD.

Νοέμβριος 2018. Γερμανοί αξιωματούχοι ασφαλείας ανακοίνωσαν ότι μια ομάδα συνδεδεμένη με τη Ρωσία είχε στοχεύσει στους λογαριασμούς ηλεκτρονικού

[37] Βλ. σχετικές πήροφορίες: Center for Strategic and International Studies, Significant Cyber Incidents, Διαθέσιμο στο: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (Πρόσβαση 16.11.2019)

ταχυδρομείου πολλών μελών του γερμανικού κοινοβουλίου, καθώς και του γερμανικού στρατού και αρκετών πρεσβειών.

Σεπτέμβριος 2018. Ερευνητές ανέφεραν ότι 36 διαφορετικές κυβερνήσεις χρησιμοποίησαν το spyware της Pegasus έναντι στόχων σε τουλάχιστον 45 χώρες, συμπεριλαμβανομένων των ΗΠΑ, της Γαλλίας, του Καναδά και του Ηνωμένου Βασιλείου.

Ιούνιος 2018. Η αστυνομία της Ουκρανίας ισχυρίστηκε ότι Ρώσοι hackers στόχευαν συστηματικά ουκρανικές τράπεζες, εταιρείες ενέργειας και άλλες οργανώσεις για να δημιουργήσουν backdoors[38] υπό προετοιμασία για μια ευρείας κλίμακας επίθεση κατά της χώρας.

Απρίλιος 2018. Ο διευθυντής του Κεντρικού Γραφείου Κυβερνητικών Επικοινωνιών του Ηνωμένου Βασιλείου ανακοίνωσε ότι ο οργανισμός είχε πραγματοποιήσει επιθετικές επιχειρήσεις στον κυβερνοχώρο εναντίον του ISIS με σκοπό την καταστολή της προπαγάνδας του.

Φεβρουάριος 2018. Γερμανικά νέα ανέφεραν ότι μια ρωσική ομάδα hackers είχε παραβιάσει τα ηλεκτρονικά δίκτυα των υπουργείων εξωτερικών και εσωτερικών της Γερμανίας, υποκλέπτοντας τουλάχιστον 17 gigabytes δεδομένων, μια εισβολή που δεν είχε εντοπιστεί για ένα χρόνο.

Ιανουάριος 2018. Νορβηγοί αξιωματούχοι ανακάλυψαν μια «πολύ επαγγελματική» προσπάθεια να υποκλαπούν δεδομένα ασθενών από νορβηγικό νοσοκομειακό σύστημα, σε μια επίθεση που εικάζουν ότι συνδέεται με την επερχόμενη στρατιωτική άσκηση του NATO Trident Juncture 18.

Οι καταγραφές κυβερνοεπιθέσεων αντικατοπτρίζουν την έκταση του φαινομένου του κυβερνοπολέμου στη στρατηγική των κρατών είτε για οικονομικούς είτε για πολιτικούς σκοπούς. Η ουσιαστική όμως παρατήρηση η οποία μπορεί να εξαχθεί είναι πως απαιτείται έλεγχος και μέτρα αποτροπής στον κυβερνοχώρο και στα εργαλεία του, οι πλούσιες χώρες μπορούν να πιέσουν οικονομικά τις χώρες που δεν καταπολεμούν το ηλεκτρονικό έγκλημα. Έτσι, μπορεί να συσταθεί διεθνές κέντρο που θα παρακολουθεί τις επιθέσεις στον κυβερνοχώρο. Το Internet δεν είναι κοινό αγαθό. Είναι ένα δίκτυο δικτύων από τα οποία τα περισσότερα είναι ιδιωτικά. Αρά χρειάζεται συνεργασία των κυβερνήσεων με τον ιδιωτικό τομέα. Οι πάροχοι του Internet θα πρέπει να φροντίσουν να μη γίνουν οι υπολογιστές απλών ανθρώπων όργανα εγκλήματος ή επιθέσεων[39].

[38] Ένα backdoor είναι συνήθως μια κρυφή μέθοδος εισβολής παρακάμπτοντας τον κανονικό έλεγχο ταυτότητας ή την κρυπτογράφηση σε έναν υπολογιστή. https://en.wikipedia.org/wiki/Backdoor_(computing) (Πρόσβαση 17.11.2019)

[39] Βλ. σχετικές πληροφορίες: Ο κυβερνοπόλεμος άρχισε, 8 Ιουλίου 2010, Ελευθεροτυπία, Διαθέσιμο στο: http://www.enet.gr/?i=news.el.article&id=181298 (Πρόσβαση 17.11.2019)

2.3 Ανάγκη συντονισμένης προσέγγισης εντός της Ευρωπαϊκής Ένωσης στον τομέα πρόληψης των κυβερνοεπιθέσεων.

Ο πρώην Πρόεδρος της Ευρωπαϊκής Επιτροπής Jean-Claude Juncker έχει δηλώσει πως «Οι κυβερνοεπιθέσεις δεν γνωρίζουν σύνορα και κανείς δεν είναι απρόσβλητος» (13.09.2017). Η φράση αυτή είναι αρκετή ώστε να κατανοήσει κανείς το πρίσμα μέσω του οποίου αντιλαμβάνεται η Ένωση τον τομέα της κυβερνοασφάλειας και την αναγκαιότητα η οποία διέπει την ανάπτυξη αντίστοιχων συντονισμένων στρατηγικών δράσεων απέναντι στον κυβερνοπόλεμο και τις απειλές που αυτός επιφέρει στο παγκόσμιο γίγνεσθαι. Ένα ακόμη σημείο μέσω του οποίου διαφαίνεται η διάθεση για συντονισμένη δράση από την πλευρά της Ευρωπαϊκής Ένωσης πέραν της δημόσιας αποδοχής, αποτελεί η πληθώρα Προτάσεων, Οδηγιών, Κανονισμών αλλά και Διεθνών Συμφωνιών/Συνεργασιών εκδιδόμενων και συναπτόμενων προς αυτή την κατεύθυνση.

Τα συστήματα δικτύου και πληροφοριών και οι υπηρεσίες ηλεκτρονικών επικοινωνιών διαδραματίζουν ζωτικό ρόλο στην κοινωνία και αποτελούν κεντρικό πυλώνα της οικονομικής ανάπτυξης. Η τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ) ενισχύει τα σύνθετα συστήματα που στηρίζουν τις καθημερινές κοινωνικές δραστηριότητες, επιτρέπει την απρόσκοπτη και συνεχή λειτουργία των οικονομιών σε βασικούς τομείς όπως της υγείας, της ενέργειας, και των μεταφορών και υποστηρίζει γενικότερα τη λειτουργία της εσωτερικής αγοράς. Η αυξημένη ψηφιοποίηση και συνδεσιμότητα οδηγούν σε ολοένα και μεγαλύτερους κινδύνους για την κυβερνοασφάλεια, με αποτέλεσμα να καθίσταται η κοινωνία εν γένει πιο ευάλωτη σε κυβερνοαπειλές και να οξύνονται οι κίνδυνοι που αντιμετωπίζουν τα φυσικά πρόσωπα, συμπεριλαμβανομένων των πλέον ευάλωτων ομάδων όπως τα παιδιά[40].

Η οικονομική αυτή διάσταση οδηγεί την Ένωση σε συντονισμένη ανάληψη δράσεων στον τομέα της κυβερνοασφάλειας βασιζόμενη στο γεγονός πως η ασφάλεια στον κυβερνοχώρο είναι κρίσιμης σημασίας, τόσο για την ευημερία όσο και για την ασφάλειά των κρατών μελών άρα και της Ένωσης ως σύνολο. Οι κακόβουλες δραστηριότητες στον κυβερνοχώρο δεν απειλούν μόνο τις οικονομίες και την πορεία προς την ψηφιακή ενιαία αγορά, αλλά και την ίδια τη λειτουργία της δημοκρατίας, τις ελευθερίες και τις αξίες της Ένωσης. Η μελλοντική ασφάλεια εξαρτάται από την προσαρμογή της Ένωσης στο νέο περιβάλλον και από τις δράσεις πρόληψης των απειλών στον κυβερνοχώρο καθώς είναι γεγονός πως τόσο οι μη στρατιωτικές όσο και οι στρατιωτικές υποδομές βασίζονται σε ψηφιακά συστήματα. Αυτό αναγνωρίστηκε στο Ευρωπαϊκό Συμβούλιο του Ιουνίου 2017, καθώς και στη συνολική στρατηγική για την εξωτερική πολιτική και την πολιτική ασφαλείας[41]. Από μελέτες προκύπτει πως οι οικονομικές επιπτώσεις του εγκλήματος στον κυβερνοχώρο πενταπλασιάστηκαν από το 2013 έως το 2017 και ενδέχεται μάλιστα να

[40] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 15

[41] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, Βρυξέλλες, 13.9.2017

τετραπλασιαστούν έως το τέλος του 2019. Ιδιαίτερη αύξηση έχει διαπιστωθεί στις περιπτώσεις που αφορούν το λογισμικό ransomware (λυτρισμικό), καθώς οι πρόσφατες επιθέσεις αντικατοπτρίζουν τη ραγδαία αύξηση της εγκληματικής δραστηριότητας στον κυβερνοχώρο. Ωστόσο, το λυτρισμικό δεν αποτελεί σε καμία περίπτωση τη μοναδική απειλή[42].

Πέραν της οικονομικής διάστασης των απειλών που εξαπολύονται στην εσωτερική αγορά και παρά το γεγονός πως οι πολιτικές ασφαλείας εναπόκεινται ακόμη στα κράτη μέλη, η Ένωση αναγνωρίζει το διασυνοριακό χαρακτήρα του φαινομένου και το γεγονός πως οι απειλές στον κυβερνοχώρο προέρχονται τόσο από μη κρατικούς όσο και από κρατικούς δρώντες και συχνά πρόκειται για εγκληματικές ενέργειες, με κίνητρο το κέρδος, αλλά μπορεί επίσης να έχουν πολιτικό και στρατηγικό χαρακτήρα. 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 δημοκρατικές διαδικασίες. Η χρήση του κυβερνοχώρου ως πεδίο 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[43].

Η αποτελεσματική αντιμετώπιση των προκλήσεων ασφάλειας των συστημάτων δικτύου και πληροφοριών απαιτεί, συνεπώς, μια σφαιρική προσέγγιση σε επίπεδο Ένωσης που να καλύπτει κοινές ελάχιστες απαιτήσεις σχεδιασμού, την ανταλλαγή πληροφοριών, τη συνεργασία και τις κοινές απαιτήσεις ασφάλειας για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών[44]. Ακόμη, τα μεγάλης κλίμακας συμβάντα διαταράσσουν την παροχή βασικών υπηρεσιών σε όλη την Ένωση. Αυτό απαιτεί αποτελεσματική και συντονισμένη απόκριση και διαχείριση κρίσεων σε επίπεδο Ένωσης, με βάση ειδικές πολιτικές και αποτελεσματικότερα μέσα διασφάλισης της ευρωπαϊκής αλληλεγγύης και της αμοιβαίας συνδρομής. Επιπλέον, η τακτική εκτίμηση της κατάστασης της κυβερνοασφάλειας και της ανθεκτικότητας της στην Ένωση με βάση αξιόπιστα δεδομένα, καθώς και η συστηματική πρόληψη μελλοντικών εξελίξεων, προκλήσεων και απειλών, σε ενωσιακό και σε παγκόσμιο επίπεδο, είναι σημαντικές για τους υπευθύνους χάραξης πολιτικής, τη βιομηχανία και τους τελικούς χρήστες[45].

Ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων, ο στρατηγικός κίνδυνος στον οποίο τίθενται οι πάροχοι υπηρεσιών και ως εκ τούτου τα κράτη μέλη και τα

[42] Βλ. 41.
[43] Ομοίως με 42.
[44] ΕΕ L 194, Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, σελ.2
[45] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 16

φυσικά και νομικά πρόσωπα της Ένωσης αλλά και η διεθνής διάσταση της κατάστασης, οδήγησε στην εφαρμογή νομοπαραγωγικής και στρατηγικής αντιμετώπισης από την πλευρά της Ένωσης.

Ταυτόχρονα αναγνωρίζεται πως οι οικονομίες και οι κοινωνίες έχουν αναπτύξει ιδιαίτερη εξάρτηση από τις συνδέσεις στο Διαδίκτυο σε όλα τα επίπεδα της καθημερινότητας με εκθετικό ρυθμό[46]. Η αναγκαία επαφή των πολιτών της Ένωσης με την τόσο εκτεταμένη διασυνδεσιμότητα και τους κινδύνους που τελικά αυτή επιφέρει ανοίγει διόδους στις δημοκρατικές διαδικασίες και αξίες των κρατών μελών οι οποίες αποτελούν τον βαθύ ιδεολογικό πυρήνα της Ένωσης ταράζοντας συθέμελά τη δημοκρατικής της υπόσταση. Το όραμα λοιπόν της Ένωσης παραμένει το ίδιο όπως και σε κάθε άλλη πρόκληση την οποία έχει κληθεί να αντιμετωπίσει, να ενθαρρύνει τις ευρωπαϊκές αξίες της ελευθερίας και της δημοκρατίας και να εξασφαλίσει ότι η ψηφιακή οικονομία μπορεί να αναπτυχθεί σε πλαίσιο ασφαλείας.

[46] SWD(2017) 295 final, Commission Staff Working Document Assessment of the EU2013 cybersecurity strategy, 13.09.2017, σελ. 6

3. Ενωσιακό Νομοθετικό πλαίσιο κυβερνοασφάλειας

3.1 Η δημιουργία του Χώρου Ελευθερίας Ασφάλειας και Δικαιοσύνης

Ο Χώρος Ελευθερίας Ασφάλειας και Δικαιοσύνης έχει αναπτυχθεί προοδευτικά από το 1975. Η θεσμοθέτηση του, έλαβε χώρα για πρώτη φορά το 1986 με την Ενιαία Ευρωπαϊκή Πράξη (ΕΕΠ) μέσω της οποίας αναδείχθηκε η ελεύθερη κυκλοφορία των προσώπων ως ένα από τα τέσσερα βασικά συστατικά στοιχεία της ενιαίας αγοράς και ανατέθηκε ρητά ο τομέας αυτός στην κοινοτική (τότε) αρμοδιότητα. Η συνεργασία σε θέματα δικαιοσύνης και εσωτερικών υποθέσεων (ΔΕΥ) απετέλεσε τον τρίτο πυλώνα της Συνθήκης για την Ευρωπαϊκή Ένωση[47].

Εν συνεχεία, η εξέλιξη του Χώρου δρομολογείται με τη Συνθήκη του Άμστερνταμ. Οι Ευρωπαίοι εταίροι αναγνωρίζουν ότι η συνεργασία στον τομέα της δικαιοσύνης και των εσωτερικών υποθέσεων είναι στενά συνδεδεμένη με την ελεύθερη κυκλοφορία των προσώπων -ύλη του πρώτου πυλώνα- και ότι στον τομέα αυτό οφείλουν να θεσπίσουν μέτρα ικανά να αντισταθμίσουν την κατάργηση των ελέγχων στα εσωτερικά σύνορα και τους κινδύνους που αυτή συνεπάγεται[48]. Με αυτή τη βάση η Συνθήκη του Άμστερνταμ (1997) ορίζει πως στόχος της ΕΕ είναι: «να διατηρήσει και να αναπτύξει την Ένωση ως χώρο ελευθερίας, ασφάλειας και δικαιοσύνης, μέσα στον οποίο εξασφαλίζεται η ελεύθερη κυκλοφορία των προσώπων σε συνδυασμό με κατάλληλα μέτρα όσον αφορά τους ελέγχους στα εξωτερικά σύνορα, το άσυλο, τη μετανάστευση, και την πρόληψη και καταστολή της εγκληματικότητας»[49].

Αμέσως μετά την εμπέδωση του Χώρου από τη Συνθήκη του Άμστερνταμ ακολούθησαν τρία προγράμματα τα οποία ορίστηκαν από αντίστοιχα Συμβούλια με στόχο την προώθηση και εξέλιξη ΧΕΑΔ. Πρώτο εγκρίθηκε από το Ευρωπαϊκό Συμβούλιο το πολυετές Πρόγραμμα του Τάμπερε με διάρκεια 5 ετών (1999-2004). Οι κύριοι στόχοι του προγράμματος ήταν η επίτευξη συμφωνίας για τη θέσπιση κοινού συστήματος ασύλου, η θέσπιση μέτρων για τη βελτίωση ως προς την πρόσβαση στη δικαιοσύνη και την αμοιβαία αναγνώριση δικαστικών αποφάσεων και η δημιουργία της Eurojust και της Ευρωπαϊκής Αστυνομικής Ακαδημίας[50]. Με τη λήξη του Προγράμματος του Τάμπερε το Ευρωπαϊκό Συμβούλιο εγκρίνει το δεύτερο πολυετές πρόγραμμα -γνωστό ως πρόγραμμα της Χάγης- για την περίοδο 2005-2009. Κύριοι στόχοι του ήταν η δημιουργία μιας συνολικής ευρωπαϊκής πολιτικής ασύλου, η προσθήκη της αξιολόγησης απειλών εγκληματικών ενεργειών στις λειτουργίες της Europol, η ενίσχυση του συστήματος πληροφοριών Σένγκεν και η υπαγωγή των θεμάτων ασύλου, λαθρομετανάστευσης, ελέγχων στα εξωτερικά σύνορα και ορισμένων θεμάτων

[47] Βλ. σχετικές πληροφορίες: Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Open courses, Διαθέσιμο στο: https://opencourses.auth.gr/modules/document/file.php/OCRS394/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/%CE%B5%CE%BD%CF%8C%CF%84%CE%B7%CF%84%CE%B1%2010%20%CE%A7%CE%95%CE%91%CE%94.pdf, (Πρόσβαση 6.12.2019)

[48] Μάρκος Παπακωνστάντης Η Τρομοκρατία στο Χώρο Ελευθερίας Ασφάλειας και Δικαιοσύνης, Μάρκος Παπακωνστάντης, Νομική Βιβλιοθήκη, 2019, σελ. 205

[49] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:11997D/TXT&from=EL, Συνθήκη του Άμστερνταμ, Άρθρο Β.

[50] Βλ. 47

συνεργασίας σε αστικές υποθέσεις στη διαδικασία συναπόφασης με ειδική πλειοψηφία στο Συμβούλιο[51].

Σε συνέχεια των προγραμμάτων η εξέλιξη και περαιτέρω προώθηση του ΧΕΑΔ επήλθε με τη Συνθήκη της Λισαβόνας (2007) με την εφαρμογή της οποίας Καταργείται η διάκριση ανάμεσα σε ζητήματα πρώτου και τρίτου πυλώνα και η ΕΕ παρεμβαίνει πλέον στο σύνολο των θεμάτων που άπτονται του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης. Τα θέματα που άπτονται του ΧΕΑΔ κατανέμονται σε τέσσερις τομείς: πολιτικές σχετικά με τον έλεγχο στα σύνορα, το άσυλο και τη μετανάστευση, δικαστική συνεργασία σε αστικές υποθέσεις, δικαστική συνεργασία σε ποινικές υποθέσεις και αστυνομική συνεργασία [52].

Τέλος, το 2009 το Ευρωπαϊκό Συμβούλιο ενέκρινε το πρόγραμμα της Στοκχόλμης για την περίοδο 2010-2014 με προτεραιότητες: την προαγωγή της ιθαγένειας και των θεμελιωδών δικαιωμάτων, την προαγωγή του δικαίου και της δικαιοσύνης και την περαιτέρω προστασία των πολιτών από την τρομοκρατία και το οργανωμένο έγκλημα[53].

3.2 Η εμπέδωση του Χώρου Ελευθερίας Ασφάλειας και Δικαιοσύνης

Ο Χώρος Ελευθερίας Ασφάλειας και Δικαιοσύνης αναφέρεται κατά βάση στον πολίτη για χάρη του οποίου και δημιουργήθηκε[54]. Το άρθρο 3 παράγραφος 2 της ΣΕΕ ορίζει τα εξής: «*Η Ένωση παρέχει στους πολίτες της χώρο ελευθερίας, ασφάλειας και δικαιοσύνης χωρίς εσωτερικά σύνορα, μέσα στον οποίο εξασφαλίζεται η ελεύθερη κυκλοφορία των προσώπων σε συνδυασμό με κατάλληλα μέτρα όσον αφορά τους ελέγχους στα εξωτερικά σύνορα, το άσυλο, τη μετανάστευση και την πρόληψη και καταστολή της εγκληματικότητας*».

Οι στόχοι του ΧΕΑΔ καθορίζονται στο άρθρο 67 της ΣΛΕΕ:

- Η Ένωση συγκροτεί χώρο ελευθερίας, ασφάλειας και δικαιοσύνης, με σεβασμό των θεμελιωδών δικαιωμάτων και των διαφορετικών νομικών συστημάτων και παραδόσεων των κρατών μελών.
- Εξασφαλίζει την απουσία ελέγχων των προσώπων στα εσωτερικά σύνορα και αναπτύσσει κοινή πολιτική στους τομείς του ασύλου, της μετανάστευσης και του ελέγχου των εξωτερικών συνόρων, η οποία βασίζεται στην αλληλεγγύη μεταξύ των κρατών μελών και είναι δίκαιη έναντι των υπηκόων τρίτων χωρών. Για τους σκοπούς του παρόντος τίτλου, οι ανιθαγενείς εξομοιώνονται με τους υπηκόους των τρίτων χωρών.
- Η Ένωση καταβάλλει προσπάθεια για να εξασφαλίζει υψηλό επίπεδο ασφάλειας με τη θέσπιση μέτρων πρόληψης και καταπολέμησης της εγκληματικότητας, του ρατσισμού και της ξενοφοβίας, μέτρων συντονισμού και συνεργασίας μεταξύ αστυνομικών και δικαστικών αρχών και των λοιπών αρμοδίων αρχών καθώς και με την αμοιβαία αναγνώριση των δικαστικών

[51] Βλ. 47
[52] Βλ. 47
[53] Βλ. 47
[54] Δονάτος Παπαγιάννης, Ευρωπαϊκό Δίκαιο, Νομική Βιβλιοθήκη, 5η Έκδοση, 2016, σελ. 553

αποφάσεων σε ποινικές υποθέσεις και, εάν χρειάζεται, την προσέγγιση των ποινικών νομοθεσιών.

- Η Ένωση διευκολύνει την πρόσβαση στη δικαιοσύνη, ιδίως με την αρχή της αμοιβαίας αναγνώρισης των δικαστικών και εξώδικων αποφάσεων σε αστικές υποθέσεις.

Στο πλαίσιο του Χώρου Ελευθερίας Ασφάλειας και Δικαιοσύνης όπως αυτός οριοθετείται από τη Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης τα θεσμικά όργανα επιφορτίζονται της διασφάλισης υψηλού επιπέδου ασφάλειας στους κόλπους της Ένωσης. Ειδικότερα στο πλαίσιο της συνεργασίας μεταξύ αστυνομικών και δικαστικών αρχών τα Όργανα αντλούν τη νομική βάση και εξουσιοδότηση ώστε να καθορίσουν κοινούς κανόνες και κατευθύνσεις για μείζονα ζητήματα ασφαλείας τα οποία υπάγονται στη δικαιοδοσία των κρατών μελών όμως ο συντονισμός δράσης σε επίπεδο Ένωσης κρίνεται απαραίτητος.

Πλέον, οι απειλές τις οποίες καλούνται να αντιμετωπίσουν τα κράτη αποκτούν νέα μορφή επιφέροντας συνέπειες πολύ διαφορετικές από αυτές του παρελθόντος, η κυριότερη και πλέον δύσκολα αντιμετωπίσιμη απειλή δεν είναι άλλη από τις κυβερνοεπιθέσεις. Η κυβερνοασφάλεια ανάγεται σε κεντρικό τομέα δράσης της Ευρωπαϊκής Ένωσης καθώς παράλληλα με την ασφάλεια του κυβερνοχώρου διασφαλίζεται τόσο η ακεραιότητα της εσωτερικής αγοράς όσο και η ασφάλεια και η ευημερία των πολιτών.

3.3 Ευρωπαϊκοί Οργανισμοί καταπολέμησης κυβερνοαπειλών

Όπως συνεπάγεται από το προηγούμενο υποκεφάλαιο και την ανάλυση του Χώρου Ελευθερίας Ασφάλειας και Δικαιοσύνης καθίσταται απαραίτητο η ενωσιακή προσέγγιση απέναντι στις όλο και κλιμακούμενες κυβερνοαπειλές, να διαπνέεται από δομημένη και ξεκάθαρα διαχωρισμένη διάρθρωση.

Η νομοπαρασκευαστική διαδικασία καταδεικνύει την πρόθεση των ευρωπαϊκών θεσμικών οργάνων να καταμερίσουν αρμοδιότητες και εξουσίες σε οργανισμούς των οποίων η δραστηριότητα θα περιορίζεται στον τομέα της κυβερνοασφάλειας. Η ανάθεση καθηκόντων σε οργανισμούς συμπλέει με την κατεύθυνση της ενωσιακής στρατηγικής για την κυβερνοασφάλεια η οποία προτάσσει την εναρμόνιση των εθνικών στρατηγικών και τη συντονισμένη αντιμετώπιση των κυβερνοαπειλών σε επίπεδο Ένωσης υποστηρικτικά και σε εθνικό επίπεδο επιχειρησιακά.

Πέραν της εξουσιοδότησης των αρμόδιων οργανισμών, το χαοτικό πλαίσιο του κυβερνοχώρου απαιτεί τη δημιουργία και συνεργασία δικτύων εντός και εκτός της Ένωσης, τη σύμπνοια και αλληλεγγύη των εθνικών κυβερνήσεων αλλά και την αγαστή συνεργασία δημόσιου και ιδιωτικού τομέα. Ειδικότερα η αναβάθμιση του ιδιωτικού τομέα σε ισχυρό δρώντα απέναντι στη θωράκιση της εσωτερικής αγοράς από τις κυβερνοαπειλές κρίνεται ως προτεραιότητα δεδομένου πως οι μικρομεσαίες επιχειρήσεις (ΜΜΕ) είναι αυτές που αναμένεται να ωφεληθούν περισσότερο από την εδραίωση του ευρωπαϊκού πλαισίου για την κυβερνοασφάλεια.

Η ευρωπαϊκή στρατηγική για την κυβερνοασφάλεια υποσκελίζεται σε πολιτικό όσο και αμυντικό επίπεδο. Από την πολιτική σκοπιά με τον πρόσφατο Κανονισμό (ΕΕ) 2019/881, ο ENISA αναλαμβάνει την πρωτοκαθεδρία στην διεκπεραίωση της ευρωπαϊκής στρατηγικής για την κυβερνοασφάλεια έχοντας υπό την αιγίδα του την CERT-EU και τα δίκτυα CSIRT. Όσον αφορά την αμυντική προοπτική, την πρωτοκαθεδρία δραστηριοτήτων αναλαμβάνει η Europol έχοντας αναπτύξει το ειδικό σκέλος της, αυτό της EC3.

3.3.1 Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια (ENISA)

Ο ENISA αποτελεί όργανο της Ένωσης και διαθέτει νομική προσωπικότητα[55]. Ο ENISA ιδρύθηκε με τον Κανονισμό (ΕΚ) αριθ. 460/2004[56] ως Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών. Η διάρκεια του καθορίστηκε με τον με τον Κανονισμό (ΕΚ) αριθ. 1007/2008[57] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, για την τροποποίηση του Κανονισμού (ΕΚ) αριθ. 460/2004 και η σύσταση του με τον Κανονισμό (ΕΚ) αριθ. 580/2011[58] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Η τελευταία τροποποίηση που δέχτηκε ο Οργανισμός πριν αναβαθμιστεί επήλθε με τον Κανονισμό (ΕΕ) αριθ. 526/2013[59] ο οποίος κατήργησε τον πρώτο Κανονισμό του 2004. Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών αναβαθμίζεται σε Οργανισμό της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια με τον Κανονισμό (ΕΕ) 2019/881 και αναλαμβάνει ενισχυμένες εξουσίες και καθήκοντα.

Δομή

Η διοικητική και διαχειριστική δομή του ENISA απαρτίζονται από[60]:

α) το διοικητικό συμβούλιο[61] το οποίο απαρτίζεται από ένα μέλος που διορίζεται από κάθε κράτος μέλος και δύο μέλη που διορίζονται από την Επιτροπή. Όλα τα μέλη έχουν δικαίωμα ψήφου και ένα αναπληρωματικό μέλος το καθένα. Η θητεία τους είναι τετραετής.

β) το εκτελεστικό συμβούλιο[62] το οποίο επικουρεί το διοικητικό συμβούλιο από το οποίο διορίζονται και τα πέντε μέλη που το απαρτίζουν επίσης με τετραετή θητεία.

γ) τον εκτελεστικό διευθυντή[63] ο οποίος λειτουργεί και ως εκπρόσωπος του Οργάνου, διακρίνεται από ανεξαρτησία και λογοδοτεί στο διοικητικό συμβούλιο.

---

[55] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 52

[56] ΕΕ L 77, Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών

[57] ΕΕ L 293, Κανονισμός (ΕΚ) αριθ. 1007/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Σεπτεμβρίου 2008, περί τροποποιήσεως του κανονισμού (ΕΚ) αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών ως προς τη διάρκειά του

[58] ΕΕ L 165, Κανονισμός (ΕΕ) αριθ. 580/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011 , περί τροποποιήσεως του κανονισμού (ΕΚ) αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών ως προς τη διάρκειά του

[59] ΕΕ L 165, Κανονισμός (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013 , σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004

[60] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 40

[61] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 40

[62] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 43

[63] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 43

δ) τη συμβουλευτική ομάδα του ENISA[64] η οποία συγκροτείται από το διοικητικό συμβούλιο και κατόπιν πρότασης του εκτελεστικού διευθυντή με διαφανή τρόπο και απαρτίζεται από εμπειρογνώμονες εγνωσμένου κύρους που αντιπροσωπεύουν τους σχετικούς συμφεροντούχους, όπως τον κλάδο ΤΠΕ, τους παρόχους δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών για το κοινό, μικρομεσαίες επιχειρήσεις, τους φορείς εκμετάλλευσης βασικών υπηρεσιών, ομάδες καταναλωτών, τους πανεπιστημιακούς που είναι ειδικοί στον τομέα της κυβερνοασφάλειας, και εκπροσώπους των αρμόδιων αρχών, ευρωπαϊκών οργανισμών τυποποίησης, όπως επίσης και των αρχών επιβολής του νόμου και των εποπτικών αρχών προστασίας δεδομένων. Το διοικητικό συμβούλιο επιδιώκει να διασφαλίζει κατάλληλη ισορροπία των φύλων και γεωγραφική ισορροπία, καθώς και ισορροπία μεταξύ των διαφόρων ομάδων συμφεροντούχων.

ε) δίκτυο εθνικών υπαλλήλων-συνδέσμων[65] το οποίο συγκροτείται με την ίδια διαδικασία συγκρότησης της συμβουλευτικής ομάδας και απαρτίζεται από αντιπροσώπους όλων των κρατών μελών (εθνικοί υπάλληλοι-σύνδεσμοι). Κάθε κράτος μέλος ορίζει έναν αντιπρόσωπο στο δίκτυο εθνικών υπαλλήλων-συνδέσμων.

Λειτουργία

Βάση της λειτουργίας του Οργανισμού αποτελεί το ενιαίο έγγραφο προγραμματισμού[66] που περιέχει το ετήσιο και πολυετές πρόγραμμά του και περιλαμβάνει όλες τις προγραμματισμένες δραστηριότητές του. Το έγγραφο προγραμματισμού συντάσσεται από τον εκτελεστικό διευθυντή και περιλαμβάνει ακόμη τον αντίστοιχο προγραμματισμό των οικονομικών και ανθρώπινων πόρων.

Αρχές Λειτουργίας

Δήλωση συμφερόντων[67]
Τα μέλη του διοικητικού συμβουλίου, ο εκτελεστικός διευθυντής και οι υπάλληλοι που αποσπώνται προσωρινά από τα κράτη μέλη υποβάλλουν έκαστος δήλωση δεσμεύσεων και γραπτή δήλωση συμφερόντων όπου καταδεικνύεται η απουσία ή ύπαρξη οποιουδήποτε άμεσου ή έμμεσου συμφέροντος που θα μπορούσε να επηρεάσει την ανεξαρτησία τους.

[64] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 45
[65] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 46
[66] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 46
[67] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 47

Διαφάνεια[68]

Ο ENISA μεριμνά ώστε να παρέχονται στο κοινό και σε κάθε ενδιαφερόμενο μέρος οι ενδεδειγμένες αντικειμενικές, αξιόπιστες και εύκολα προσβάσιμες πληροφορίες, ιδίως όσον αφορά τα αποτελέσματα των εργασιών του.
Εμπιστευτικότητα[69]
Ο ENISA δεν αποκαλύπτει σε τρίτους πληροφορίες που επεξεργάζεται ή λαμβάνει και σχετικά με τις οποίες έχει υποβληθεί τεκμηριωμένο αίτημα για πλήρη ή μερική τήρηση του απορρήτου

Πρόσβαση σε έγγραφα[70]

Οι αποφάσεις που λαμβάνονται από τον ENISA είναι δυνατόν να αποτελέσουν αντικείμενο καταγγελίας στον Ευρωπαίο Διαμεσολαβητή σύμφωνα με το άρθρο 228 ΣΛΕΕ ή προσφυγής ενώπιον του Δικαστηρίου της Ευρωπαϊκής Ένωσης σύμφωνα με το άρθρο 263 ΣΛΕΕ.

Δράση ENISA

Η βασική εντολή που λαμβάνει ο Οργανισμός[71] τον αναβαθμίζει σε σημείο αναφοράς για την παροχή συμβουλών και εμπειρογνωμοσύνης σχετικά με την κυβερνοασφάλεια για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και άλλους σχετικούς συμφεροντούχους στην Ένωση με κύριο σκοπό τη μείωση του κατακερματισμού της εσωτερικής αγοράς. Τα καθήκοντα του ανατίθενται με νομικές πράξεις της Ένωσης που καθορίζουν μέτρα για την προσέγγιση νόμων, κανονισμών και διοικητικών διατάξεων των κρατών μελών που σχετίζονται με την κυβερνοασφάλεια. Κατά την εκτέλεση των καθηκόντων του, ο ENISA ενεργεί ανεξάρτητα, αποφεύγοντας τις αλληλεπικαλύψεις των δραστηριοτήτων των κρατών μελών και λαμβάνοντας υπόψη την υπάρχουσα εμπειρογνωσία των κρατών μελών.

Στόχοι

Ο ENISA δραστηριοποιείται έτσι ώστε να[72]:

- επικουρεί τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και τα κράτη μέλη, στην ανάπτυξη και την εφαρμογή πολιτικών της Ένωσης που σχετίζονται με την κυβερνοασφάλεια
- στηρίζει την ανάπτυξη ικανοτήτων και την ετοιμότητα στην Ένωση, επικουρώντας τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης,

[68] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 47
[69] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 47
[70] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 48
[71] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 34
[72] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 34

καθώς και τα κράτη μέλη και τους ιδιωτικούς και δημόσιους συμφεροντούχους, με σκοπό την ενίσχυση της προστασίας των συστημάτων δικτύου και πληροφοριών τους
- προάγει τη συνεργασία, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, και τον συντονισμό σε ενωσιακό επίπεδο
- συμβάλλει στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε επίπεδο Ένωσης προκειμένου να στηρίζει τις ενέργειες των κρατών μελών όσον αφορά την πρόληψη και την αντιμετώπιση κυβερνοαπειλών
- προάγει τη χρήση της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς
- προάγει ένα υψηλό επίπεδο ευαισθητοποίησης ως προς την κυβερνοασφάλεια, συμπεριλαμβανομένης της κυβερνοϋγιεινής[73] και του κυβερνογραμματισμού[74] μεταξύ πολιτών, οργανισμών και επιχειρήσεων.

Καθήκοντα ENISA

Α. Χάραξη και εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης[75]
Ο ENISA δρα επικουρικά, υποστηρικτικά και συμβουλευτικά ως προς την επανεξέταση της πολιτικής και του δικαίου της Ένωσης όσον αφορά την κυβερνοασφάλεια αλλά και ως προς την συνεπή εφαρμογή των ανωτέρω από τα κράτη μέλη. Συμμετέχει επικουρικά στην προώθηση πολιτικών κυβερνοασφάλειας που συνδέονται με την υποστήριξη της γενικής διαθεσιμότητας ή της ακεραιότητας του δημόσιου πυρήνα του ανοιχτού διαδικτύου αλλά και υποστηρίζει την προαγωγή ενισχυμένου επιπέδου ασφάλειας των ηλεκτρονικών επικοινωνιών, μεταξύ άλλων με την παροχή συμβουλών και εμπειρογνωμοσύνης, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών. Τέλος εκπονεί ετήσια έκθεση σχετικά με την κατάσταση εφαρμογής του νομικού πλαισίου για τις κοινοποιήσει συμβάντων και παραβίασης ασφαλείας.

Β. Ανάπτυξη ικανοτήτων[76]
Μέρος των καθηκόντων του ENISA αποτελεί και η υποβοήθηση των κρατών μελών, θεσμικών οργάνων της Ένωσης και Οργανισμών στις προσπάθειές τους να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης κυβερνοαπειλών και συμβάντων αλλά και αντιμετώπισης των κινδύνων αυτών. Πέραν των θεσμικών φορέων ο ENISA επικουρεί και τις εθνικές και ενωσιακές

[73] Επί του παρόντος δεν υπάρχει ενιαία πρότυπη ή από κοινού συμφωνηθείσα προσέγγιση όσον αφορά την υγιεινή στον κυβερνοχώρο σε όλη την Ευρώπη καθώς κάθε κράτος μέλος έχει τα δικά του προγράμματα και καθοδήγηση. Κυρίως, αυτά τα προγράμματα ευθυγραμμίζονται ή κατευθύνονται από τις εθνικές στρατηγικές για την ασφάλεια στον κυβερνοχώρο που δημοσιεύονται από κάθε κράτος μέλος και ως εκ τούτου έχουν διαφορετικά επίπεδα ωριμότητας. Review of Cyber Hygiene practices, Δεκέμβριος 2016, ENISA

[74] ασκήσεις που επιτρέπουν στις αρμόδιες αρχές να στοχεύουν συγκεκριμένες αδυναμίες, να αυξάνουν τη συνεργασία, να εντοπίζουν τις αλληλεξαρτήσεις, να ενθαρρύνουν τη βελτίωση του σχεδιασμού συνέχειας και να δημιουργούν μια κουλτούρα συνεργατικής προσπάθειας για την ενίσχυση της ανθεκτικότητας. https://www.enisa.europa.eu/topics/cyber-exercises/trainings/cyber_exercises (Πρόσβαση 22.11.2019)

[75] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 35

[76] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 36

CSIRT με στόχο την αύξηση του επιπέδου ικανότητάς τους όσο αφορά την προώθηση του διαλόγου και της ανταλλαγής πληροφοριών σχετικά με την τεχνολογία αιχμής. Τέλος, ο ENISA είναι επιμορφωμένος με την παροχή κατάρτισης στους αρμόδιους δημόσιους φορείς και αν κριθεί απαραίτητο και στους συμφεροντούχους.

Γ. Επιχειρησιακή συνεργασία σε Επίπεδο Ένωσης[77]
Η υποστηρικτική δράση του ENISA στο επιχειρησιακό επίπεδο συνεργασίας των κρατών μελών και των οργάνων κατά βάση διέπεται από τη γραμματειακή υποστήριξη την οποία παρέχει στο δίκτυο CSIRT, αλλά πέραν αυτού παρέχει συμβουλές και καθοδήγηση για τη βελτίωση των ικανοτήτων τους στον εντοπισμό, την αντιμετώπιση και την εκτίμηση συμβάντων σχετικά με την κυβερνοασφάλεια. Σε αυτή τη επιχειρησιακή δραστηριότητα ο ENISA δεσμεύεται να βρίσκεται σε συνεργασία με τη CERT-EU. Τέλος, συμβάλλει στη διοργάνωση ασκήσεων κυβερνοασφάλειας ενώ προβαίνει και στην εκπόνηση τεχνικών εκθέσεων ανάλυσης κινδύνων.

Δ. Αγορά, πιστοποίηση της κυβερνοασφάλειας και προτυποποίηση[78]
Όσο αφορά το υπό δημιουργία (2019) πλαίσιο πιστοποίησης της Ευρωπαϊκής Ένωσης ο ENISA υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ. Εντός αυτής της κατεύθυνσης και προς επίτευξη των σκοπών του παρακολουθεί τα υπό εξέλιξη πλαίσια πιστοποίησης συντάσσοντας και δημοσιεύοντας κατευθυντήριες γραμμές για ορθές πρακτικές και αξιολογεί τα ήδη εγκριθέντα.

Ε. Γνώσεις και πληροφορίες[79]
Ο ρόλος του ENISA εμπλουτίζεται υπό την έννοια της εμπειρογνωμοσύνης την οποία απαιτείται να παρέχει. Πιο συγκεκριμένα διενεργεί αναλύσεις και αξιολογήσεις νέων τεχνολογιών παρέχοντας έτσι καθοδήγηση για τις βέλτιστες πρακτικές μειώνοντας τον διασκορπισμό της κοινωνίας των πληροφοριών, ενώ παράλληλα συγκεντρώνει, οργανώνει και γνωστοποιεί στο κοινό πληροφορίες σχετικά με την κυβερνοασφάλεια, τις οποίες παρέχουν τα θεσμικά και λοιπά όργανα και οι οργανισμοί της Ένωσης και πληροφορίες σχετικά με την κυβερνοασφάλεια που παρέχουν, εθελοντικώς, τα κράτη μέλη και οι ιδιωτικοί και δημόσιοι συμφεροντούχοι μέσω ειδικής διαδικτυακής πύλης.

ΣΤ. Ευαισθητοποίηση και εκπαίδευση[80]
Ο ENISA αναλαμβάνει μεταξύ των υπολοίπων και το έργο της ευαισθητοποίησης του κοινού σχετικά με την κυβερνοασφάλεια. Με σκοπό την ενημέρωση του κοινού για ένα θέμα τόσο κομβικής σημασίας διοργανώνει, σε συνεργασία με τα

[77] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 36
[78] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 38
[79] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 38
[80] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 39

κράτη μέλη, τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και τον κλάδο, τακτικές εκστρατείες προβολής για την αύξηση της κυβερνοασφάλειας και της ορατότητάς της στην Ένωση και ενθαρρύνει την ευρεία δημόσια συζήτηση.

Η. Έρευνα και καινοτομία[81]
Στον όλο και εξελισσόμενο τομέα της έρευνας και της καινοτομίας ο ENISA παρέχει υπηρεσίες συμβούλου σχετικά με ερευνητικές ανάγκες και προτεραιότητες στον τομέα της κυβερνοασφάλειας και εφόσον του ανατεθούν οι ανάλογες εξουσίες εκ της Επιτροπής, συμμετέχει στην υλοποίηση των προγραμμάτων χρηματοδότησης της έρευνας και της καινοτομίας ακόμη και ως δικαιούχος.

Θ. Διεθνής συνεργασία[82]
Ο ENISA συμμετέχει, διευκολύνει και παρέχει εμπειρογνωμοσύνη στις προσπάθειες της Ένωσης για συνεργασία της με τρίτες χώρες και διεθνείς οργανισμούς και της Επιτροπής σε θέματα σχετικά με συμφωνίες για την αμοιβαία αναγνώριση των πιστοποιητικών κυβερνοασφάλειας με τρίτες χώρες.
Ταυτόχρονα ο ίδιος δύναται να συνεργάζεται με τις αρμόδιες αρχές τρίτων χωρών ή με διεθνείς οργανισμούς ή και με τα δύο. Για τον σκοπό αυτό, ο ENISA δύναται, κατόπιν προηγούμενης έγκρισης της Επιτροπής, να συνάπτει συμφωνίες συνεργασίας με τις εν λόγω αρχές τρίτων χωρών και διεθνείς οργανισμούς. Οι εν λόγω συμφωνίες συνεργασίας δεν δημιουργούν έννομες υποχρεώσεις στην Ένωση και τα κράτη μέλη της[83].

3.3.2 CSIRT (Ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών)

Οι CSIRT δεν αποτελούν όργανο ούτε φορέα της Ευρωπαϊκής Ένωσης, όμως ο ρόλος τους κρίνεται απαραίτητος και ιδιαίτερα κομβικός στο οικοδόμημα της ενιαίας ενωσιακής στρατηγικής για την κυβερνοασφάλεια.
Οι Ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών ορίζονται στην Οδηγία 2016/1148[84]. Στόχος της οδηγίας ήταν η επίτευξη υψηλού κοινού επιπέδου ασφάλειας των δικτύων και των συστημάτων πληροφοριών εντός της ΕΕ μέσω βελτιωμένων δυνατοτήτων στον κυβερνοχώρο σε εθνικό επίπεδο, αυξημένης συνεργασίας και διαχείρισης κινδύνων σε επίπεδο ΕΕ, υποχρεώσεων υποβολής εκθέσεων σχετικά με τα περιστατικά για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών. Η οδηγία αποτέλεσε σημαντικό ορόσημο για την οικοδόμηση της ανθεκτικότητας

[81] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 39
[82] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 39
[83] ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA, σελ. 53
[84] ΕΕ L 194, Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

στον κυβερνοχώρο σε ευρωπαϊκό επίπεδο και τέθηκε σε ισχύ τον Αύγουστο του 2016. Ταυτόχρονα καθιερώνεται και το δίκτυο των CSIRT με σκοπό να συμβάλει στην ανάπτυξη εμπιστοσύνης μεταξύ των κρατών μελών για την πλέον γρήγορη και αποτελεσματική επιχειρησιακή συνεργασία.
Το Δίκτυο CSIRT είναι ένα δίκτυο που αποτελείται από τις CSIRT και τα CERT-EU ("μέλη του Δικτύου CSIRT") των κρατών μελών της ΕΕ. Η Ευρωπαϊκή Επιτροπή συμμετέχει στο δίκτυο ως παρατηρητής. Ο ENISA είναι επιφορτισμένος με την ενεργό υποστήριξη της συνεργασίας των CSIRT, την παροχή γραμματείας και την ενεργό υποστήριξη του συντονισμού των περιστατικών, κατόπιν αιτήματος.

Το Δίκτυο CSIRT παρέχει ένα φόρουμ όπου τα μέλη μπορούν να συνεργάζονται, να ανταλλάσσουν πληροφορίες και να δημιουργούν εμπιστοσύνη. Τα μέλη με αυτό τον τρόπο θα είναι σε θέση να βελτιώσουν τη διαχείριση των διασυνοριακών περιστατικών και ακόμη θα συζητήσουν πώς να ανταποκριθούν με συντονισμένο τρόπο σε συγκεκριμένα περιστατικά[85]. Όλα τα κράτη μέλη της Ένωσης έχουν δημιουργήσει μία ή/και παραπάνω CSIRT.

3.3.3 Ευρωπαϊκή Υπηρεσία για τη συνεργασία στον τομέα της επιβολής του νόμου (Europol - Ευρωπόλ)

Η Europol ιδρύθηκε με την Απόφαση 2009/371/ΔΕΥ του Συμβουλίου ως οργανισμός της Ένωσης του οποίου αποστολή είναι η υποστήριξη και η ενίσχυση της δράσης των αρμόδιων αρχών των κρατών μελών και της αμοιβαίας συνεργασίας τους για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος, της τρομοκρατίας και άλλων μορφών σοβαρού εγκλήματος που επηρεάζουν δύο ή περισσότερα κράτη μέλη.
Η Europol ως υπηρεσία επιβολής του νόμου της Ευρωπαϊκής Ένωσης ιδρύεται με τον Κανονισμό (ΕΕ) 2016/794[86] ο οποίος καταργεί την προηγούμενη απόφαση του Συμβουλίου. Η Europol αναγνωρίζεται ως οργανισμός της Ένωσης και της αποδίδεται νομική προσωπικότητα.
Σήμερα η Europol με έδρα τη Χάγη των Κάτω-Χωρών στηρίζει τα 28 κράτη μέλη της ΕΕ στην καταπολέμηση της σοβαρής διεθνούς εγκληματικότητας και τρομοκρατίας. Οι σοβαρότερες απειλές οι οποίες αντιμετωπίζονται από την Europol:

- τρομοκρατία·
- διεθνής διακίνηση ναρκωτικών και νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες
- οργανωμένη απάτη
- παραχάραξη του ευρώ
- παράνομη διακίνηση ανθρώπων

[85] Βλ. σχετικές πληροφορίες: CSIRTS Network, Διαθέσιμο στο: https://csirtsnetwork.eu/ (Πρόσβαση 22.11.2019)
[86] ΕΕ L. 135 Κανονισμός (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ

Φυσικά στις δραστηριότητες της έχει ενταχθεί πλέον και η καταπολέμηση του κυβερνοεγκλήματος και η υποστήριξη της κυβερνοασφάλειας της Ένωσης[87].
Η κυβερνοασφάλεια αντιμετωπίζεται από την Europol από την αμυντική στρατηγική σκοπιά της.
Στο πλαίσιο των δραστηριοτήτων της η Europol ίδρυσε το Ευρωπαϊκό Κέντρο Καταπολέμησης της Πληροφορίας (EC3) το 2013 για να ενισχύσει την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο στην ΕΕ και, ως εκ τούτου, να βοηθήσει στην προστασία των ευρωπαίων πολιτών, επιχειρήσεων και κυβερνήσεων από εγκλήματα στο Διαδίκτυο. Από την ίδρυσή της, η EC3 έχει συμβάλει σημαντικά στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο: έχει συμμετάσχει σε δεκάδες επιχειρήσεις υψηλού προφίλ και εκατοντάδες επιτόπιες λειτουργικές ενισχύσεις που έχουν ως αποτέλεσμα εκατοντάδες συλλήψεις και έχουν αναλύσει εκατοντάδες χιλιάδες των αρχείων, η μεγάλη πλειοψηφία των οποίων αποδείχθηκε κακόβουλη[88].
Κάθε χρόνο, δημοσιεύεται από την EC3 εκτίμηση απειλής οργανωμένου εγκλήματος στο Διαδίκτυο (IOCTA), στρατηγική έκθεσή σχετικά με τα κύρια πορίσματα και τις αναδυόμενες απειλές και τις εξελίξεις όσον αφορά την εγκληματικότητα στον κυβερνοχώρο. Το Ευρωπαϊκό Κέντρο Καταπολέμησης της Πληροφορίας διαθέτει δύο ομάδες εγκληματολογίας, για τη ψηφιακή εγκληματολογία και για την εγκληματολογία εγγράφων, η καθεμία από τις οποίες επικεντρώνεται στην επιχειρησιακή υποστήριξη, στην έρευνα και την ανάπτυξη. Οι δραστηριότητες του κέντρου υποστηρίζονται από την Cyber Intelligence Team (CIT), της οποίας οι αναλυτές συλλέγουν και επεξεργάζονται πληροφορίες σχετικές με το έγκλημα στον κυβερνοχώρο από δημόσιες, ιδιωτικές και ανοικτές πηγές και εντοπίζουν αναδυόμενες απειλές και πρότυπα. Η δράση της βασίζεται στην υπάρχουσα ικανότητα επιβολής του νόμου της Europol - αλλά επεκτείνεται επίσης σημαντικά και σε άλλες δυνατότητες, παρέχοντας ιδίως επιχειρησιακή και αναλυτική υποστήριξη στις έρευνες των κρατών μελών. Πιο συγκεκριμένα λειτουργεί ως κεντρικός κόμβος ανταλλαγής πληροφοριών, συντονίζοντας και προσφέροντας εμπειρογνωμοσύνη αλλά και παρέχοντας μια ποικιλία προϊόντων στρατηγικής ανάλυσης που επιτρέπουν τη λήψη τεκμηριωμένων αποφάσεων σε τακτικά και στρατηγικά επίπεδα για την καταπολέμηση και την πρόληψη του εγκλήματος στον κυβερνοχώρο. Η κυριότερη ίσως συμβολή της είναι η παροχή ολοκληρωμένης λειτουργίας ενημέρωσης που συνδέει τις αρχές επιβολής του νόμου που ασχολούνται με το έγκλημα στον κυβερνοχώρο με τον ιδιωτικό τομέα, τον ακαδημαϊκό χώρο και άλλους εταίρους που δεν ασκούν την επιβολή του νόμου[89].

Η συμβολή της Europol στη στρατηγική της κυβερνοασφάλειας μέσω της δράσης της EC3 παρέχει σημαντική καθοδήγηση στα κράτη μέλη αλλά και στην Ένωση σχετικά με τους συνεχώς εναλασσόμενους κινδύνους.

[87] Βλ. σχετικές πληροφορίες: Europol, Διαθέσιμο στο: https://www.europol.europa.eu/el/about-europol (Πρόσβαση 22.11.2019)
[88] Βλ. σχετικές πληροφορίες: Europol, Διαθέσιμο στο: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Πρόσβαση 22.11.2019)
[89] Βλ. 88

3.4 Νομοθετικές Δράσεις της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Ο τομέας της κυβερνοασφάλειας έχει ενταχθεί στην ατζέντα της Ευρωπαϊκής Ένωσης σε επίπεδο εσωτερικής πολιτικής, όπως οι τομείς της δικαιοσύνης και των εσωτερικών υποθέσεων, της ψηφιακής ενιαίας αγοράς και των πολιτικών για την έρευνα. Στον τομέα της εξωτερικής πολιτικής, η κυβερνοασφάλεια αποτελεί ζήτημα που απασχολεί τους διπλωματικούς κύκλους, και εισέρχεται όλο και περισσότερο στην αναδυόμενη πολιτική της Ένωσης στον τομέα της άμυνας.

Το «οικοσύστημα» του κυβερνοχώρου σε ενωσιακό επίπεδο είναι πολυεπίπεδο και πολύπλευρο με ακρογωνιαίο λίθο τη νομοπαραγωγική δράση στην προσπάθεια να θωρακιστεί το ψηφιακό περιβάλλον της Ένωσης μέσω μίας κοινής στρατηγικής κυβερνοασφάλειας. Όπως προελέχθη, παρά το γεγονός πως η αμυντική πολιτική και η θωράκιση ασφαλείας παραμένει ακόμη στην αρμοδιότητα των κρατών μελών, η κυβερνοάμυνα λόγω του διασυνοριακού της χαρακτήρα εντάσσεται πλέον στα πεδία άσκησης πολιτικής από την Ένωση. Στόχος των στρατηγικών σχετικά με την κυβερνοασφάλεια είναι να εξασφαλιστεί υψηλό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης στο πλαίσιο εναρμόνισης των εθνικών πολιτικών. Είναι γεγονός πως τα κράτη μέλη έχουν πολύ διαφορετικά επίπεδα ετοιμότητας, που έχουν οδηγήσει στον κατακερματισμό προσεγγίσεων στην Ένωση με συνέπεια την μη αποτελεσματική προστασία τόσο της ενιαίας ψηφιακής αγοράς όσο και των ίδιων των πολιτών που αλληλοεπιδρούν καθημερινά μέσω του κυβερνοχώρου. Έχει γίνει πλέον σαφές πως η αποτελεσματική αντιμετώπιση των προκλήσεων ασφάλειας των συστημάτων δικτύων και πληροφοριών απαιτεί, μια σφαιρική προσέγγιση σε επίπεδο Ένωσης που να καλύπτει κοινές ελάχιστες απαιτήσεις δημιουργίας και σχεδιασμού, την ανταλλαγή πληροφοριών, τη συνεργασία και τις κοινές απαιτήσεις ασφάλειας για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών.

Οι στρατηγικές της Ευρωπαϊκής Ένωσης θέτουν σε θεωρητικό επίπεδο πέντε βασικούς στόχους:

i) ενίσχυση της κυβερνοανθεκτικότητας

ii) μείωση της κυβερνοεγκληματικότητας

iii) ανάπτυξη πολιτικών και ικανοτήτων κυβερνοάμυνας

iv) ανάπτυξη βιομηχανικών και τεχνολογικών πόρων κυβερνοασφάλειας και

v) θέσπιση διεθνούς πολιτικής για τον κυβερνοχώρο, σύμφωνη με τις θεμελιώδεις αξίες της Ευρωπαϊκής Ένωσης[90].

[90] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 16

3.4.1 Ιστορική Εξέλιξη Νομοθετικών Πράξεων της Ευρωπαϊκής Ένωσης.

Από το 2002 έχουν εγκριθεί νομοθετικές πράξεις σε Ενωσιακό επίπεδο οι οποίες σχετίζονται, έκαστη σε διαφορετικό βαθμό, με την κυβερνοασφάλεια προσπαθώντας να θέσουν επί του πρακτέου τους ανωτέρω στόχους και να ενσωματώσουν την κυβερνοάμυνα στον πυρήνα της Ένωσης ως βασικό άξονα πολιτικής και στρατηγικής.

Το 2001 εκδίδεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής για την ασφάλεια δικτύων και πληροφοριών: «Πρόταση Ευρωπαϊκής Πολιτικής». Η Ευρωπαϊκή Επιτροπή υπογραμμίζει την αυξανόμενη σημασία της Ασφάλειας Δικτύων και Πληροφοριών[91].
Ακολουθεί Απόφαση-Πλαίσιο[92] του Συμβουλίου της Ευρωπαϊκής Ένωσης της 28ης Μαΐου 2001, σχετικά με την καταπολέμηση της απάτης και της πλαστογραφίας στα μέσα πληρωμών, πλην των μετρητών.
Τέλος την 23η Νοεμβρίου 2001 επικυρώνεται η Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.

Την 12η Ιουλίου 2002 εκδίδεται Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των δεδομένων[93], σύμφωνα με την οποία όλοι οι φορείς οι οποίοι είναι υπεύθυνοι επεξεργασίας δεδομένων υποχρεούνται να θεσπίσουν μέτρα ασφάλειας για την προστασία των δεδομένων προσωπικού χαρακτήρα. Στο σημείο αυτό γίνεται η πρώτη διασύνδεση του τομέα της κυβερνοασφάλειας με αυτόν της προστασίας δεδομένων προσωπικού χαρακτήρα.

Την 10η Μαρτίου 2004 εκδίδεται Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[94] με τον οποίο ιδρύεται ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών (ENISA), με βασική του αρμοδιότητα την εξασφάλιση υψηλού επιπέδου ασφάλειας ώστε να αναπτυχθεί στην Ένωση κλίμα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών.

Την 31η Μάϊου 2006 εκδίδεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων»[95] θέτοντας ως στόχο την δημιουργία βάσεων

[91] COM/2001/0298, Ανακοίνωση από την Επιτροπή προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών - Ασφάλεια δικτύων και πληροφοριών: Πρόταση ευρωπαϊκής πολιτικής

[92] ΕΕ L 2001_149_R_0001_01, 2001/413/ΔΕΥ: Απόφαση-πλαίσιο του Συμβουλίου, της 28ης Μαΐου 2001, για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών

[93] ΕΕ L 201, Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

[94] ΕΕ L 77, Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών

[95] COM/2006/0251, Ανακοινωση της Επιτροπης στο Συμβουλιο, στο Ευρωπαϊκο Κοινοβουλιο, στην Ευρωπαϊκη Οικονομικη και Κοινωνικη Επιτροπη και στην Επιτροπη των Περιφερειων - Στρατηγική για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων»

συνεργασίας για την ασφάλεια δικτύων και πληροφοριών στην Ένωση. Η Ανακοίνωση εγκρίνεται με ψήφισμα του Συμβουλίου.

Την 8η Δεκεμβρίου 2008 εκδίδεται Οδηγία του Συμβουλίου της Ευρωπαϊκής Ένωσης[96] η οποία εισάγει τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας (ΕΥΖΣ)[97], την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους.

Την 30η Μαρτίου 2009 εκδίδεται Ανακοίνωση της Επιτροπής[98] με στόχο την προστασία υποδομών πληροφοριών ζωτικής σημασίας (Critical Information Infrastructure Protection - CIIP). Η Ανακοίνωση επικεντρώνεται στην προστασία της Ευρώπης από διαταραχές στον κυβερνοχώρο μέσω ενίσχυσης της ασφάλειας και ταυτόχρονη υποστήριξη των προσπαθειών των κρατών μελών να εξασφαλίσουν πρόληψη και αντίδραση. Το σχέδιο δράσης εγκρίθηκε στα συμπεράσματα τη προεδρίας της υπουργικής διάσκεψης στο Τάλιν το 2009.
Επακόλουθα την 18η Δεκεμβρίου 2009 εκδίδεται Ψηφίσμα του Συμβουλίου της Ευρωπαϊκής Ένωσης[99], με θέμα «μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών».

Την 19η Μαΐου 2010 εκδίδεται Ανακοίνωση της Επιτροπής με τίτλο «Το ψηφιακό θεματολόγιο για την Ευρώπη»[100].
Στο Συμβούλιο την 31η Μαΐου 2010 (10130/10), εξάγεται στα συμπεράσματα η κοινή πεποίθηση ότι η εμπιστοσύνη και η ασφάλεια αποτελούν θεμελιώδεις προϋποθέσεις για την ευρεία αφομοίωση των τεχνολογιών πληροφοριών και επικοινωνίας (ΤΠΕ) καθώς και για την επίτευξη των στόχων της στρατηγικής «Ευρώπη 2020» που αφορά την «έξυπνη ανάπτυξη». Στο κεφάλαιο σχετικά με την εμπιστοσύνη και την ασφάλεια, το Ψηφιακό θεματολόγιο εστιάζει στην ανάγκη όλοι οι ενδιαφερόμενοι να κατευθυνθούν σε μια κοινή προσπάθεια με σκοπό να εξασφαλιστεί η ασφάλεια και η ανθεκτικότητα της υποδομής σε ΤΠΕ, θέτοντας ως κύριους στόχους την πρόληψη, την ετοιμότητα και την ευαισθητοποίηση του κοινού, αλλά και την ανάπτυξη αποτελεσματικών και συντονισμένων μηχανισμών ασφαλείας. Πιο συγκεκριμένα η κεντρική δράση του

---

[96] ΕΕ L 345, Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008 , σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους

[97] Περιουσιακά στοιχεία ή συστήματα τα οποία είναι ουσιώδη για τη διατήρηση των κοινωνικών λειτουργιών ζωτικής σημασίας, της υγείας, της ασφάλειας και της οικονομικής ή κοινωνικής ευπραγίας των ατόμων. Οι ευρωπαϊκές υποδομές ζωτικής σημασίας (ΕΥΖΣ) είναι υποδομές ζωτικής σημασίας στις χώρες της ΕΕ των οποίων η βλάβη ή η καταστροφή θα είχε σημαντικό αντίκτυπο σε τουλάχιστον δύο χώρες της ΕΕ (π.χ. σταθμούς παραγωγής ηλεκτρικής ενέργειας ή αγωγούς μεταφοράς πετρελαίου). http://publications.europa.eu/resource/cellar/15306167-9a7e-4022-9f02-ce742f9d7850.0009.02/DOC_1 (Πρόσβαση 25.11.2019)

[98] ΕΕ L 313, Οδηγία 2009/149/ΕΚ της Επιτροπής, της 27ης Νοεμβρίου 2009 , για την τροποποίηση της οδηγίας 2004/49/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τους κοινούς δείκτες ασφάλειας και τις κοινές μεθόδους υπολογισμού του κόστους ατυχήματος

[99] 2009/C 321/01, Ψήφισμα του Συμβουλίου, της 18ης Δεκεμβρίου 2009, για μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών

[100] COM/2010/0245, Ανακοίνωση της Επιτροπής της 19ης Μαΐου 2010, προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, σχετικά με το Ψηφιακό Θεματολόγιο για την Ευρώπη.

Ψηφιακού θεματολογίου για την Ευρώπη εισάγει μέτρα που αποβλέπουν σε ενισχυμένη και υψηλού επιπέδου πολιτική ασφάλειας δικτύων και πληροφοριών.

Την 30η Σεπτεμβρίου 2010 εγκρίνεται πρόταση της Ευρωπαϊκής Επιτροπής για τον εκσυγχρονισμό του Ευρωπαϊκού Οργανισμού για την ασφάλεια δικτύων και πληροφοριών ENISA[101].

Την 20η Απριλίου 2010 εκδίδεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής «Για ένα χώρο ελευθερίας, ασφάλειας και δικαιοσύνης στην υπηρεσία των πολιτών της Ευρώπης - Σχέδιο δράσης για την εφαρμογή του προγράμματος της Στοκχόλμης»[102], και την 22η Νοεμβρίου 2010 η Ανακοίνωση Ευρωπαϊκής της Επιτροπής «Η στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη»[103].
Γίνεται πλέον όλο και πιο εμφανής η έμφαση στην ορθή υλοποίηση δράσεων ασφαλείας.

Την 31η Μαρτίου εκδίδεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής, με τίτλο «Επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο»[104]. Η Ευρωπαϊκή Επιτροπή μετά τον απολογισμό των αποτελεσμάτων που επιτεύχθηκαν μετά την έγκριση του σχεδίου δράσης το 2009, καταλήγει στο συμπέρασμα ότι από την εφαρμογή του προγράμματος προέκυψε οι αμιγώς εθνικές προσεγγίσεις για την αντιμετώπιση των προκλήσεων που αφορούν την ασφάλεια και την ανθεκτικότητα δεν επαρκούν, και ότι η Ευρώπη πρέπει να συνεχίσει τις προσπάθειες για την οικοδόμηση μιας συνεκτικής και συνεργατικής προσέγγισης σε ολόκληρη την ΕΕ. Στην ανακοίνωση του 2011 αναγγέλθηκε σειρά δράσεων, ενώ η Ευρωπαϊκή Επιτροπή καλεί τα κράτη μέλη να συγκροτήσουν διασυνοριακή συνεργασία.

Στα συμπεράσματά του της 27ης Μαΐου 2011, το Ευρωπαϊκό Συμβούλιο υπογράμμισε την επείγουσα ανάγκη τα συστήματα και τα δίκτυα ΤΠΕ:

- να καταστούν ανθεκτικά και ασφαλή από κάθε πιθανή διαταραχή, τυχαία ή εσκεμμένη,
- να αναπτυχθεί σε ολόκληρη την Ένωση υψηλό επίπεδο ετοιμότητας, ασφάλειας και ανθεκτικότητας των ικανοτήτων,
- να αναβαθμιστούν οι τεχνικές ικανότητες ώστε να μπορέσει η Ένωση να αντιμετωπίσει τα προβλήματα που συνεπάγεται η προστασία δικτύων και υποδομών πληροφοριών, καθώς και
- να ενισχυθεί η συνεργασία μεταξύ των κρατών μελών με την ανάπτυξη μηχανισμών συνεργασίας έναντι συμβάντων ασφάλειας.

[101] COM/2010/521, Πρόταση, Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον Ευρωπαϊκό Οργανισμό για την ασφάλεια Δικτύων και Πληροφοριών (ENISA)

[102] COM/2010/0171, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών για ένα χώρο ελευθερίας, ασφάλειας και δικαιοσύνης στην υπηρεσία των πολιτών της Ευρώπης Σχέδιο δράσης για την εφαρμογή του προγράμματος της Στοκχόλμης

[103] COM/2010/0673 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο Η στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη

[104] ΕΕ L 70, Απόφαση της Επιτροπής της 16ης Μαρτίου 2011 για την έγκριση σχεδίων που υποβλήθηκαν από τρίτες χώρες σύμφωνα με το άρθρο 29 της οδηγίας 96/23/ΕΚ του Συμβουλίου

Την 22η Μαΐου 2012 ανακοινώνεται Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου, σχετικά με τη Στρατηγική Εσωτερικής Ασφάλειας της Ένωσης.

Την 7η Ιουνίου εκδίδεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής με τίτλο «Αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο»[105] και σχετικά συμπεράσματα του Συμβουλίου.

Την 27η Σεπτεμβρίου 2012 εκδίδεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής[106], με τίτλο «Αξιοποίηση των δυνατοτήτων του cloud computing στην Ευρώπη». Την οποία ακολουθεί Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 22ης Νοεμβρίου 2012 σχετικά με την ασφάλεια και την άμυνα στον κυβερνοχώρο και Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 11ης Δεκεμβρίου 2012 σχετικά με την ολοκλήρωση της ενιαίας ψηφιακής αγοράς το οποίο με τη σειρά του ακολουθείται από Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 11ης Δεκεμβρίου 2012, σχετικά με τη θέσπιση μιας Στρατηγικής Ψηφιακής Ελευθερίας στο πλαίσιο της εξωτερικής πολιτικής της ΕΕ. Οι πράξεις αυτές επιστεγάζονται με την Ανακοίνωση της Ευρωπαϊκής Επιτροπής της 18ης Δεκεμβρίου 2012 με τίτλο «Το ψηφιακό θεματολόγιο για την Ευρώπη - Η υλοποίηση της ευρωπαϊκής ανάπτυξης ψηφιακά»[107].

Την 12η Αυγούστου 2013 εκδίδεται Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών[108] προς αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Η οποία ακολουθείται από Νομοθετικό ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Απριλίου 2013 επί της πρότασης[109] κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

Την 7η Φεβρουαρίου 2013 εκδίδεται Πρόταση για Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[110] σχετικά με τα μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση. Η οποία ακολουθείται με Κοινή Ανακοίνωση της Ευρωπαϊκής

[105] COM/2012/0140, Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, Αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο

[106] COM/2012/0529, Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους

[107] COM/2012/0784, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών. Ψηφιακό θεματολόγιο για την Ευρώπη. Οδηγώντας την Ευρώπη στη ψηφιακή ανάπτυξη.

[108] ΕΕ L 218, Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013 , για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

[109] COM/2010/521, Πρόταση της Επιτροπής, στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)

[110] COM/2013/0027, Πρόταση της Επιτροπής, στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση.

Επιτροπής[111] της 7ης Φεβρουαρίου 2013 προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών σχετικά με μια στρατηγική για την ασφάλεια στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο.

Το Ευρωπαϊκό κοινοβούλιο στην Πρόταση Ψηφίσματος της 6ης Σεπτεμβρίου 2013 σχετικά με μια στρατηγική για την ασφάλεια στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο[112], καλεί τα κράτη μέλη να δραστηριοποιηθούν και να αναλάβουν όλες τις απαραίτητες ενέργειες, προτείνει δράσεις για τη βελτίωση της υφιστάμενης κατάστασης και ζητά από την Επιτροπή, τα κράτη μέλη, την Europol και το EC3, την Eurojust και τον ENISA να προβούν στη σύνταξη τακτικών εκθέσεων με αποτίμηση της προόδου που σημειώνεται σχετικά με τους στόχους που θέτει η στρατηγική ασφαλείας στον κυβερνοχώρο.

[111] JOIN/2013/1, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών. Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο

[112] ΕΕ L 93, Στρατηγική για την ασφάλεια στον κυβερνοχώρο της ΕΕ: ένας ανοιχτός, ασφαλής και προστατευμένος κυβερνοχώρος. Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 12ης Σεπτεμβρίου 2013 σχετικά με μια στρατηγική για την ασφάλεια στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο

3.4.2 Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

Η Οδηγία 2016/1148 εκδίδεται στη βάση δημιουργίας μίας ολοκληρωμένης και κλιμακούμενης συμπόρευσης και ευθυγράμμισης της πολιτικής αλλά και της ευρύτερης σκοπιάς με την οποία τα κράτη μέλη αντιμετωπίζουν την κυβερνοασφάλεια αλλά και πως δρουν προς τη θωράκιση των πληροφοριακών τους συστημάτων. Όπως έχει ήδη διατυπωθεί η Ευρωπαϊκή Ένωση έχει αναλάβει την υποστήριξη των κρατών μελών στον τομέα της κυβερνοασφάλειας και της πρόληψης περιστατικών που στόχο έχουν να προκαλέσουν ζημίες. Με την Οδηγία αυτή ουσιαστικά τίθενται τα θεμέλια μιας κοινής αντιμετώπισης του εν λόγω ζητήματος. Η Οδηγία θέτει το θέμα της ασφάλειας δικτύων και συστημάτων με αποστερώ σκοπό την εύρυθμη και απρόσκοπτη λειτουργία της εσωτερικής αγοράς ανάγοντας το θέμα σε μία βάση πιότερο οικονομική παρά αμυντική. Παρόλα αυτά τα αποτελέσματα που προκύπτουν από την Οδηγία αναπόφευκτα αγγίζουν και τους δύο τομείς.
Πιο συγκεκριμένα οι βασικές κατευθύνσεις της Οδηγίας είναι οι ακόλουθες[113]:

Α. προβλέπει τις υποχρεώσεις να θεσπιστεί εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών από όλα τα κράτη μέλη
Β. δημιουργεί ομάδα συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, καθώς και την ανάπτυξη της εμπιστοσύνης και της αξιοπιστίας μεταξύ τους
Γ. δημιουργεί δίκτυο ομάδων απόκρισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών («δίκτυο CSIRT»), προκειμένου να συμβάλει στην ανάπτυξη της της αξιοπιστίας και εμπιστοσύνης μεταξύ των κρατών μελών και να προωθήσει την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία
Δ. θεσπίζει απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών·
Ε. προβλέπει τις υποχρεώσεις των κρατών μελών να ορίζουν εθνικές αρμόδιες αρχές, ενιαία κέντρα επαφής και CSIRT με καθήκοντα σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

Τα κράτη μέλη καλούνται να θεσπίσουν τις εθνικές τους στρατηγικές σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών καθορίζοντας ξεκάθαρα τους στόχους, το πλαίσιο διακυβέρνησης, τα μέτρα ετοιμότητας, τα προγράμματα ενημέρωσης, εκπαίδευσης και έρευνας καθώς και το σχέδιο εκτίμησης των κινδύνων. Η πιο ουσιώδης ίσως προτεραιότητα που ανατίθεται στα κράτη μέλη για τους σκοπούς της Οδηγίας είναι ο προσδιορισμός των φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας συστημάτων δικτύου και πληροφοριών.

[113] ΕΕ L 194, Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, σελ. 11

Για την ακρίβεια το εκάστοτε κράτος μέλος πρέπει να ορίσει ένα εθνικό ενιαίο κέντρο επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών το οποίο θα ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών μελών καθώς και με τις αρμόδιες αρχές άλλων κρατών μελών και την ομάδα συνεργασίας η οποία απαρτίζεται από αντιπροσώπους των κρατών μελών, την Επιτροπής και τον ENISA. Κατά τον ίδιο χρόνο τα κράτη – μέλη καλούνται να ορίσουν ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT). Οι ομάδες αυτές ανήκουν σε ένα ευρύτερο δίκτυο στο οποίο συμμετέχουν οι CSIRT όλων των κρατών μελών αλλά και η CERT-EU[114] με την υποστήριξη της Επιτροπής και του ENISA. Οι κύριες αρμοδιότητες του δικτύου CSIRT είναι η ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, μετά από αίτημα κράτους μέλους καθορισμός συντονισμένης απόκρισης για ένα συμβάν που έχει διαπιστωθεί εντός της δικαιοδοσίας του συγκεκριμένου κράτους μέλους και η υποστήριξη των κρατών μελών για την αντιμετώπιση διασυνοριακών συμβάντων βάσει της εθελούσιας αμοιβαίας συνδρομής τους.
Η Οδηγία προβαίνει σε μία ρητή διάκριση ανάμεσα στους φορείς εκμετάλλευσης βασικών υπηρεσιών και στου παρόχους υπηρεσιών τονίζοντας το απαραίτητο της συνεργασίας τους καθώς οι δεύτεροι ανήκουν ως επί το πλείστον στον ιδιωτικό τομέα και καλεί τα κράτη μέλη να παροτρύνουν και τις δύο μεριές να διατηρούν τους δικούς τους άτυπους μηχανισμούς συνεργασίας για την εξασφάλιση της ασφάλειας των συστημάτων δικτύου και πληροφοριών. Η ομάδα συνεργασίας θα πρέπει να είναι σε θέση να καλεί τους αρμόδιους φορείς στις συζητήσεις κατά περίπτωση. Προκειμένου να ενθαρρυνθεί αποτελεσματικά η ανταλλαγή πληροφοριών και βέλτιστων πρακτικών, είναι αναγκαίο να εξασφαλίζεται ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών που συμμετέχουν σε αυτές τις ανταλλαγές, δεν είναι σε μειονεκτική θέση λόγω της συνεργασίας τους.
Άλλη μία σημαντική προσθήκη της Οδηγίας προς μία συνολική προσέγγιση της στρατηγικής για την κυβερνοασφάλεια είναι η θέσπιση ελάχιστων απαιτήσεων ασφαλείας αλλά και η άμεση κοινοποίηση των συμβάντων. Ακόμη τα κράτη μέλη καλούνται να αποδώσουν στις αρμόδιες αρχές τις απαραίτητες εξουσίες για την αξιολόγηση της συμμόρφωσης των φορέων εκμετάλλευσης βασικών υπηρεσιών προς τις υποχρεώσεις τους προκειμένου η συντονισμένη δράση να μην μείνει κενό γράμμα. Ταυτόχρονα κρίνεται σημαντικό οι αρμόδιες αρχές να εφοπλιστούν και με εποπτικά μέτρα ώστε να εξακριβώνεται πως οι πάροχοι υπηρεσιών τηρούν τα απαραίτητα επίπεδα ασφαλείας.
Επαφίεται στα κράτη μέλη, επίσης, ο προσδιορισμός των κυρώσεων σε περίπτωση παράβασης των εθνικών διατάξεων που θα θεσπιστούν κατ' εφαρμογή της Οδηγίας, έπειτα από ενημέρωση της Επιτροπής.

Πέραν της εναρμόνισης των νομοθεσιών των κρατών μελών και των ξεκάθαρων στόχων που θέτει η Οδηγία, αποσκοπεί κατά βάση στη αγαστή συνεργασία και την ανταλλαγή τεχνογνωσίας αναγνωρίζοντας για ακόμη μία φορά τη διασυνοριακότητα του τομέα της κυβερνοασφάλειας και επιδιώκοντας μία συντονισμένη και ισχυρή αντιμετώπιση στο πλαίσιο της αλληλεγγύης και της αμοιβαιότητας.

[114] Βλ. σχετικές πληροφορίες: CERT-EU, Διαθέσιμο στο: https://cert.europa.eu/cert/plainedition/en/cert_about.html (Πρόσβαση 27.11.2019)

3.4.3 Κανονισμός (ΕΕ) 2019/881 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)

Ο Κανονισμός της 17ης Απριλίου 2019 εκδόθηκε ως επιστέγασμα της αναβάθμισης της πολιτικής για την κυβερνοασφάλεια σε ενωσιακό επίπεδο επιβεβαιώνοντας για μία ακόμη φορά, την πρόθεση των θεσμικών ευρωπαϊκών οργάνων να θέσουν τον τομέα της κυβερνοάμυνας σε μείζον θέμα στρατηγικής. Η ραγδαία τεχνολογική εξέλιξή αποτέλεσε για ακόμη μια φόρα το βασικότερο λόγο ανάληψης νομοθετικής δράσης της Ένωσης.
Η ευρεία και καθημερινή χρήση συστημάτων δικτύου και πληροφοριών αλλά και η εξάπλωση του διαδικτύου των πραγμάτων (IoT)[115], κατέδειξε τα σημαντικά κενά τα οποία υπάρχουν σε επίπεδο πιστοποίησης τεχνολογικών προϊόντων και υπηρεσιών. Η πλήρης διασυνδεσιμότητα ανοίγει το δρόμο για μεγάλης κλίμακας συμβάντα κυβερνοαπειλών τα οποία να και συνήθως έχουν διασυνοριακό χαρακτήρα, είναι ικανά να διαταράξουν την παροχή βασικών υπηρεσιών σε όλη την Ένωση. Η ελλιπής ενημέρωση των πολιτών σχετικά με τον τομέα της κυβερνοασφάλειας οδηγεί στη μείωση της εμπιστοσύνης τους τόσο προς τους παρόχους υπηρεσιών όσο και προς τους αρμόδιους φορείς. Δεδομένων αυτών των συνθηκών, οι κίνδυνοι και οι απειλές που αντιμετωπίζει η Ένωση ολοένα και αυξάνονται και ως εκ τούτου με τον Κανονισμό 2019/881 επιδιώκεται η πραγμάτωση δύο βασικών απαιτήσεων[116]:
Α. της θέσπισης των στόχων, των καθηκόντων και των οργανωτικών θεμάτων που σχετίζονται με τον ENISA
Β. της δημιουργίας πλαισίου για τη θέσπιση ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό τη διασφάλιση επαρκούς επιπέδου κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, καθώς και για τον σκοπό της αποφυγής του κατακερματισμού της εσωτερικής αγοράς όσον αφορά τα συστήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση
Τονίζεται πως για την επίτευξη των σκοπών αυτών η ανάληψη δράσης από τα κράτη μέλη δεν επαρκεί και επομένως η Ένωση τηρώντας την αρχή της αναλογικότητας αναλαμβάνει δράση δίχως να υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

[115] Βλ. σχετικές πληροφορίες: SAS, Διαθέσιμο στο: https://www.sas.com/el_gr/insights/big-data/internet-of-things.html (Πρόσβαση 28.11.2019)
[116] ΕΕ L 151, ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), σελ. 32

Α. ENISA (ο Οργανισμός της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια)[117]

Ο ENISA αναβαθμίζεται μέσω των επιπλέον καθηκόντων που του ανατίθενται και καλείται να ενεργεί ως σημείο αναφοράς για την παροχή συμβουλών και εμπειρογνωμοσύνης σχετικά με την κυβερνοασφάλεια για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και άλλους σχετικούς συμφεροντούχους στην Ένωση. Αναγνωρίζεται η ανεξαρτησία του και του παρέχεται η αυτόνομη ανάπτυξη ιδίων πόρων για την εκτέλεση των καθηκόντων του.
Ο Οργανισμός αποκτά συμβουλευτικά, επικουρικά, επιχειρησιακά και εκπαιδευτικά καθήκοντα. Αρχικά αποτελεί πλέον κέντρο εμπειρογνωσίας σε θέματα κυβερνοασφάλειας και μέσω αυτής της ιδιότητας είναι σε θέση να επικουρεί τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και τα κράτη μέλη, στην ανάπτυξη και την εφαρμογή πολιτικών της Ένωσης, να προάγει τη συνεργασία, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, και τον συντονισμό, να συμβάλλει στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε ενωσιακό επίπεδο, να προάγει τη χρήση της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς και να προάγει ένα υψηλό επίπεδο ευαισθητοποίησης ως προς την κυβερνοασφάλεια, συμπεριλαμβανομένης της κυβερνοϋγιεινής και του κυβερνογραμματισμού μεταξύ πολιτών, οργανισμών και επιχειρήσεων. Ακόμη ανάγεται σε ενεργό δρών όσον αφορά τη χάραξη και εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης επικουρώντας και παρέχοντας συμβουλές. Επιπλέον επιχειρεί συνεργαζόμενος σε επιχειρησιακό επίπεδο και αναπτύσσοντας συνέργειες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, συμπεριλαμβανομένων της CERT-EU ενώ ταυτόχρονα διοργανώνει τακτικά ασκήσεις κυβερνοασφάλειας σε επίπεδο Ένωσης και παρέχει συνδρομή στα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης στην οργάνωση ασκήσεων κυβερνοασφάλειας κατόπιν αιτήματός τους. Τέλος, η σημαντικότερη ίσως δράση που του ανατίθεται είναι η υποστήριξη στην εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, συντάσσοντας και δημοσιεύοντας κατευθυντήριες γραμμές και αναπτύσσοντας ορθές πρακτικές, όσον αφορά τις απαιτήσεις κυβερνοασφάλειας.
Τα καθήκοντα του ENISA βασίζονται στα ανωτέρω συμπεριλαμβανομένων των εκπαιδευτικών, ερευνητικών και όσων έχουν να κάνουν με διεθνείς συνεργασίες στον τομέα της κυβερνοασφάλειας.
Παρατηρείται η συγκέντρωση καθηκόντων τόσο υποστηρικτικών όσο και πρωτευόντων σε έναν οργανισμό. Η πρακτική αυτή η οποία αποτελεί πάγια λογική αντιμετώπισής ζητημάτων στο ενωσιακό επίπεδο φαίνεται να είναι ο πλέον αξιόλογος τρόπος αντιμετώπισης ενός τόσο χαοτικού και άνευ συνόρων πεδίου. Ο ENISA τίθεται θεματοφύλακας των πολιτικών και πρακτικών

[117] ΕΕ L 151, ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), σελ. 34

στρατηγικών της Ένωσης και των κρατών μελών τόσο στους ενδότερους κόλπους όσο και στο εξωτερικό περιβάλλον.

Β. Πλαίσιο πιστοποίησης της κυβερνοασφάλειας[118]

Τη βασικότερη καινοτομία του Κανονισμού σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών, αποτελεί το δεύτερο σκέλος του.

Η Ένωση θωρακίζει νομικά τη σύγκλιση των μέτρων που πρέπει να λαμβάνουν τα κράτη μέλη επηρεάζοντας τόσο το δημόσιο όσο και τον ιδιωτικό τομέα.

Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας προβλέπει ένα μηχανισμό μέσω του οποίου θεσπίζονται ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας και βεβαιώνεται ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν αξιολογηθεί σύμφωνα με τα εν λόγω συστήματα συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό να διαφυλάσσεται η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα και η εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών σε όλη τη διάρκεια του κύκλου ζωής τους.

Η εφαρμογή του πλαισίου πιστοποίησης θα ξεκινήσει με τη δημοσίευση εκ της Επιτροπής κυλιόμενου προγράμματος εργασιών το οποίο θα περιλαμβάνει ειδικά κατάλογο των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ ή των κατηγοριών τους που μπορούν να έχουν όφελος από τη συμπερίληψή τους στο πεδίο εφαρμογής ευρωπαϊκού συστήματος πιστοποίησης. Το πρόγραμμα θα επικαιροποιείται αναλόγως, ενώ ανατίθεται στην Επιτροπή να ζητά από τον ENISA να προτείνει υποψήφιο πρόγραμμα πιστοποίησης ή να αξιοποιήσει κάποιο ήδη υπάρχον. Ο ENISA στο έργο του αυτό θα προχωρά σε διαβουλεύσεις με τους εμπλεκόμενους και ενδιαφερόμενους φορείς ενώ θα συγκροτεί και ειδικές ad hoc ομάδες εργασίας προς τον σκοπό αυτό. Σε συνέχεια της πρότασης του ENISA η Επιτροπή θα δύναται να εκδίδει εκτελεστικές πράξεις σε σχέση με το πλαίσιο πιστοποίησης. Οι προτάσεις του ENISA θα βρίσκονται σε συγκεκριμένο διαδικτυακό τόπο πληρώντας έτσι το κενό της διαφάνειας το οποίο ίσως αντιμετωπίζει σήμερα ο τομέας της κυβερνοασφάλειας στον οποίο θα δηλώνονται και τα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας που θα έχουν αντικατασταθεί από το ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας.

Ο Κανονισμός, πέραν της κατεύθυνσης για το πως θα δομηθεί το επικείμενο πλαίσιο πιστοποίησης θέτει και τους στόχους στους οποίους πρέπει να ανταποκρίνεται, πιο συγκεκριμένα δίνεται ιδιαίτερη βαρύτητα στην ασφάλεια. Το

[118] ΕΕ L 151, ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), σελ. 53

πλαίσιο θα πρέπει να ανταποκρίνεται σε υψηλό επίπεδο προστασίας όσον αφορά τα δεδομένα που υπόκεινται επεξεργασία, ενώ το ίδιο υψηλό επίπεδο ασφαλείας απαιτείται και για την πρόσβαση σε αυτά τα δεδομένα. Το πλαίσιο πρέπει να παρέχει:

- τον εντοπισμό και την τεκμηρίωση γνωστών εξαρτήσεων και τρωτών σημείων
- την καταγραφή των δεδομένων, υπηρεσιών ή λειτουργιών στα οποία πραγματοποιήθηκε πρόσβαση
- τη δυνατότητα να ελέγχεται σε ποια δεδομένα, υπηρεσίες ή λειτουργίες πραγματοποιήθηκε πρόσβαση
- την επαλήθευση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ δεν έχουν γνωστά τρωτά σημεία
- την έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα, υπηρεσίες και λειτουργίες σε περίπτωση φυσικού ή τεχνικού συμβάντος
- τη διαβεβαίωση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ προστατεύονται εξ ορισμού και από τον σχεδιασμό τους
- ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ παρέχονται με επικαιροποιημένο λογισμικό και υλισμικό που δεν περιέχουν γνωστά στο κοινό τρωτά σημεία, και προβλέπονται μηχανισμοί για ασφαλείς επικαιροποιήσεις

Ακόμη εντός του πλαισίου θα διακρίνονται επίπεδα διασφάλισης των προϊόντων, υπηρεσιών και διαδικασιών τα οποία τα οποία θα πιστοποιούνται μέσω των ευρωπαϊκών πιστοποιητικών ασφαλείας ή των δηλώσεων συμμόρφωσης της Ευρωπαϊκής Ένωσης, τα οποία θα χορηγούνται κατόπιν αξιολόγησης των ανωτέρω. Τα πιστοποιητικά θα διασφαλίζουν πως το προϊόν, η υπηρεσία ή η διαδικασία που αξιολογήθηκε πληροί το αντίστοιχο επίπεδο ασφαλείας.

Οι δραστηριότητες αξιολόγησης θα περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία γνωστών στο κοινό τρωτών σημείων, έλεγχος για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι διαδικασίες ΤΠΕ και οι υπηρεσίες ΤΠΕ εφαρμόζουν ορθά την αναγκαία λειτουργία ασφάλειας προηγμένης τεχνολογίας και εκτίμηση της ανθεκτικότητάς τους σε επιδέξιους επιτιθέμενους μέσω δοκιμών διείσδυσης.

Το πλαίσιο πέραν της αξιολόγησης και πιστοποίησης θα παρέχει τη δυνατότητα αυτοσυμμόρφωσης. Πιο συγκεκριμένα, ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ θα δύναται να εκδίδει δήλωση συμμόρφωσης της Ευρωπαϊκής Ένωσης (η οποία θα διαθέτει πανευρωπαϊκή ισχύ) με την οποία θα δεσμεύεται για την εκπλήρωση των απαιτήσεων που ορίζονται στο σύστημα ενώ θα υποχρεούται να καταθέσει στην εκάστοτε εθνική αρχή πιστοποίησης την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που αφορούν τη συμμόρφωση των προϊόντων ΤΠΕ ή των υπηρεσιών ΤΠΕ.

Πέρα της αξιολόγησης ο κανονισμός εξειδικεύει τα τεχνικά στοιχεία τα οποία θα πρέπει να συμπεριλαμβάνει ένα ευρωπαϊκό σύστημα πιστοποίησης. Τα σημαντικότερα συνοψίζονται ως εξής:

- επακριβή περιγραφή του σκοπού του συστήματος και του τρόπου με τον οποίο τα επιλεγέντα πρότυπα, οι μέθοδοι αξιολόγησης και τα επίπεδα διασφάλισης αντιστοιχούν στις ανάγκες των προβλεπόμενων χρηστών του συστήματος

- αναφορά σε διεθνή, ευρωπαϊκά ή εθνικά πρότυπα που εφαρμόζονται κατά την αξιολόγηση
- ένδειξη του αν η αυτοαξιολόγηση της συμμόρφωσης επιτρέπεται στο πλαίσιο του συστήματος
- τα ειδικά κριτήρια και τις μεθόδους αξιολόγησης που πρόκειται να χρησιμοποιούνται
- τους κανόνες παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ με τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας ή των δηλώσεων συμμόρφωσης της Ευρωπαϊκής Ένωσης τους κανόνες σχετικά με τις συνέπειες προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που έχουν πιστοποιηθεί ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης της Ευρωπαϊκής Ένωσης τα οποία όμως δεν συμμορφώνονται προς τις απαιτήσεις του συστήματος
- την περίοδο διαθεσιμότητας της δήλωσης συμμόρφωσης της Ευρωπαϊκής Ένωσης, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που πρέπει να καταστούν διαθέσιμες από τον κατασκευαστή ή τον πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ
- τις προϋποθέσεις για την αμοιβαία αναγνώριση συστημάτων πιστοποίησης με τρίτες χώρες
- τον μορφότυπο και τις διαδικασίες που πρέπει να τηρούν οι κατασκευαστές ή οι πάροχοι προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ.

Όπως προβλέπεται σε όλες τις νομικές πράξεις του ενωσιακού νομοπαραγωγικού συστήματος ο Κανονισμός δεν προβλέπει μόνο υποχρεώσεις πιστοποίησης για κατασκευαστές και παρόχους αλλά και το υψηλότερο επίπεδο διασφάλισης και υποστήριξης των καταναλωτών. Οι κατασκευαστές και πάροχοι πιστοποιημένων προϊόντων θα πρέπει να δημοσιοποιούν καθοδήγηση και συστάσεις για τη συνδρομή προς τους τελικούς χρήστες ως προς τις ασφαλείς ρυθμίσεις, την εγκατάσταση, τη διάθεση, τη λειτουργία και τη συντήρηση των προϊόντων ΤΠΕ ή των υπηρεσιών ΤΠΕ, την περίοδο κατά την οποία θα προσφέρεται υποστήριξη ασφαλείας προς τους τελικούς χρήστες, τα στοιχεία επικοινωνίας του κατασκευαστή ή του παρόχου και τις αποδεκτές μεθόδους για τη λήψη πληροφοριών από τελικούς χρήστες και ερευνητές ασφαλείας σχετικά με τρωτά σημεία, παραπομπή σε επιγραμμικά αποθετήρια με καταλόγους δημοσιοποιημένων τρωτών σημείων που συνδέονται με το προϊόν ΤΠΕ, την υπηρεσία ΤΠΕ ή τη διαδικασία ΤΠΕ και σε οποιεσδήποτε συμβουλές σχετικά με την κυβερνοασφάλεια. Η απαίτηση αυτή από τους κατασκευαστές και τους παρόχους είναι εμφανές πως προσβλέπει σε μία ευρύτερη αναβάθμιση στην εσωτερική αγορά τεχνολογικών προϊόντων και υπηρεσιών η οποία πέραν της επίτευξης υψηλού επιπέδου ασφαλείας ταυτόχρονα αναβαθμίζει και την ανταγωνιστικότητα της απέναντι στο παγκόσμιο εμπορικό σύστημα.

Μέσω του Κανονισμού οριοθετούνται εξίσου σε αρχικό πλαίσιο και τα εθνικά συστήματα πιστοποίησης και τα πιστοποιητικά. Τα κράτη-μέλη καλούνται να ορίσουν μία ή περισσότερες εθνικές αρχές πιστοποίησης κυβερνοασφάλειας ενημερώνοντας την Επιτροπή. Οι αρχές αυτές πρέπει να μπορούν να διατηρούν την ανεξαρτησία τους σχετικά με τις οντότητες που καλείται να επιβλέπει σε επίπεδο οργάνωσης, αποφάσεων χρηματοδότησης, νομικής διάρθρωσης και λήψης αποφάσεων. Ακόμη όσες εκδίδουν και πιστοποιητικά πρέπει να διασφαλίζουν διαχωρισμό ανάμεσα στη δραστηριότητα αυτή και τις εποπτικές τους δραστηριότητες.

Τα καθήκοντα των εθνικών αρχών συνοψίζονται ως εξής:
Α. εποπτεύουν και μεριμνούν για την εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας και είναι υπεύθυνες για την παρακολούθηση της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ προς τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας
Β. παρακολουθούν τη συμμόρφωση με τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ
Γ. παρέχουν ενεργό βοήθεια και υποστήριξη στους εθνικούς οργανισμούς διαπίστευσης
Δ. παρακολουθούν και εποπτεύουν τις δραστηριότητες των δημόσιων οργανισμών
Ε. κατά περίπτωση, εξουσιοδοτούν τους οργανισμούς αξιολόγησης της συμμόρφωσης και περιορίζουν, αναστέλλουν ή ανακαλούν υπάρχουσα αδειοδότηση
ΣΤ. διεκπεραιώνουν καταγγελίες από φυσικά ή νομικά πρόσωπα σε σχέση με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή σε σχέση με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης, ή σε σχέση με τις δηλώσεις συμμόρφωσης της Ευρωπαϊκής Ένωσης και διερευνούν το αντικείμενο των εν λόγω καταγγελιών στον βαθμό που ενδείκνυται και ενημερώνουν τον καταγγέλλοντα σχετικά με την πρόοδο και το αποτέλεσμα της έρευνας εντός εύλογου χρονικού διαστήματος
Ζ. εκπονούν ετήσια συνοπτική έκθεση σχετικά με τις δραστηριότητες που διενεργούν
Η. συνεργάζονται με άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή άλλες δημόσιες αρχές, μεταξύ άλλων μέσω της ανταλλαγής πληροφοριών σχετικά με πιθανή μη συμμόρφωση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ
Θ. παρακολουθούν τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της κυβερνοασφάλειας
Οι εξουσίες των εθνικών αρχών πιστοποίησης ορίζονται ως εξής:
Α. ζητούν από τους οργανισμούς αξιολόγησης της συμμόρφωσης, τους κατόχους ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και τους εκδότες δηλώσεων συμμόρφωσης της Ευρωπαϊκής Ένωσης να προσκομίσουν τις πληροφορίες που απαιτούνται για την άσκηση των καθηκόντων τους
Β. διενεργούν έρευνες, υπό μορφή ελέγχων, των οργανισμών αξιολόγησης της συμμόρφωσης, των κατόχων ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των εκδοτών δηλώσεων συμμόρφωσης της Ευρωπαϊκής Ένωσης
Γ. λαμβάνει τα ενδεδειγμένα μέτρα, σύμφωνα με το εθνικό δίκαιο, προκειμένου να διασφαλίζεται η συμμόρφωση των οργανισμών αξιολόγησης της συμμόρφωσης, των κατόχων ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των εκδοτών δηλώσεων συμμόρφωσης της Ευρωπαϊκής Ένωσης
Δ. έχουν πρόσβαση στους χώρους οποιωνδήποτε οργανισμών αξιολόγησης της συμμόρφωσης ή των κατόχων ευρωπαϊκών πιστοποιητικών της κυβερνοασφάλειας, με σκοπό τη διενέργεια ερευνών σύμφωνα με το δικονομικό δίκαιο της Ένωσης ή των κρατών μελών
Ε. ανακαλούν, σύμφωνα με το εθνικό δίκαιο, ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από εθνικές αρχές πιστοποίησης της

κυβερνοασφάλειας ή ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης,
ΣΤ. επιβάλλουν κυρώσεις σε συμφωνία με το εθνικό δίκαιο
Οι εθνικές αρχές πέραν των καθηκόντων και εξουσιών που αναλαμβάνουν τίθενται σε αξιολόγηση από ομότιμους σχετικά με τις δραστηριότητες τους, τον διαχωρισμό αυτών και τις διαδικασίες που ακολουθούν για να εκπληρώσουν τους στόχους τους.
Στο ευρωπαϊκό επίπεδο συστήνεται η Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας (ΕΟΠΙΚ) η οποία απαρτίζεται από αντιπροσώπους των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας ή αντιπροσώπους άλλων σχετικών εθνικών αρχών. Τα καθήκοντα που ανατίθενται στην ΕΟΠΙΚ είναι συμβουλευτικά, επικουρικά και υποστηρικτικά προς την Επιτροπή και τον ENISA.
Όσον αφορά τη δικαστική προστασία η οποία θα διέπει το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας αυτό προβλέπει:
Α. Το δικαίωμα καταγγελίας από φυσικά και νομικά πρόσωπα προς εκδότες ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και προς τις εθνικές αρχές πιστοποίησης,
Β. Το δικαίωμα πραγματικής δικαστικής προσφυγής από φυσικά και νομικά πρόσωπα με αντικείμενο αποφάσεις που λαμβάνονται από τις ανωτέρω αρχές όσον αφορά, κατά περίπτωση, την αντικανονική έκδοση, την παράλειψη έκδοσης ή την αναγνώριση ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας το οποίο έχουν στην κατοχή τους τα εν λόγω φυσικά και νομικά πρόσωπα και την παράλειψη να δοθεί συνέχεια σε καταγγελία που έχει ήδη υποβληθεί.
Αρμόδια για τα δικαιώματα αυτά είναι τα δικαστήρια του κράτους μέλους όπου είναι εγκατεστημένη η αρχή κατά της οποίας ασκείται η δικαστική προσφυγή.
Οι προβλεπόμενες κυρώσεις σχετικά με την τήρηση των κανόνων για το πλαίσιο πιστοποίησης της κυβερνοασφάλειας επαφίονται στα κράτη μέλη και πρέπει να είναι αναλογικές, αποτελεσματικές και αποτρεπτικές.
Με τη θέσπιση των κανόνων του ευρωπαϊκού πλαισίου για την κυβερνοασφάλεια η Ευρωπαϊκή Ένωση γίνεται πιο απρόσβλητη στις κυβερνοεπιθέσεις[119].
Ο αντιπρόεδρος της Επιτροπής και αρμόδιος για την Ψηφιακή Ενιαία Αγορά, κ. Άντρους Άνσιπ, δήλωσε: «Η ψηφιακή ενιαία αγορά της Ευρώπης μπορεί να υλοποιηθεί μόνον εάν περιλαμβάνει ισχυρές δεσμεύσεις για την κυβερνοασφάλεια. Η παρούσα Επιτροπή προώθησε τη διασφάλιση ότι η Ευρώπη διαθέτει τις απαραίτητες ικανότητες προτείνοντας, μεταξύ άλλων, ένα ευρωπαϊκό πλαίσιο πιστοποίησης και χρηματοδοτώντας την έρευνα και την ανάπτυξη στον τομέα της κυβερνοασφάλειας στο πλαίσιο του επόμενου μακροπρόθεσμου προϋπολογισμού της της Ευρωπαϊκής Ένωσης. Οι εργασίες για την ασφάλεια του 5G αποτελούν ιδιαίτερη προτεραιότητα, δεδομένου ότι έχει τη δυνατότητα να επηρεάσει όλες τις πτυχές του μέλλοντος μας.» Η επίτροπος Ψηφιακής Οικονομίας και Κοινωνίας, κ. Μαρίγια Γκαμπριέλ, πρόσθεσε: «Η πράξη της της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια έχει καταδείξει την ανάγκη για μια ενωσιακή προσέγγιση που θα ανταποκρίνεται σε όλες τις προκλήσεις, θα προστατεύει τους πολίτες μας και θα παραμένει ανταγωνιστική. Για την επίτευξη αυτού του στόχου, η Ευρώπη έχει δώσει μόνιμη εντολή στον

[119] Βλ. σχετικές πληροφορίες: Ευρωπαϊκό Συμβούλιο, Διαθέσιμο στο: https://www.consilium.europa.eu/el/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/ (Πρόσβαση 27.11.2019)

Οργανισμό κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης. Η πράξη της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια καθιστά επίσης δυνατή την πιστοποίηση της κυβερνοασφάλειας σε επίπεδο Ευρωπαϊκής Ένωσης. Με την πράξη για την κυβερνοασφάλεια, με την Οδηγία για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων, καθώς και με το προτεινόμενο ευρωπαϊκό κέντρο ικανοτήτων κυβερνοασφάλειας, έχουμε υποβάλει ένα ισχυρό ευρωπαϊκό πρότυπο, το οποίο βασίζεται στις δημοκρατικές μας αξίες και διαφυλάσσει τα συμφέροντα των πολιτών μας.»[120]
Αυτοί που επωφελούνται κατά κύριο λόγο από τη θέσπιση του πλαισίου είναι:
Οι πολίτες και οι τελικοί χρήστες οποίοι θα είναι σε θέση να λαμβάνουν πιο τεκμηριωμένες αποφάσεις αγοράς σχετικά με προϊόντα και υπηρεσίες που βασίζονται σε καθημερινή βάση
Οι πωλητές και οι πάροχοι προϊόντων και υπηρεσιών [συμπεριλαμβανομένων των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ) και των νέων επιχειρήσεων] που θα εξοικονομούν κόστος και χρόνο, καθώς θα υποβάλλονται σε μία και μόνη διαδικασία για την απόκτηση του ευρωπαϊκού πιστοποιητικού, το οποίο ισχύει σε όλα τα κράτη μέλη κι επομένως τους δίνει τη δυνατότητα να αντιμετωπίζουν αποτελεσματικά τον ανταγωνισμό.
Οι κυβερνήσεις, οι οποίες, όπως όλοι οι ιδιώτες και οι εμπορικοί αγοραστές, θα είναι σε καλύτερη θέση για να λαμβάνουν τεκμηριωμένες αποφάσεις αγοράς.
Ειδικότερα όσον αφορά τον ιδιωτικό τομές και τις ΜΜΕ Το πλαίσιο θα συμβάλει στη μείωση των εν λόγω εμποδίων για είσοδο στην αγορά για τις ΜΜΕ και τις νέες επιχειρήσεις, διότι οι εταιρείες θα πρέπει να υποβληθούν στη διαδικασία πιστοποίησης των προϊόντων τους μόνο μία φορά και το αντίστοιχο πιστοποιητικό θα ισχύει σε ολόκληρη την Ευρωπαϊκή Ένωση. Επιπλέον, δεδομένου ότι η ζήτηση για ασφαλέστερες λύσεις αναμένεται να αυξηθεί σε παγκόσμιο επίπεδο, οι εταιρείες, συμπεριλαμβανομένων των ΜΜΕ, των οποίων τα προϊόντα πιστοποιούνται, θα διαθέτουν ανταγωνιστικό πλεονέκτημα στην αγορά για την ικανοποίηση της ανάγκης αυτής. Επίσης, η δυνατότητα των εταιρειών να βεβαιώνουν οι ίδιες τη συμμόρφωση με τις απαιτήσεις ασφάλειας για τα προϊόντα, τις διαδικασίες και τις υπηρεσίες που παρουσιάζουν χαμηλό κίνδυνο καθιστά το πλαίσιο ακόμη πιο ελκυστικό για τις ΜΜΕ και τις νέες επιχειρήσεις [121].
Ο νέος Κανονισμός πέραν του γεγονότος πως θέτει την κυβερνοασφάλεια σε μείζονα τομέα δράσης της Ένωσης οριοθετεί νομικά και στρατηγικά τις πολιτικές που πρέπει να ακολουθήσουν τα κράτη μέλη θέτοντας ως σημαντικότερο στόχο την προστασία των ευρωπαίων πολιτών και επιχειρήσεων. Η σύνδεση της κυβερνοασφάλειας με την ανταγωνιστικότητα και συνοχή της ενιαίας αγοράς είναι πλέον καταφανής και η Ένωση εμφανίζεται ως προστάτιδα δύναμη των κεκτημένων της.

3.4.4 Απόφαση (ΕΕ) 299/19 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της

[120] Βλ. σχετικές πληροφορίες: Η πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο εισάγει νέους ενωσιακούς κανόνες για την πιστοποίηση της κυβερνοασφάλειας Διαθέσιμο στο: https://ec.europa.eu/greece/news/20190626_3_el_el (Πρόσβαση 27.11.2019)
[121] https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-stin-eyropaiki-enosi-hrisimes-plirofories-me-aformi-ti-nea-praxi-gia-tin (Πρόσβαση 20.11.2019)

Στο πλαίσιο της προσπάθειας για τη θεμελίωση μία συντονισμένης και από κοινού στρατηγικής κυβερνοασφάλειας για την Ένωση, το Συμβούλιο προέβη στην έκδοση Απόφασης σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της. Η βασική κατεύθυνση με την οποία το Συμβούλιο κατέληξε σε αυτή την Απόφαση, έγκειται στη διαπίστωση πως η σαφής ενημέρωση σχετικά με τις πιθανές συνέπειες μιας κοινής διπλωματικής αντίδρασης της Ένωσης στις κακόβουλες δραστηριότητες στον κυβερνοχώρο επηρεάζει τη συμπεριφορά των εν δυνάμει δραστών του κυβερνοχώρου, πράγμα που ενισχύει την ασφάλεια της Ένωσης και των κρατών μελών της. Με την απόφαση αυτή σκιαγραφείται να πλαίσιο κοινής διπλωματικής αντίδρασης της Ένωσης έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.
Πιο συγκεκριμένα με την εν λόγω απόφαση θεσπίζει ένα πλαίσιο στοχευμένων περιοριστικών μέτρων για την αποτροπή και την αντιμετώπιση κυβερνοεπιθέσεων με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για την Ευρωπαϊκή Ένωση ή τα κράτη μέλη της. Ακόμη, τα μέτρα αυτά συνδέονται άμεσα με την Κοινή Εξωτερική Πολιτική Ασφάλειας και Άμυνας καθώς δεν αποκλείεται η εφαρμογή των μέτρων αυτών ως απόκριση σε κυβερνοεπιθέσεις με σημαντικό αντίκτυπο κατά τρίτων χωρών ή διεθνών οργανισμών.
Με την Απόφαση αυτή προσδιορίζονται με σαφή τρόπο η έννοια του σημαντικού αντίκτυπου των κυβερνοεπιθέσεων και τα γνωρίσματα τα οποία πρέπει να συγκεντρώνει μία κυβερνοεπίθεση ώστε να εφαρμοστούν τα περιοριστικά μέτρα[122].
Πρώτον, η σημαντικότητα του αντίκτυπου καθορίζεται[123] από τη σοβαρότητα της διαταραχής που προκλήθηκες σε διάφορα επίπεδα κρατικών λειτουργιών ζωτικής σημασίας, από τον αριθμό των θιγόμενων νομικών και φυσικών προσώπων, τον αριθμό των κρατών που επηρεάστηκα, το ύψος της οικονομικής ζημιάς των προσβαλλόμενων και του οφέλους του επιτιθέμενου αντίστοιχα και τέλος από την ποσότητα και τη φύση των δεδομένων που κλάπηκαν ή/και παραβιάστηκαν.
Δεύτερον, η κυβερνοεπίθεση θα πρέπει να προέρχεται από το εξωτερικό της Ένωσης και να επιτίθεται στις υποδομές της. Ακόμη στην ίδια κατηγορία ανήκει και μία κυβερνοεπίθεση η οποία πλήττει κράτος μέλος της ένωσης προσβάλοντας υποδομές ζωτικής σημασίας, υπηρεσίες που είναι απαραίτητες για τη διατήρηση ουσιωδών κοινωνικών ή/και οικονομικών δραστηριοτήτων, κρατικές λειτουργίες ζωτικής σημασίας.
Στην περίπτωση που πληρούνται οι ανωτέρω προϋποθέσεις, τα κράτη μέλη καλούνται να λάβουν τα ακόλουθα στοχευμένα μέτρα:
Α. μέτρα που είναι αναγκαία ώστε να απαγορευθεί η είσοδος στο έδαφός τους ή η διέλευση μέσω αυτού φυσικών προσώπων που είναι υπεύθυνα ή χρηματοδοτούν ή υποστηρίζουν με κάθε τρόπο περιστατικά κυβερνοεπιθέσεων[124]

Β. μέτρα που είναι αναγκαία για τη δέσμευση όλων των κεφαλαίων και των οικονομικών πόρων που βρίσκονται υπό την ιδιοκτησία, την κατοχή ή τον έλεγχο

[122] ΕΕ L, 129I, ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2019/797 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της, σελ. 14
[123] ΕΕ L, 129I, ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2019/797 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της, σελ. 15
[124] ΕΕ L, 129I, ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2019/797 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της, σελ. 15

φυσικών και νομικών προσώπων, οντοτήτων ή και φορέων που είναι υπεύθυνα ή χρηματοδοτούν ή υποστηρίζουν με κάθε τρόπο περιστατικά κυβερνοεπιθέσεων[125]

Με την απόφαση αυτή παρατηρείται για πρώτη φορά η αποτρεπτική δράση της Ένωσης στην αντιμετώπιση των κυβερνοαπειλών. Τα περιοριστικά μέτρα προσδίδουν στην Ενωσιακή στρατηγική κυβερνοασφάλειας το μέσο της αποτροπής δεδομένου πως μέχρι στιγμής ο προσανατολισμός της Ένωσης ήταν κατά κύριο λόγο προληπτικός.

[125] ΕΕ L, 129Ι, ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2019/797 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της, σελ. 16

3.5 Διεθνείς συνεργασίες της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια

Η Ευρωπαϊκή Ένωση έχει υπάρξει κοινωνός και ένθερμος υποστηρικτής της διεθνούς συνεργασίας σε τομείς παγκόσμιου ενδιαφέροντος καθιστώντας σαφές με κάθε ευκαιρία πως η από κοινού δράση απέναντι σε κοινές και μη αποφευκτές απειλές αποτελεί τη βέλτιστη πρακτική. Δεδομένου του διασυνοριακού και πολύπλευρου χαρακτήρα των κυβερνοεπιθέσεων, η Ένωση θεωρεί ζωτικής σημασίας την προώθηση της συνεργασίας με άλλους διεθνείς δρώντες με σκοπό τη θωράκιση των πληροφοριακών συστημάτων και τη μείωση -όσο το δυνατόν μεγαλύτερη- των οικονομικά ζημιογόνων συνεπειών.

Σε αυτή την κατεύθυνση η Ένωση προωθεί και υποστηρίζει προσπάθειες προς μία διεθνή σύμπλευση απέναντι στις κυβερνοαπειλές. Η αρχή αυτή οδήγησε τα κράτη μέλη τον Ιούνιο του 2019 να αναθέσουν στην Επιτροπή δύο εντολές συμμετοχής σε διεθνείς διαπραγματεύσεις για τη βελτίωση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία στο πλαίσιο ποινικών ερευνών. Υπό το ίδιο πρίσμα το Συμβούλιο συμφώνησε να αναθέσει στην Επιτροπή εντολές διαπραγμάτευσης με τις Ηνωμένες Πολιτείες και για το δεύτερο πρόσθετο πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, της λεγόμενης «Σύμβασης της Βουδαπέστης»[126].

Οι σχετικές δηλώσεις ευρωπαίων επιτρόπων έχουν ιδιαίτερη σημασία καθώς καταδεικνύουν την ισχυρή πολιτική βούληση για στενότερη συνεργασία στα θέματα της κυβερνοασφάλειας.

Ο επίτροπος Μετανάστευσης, Εσωτερικών Υποθέσεων και Ιθαγένειας κ. Δημήτρης Αβραμόπουλος δήλωσε σχετικά: «Οι εγκληματίες λειτουργούν σε διασυνοριακό επίπεδο και τα αποδεικτικά στοιχεία που χρειαζόμαστε για να διερευνήσουμε τα εγκλήματά τους βρίσκονται συχνά σε άλλες δικαιοδοσίες. Οι αρχές επιβολής του νόμου πρέπει να έχουν τη δυνατότητα να αποκτούν γρήγορα πρόσβαση στα εν λόγω αποδεικτικά στοιχεία. Από σήμερα μπορούμε να εργαστούμε για τη διαπραγμάτευση αυτών των πλαισίων με τις Ηνωμένες Πολιτείες και το Συμβούλιο της Ευρώπης».

Ο Τζούλιαν Κινγκ, επίτροπος αρμόδιος για την Ένωση Ασφάλειας, δήλωσε: «Οι εγκληματίες και οι τρομοκράτες αξιοποιούν εδώ και πολύ καιρό τη σύγχρονη τεχνολογία για να διαπράττουν τα εγκλήματά τους. Με τη θέσπιση διεθνών προτύπων για την απόκτηση πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία, κάνουμε ένα ακόμη βήμα για να συρρικνώσουμε το πεδίο δράσης τους, εξασφαλίζοντας ότι οι αρχές επιβολής του νόμου μπορούν να διεξάγουν αποτελεσματικότερες έρευνες και να τους διώκουν αποτελεσματικότερα, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων».

Πέραν αυτού του ιδιαίτερα ελπιδοφόρου βήματος για μία αποτελεσματικότερη διεθνή συνεργασία η Ευρωπαϊκή Ένωση διατηρεί και προάγει συνεργασία με το

[126] Βλ. σχετικές πληροφορίες: Ένωση Ασφάλειας: Η Επιτροπή λαμβάνει εντολή για την έναρξη διαπραγματεύσεων με αντικείμενο διεθνείς κανόνες λήψης ηλεκτρονικών αποδεικτικών στοιχείων, Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/IP_19_2891 (Πρόσβαση 29.11.2019)

ΝΑΤΟ στο πλαίσιο της άμυνας συμπεριλαμβανομένης και της κυβερνοασφάλειας.

Η Ευρωπαϊκή Ένωση και το ΝΑΤΟ (North Atlantic Treaty Alliance – Οργανισμός Βορειοατλαντικού Συμφώνου) διατηρούν συνεργασία στον τομέα της άμυνας και της ασφάλειας, παραπάνω από δεκαπέντε χρόνια [127]. Η συνεργασία τους ξεκίνησε να διαφαίνεται ήδη από τη ψυχροπολεμική περίοδο με τη μορφή της Δυτικής Ευρωπαϊκής Ένωσης (ΔΕΕ). Η πρωταρχική βάση τέθηκε το 1992 με τη Συνθήκη του Μάαστριχτ η οποία εισήγαγε την Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας η οποία λίγα χρόνια αργότερα υποστηρίχθηκε από το ΝΑΤΟ κατά την σύνοδο των Υπουργών Αμύνης των μελών της συμμαχίας[128]. Το πρώτο όμως παράδειγμα πραγματικής συνεργασίας δεν επετεύχθη πριν τον Φεβρουάριο του 2001, στο αποκορύφωμα του ενδο-εθνικού αλληλοσπαραγμού μεταξύ των δυνάμεων ασφαλείας του κράτους και ενόπλων Αλβανών ανταρτών, όπου το ΝΑΤΟ και η Ευρωπαϊκή Ένωση συντόνισαν τις διαπραγματεύσεις που οδήγησαν στην Συμφωνία της Οχρίδας τον Αύγουστο του ιδίου χρόνου [129]. Η συνεργασία τους επεκτάθηκε περαιτέρω το 2003 με την υπογραφή της συμφωνίας Berlin Plus[130] με την οποία η Ένωση απέκτησε τη δυνατότητα να χρησιμοποίει τις δυνάμεις του ΝΑΤΟ όταν αυτό κρίνεται απαραίτητο. Η υλοποίηση της συμφωνίας έλαβε χώρα με επιτυχία στις περιπτώσεις της Βόρειας Δημοκρατίας της Μακεδονίας και της Βόσνιας όπου η Ένωση ανέλαβε τις επιχειρήσεις διατηρώντας τις διοικητικές δομές του ΝΑΤΟ.

Η συνεργασία τους συνεχίστηκε με τακτικές συναντήσεις αξιωματούχων και των δύο πλευρών κατά τις οποίες προωθούταν η κοινή κατεύθυνση των δύο μερών προς την πρόληψη κρίσεων και τη θωράκιση της ασφάλειας περιοχών που διέτρεχαν κίνδυνο. Στην πορεία, η ραγδαία κλιμάκωση διασυνοριακών απειλών κατέδειξε την αναγκαιότητα για μία στενότερη και σε πλέον σταθερότερη βάση συνεργασία. Η συνεργασία της Ένωσης με τον Οργανισμό για την καταπολέμηση των κυβερνοαπειλών έχει ως ορόσημο το 2010, μέσω ανεπίσημων συναντήσεων και διαβουλεύσεων υψηλού επιπέδου μεταξύ στελεχών και προσωπικού που εξακολουθούν να διεξάγονται ετησίως. Ένα χρόνο αργότερα, μετά τη δημιουργία της ομάδας αντιμετώπισης έκτακτων περιστατικών (CERT-EU), η ικανότητα αντιμετώπισης περιστατικών πληροφορικής του ΝΑΤΟ (NCIRC) και η CERT-EU δημιούργησαν συνεργασία στην οποία συμμετείχαν και άλλες υπηρεσίες της ΕΕ και του ΝΑΤΟ. Πιο συγκεκριμένα, η CCDCOE (Cooperative Cyber Defense Centre of Excellence) του N.A.T.O. καθιέρωσε μια σύνδεση με τον Ευρωπαϊκό Οργανισμό Άμυνας με στόχο την ανταλλαγή πληροφοριών σχετικά με κοινά

[127] Κοινή Δήλωση Ε.Ε.-ΝΑΤΟ, 2016, https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

[128] Βλ. σχετικές πληροφορίες: Declaration of the Heads of State and Government, Διαθέσιμο στο: https://www.nato.int/cps/en/natohq/official_texts_24470.htm?mode=pressrelease (Πρόσβαση 30.11.2019)

[129] Βλ. σχετικές πληροφορίες: ΝΑΤΟ και Ευρωπαϊκή Ένωση: Συνεργασία και ασφάλεια, Διαθέσιμο στο: https://www.nato.int/docu/review/2007/issue2/Greek/art6.html (Πρόσβαση 30.11.2019)

[130] Βλ. σχετικές πληροφορίες: Shaping of a Common Security and Defence Policy, Διαθέσιμο στο: https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5388/shaping-of-a-common-security-and-defence-policy-_en (Πρόσβαση 30.11.2019)

θέματα. Ωστόσο, μόνο τα τελευταία δύο χρόνια η συνεργασία μεταξύ της Ευρωπαϊκής Ένωσης και του ΝΑΤΟ για την ασφάλεια στον κυβερνοχώρο απέκτησε πιο συγκεκριμένη μορφή.

Το Φεβρουάριο του 2016 τα δύο μέρη υπέγραψαν τεχνική συμφωνία[131] για την άμυνα στον κυβερνοχώρο και για τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ της CERT-EU και του NCIRC, προκειμένου να υπάρξει ένα αναβαθμισμένο πλαίσιο βελτίωσης των προηγμένων διαδικασιών πρόληψης, ανίχνευσης και απόκρισης σε περιστατικά κυβερνοεπιθέσεων. Η συμφωνία υπογράφηκε στα κεντρικά γραφεία του ΝΑΤΟ στις Βρυξέλλες , πριν από την ετήσια συνάντηση των υπουργών Άμυνας του ΝΑΤΟ, από τον επικεφαλής της CERT-EU Freddy Dezeure και τον επικεφαλής του NCIRC Ian West, παρουσία του Αναπληρωτή Γενικού Γραμματέα της. Η συμφωνία θεωρήθηκε σημαντικό βήμα στη συνεργασία ΕΕ-ΝΑΤΟ, καθώς έθεσε τα θεμέλια για την περαιτέρω διεύρυνση της.

Πράγματι το επιστέγασμα της συμφωνίας επήλθε με την Κοινή Δήλωση ΝΑΤΟ-ΕΕ[132] η οποία υπογράφηκε από τον Πρόεδρο του Ευρωπαϊκού Συμβουλίου κ. Donald Tusk, τον Πρόεδρο της Ευρωπαϊκής Επιτροπής κ. Jean-Claude Juncker και τον Γενικό Γραμματέα του ΝΑΤΟ Jens Stoltenberg στη Σύνοδο Κορυφής της Βαρσοβίας τον Ιούλιο του 2016. Υπάλληλοι και των δύο οργανώσεων συναντήθηκαν και πάλι τον Νοέμβριο του 2016[133] με σκοπό την ενίσχυση της συνεργασίας και την προπαρασκευή επικείμενων πρακτικών βημάτων. Στη συνάντηση τέθηκαν επί τάπητος οι πρόσφατες επικαιροποιήσεις και εξελίξεις των δύο οργανισμών, όπως π.χ. η εφαρμογή της Οδηγίας της Ευρωπαϊκής Ένωσης σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών του 2016 και η υιοθέτηση της κυβερνητικής άμυνας του ΝΑΤΟ. Συμφωνήθηκε η προώθηση της συνεργασίας κυρίως στους τομείς της ανταλλαγής πληροφοριών και του συντονισμού των προσπαθειών για την αποτελεσματικότερη αντιμετώπιση των απειλών στον κυβερνοχώρο.

Τόσο ο Αναπληρωτής Γενικός Γραμματέας της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης όσο και ο Βοηθός Γενικός Γραμματέας του ΝΑΤΟ για τις Αναδυόμενες Προκλήσεις για την Ασφάλεια τόνισαν τη σημασία να καταστεί η συνεργασία πιο συνεκτική και ανθεκτική όσον αφορά την ασφάλεια στον κυβερνοχώρο.

Το Δεκέμβριο του ίδιου έτους κατά τη συνεδρίαση των υπουργών εξωτερικών της Βρυξελλών η Συμμαχία, η Ύπατη Εκπρόσωπος της Ευρωπαϊκής Ένωσης Federica Mogherini και ο Γραμματέας του ΝΑΤΟ Jens Stoltenberg παρουσίασαν τις προτάσεις τους για την ενδυνάμωση της συμφωνίας. Με κατεύθυνση την οικοδόμηση μίας νέας εποχής για τη συνεργασία των δύο μερών,

[131] Βλ. σχετικές πληροφορίες: NATO and EU press ahead with cooperation on cyber defence, Διαθέσιμο στο: https://eeas.europa.eu/headquarters/headquarters-homepage/15917/nato-and-eu-press-ahead-with-cooperation-on-cyber-defence_en (Πρόσβαση 30.11.2019)
[132] Κοινή Δήλωση ΕΕ-ΝΑΤΟ 2016, https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf (Πρόσβαση 30.11.2019)
[133] Βλ. 131

παρουσιάστηκαν σαράντα δύο προτάσεις[134]. Αφότου υπέγραψαν δεσμεύτηκαν, αφενός η Ύπατη εκπρόσωπος να ενημερώνει τακτικά τα κράτη μέλη και αφετέρου ο Γραμματέας τους συμμάχους σχετικά με την πρόοδο των συμφωνηθέντων με την πρόθεση το πρόγραμμα να υλοποιηθεί το συντομότερο δυνατόν.

Οι σαράντα δυο προτάσεις διαχωρίζονται σε επτά υποενότητες οι οποίες αποσαφηνίζονται στην Κοινή Δήλωση:

1. Αντιμετώπιση των υβριδικών απειλών.

2. Επιχειρησιακή συνεργασία συμπεριλαμβανομένων των ναυτιλιακών θεμάτων.

3. Ασφάλεια και άμυνα στον κυβερνοχώρο ·

4. Δυνατότητες άμυνας ·

5. Βιομηχανία και έρευνα στον τομέα της άμυνας ·

6. Παράλληλες και συντονισμένες ασκήσεις.

7. Δημιουργία ικανοτήτων για την άμυνα και την ασφάλεια.

Ο τομέας της άμυνας και της ασφάλειας στον κυβερνοχώρο αποτελεί προτεραιότητα της συνεργασίας ανάμεσα στην Ένωση και στο NATO[135], δεδομένης της αμοιβαίας αναγνώρισης του ως νέου πεδίου διεξαγωγής πολέμου. Προτείνεται η άμεση θεμελίωση του συστήματος ανταλλαγής πληροφοριών σχετικά με τον προγραμματισμό της κυβερνοαμυντικής στρατηγικής. Οι προτάσεις τονίζουν την ανάγκη διασφάλισης της διαλειτουργικότητας μεταξύ των επιχειρησιακών εργαλείων και των κλασικών απαιτήσεων και πρότυπων. Προβλέπεται ακόμη η δημιουργία προτύπων σχετικά με την κατάρτιση στον κυβερνοχώρο, με σκοπό την εναρμόνιση του γνωσιακού επιπέδου του προσωπικού και των δύο μερών. Το Κέντρο Αριστείας του NATO, ανέλαβε να καθορίσει συγκεκριμένους τομείς οι οποίοι χρειάζεται να αναδιαρθρωθούν. Τέλος για πρώτη φορά διατυπώθηκε η θέληση για ενίσχυση της συνεργασίας μέσω συντονισμένων ασκήσεων.

Η Κοινή Δήλωση επισφραγίστηκε με εκ νέου Κοινή Δήλωση η οποία υπογράφηκε στις 10 Ιουλίου 2018[136] από τον Πρόεδρο του Ευρωπαϊκού Συμβουλίου κ. Donald Tusk, τον Πρόεδρο της Ευρωπαϊκής Επιτροπής κ. Jean-Claude Juncker και τον Γενικό Γραμματέα του NATO Jens Stoltenberg. Στη δήλωση επαναλαμβάνονται οι τομείς προτεραιότητας ενώ τονίζεται πως μέσω της μέχρι τώρα εξέλιξης της συνεργασίας αυξήθηκε αμφίδρομα η ικανότητά ανταπόκρισης σε υβριδικές απειλές μέσω της ενίσχυσης των δυνατοτήτων αντιμετώπισης κρίσεων συμπεριλαμβανομένων των κυβερνοεπιθέσεων, της έγκαιρης ανταλλαγής πληροφοριών, της διεξαγωγής ασκήσεων και της αντιμετώπισης της

[134] Συμβούλιο της ΕΕ, 2016, 15283/16, http://www.europarl.europa.eu/cmsdata/121581/ST_15283_2016_INIT_EN.pdf (Πρόσβαση 30.11.2019)
[135] Βλ. 134
[136] Κοινή Δήλωση ΕΕ-NATO 2018, https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf (Πρόσβαση 30.11.2019)

παραπληροφόρησης, επιτυγχάνοντας έτσι το συντονισμό των μελών και εταίρων. Τέλος διαμηνύεται για μία ακόμη φορά πως ο πρωταρχικός σκοπός της συνεργασίας είναι η αντιμετώπιση των απειλών που αντιμετωπίζουν μέλη και εταίροι στο κυβερνοχώρο και πως η δήλωση αποτελεί δέσμευση για εμβάθυνση της συνεργασίας στη βάση των ήδη συμφωνηθεισών προτάσεων.

3.6 Ενωσιακές πολιτικές για την κυβερνοασφάλεια

3.6.1 Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο - Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών (2013)

Ακρογωνιαίος λίθος της πολιτικής της Ένωσης αποτελεί η Στρατηγική για την ασφάλεια στον κυβερνοχώρο του 2013[137].

Η Ανακοίνωση σχετικά με τη Στρατηγική για την ασφάλεια στον κυβερνοχώρο θέτει τις βασικές αρχές της Ευρωπαϊκής Ένωσης στον ψηφιακό κόσμο συνδέοντας τους με αυτούς του πραγματικού κόσμου συνοψίζονται ως εξής:

1. Προστασία των θεμελιωδών δικαιωμάτων, της ελευθερίας της έκφρασης, των προσωπικών δεδομένων και της ιδιωτικότητας
2. Προσβασιμότητα για όλους
3. Δημοκρατική και αποτελεσματική πολυμερής διακυβέρνηση
4. Συναρμοδιότητα για να κατοχυρωθεί η ασφάλεια[138]

Η Στρατηγική διακρίνεται σε πέντε βασικές προτεραιότητες βραχυπρόθεσμες και μακροπρόθεσμες οι οποίες περιλαμβάνουν ποικιλία εργαλείων πολιτικής και αφορούν φορείς διαφόρων τύπων, ανεξάρτητα αν είναι θεσμικά όργανα της Ευρωπαϊκής Ένωσης, κράτη μέλη ή επιχειρήσεις.

Α. Επίτευξη ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο

Οι δημόσιες αρχές όσο και ο ιδιωτικός τομέας καλούνται να αναπτύξουν ικανότητες και να συνεργαστούν αποτελεσματικά. Παρά τις εθελοντικές δεσμεύσεις και την όποια πρόοδο αυτές έχουν επιφέρει αναγνωρίζεται πως υφίστανται ακόμη κενά ανά την ΕΕ, ιδίως όσον αφορά τις εθνικές ικανότητες, τον συντονισμό σε περιπτώσεις συμβάντων διασυνοριακής διάστασης και όσον αφορά την συμμετοχή και την ετοιμότητα ου ιδιωτικού τομέα. Γι' αυτό το λόγο προτείνεται να καθιερωθούν κοινές ελάχιστες απαιτήσεις για την ασφάλεια δικτύων και πληροφοριών σε εθνικό επίπεδο, ώστε τα κράτη μέλη να υποχρεωθούν στη συγκρότηση καλά οργανωμένων ομάδων έκτακτης ανάγκης

[137] JOIN/2013/1, κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκη Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο

[138] Όλοι οι συναφείς φορείς, ήτοι οι δημόσιες αρχές, ο ιδιωτικός τομέας ή οι μεμονωμένοι πολίτες, πρέπει να αναγνωρίσουν αυτήν την συνυπευθυνότητα, να αναλάβουν δράση για να αυτοπροστατευθούν και εάν χρειαστεί να εξασφαλίσουν συντονισμένη αντίδραση για ενίσχυση της ασφάλειας του κυβερνοχώρου.

θεσπίζοντας εθνικές στρατηγικές, στο πλαίσιο μηχανισμών συντονισμένης πρόληψης, ανίχνευσης, άμβλυνσης των επιπτώσεων και επέμβασης, που να επιτρέπουν την ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή των εθνικών αρμόδιων αρχών ασφάλειας δικτύων και πληροφοριών. Έμφαση δίνεται και στην ενεργοποίηση του ιδιωτικού τομέα προς αυτή την κατεύθυνση.

Οι κατευθυντήριες γραμμές και η υποβοήθηση για την επίτευξη του ανωτέρω στόχου θα δίνονται από τον ENISA ώστε κράτη μέλη να αναπτύξουν ισχυρές εθνικές ικανότητες ανθεκτικότητας όσον αφορά την ασφάλεια του κυβερνοχώρου, ιδίως με την ανάπτυξη εμπειρογνωμοσύνης στην ασφάλεια και την ανθεκτικότητα βιομηχανικών συστημάτων ελέγχου, και υποδομών μεταφορών και ενέργειας.

Τέλος, τονίζεται πως η ευθύνη για την ασφάλεια στον κυβερνοχώρο είναι κοινή και επομένως η ευαισθητοποίηση των τελικών χρηστών απαραίτητη μέσω δημόσιων εκθέσεων, διοργάνωσης συναντήσεων εργασίας εμπειρογνωμόνων και μέσω σύστασης συμπράξεων δημόσιου-ιδιωτικού τομέα[139].

Β. Δραστική μείωση του ηλεκτρονικού εγκλήματος

Τονίζεται πως το ηλεκτρονικό έγκλημα δεν διαθέτει σύνορα και ως εκ τούτου αποτελεί μια από τις ταχύτερα αναπτυσσόμενες μορφές εγκλήματος, με θύματα σε παγκόσμιο επίπεδο που ξεπερνούν το ένα εκατομμύριο άτομα ημερησίως. Ο κυριότερος τρόπος αντιμετώπισης του ηλεκτρονικού εγκλήματος λόγω της χαώδους φύσης του είναι η επιβολή ισχυρής και αποτελεσματικής νομοθεσίας μέσω της παρότρυνσης των κρατών-μελών να κυρώσουν τη Σύμβαση της Βουδαπέστης και της ταχείας ενσωμάτωσης στα εθνικά δίκαια των πράξεων που αφορούν την καταπολέμηση του ηλεκτρονικού εγκλήματος.

Ακόμη, προτείνεται η ανάπτυξη χρηματοδοτικών προγραμμάτων ώστε η Επιτροπή να στηρίξει τα κράτη-μέλη να εντοπίσουν κενά και να ενισχύσουν τις ικανότητές τους όσον αφορά την διερεύνηση και την καταπολέμηση του ηλεκτρονικού εγκλήματος.

Συνεργαζόμενοι φορείς για την προώθηση του ανωτέρω στόχου θα είναι: η Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL), η Europol και η Eurojust.

Γ. Επεξεργασία πολιτικής και ανάπτυξη ικανοτήτων για την άμυνα στον κυβερνοχώρο σε σχέση με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)

Η διάσταση της άμυνας συμπεριλαμβάνεται στον τομέα της ασφάλειας στον κυβερνοχώρο προκειμένου ενισχυθεί η ανθεκτικότητα των συστημάτων επικοινωνιών και πληροφοριών που υποστηρίζουν τα αμυντικά και εθνικά συμφέροντα των κρατών μελών.

Η Ύπατη εκπρόσωπος σε συνεργασία με τα κράτη μέλη και τον Ευρωπαϊκό Οργανισμό Άμυνας καλούνται να διαμορφώσουν του ενωσιακό πλαισίου

[139] Τον Οκτώβριο του 2012, ο ENISA και ορισμένα κράτη μέλη έθεσαν σε δοκιμαστική εφαρμογή την «Πανευρωπαϊκή Εβδομάδα Ασφάλειας στην Κυβερνοχώρο». Η ευαισθητοποίηση είναι ένας από τους τομείς που θα προωθήσει η ομάδα εργασίας ΕΕ-ΗΠΑ για την ασφάλεια στον κυβερνοχώρο και το ηλεκτρονικό έγκλημα και είναι επίσης ζωτικής σημασίας στο πλαίσιο του προγράμματος για ασφαλέστερη χρήση του διαδικτύου (που εστιάζεται στην ασφάλεια των παιδιών στο διαδίκτυο).

πολιτικής της άμυνας στον κυβερνοχώρο για την προστασία δικτύων στο πλαίσιο των αποστολών της ΚΠΑΑ, να προωθήσουν το διάλογο και το συντονισμό μεταξύ πολιτικών και στρατιωτικών φορέων στην ΕΕ και να παροτρύνουν το διάλογο με διεθνείς εταίρους, συμπεριλαμβανομένου του ΝΑΤΟ, άλλους διεθνείς οργανισμούς και διεθνή κέντρα αριστείας.

Δ. Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο

Γίνεται σαφές πως για την επίτευξη του επιθυμητού επιπέδου ασφαλείας είναι κρίσιμη η συνεργασία όλων των φορέων (δημόσιων και ιδιωτικών), οι οποίοι συμμετέχουν στην αξιακή αλυσίδα προϊόντων ΤΠΕ. Προτείνεται η επιβολή κατάλληλων απαιτήσεων ως προς τις επιδόσεις των ανωτέρω στο επίπεδο της κυβερνοασφάλειας λαμβάνοντας υπόψιν παράλληλα την αύξηση της παραγωγικότητας και ανταγωνιστικότητάς τους. Βασικός σκοπός αυτής της προτεραιότητας είναι η τόνωση της πανευρωπαϊκής ζήτησης της αγοράς για εξαιρετικά ασφαλή προϊόντα στη βάση της δημιουργίας κινήτρων για την κατάλληλη διαχείριση του κινδύνου και την θέσπιση προτύπων και λύσεων ασφάλειας, καθώς και για την ενδεχόμενη δημιουργία εθελοντικών πανενωσιακών προγραμμάτων πιστοποίησης που θα αξιοποιούν υφιστάμενα προγράμματα στην ΕΕ αλλά και διεθνώς.

Η Ευρωπαϊκή Επιτροπή θα στηρίξει τα εθελοντικά προγράμματα πιστοποίησης στον τομέα του υπολογιστικού νέφους[140] αξιοποιώντας τις εν εξελίξει εργασίες τυποποίησης των ευρωπαϊκών οργανισμών τυποποίησης (CEN, CENELEC και ETSI), της Ομάδας συντονισμού για την ασφάλεια του κυβερνοχώρου (CSCG), καθώς και της εμπειρογνωμοσύνης του ENISA. Ο ENISA καλείται Να αναπτύξει, σε συνεργασία με τις συναφείς αρμόδιες εθνικές αρχές, τους ενδιαφερόμενους φορείς, τους διεθνείς και ευρωπαϊκούς οργανισμούς τυποποίησης και το Κοινό Κέντρο Ερευνών της Ευρωπαϊκής Επιτροπής, τεχνικές κατευθυντήριες γραμμές και συστάσεις για την θέσπιση προτύπων ΑΔΠ και καλών πρακτικών στον δημόσιο και τον ιδιωτικό τομέα.

Ε. Θέσπιση συνεκτικής διεθνούς πολιτικής κυβερνοχώρου για την Ευρωπαϊκή Ένωση και προώθηση των βασικών αξιών της Ευρωπαϊκής Ένωσης

[140] Υπολογιστικό Νέφος ονομάζεται η κατ' αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων (όπως δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία, ελάχιστη προσπάθεια από τον χρήστη και υψηλή αυτοματοποίηση.
Στο Υπολογιστικό Νέφος η αποθήκευση, η επεξεργασία και η χρήση δεδομένων, λογισμικού και υπηρεσιών γίνεται διαδικτυακά, μέσω απομακρυσμένων υπολογιστών σε κεντρικά Datacenter. Υπηρεσίες όπως η κατ' αίτηση παροχή εικονικών μηχανών, το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα συχνά βασίζονται στην τεχνολογία του Υπολογιστικού Νέφους.
Οι χρήστες εξοικονομούν πόρους από την αγορά και συντήρηση λογισμικού, τη συντήρηση ακριβών εξυπηρετητών και εγκαταστάσεων αποθήκευσης δεδομένων. Το SaaS (Software as a Service) αποτελεί μια από τις εκδοχές του Υπολογιστικού Νέφους και αναφέρεται σε Λογισμικό που προσφέρεται διαδικτυακά ως Υπηρεσία στο Νέφος. Διαθέσιμο στο: http://www.epset.gr/el/content/ypologistiko-nefos-cloud-computing (Πρόσβαση 27.11.2019)

Η Ευρωπαϊκή Ένωση θα εργαστεί προς την κατεύθυνση κάλυψης του ψηφιακού χάσματος και θα συμμετάσχει ενεργά στις διεθνείς προσπάθειες δημιουργίας ικανότητας ασφάλειας στον κυβερνοχώρο. Η διεθνής δέσμευση σε θέματα κυβερνοχώρου θα στηριχθεί στις θεμελιώδεις αξίες της για ανθρώπινη αξιοπρέπεια, ελευθερία, δημοκρατία, ισότητα, κράτος δικαίου και σεβασμό των θεμελιωδών δικαιωμάτων.

Η Επιτροπή, η Ύπατη Εκπρόσωπος και τα κράτη μέλη θα διαμορφώσουν μια συνεκτική διεθνή πολιτική της ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ για τον κυβερνοχώρο. Πιο συγκεκριμένα θα προωθηθεί ο διάλογος με τρίτες χώρες και θα επιδιωχθεί στενότερη συνεργασία με φορείς που ασκούν δραστηριότητα στον τομέα της κυβερνοασφάλειας, όπως το Συμβούλιο της Ευρώπης, ο ΟΟΣΑ, τα Ηνωμένα Έθνη, ο ΟΑΣΕ, το ΝΑΤΟ, η Αφρικανική Ένωση, η Ένωση κρατών της νοτιοανατολικής Ασίας (ASEAN) και ο Οργανισμός Αμερικανικών Κρατών (OAS). Σε διμερές επίπεδο, η συνεργασία με τις Ηνωμένες Πολιτείες έχει ιδιαίτερη σημασία και θα αναπτυχθεί περαιτέρω, ιδίως στο πλαίσιο της ομάδας εργασίας ΕΕ-ΗΠΑ για την ασφάλεια στην κυβερνοχώρο και το ηλεκτρονικό έγκλημα.

Ο κυριότερος στόχος είναι η προβολή του κυβερνοχώρου ως περιοχή ελευθερίας και θεμελιωδών δικαιωμάτων μέσω της ανάπτυξης ικανοτήτων στους τομείς της ασφάλειας του κυβερνοχώρου και των ανθεκτικών υποδομών πληροφοριών σε τρίτες χώρες.

Τα κράτη μέλη, η Ευρωπαϊκή Επιτροπή και η Ύπατη Εκπρόσωπος θα συνεργαστούν προς την ανωτέρω κατεύθυνση προωθώντας το διάλογο και την κατάρτιση συναφών εθνικών πολιτικών, στρατηγικών και θεσμικών οργάνων σε τρίτες χώρες.

Καταμερισμός αρμοδιοτήτων

Σκοπός της παρούσας Οδηγίας δεν αποτελεί η συγκέντρωση της κεντρικής επιτήρησης της ασφάλειας σε ενωσιακό επίπεδο καθώς η πολυδιάσπαση του τομέα επιβάλλει την πλήρη δραστηριοποίηση των φορέων σε εθνικό επίπεδο με την Ένωση να επεμβαίνει όταν αυτό κρίνεται απαραίτητο και κατά κύριο λόγο συντονιστικά και υποστηρικτικά. Αναμένεται η αναβάθμιση των εθνικών στρατηγικών κυβερνοασφάλειας και η πλέουσα δυνατή συνεργασία μεταξύ των ενωσιακών, εθνικών και τρίτων χωρών φορέων. Ουσιαστικά επιδιώκεται η δημιουργία μιας συνεργατικής βάσης δράσης ώστε να αναχθεί η κυβερνοασφάλεια σε στρατηγική αλλά και πολιτική προτεραιότητα.

3.6.2 Πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (CDPF) 14413/18 (επικαιροποίηση 2018)

Η επικαιροποίηση του πλαισίου πολιτικής της Ευρωπαϊκής Ένωσης για την κυβερνοάμυνα θέτει την κυβερνοασφάλεια προτεραιότητα για τη συνολική στρατηγική για την εξωτερική πολιτική και την πολιτική ασφαλείας και για το ενωσιακό επίπεδο φιλοδοξίας. Η συνολική στρατηγική υπογραμμίζει την ανάγκη να ενισχυθεί η Ευρωπαϊκή Ένωση ως κοινότητα ασφάλειας μέσω της προώθησης της αποτελεσματικότητας και της διαλειτουργικότητας των ικανοτήτων στρατιωτικών και μη. Η επικαιροποίηση έρχεται ως επιστέγασμα της

κοινής δέσμης προτάσεων για την εφαρμογή της κοινής δήλωσης που υπέγραψαν ο Πρόεδρος του Ευρωπαϊκού Συμβουλίου, ο Πρόεδρος της Ευρωπαϊκής Επιτροπής και ο Γενικός Γραμματέας του Οργανισμού Βορειοατλαντικού Συμφώνου στη Βαρσοβία στις 8 Ιουλίου 2016[141], ακόμη της τεχνικής συμφωνία μεταξύ της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-EU) και της ομάδας αντιμετώπισης συμβάντων πληροφορικής του NATO (NCIRC), που υπεγράφη τον Φεβρουάριο του 2016, με στόχο τη διευκόλυνση της ανταλλαγής τεχνικών πληροφοριών και της θέσπισης της μόνιμης διαρθρωμένη συνεργασία (PESCO) μεταξύ 25 κρατών μελών για την ενίσχυση των προσπαθειών συνεργασίας για θέματα κυβερνοάμυνας.

Με βάση όλα τα ανωτέρω το επικαιροποιημένο πλαίσιο ανάγει την κυβερνοασφάλεια σε κομβικό σημείο της ενωσιακής πολιτικής και αναγνωρίζει την ανάγκη για αμυντικές κυβερνοεπιχειρήσεις σε οποιοδήποτε επιχειρησιακό πλαίσιο. Οι προτεραιότητες που τίθενται αφορούν:

- Υποστήριξη της ανάπτυξης ικανοτήτων κυβερνοάμυνας των κρατών μελών
- Ενίσχυση της προστασίας των δικτύων επικοινωνίας και πληροφοριών της ΚΠΑΑ που χρησιμοποιούνται από οντότητες της Ευρωπαϊκής Ένωσης
- Προώθηση πολιτικό-στρατιωτικής συνεργασίας
- Έρευνα και τεχνολογία
- Βελτίωση των δυνατοτήτων κατάρτισης, εκπαίδευσης και ασκήσεων
- Ενίσχυση της συνεργασίας με τους οικείους διεθνείς εταίρους

Α. Υποστήριξη της ανάπτυξης ικανοτήτων κυβερνοάμυνας των κρατών μελών

Τα κράτη μέλη καλούνται να εντείνουν τις προσπάθειες τους για την παροχή αποτελεσματικών ικανοτήτων κυβερνοάμυνας υπό τη στήριξη της ΕΥΕΔ, της Επιτροπής και του ΕΟΑ. Ως ένας από τους κύριους στόχους των δραστηριοτήτων τίθεται η διατήρηση της διαθεσιμότητας, της αρτιότητας και της εμπιστευτικότητας των δικτύων επικοινωνίας και πληροφοριών Κοινής Πολιτικής Ασφάλειας και Άμυνας.
Πιο συγκεκριμένα η ΕΥΕΔ και ο ΕΟΑ θα χρησιμοποιήσουν όλα τα μέσα που έχουν στη διάθεση τους για τη σύγκλιση κατά τον σχεδιασμό των απαιτήσεων κυβερνοάμυνας των κρατών μελών σε στρατηγικό επίπεδο και για την επίτευξη κατώτατου επιπέδου κυβερνοασφαλείας και εμπιστοσύνης που θα πρέπει να κατέχουν τα κράτη μέλη.
Στον αντίποδα τα κράτη μέλη θα προωθήσουν την περαιτέρω αξιοποίηση των CERT, της PESCO, του Ευρωπαϊκού Ταμείου Άμυνας, αλλά και της μη στρατιωτικής εμπειρογνωμοσύνης του ENISA σχετικά με την ασφάλεια πληροφοριών και δικτύων και με την κυβερνοασφάλεια των πολιτών.
Τέλος, προτείνεται η εξέταση της ένταξης της κυβερνοασφάλειας στα προγράμματα εργασίας του ευρωπαϊκού προγράμματος βιομηχανικής ανάπτυξης στον τομέα της άμυνας και του Ευρωπαϊκού Ταμείου Άμυνας

Β. Ενίσχυση της προστασίας των δικτύων επικοινωνίας και πληροφοριών της ΚΠΑΑ που χρησιμοποιούνται από οντότητες της Ευρωπαϊκής Ένωσης

[141] Διαθέσιμο στο: http://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf (Πρόσβαση 27.11.2019)

Παράλληλα και με την επιφύλαξη του ρόλου των CERT-EU η ΕΥΕΔ καλείται να αναπτύξει κατάλληλη και αυτόνομη αντίληψη των θεμάτων ασφάλειας και άμυνας δικτύου και θα αναπτύξει ίδια ικανότητα σε θέματα ασφάλειας με σκοπό την ενίσχυση της ανθεκτικότητας των δικτύων ΚΠΑΑ.
Η ΕΥΕΔ αναβαθμίζεται σε βραχίονα της αντιμετώπισης κυβερνοσυμβάντων για όλα τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και ταυτόχρονα υποστηρίζεται από τη Γενική Διεύθυνση Διαχείρισης Προϋπολογισμού και Διοίκησης (ΒΑ) της ΕΥΕΔ, το Στρατιωτικό Επιτελείο της ΕΕ (EUMS), τη Διεύθυνση Διαχείρισης Κρίσεων και Σχεδιασμού (CMPD) και τη Μη Στρατιωτική Δυνατότητα Σχεδιασμού και Διεξαγωγής Επιχειρήσεων (CPCC).

Γ. Προώθηση πολιτικό-στρατιωτικής συνεργασίας

Επιστεγάζεται η προώθηση της σύμπλευσης πολιτικών και στρατιωτικών μέσων για την κυβερνοάμυνα. Πιο συγκεκριμένα, υποστηρίζεται ότι η πολιτικό-στρατιωτική συνεργασία στον κυβερνοχώρο μπορεί να θεωρηθεί ενδεδειγμένη μεταξύ άλλων για την ανταλλαγή βέλτιστων πρακτικών, για την ανταλλαγή πληροφοριών και για τους μηχανισμούς έγκαιρης προειδοποίησης, για τις αξιολογήσεις κινδύνου για την αντιμετώπιση συμβάντων και για τις δράσεις ευαισθητοποίησης, καθώς και για κατάρτιση και ασκήσεις. Ταυτόχρονα προάγεται η συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών CERT.
Ο Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ), ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) και η CERT-EU, μαζί με άλλα συναφή όργανα και οργανισμούς της Ευρωπαϊκής Ένωσης, στο πλαίσιο των αντίστοιχων εντολών τους και χωρίς αλληλοεπικάλυψη με τις αρμοδιότητες των κρατών μελών, καθώς και τα κράτη μέλη, ενθαρρύνονται να ενισχύσουν περαιτέρω τη συνεργασία τους για την ανάπτυξη κοινών προφίλ αρμοδιοτήτων στους τομείς της ασφάλειας και της άμυνας στον κυβερνοχώρο, την προσαρμογή των οργανωτικών και τεχνικών προτύπων του δημόσιου τομέα για την κυβερνοασφάλεια και την κυβερνοάμυνα, την περαιτέρω ανάπτυξη μηχανισμών εργασίας και ρυθμίσεων για την ανταλλαγή βέλτιστων πρακτικών και την αξιοποίηση των δυνατοτήτων πρόληψης, έρευνας και εγκληματολογικών ερευνών που υπάρχουν σε επίπεδο Ευρωπαϊκής Ένωσης στον τομέα του ηλεκτρονικού εγκλήματος.

Δ. Έρευνα και τεχνολογία

Στο σημείο αυτό αναγνωρίζεται πως οι φορείς υποδομών και υπηρεσιών τεχνολογίας της πληροφορίας και των επικοινωνιών (ΤΠΕ) για μη στρατιωτικούς σκοπούς και σκοπούς άμυνας αντιμετωπίζουν αντίστοιχα προβλήματα ασφάλειας στον κυβερνοχώρο, λόγω των κοινών απαιτήσεων τεχνολογικής και επιχειρησιακής ικανότητας. Η ανάπτυξη τεχνολογικών ικανοτήτων στην Ευρώπη για τον περιορισμό των απειλών και των τρωτών σημείων κρίνεται ουσιαστικής σημασίας και συνάγεται πως η βιομηχανία θα παραμείνει ο βασικός μοχλός της τεχνολογίας και της καινοτομίας όσον αφορά την κυβερνοάμυνα. Σκοπός είναι η διασφάλιση ότι η Ευρώπη είναι σε θέση να συμβαδίσει με διεθνείς ανταγωνιστές όσον αφορά τις τεχνολογικές ικανότητες στον κυβερνοχώρο, με την υποστήριξη της συμμετοχής των μικρών και μεσαίων επιχειρήσεων.

Για τη διευκόλυνση της ανάπτυξης ικανοτήτων στο συγκεκριμένο τομέα καλούνται ο ΕΟΑ, η Επιτροπή και τα κράτη μέλη να αναζητήσουν συνέργειες μεταξύ των προσπαθειών Έρευνας και Τεχνολογίας στον στρατιωτικό τομέα με μη στρατιωτικά προγράμματα έρευνας και ανάπτυξης, να έχουν κοινά θεματολόγια έρευνας όσον αφορά την κυβερνοασφάλεια και να συμβάλουν ώστε να βελτιωθεί η ενσωμάτωση των διαστάσεων της κυβερνοασφάλειας και της κυβερνοάμυνας στα προγράμματα που έχουν διάσταση ασφάλειας και άμυνας διπλής χρήσης. Ταυτόχρονα η Επιτροπή καλείται να εξετάσει το ενδεχόμενο δημιουργίας ευρωπαϊκού κέντρου βιομηχανικών, τεχνολογικών και ερευνητικών ικανοτήτων στον τομέα της κυβερνοασφάλειας, με ένα δίκτυο εθνικών κέντρων συντονισμού για τη στήριξη των τεχνολογικών και βιομηχανικών ικανοτήτων στον τομέα της κυβερνοασφάλειας και να υποστηρίξει την ανάπτυξη βιομηχανικών οικοσυστημάτων και καινοτομικών συσπειρώσεων που θα καλύπτουν ολόκληρη την αλυσίδα αξίας της ασφάλειας με βάση τις ακαδημαϊκές γνώσεις, την καινοτομία των ΜΜΕ και τη βιομηχανική παραγωγή.

Ε. Βελτίωση των δυνατοτήτων κατάρτισης, εκπαίδευσης και ασκήσεων

Αναγνωρίζεται πλέον πως η σύγκλιση στην αντιμετώπιση των κυβερνοαπειλών και στην υποστήριξη ενός ενιαίου συστήματος κυβερνοασφάλειας δεν μπορεί να κριθεί επιτυχής δίχως την ποιοτική αξιοποίηση των πόρων για εκπαίδευση και κατάρτιση σε αυτό τον τομέα.
Για τον σκοπό αυτό καλούνται η Ευρωπαϊκή Ακαδημία Ασφάλειας και Άμυνας (ΕΑΑΑ), η ΕΥΕΔ, ο ΕΟΑ, η Επιτροπή και τα κράτη μέλη να καταρτίσουν προγράμματα εκπαίδευσης και κατάρτισης σε θέματα ΚΠΑΑ που θα απευθύνονται σε διάφορα ακροατήρια, συμπεριλαμβανομένων της ΕΥΕΔ, του προσωπικού των αποστολών και επιχειρήσεων ΚΠΑΑ και υπαλλήλων των κρατών μελών, να προτείνουν την καθιέρωση διαλόγου όσον αφορά θέματα κυβερνοάμυνας και συγκεκριμένα πρότυπα κατάρτισης και πιστοποίησης όχι μόνο με τα κράτη μέλη και τα ενωσιακά όργανα αλλά και με τρίτες χώρες και με τον ιδιωτικό τομέα και να έλθουν σε επαφή με ευρωπαϊκούς φορείς παροχής κατάρτισης του ιδιωτικού τομέα καθώς και με πανεπιστημιακά ιδρύματα προκειμένου να αναβαθμιστεί το γνωσιακό επίπεδο του προσωπικού των εμπλεκόμενων φορέων. Τέλος προάγεται η ανάγκη να βελτιωθούν οι δυνατότητες ασκήσεων κυβερνοάμυνας για τους πολιτικό-στρατιωτικούς φορείς της ΚΠΑΑ με τις ανωτέρω να κρίνονται ως εργαλείο για την ανάπτυξη κοινών γνώσεων και κοινής αντίληψης για την κυβερνοάμυνα.

Ζ. Ενίσχυση της συνεργασίας με τους οικείους διεθνείς εταίρους

Τονίζεται η ανάγκη να εξασφαλιστεί διάλογος με τους διεθνείς εταίρους, συγκεκριμένα το ΝΑΤΟ και άλλους διεθνείς οργανισμούς, με σκοπό τη συμβολή στην ανάπτυξη αποτελεσματικών ικανοτήτων στον τομέα της κυβερνοάμυνας.
Πιο συγκεκριμένα καλούνται η ΕΥΕΔ και η ΕΟΑ, μαζί με τα κράτη μέλη, να αναπτύξουν περαιτέρω συνεργασία σε θέματα κυβερνοάμυνας μεταξύ ΕΕ και ΝΑΤΟ. Προς το σκοπό αυτό θα κινηθούν μέσω της ανταλλαγής βέλτιστων πρακτικών στον τομέα της διαχείρισης κρίσεων και μέσω της αξιοποίησης του πλαισίου συνεργασίας του ΕΟΑ με το Κέντρο αριστείας συλλογικής κυβερνοάμυνας του ΝΑΤΟ ως αρχική πλατφόρμα ενισχυμένης συνεργασίας σε πολυεθνικά σχέδια κυβερνοάμυνας, βάσει κατάλληλων αξιολογήσεων.

Στην κατεύθυνση αυτή αξίζει να σημειωθεί πως εμπλέκεται και η CERT-EE η οποία καλείται να αξιοποιήσει περαιτέρω την τεχνική συμφωνία μεταξύ της CERT-EU και συναφών υπηρεσιών κυβερνοάμυνας της Ευρωπαϊκής Ένωσης, αφενός, και της NCIRC (υπηρεσία αντιμετώπισης συμβάντων ηλεκτρονικών υπολογιστών του NATO)[142], αφετέρου.
Τέλος, καλούνται τα κράτη μέλη και η ΕΥΕΔ να προβούν σε διαβουλεύσεις με διεθνείς εταίρους της Ευρωπαϊκής Ένωσης και να προωθήσουν στους κόλπους των διεθνών οργανισμών την εφαρμογή του υπάρχοντος διεθνούς δικαίου, και ιδίως του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, στον κυβερνοχώρο.

Η επικαιροποίηση του πλαισίου αδιαμφισβήτητα αναγάγει την κυβερνοασφάλεια σε έναν από τους βασικότερους τομείς συλλογικής δράσης της Ένωσης προσδίδοντας της όχι μόνο διακρατικό αλλά και παγκόσμιο ενδιαφέρον. Παρατηρείται για πρώτη φορά η προώθηση πολιτικό-στρατιωτικής συνεργασίας αλλά και κατάρτισης και εξωστρέφειας των φορέων της Ευρωπαϊκής Ένωσης με στόχο όχι μόνο τη θωράκιση της ανταγωνιστικότητας της εσωτερικής αγοράς αλλά και την προστασία του παγκόσμιου status quo. Για ακόμη μία φορά η Ευρωπαϊκή Ένωση πρωτοστατεί στο διάλογο με τους διεθνείς της εταίρους ώστε να καταστήσει σαφές πως η απειλή αφορά όλους και πως μόνο η συντονισμένη δράση είναι ικανή να επιφέρει ως αποτέλεσμα την προστασία όχι μόνον των οικονομιών αλλά και των πολιτών.

3.6.3 Αποτίμηση εξέλιξης των Ενωσιακών πολιτικών για την κυβερνοασφάλεια

Την τελευταία δεκαετία ο τεχνολογικός τομέας και συνάμα ο τομέας της ασφάλειας έχουν αλλάξει δραστικά επηρεάζοντας το παγκόσμιο και ευρωπαϊκό στερέωμα όχι μόνο σε επίπεδο οικονομικό αλλά και πολιτικό και γεωστρατηγικό. Η Ευρωπαϊκή Ένωση ιδίως από το 2017 και έπειτα έχει προχωρήσει σε δραστικές παρεμβάσεις στην προσπάθεια της να θωρακίσει την εσωτερική από τις ασύμμετρες απειλές. Σε ίδιο χρόνο για ακόμη μια φορά επιδιώκει και προωθεί στην πράξη την παγκόσμια σύμπλευση και συνεργασία απέναντι στην κοινή απειλή των κυβερνοεπιθέσεων επιβεβαιώνοντας και προφυλάσσοντας τις αρχές πάνω στις οποίες βασίζονται τα θεμέλια της δημιουργίας της.

Παρά τα πολύ σημαντικά και καινοτόμα βήματα στα οποία έχει προβεί η Ένωση και παρά το αρκετά υψηλό επίπεδο εναρμόνισης το οποίο έχει εφαρμόσει στο επίπεδο των κρατών μελών και των εθνικών στρατηγικών ασφαλείας, πολλά αναμένονται ακόμη να λάβουν χώρα προκειμένου ο στόχος της πλήρους τόσο νομικής όσο και πρακτικής προστασίας να επιτευχθεί.

Είναι γεγονός πως το σημαντικότερο πρόβλημα της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας έγκειται στο χάσμα που υπάρχει ανάμεσα τις φιλοδοξίες και τις δυνατότητες. Το χάσμα οφείλεται στην κυοφορία τριών προβλημάτων. Αρχικά παρά την πρόοδο στην κοινή ανίχνευση και αντιμετώπιση των κυβερνοεπιθέσεων, η λήψη ψηφιακών αποδεικτικών στοιχείων σε διασυνοριακές υποθέσεις είναι ακόμα δύσκολη. Σε δεύτερο χρόνο η Ευρωπαϊκή

[142] Βλ. σχετικές πληροφορίες: NCI Agency, Διαθέσιμο στο: https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx (Πρόσβαση 28.11.2019)

Ένωση υπολείπεται τόσο χρονικά όσο και τεχνογνωσιακά συγκριτικά με τους αντιπάλους της στον κυβερνοχώρο. Τέλος, η συμφωνία με το ΝΑΤΟ και τις Ηνωμένες Πολιτείες της Αμερικής σχετικά με την κοινή τους δράση δεν είναι ακόμη πλήρως οριοθετημένη με αποτέλεσμα τις μεμονωμένες και αυτόνομες απαντήσεις σε αντίστοιχα κυβερνοπεριστατικά.

Όπως κάθε στρατηγική έτσι και η στρατηγική κυβερνοασφάλειας χρήζει συνεχούς βελτίωσης ειδικότερα λαμβάνοντας υπόψιν τους ρυθμούς με τους οποίους εξελίσσεται και μεταλλάσσεται ο κυβερνοχώρος και η Ένωση διαθέτει τόσο την εμπειρία όσο και τα τεχνικά και νομικά μέσα ώστε να ανταποκριθεί δεόντως στις όλο αυξανόμενες προκλήσεις.

Στις 24.7.2019, η Ευρωπαϊκή Επιτροπή εξέδωσε Ανακοίνωση[143] προς το Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το Συμβούλιο σχετικά με την περαιτέρω πρόοδο που έχει σημειωθεί ως προς την οικοδόμηση μιας αποτελεσματικής και πραγματικής Ένωσης ασφαλείας συμπεριλαμβανομένης και της κυβερνοασφάλειας. Στην εν προκειμένω ανακοίνωση ορίζονται οι εκκρεμούσες πρωτοβουλίες προτεραιότητας στην Ένωση ασφαλείας για τις οποίες απαιτείται η ανάληψη περαιτέρω δράσης από τους συννομοθέτες, με στόχο την ενίσχυση της ασφάλειας στον κυβερνοχώρο και τη διευκόλυνση της πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία, καθώς και την ολοκλήρωση των εργασιών για πιο ισχυρά και έξυπνα συστήματα πληροφοριών όσον αφορά την ασφάλεια και τη διαχείριση των συνόρων και της μετανάστευσης.

Σχετικά με την ενίσχυση της κυβερνοασφάλειας, ο τομέας της οποίας αναγνωρίζεται για ακόμη μια φορά ως ένα από τους σημαντικότερους τομείς δραστηριότητας της Ένωσης, επισημαίνεται η ανάγκη το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο να καταλήξουν σε συμφωνία για την πρωτοβουλία προτεραιότητας της Επιτροπής σχετικά με τη σύσταση ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού[144]. Ακόμη τονίζεται πως η Επιτροπή συνεχίζει να στηρίζει την έρευνα και την καινοτομία που αφορούν την κυβερνοασφάλεια, καθιστώντας διαθέσιμα 135 εκατ. € στο τρέχον πολυετές δημοσιονομικό πλαίσιο για έργα σε τομείς όπως η κυβερνοασφάλεια σε υποδομές ζωτικής σημασίας, η έξυπνη ασφάλεια, και η διαχείριση της ιδιωτικότητας, καθώς και εργαλεία ειδικά για πολίτες και μικρομεσαίες επιχειρήσεις[145] ενώ, προσδίδεται στα περιοριστικά μέτρα τα οποία θεσμοθετήθηκαν με την απόφαση του Συμβουλίου της 17ης Μαΐου 2019, το καθεστώς κυρώσεων που αποτελεί μέρος της εργαλειοθήκης για τη διπλωματία

[143] COM/2019/353, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το ΣΥΜΒΟΥΛΙΟ Δέκατη ένατη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας, σελ. 5
[144] Βλ. 143
[145] Βλ. 143

της Ένωσης στον κυβερνοχώρο, ένα πλαίσιο για μια κοινή διπλωματική απάντηση σε κακόβουλες δραστηριότητες στον κυβερνοχώρο[146].

Όσον αφορά τα κενά τα οποία προαναφέρθηκαν, η Επιτροπή συνιστά οι διαπραγματεύσεις για τις προτάσεις του Απριλίου του 2018 σχετικά με τη βελτίωση της πρόσβασης των αρχών επιβολής του νόμου σε ηλεκτρονικά αποδεικτικά στοιχεία να ολοκληρωθούν το συντομότερο δυνατό. Όμως πέραν των ενδοενωσιακών διαπραγματεύσεων τονίζεται η ανάγκη για τη βελτίωση και την κατοχύρωση των απαραίτητων διασφαλίσεων κατά τη διεθνή ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο των εν εξελίξει διαπραγματεύσεων για ένα δεύτερο πρόσθετο πρωτόκολλο στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο που υπογράφηκε στη Βουδαπέστη, καθώς και με τις Ηνωμένες Πολιτείες σύμφωνα με τις διαπραγματευτικές εντολές που έδωσε το Συμβούλιο κατά τη συνεδρίαση του Συμβουλίου Δικαιοσύνης και Εσωτερικών Υποθέσεων στις 6-7 Ιουνίου 2019[147].

Είναι εμφανές πως η Επιτροπή έχει αναλάβει εξολοκλήρου το ρόλο του συντονιστή στο δυσχερές επίτευγμα της εδραίωσης της ενωσιακής στρατηγικής για την κυβερνοασφάλεια προάγοντας τη συνεργασία τόσο των ευρωπαϊκών θεσμικών οργάνων μεταξύ τους όσο και των κρατών μελών αλλά και της Ένωσης ως σύνολο με τους διεθνείς συμμάχους της.

[146] COM/2019/353, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το ΣΥΜΒΟΥΛΙΟ Δέκατη ένατη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας, σελ. 6

[147] COM/2019/353, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το ΣΥΜΒΟΥΛΙΟ Δέκατη ένατη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας, σελ. 7

4. Αποτίμηση – Συμπεράσματα

Η στρατηγική της Ευρωπαϊκής Ένωσης στον τομέα του κυβερνοχώρου βρίσκεται στο επίκεντρο της δραστηριότητας της ιδίως από το 2017, δεδομένου πως αυτό το χρονικό σημείο αποτέλεσε ορόσημο για κυβερνοεπιθέσεις υψηλού επιπέδου οι οποίες έπληξαν την Ένωση. Η ευρωπαϊκή στρατηγική για την ασφάλεια στον κυβερνοχώρο καλύπτει δύο επίπεδα: το έγκλημα στον κυβερνοχώρο, όπως η ηλεκτρονική απάτη και τις επιθέσεις στον κυβερνοχώρο οι οποίες προέρχονται κυρίως από κρατικούς δρώντες. Η Ένωση έχει καταφέρει να οριοθετήσει την άμυνα της στον κυβερνοχώρο ασκώντας την πάγια πρακτική της η οποία είναι η νομοπαραγωγική διαδικασία και η ανάθεση αρμοδιοτήτων στα όργανα της. Ωστόσο, η ικανότητα της Ευρώπης να προλαμβάνει και να ανταποκρίνεται σε επιθέσεις στον κυβερνοχώρο υστερεί ακόμη αρκετά συγκριτικά με τις επιθετικές ικανότητες των αντιπάλων της όπως είναι η Ρωσία και η Βόρεια Κορέα. Δεν υπάρχει η απαίτηση για άμεση ανταπόκριση στις κυβερνοεπιθέσεις καθώς αυτό αποτελεί αρμοδιότητα που ανήκει στα κράτη μέλη και μόνο, όμως υπάρχουν σημεία τα οποία μπορούν να επιδεχθούν βελτιστοποίησης από την πλευρά της Ένωσης επιτυγχάνοντας ενίσχυση του ήδη υπάρχοντος επιπέδου ασφαλείας στον κυβερνοχώρο[148].

Τα βασικά σημεία τρωτότητας της ισχύουσας στρατηγικής τα οποία μπορούν να δεχθούν τροποποιήσεις συνοψίζονται κατωτέρω:

Α. Ενίσχυση αποτελεσματικής αντίδρασης σε κυβερνοπεριστατικά
Είναι ιδιαίτερα σημαντικό οι κρίσιμοι τομείς, τα κράτη μέλη και τα θεσμικά όργανα της ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ να είναι σε θέση να αντιδράσουν τάχιστα και κατά τρόπο συντονισμένο. Για τον σκοπό αυτό είναι απαραίτητη η έγκαιρη ανίχνευση και γνωστοποίηση. Δεδομένης της πολυπλοκότητας των πληροφοριακών συστημάτων αλλά και των κυβερνοεπιθέσεων, η αποτροπή τους κρίνεται ανέφικτη επί της ουσίας, έτσι σύμφωνα με τους εμπειρογνώμονες, πρέπει να δοθεί έμφαση στην ταχεία ανίχνευση και την άμυνα. Ωστόσο, ορισμένα εργαλεία ανίχνευσης, όπως η αυτοματοποίηση, η μηχανική μάθηση και η συμπεριφορική ανάλυση, που επιδιώκουν τη μείωση των κινδύνων και την ανάλυση και άντληση διδαγμάτων από τη συμπεριφορά του συστήματος, εμφανίζουν χαμηλά ποσοστά υιοθέτησης από τις επιχειρήσεις. Έτσι κρίνεται απαραίτητο να δοθεί ιδιαίτερη έμφαση στην ανίχνευση μεν αλλά και στη γνωστοποίηση των αποτελεσμάτων ούτως ώστε και άλλοι δημόσιοι και ιδιωτικοί φορείς να λάβουν προληπτικά μέτρα, και οι αρμόδιες αρχές να παράσχουν στήριξη σε εκείνους που επλήγησαν[149].
Στο πλαίσιο αυτό οι επαγγελματίες του κυβερνοχώρου και οι υπεύθυνοι για τη λήψη αποφάσεων αναζητούν νέους τρόπους για την πρόληψη πιθανών

[148] Βλ. σχετικές πληροφορίες: Game over? Europe's cyber problem, Camino Mortera Martinez, Ιούλιος 2018, Open Society European Policy Institute, Centre For European Reform, Διαθέσιμο στο: https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem (Πρόσβαση 01.12.2019)
[149] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 54

επιθέσεων. Σκοπός αποτελεί η απόκτηση δεδομένων και πληροφοριών που θα τους επιτρέπουν να αναλύουν και να ερευνούν την πρόθεση, τη συμπεριφορά, τα εργαλεία, τις τακτικές και τις τεχνικές των αντιπάλων ώστε να μετακινηθούν από την αντιδραστική σε μια προληπτική αμυντική στρατηγική. Αρκετά ενθαρρυντική είναι η πρόταση του ENISA για την υιοθέτηση από πλευράς του ενός προγράμματος CTI (Cyberthreat Intelligence Program) το οποίο θα καλύπτει την τη συνεχή παραγωγή σχετικών, ευνόητων και ευπροσάρμοστων πληροφοριών, για την υποστήριξη της ικανότητας των οργανισμών να αποτρέπουν τα τις κυβερνοεπιθέσεις. Η εφαρμογή του προγράμματος αναμένεται να συμβάλλει στην αύξηση της αποτελεσματικότητας των μέσων ασφάλειας και τεχνικών πόρων, στη βελτίωση της επικοινωνίας των απειλών σε τομεακό, επιχειρηματικό και γεωγραφικό πλαίσιο και στη βελτίωση της επικοινωνίας με στελέχη επιχειρήσεων[150].

Β. Ενίσχυση Προστασίας των υποδομών ζωτικής σημασίας

Μεγάλο μέρος των υποδομών ζωτικής σημασίας της Ένωσης λειτουργεί μέσω βιομηχανικών συστημάτων ελέγχου τα οποία σχεδιάστηκαν ως αυτόνομα συστήματα, με περιορισμένη δυνατότητα σύνδεσης με τον έξω κόσμο γι' αυτό το λόγο κρίνονται πολύ ευάλωτα και η αναβάθμιση τους αποτελεί μέτρο εξαιρετικής σημασίας. Ακόμη η αλληλοσύνδεση που διέπει τη βιομηχανία αυξάνει τον κίνδυνο ο αντίκτυπος ενός περιστατικού μεγάλης κλίμακας σε έναν κλάδο της βιομηχανίας να έχει αλυσιδωτές αντιδράσεις σε άλλους. Ως εκ τούτου ο ENISA επεσήμανε τη σημασία της χαρτογράφησης του αντικτύπου της αμοιβαίας εξάρτησης που υπάρχει μεταξύ κρίσιμων τομέων. Η διαδικασία αυτή είναι απαραίτητη προκειμένου να γίνει κατανοητός ο ρυθμός ενδεχόμενης εξάπλωσης ενός περιστατικού και αποτελεί προϋπόθεση για την οργάνωση καλά συντονισμένων αντιδράσεων[151].

Τα τρωτά σημεία των υποδομών ζωτικής σημασίας δεν σταματούν στα σύνορα της Ευρώπης. Μια σημαντική πρόκληση για την Επιτροπή είναι να ενθαρρύνει τις υποψήφιες χώρες να υιοθετήσουν τα ίδια πρότυπα με τα κράτη μέλη, παραδείγματος χάριν σε τομείς όπως η νομοθεσία που σχετίζεται με τον κυβερνοχώρο ή η προστασία των υποδομών ζωτικής σημασίας[152]. Τα περιοριστικά μέτρα που προτάθηκαν με την απόφαση του Συμβουλίου 7299/19, 14.5.2019 αποτελούν ένα σημαντικό βήμα για τη θωράκιση των υποδομών ζωτικής σημασίας.

Γ. Ενίσχυση των δεξιοτήτων και αύξηση της ενημέρωσης και της ευαισθητοποίησης.

Ένας σημαντικός παράγοντας στην πρόληψη των κυβερνοεπιθέσεων είναι η ορθή ενημέρωση και η κατάρτιση των τελικών χρηστών καθώς είναι ιδιαίτερα κρίσιμο κατά την καθημερινή των πληροφοριακών μέσων να δύνανται να αντιμετωπίζουν τα σημεία πιθανών απειλών και να λαμβάνουν τα κατάλληλα «πρώτα μέτρα» πρόληψης. Δυστυχώς σε έναν κόσμο που βάλλεται από

[150] Βλ. σχετικές πληροφορίες: ENISA Threat Landscape Report 2018, ETL 2018, Ιανουάριος 2019, Διαθέσιμο στο: www.enisa.europa.eu (Πρόσβαση 01.12.2019)

[151] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 58

[152] Βλ. 151

κυβερνοεπιθέσεις το έλλειμμα εξειδικευμένου εργατικού δυναμικού αυξήθηκε κατά 20% από το 2015[153]. Είναι βασικό να εξασφαλιστεί υψηλό επίπεδο κατάρτισης των απασχολούμενων τόσο σε κυβερνητικούς φορείς όσο και στον ιδιωτικό τομέα με ταυτόχρονη ευαισθητοποίηση του ευρέως κοινού προς αυτή την κατεύθυνση. Παρά το γεγονός ότι αρμόδια για τις εκπαιδευτικές πολιτικές είναι τα κράτη μέλη, σε ενωσιακό επίπεδο πραγματοποιούνται ήδη πολυάριθμες δραστηριότητες κατάρτισης και ασκήσεις. Η Ένωση μπορεί να διευκολύνει την ενσωμάτωση ευρωπαϊκών προτύπων στα εκπαιδευτικά προγράμματα που καλύπτουν όλους τους σχετικούς κλάδους[154]. Ο ENISA ήδη δημιουργεί και προωθεί προγράμματα ευαισθητοποίησης ανοιχτά στο κοινό και μεριμνά για την παραγωγή υλικού χρήσιμου για την ενημέρωση όλων των εμπλεκόμενων φορέων[155]. Πιο συγκεκριμένα κάθε έτος διεξάγεται ο Ευρωπαϊκός μήνας για την ασφάλεια στον κυβερνοχώρο (European Cyber Security Awareness Month, ECSM) καθώς και η Ημέρα Ασφαλέστερου Διαδικτύου με σκοπό την περαιτέρω ευαισθητοποίηση του κοινού.
Ακόμη η Ένωση σε συνεργασία με το NATO υποστηρίζει τη διεξαγωγή ασκήσεων στον τομέα της κυβερνοασφάλειας, όπως η ανά διετία άσκηση Cyber Europe (επιχειρησιακή) και η ετήσια άσκηση «Locked Shields» (τεχνική)– προσελκύουν περισσότερους από 1.000 συμμετέχοντες από περίπου 30 συμμετέχοντα κράτη. Και οι δύο διαδικασίες επικεντρώνονται στην προστασία και τη διατήρηση υποδομών ζωτικής σημασίας στο πλαίσιο σεναρίων προσομοίωσης επιθέσεων[156].

Η διαχείριση των επιπλοκών που επιφέρει η έλλειψη σταθερού πλαισίου κυβερνοασφάλειας από την πλευρά της Ένωσης μπορεί να αξιολογηθεί θετικά, όμως υπάρχουν πολλά τα οποία πρέπει να λάβουν χώρα για να μπορέσουμε να μιλήσουμε για μια πραγματική Ένωση ασφαλείας. Είναι γεγονός πως η Ένωση με σταθερά βήματα οδηγεί τα κράτη μέλη στο επιθυμητό στάδιο μέσα από δημοκρατικές αλλά και αποτελεσματικές διαδικασίες. Η πορεία του εγχειρήματος της κυβερνοασφάλειας βασίζεται, τουλάχιστον μέχρι στιγμής στην έκδοση νομοθετικών πράξεων με σκοπό την οριοθέτηση της κοινής ενωσιακής δράσης αλλά και την υποστήριξη των κρατών μελών. Είναι εμφανές πως τα θεσμικά όργανα αποσκοπούν στη ψηφιακή θωράκιση της εσωτερικής αγοράς μέσω της επιμέρους θωράκισης του εκάστοτε κράτους μέλους. Το περιεχόμενο των νομοθετικών πράξεων καθοδηγεί τα κράτη μέλη στην ανάληψη μέτρων όχι μόνο πρόληψης αλλά και εξέλιξης των μέχρι τώρα πρακτικών τους ώστε να μπορέσουν να αντιμετωπίσουν τις πολύπλευρες απειλές στις οποίες εκτίθενται. Η θωράκιση του τομέα της κυβερνοασφάλειας απαιτεί τη σύμπλευση στους κόλπους της Ένωσης περισσότερο από οποιονδήποτε άλλο μέχρι σήμερα. Η αναγωγή της κυβερνοασφάλειας σε πρωταρχικό θέμα στην ατζέντα της Ένωσης αποτελεί πρόκληση, κρίνεται όμως απαραίτητη δεδομένων των ιδιαίτερων χαρακτηριστικών της. Οι Ευρωπαίοι εταίροι καλούνται να επιδείξουν πειθαρχία

[153] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 43
[154] Βλ. 153, σελ. 44
[155] Βλ. σχετικές πληροφορίες: ECSM 2019, Διαθέσιμο στο: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month/ecsm-2019 (Πρόσβαση 02.12.2019)
[156] Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση, σελ. 46

και συντονισμένη πρακτική καθώς μόνον μέσω ενός ενιαίου πλαισίου δράσης θα καταστεί δυνατή η οριοθέτηση του χαοτικού πλέγματος του κυβερνοχώρου. Οι πρωτοβουλίες που έχουν αναληφθεί αναμένεται να επιφέρουν πραγματικά αποτελέσματα στο επίπεδο ασφαλείας της Ένωσης όμως πρέπει να γίνει αντιληπτό πως η όποια χάραξη πολιτικής και πρακτικής υλοποίησης μέτρων θα πρέπει συνεχώς να επικαιροποιείται και να αναπροσαρμόζεται σύμφωνα με τις συνεχείς τεχνολογικές εξελίξεις. Απαιτείται εγρήγορση στη λήψη αποφάσεων και άμεση εφαρμογή για να καταστεί δυνατή η ουσιαστική σύγκλιση. Η κυβερνοασφάλεια τείνει να εξελιχθεί σε «αγώνα δρόμου» ανάμεσα στα κράτη μέλη, στην Ένωση και τους διεθνείς εταίρους, ακόμη και ανάμεσα στους ιδιώτες. Πολλοί υποστηρίζουν πως η Ένωση αργοπόρησε να αναλάβει δράση σχετικά με ένα θέμα το οποίο απασχολεί τις υπόλοιπες δυνάμεις αρκετό χρόνο νωρίτερα. Όμως, όπως έχει ήδη γίνει αντιληπτό η Ένωση διαθέτει τόσο τις διαδικασίες όσο και την πολιτική θέληση να πρωτοστατήσει εσωτερικά και διεθνώς στις εξελίξεις για την εγκαθίδρυση ισχυρών πλαισίων κυβερνοασφάλειας.

Βιβλιογραφία (Ελληνόγλωσση)

1. https://el.wikipedia.org/wiki/Επιστήμη_συστημάτων
1. Ευρωπαϊκό Ελεγκτικό Συνέδριο, Μάρτιος 2019, Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, Λουξεμβούργο: Ευρωπαϊκή Ένωση
2. https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82
3. https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8E%CE%BD_%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%AC%CF%84%CF%89%CE%BD
4. https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81
5. Τατσούλης Περικλής, Ο κυβερνοπόλεμος ως πολυδιάστατο στρατηγικό εργαλείο και η εφαρμογή του σε κρίσιμες στρατιωτικές και μη υποδομές, Μάιος 2019, Μεταπτυχιακή Διατριβή, Διιδρυματικό Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών, Εφαρμοσμένη Επιχειρησιακή Έρευνα και Ανάλυση, Στρατιωτική Σχολή Ευελπίδων, Πολυτεχνείο Κρήτης
6. Αλέξανδρος Λιούτας, Η Έννοια της Ένοπλης Επίθεσης στον Κυβερνοχώρο, Μάιος 2019, Διπλωματική Εργασία, Δημόσιο Διεθνές Δίκαιο, Νομική Σχολή Α.Π.Θ.,
7. Κυριάκος Στεφανίδης, Προστασία Συστημάτων από Κατανεμημένες Επιθέσεις στο Διαδίκτυο, Νοέμβριος 2013, Διδακτορική Διατριβή, Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών
8. http://www.enet.gr/?i=news.el.article&id=181298
9. Παναγιώτης Νιάκαρης, Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή, οι ευρωπαϊκές απαντήσεις, Απρίλιος 2019, Ατομική διατριβή, Σχολή Εθνικής Άμυνας,
10. https://www.tovima.gr/2014/04/22/world/i-nea-tripli-stratigiki-poytin-stin-oykrania/
11. ΕΕ L 151, Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA
12. Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, Βρυξέλλες, 13.9.2017
13. ΕΕ L 194, Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση
14. https://opencourses.auth.gr/modules/document/file.php/OCRS394/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/%CE%B5%CE%BD%CF%8C%CF%84%CE%B7%CF%84%CE%B1%2010%20%CE%A7%CE%95%CE%91%CE%94.pdf
15. Μάρκος Παπακωνστάντης, Η Τρομοκρατία στο Χώρο Ελευθερίας Ασφάλειας και Δικαιοσύνης, Μάρκος Παπακωνστάντης, Νομική Βιβλιοθήκη, 2019
16. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:11997D/TXT&from=EL
17. Δονάτος Παπαγιάννης, Ευρωπαϊκό Δίκαιο, Νομική Βιβλιοθήκη, 5η Έκδοση, 2016

18. ΕΕ L 77, Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών

19. ΕΕ L 293, Κανονισμός (ΕΚ) αριθ. 1007/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Σεπτεμβρίου 2008, περί τροποποιήσεως του κανονισμού (ΕΚ) αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών ως προς τη διάρκειά του
20. ΕΕ L 165, Κανονισμός (ΕΕ) αριθ. 580/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011 , περί τροποποιήσεως του κανονισμού (ΕΚ) αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών ως προς τη διάρκειά του
21. ΕΕ L 165, Κανονισμός (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013 , σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004
22. ΕΕ L 194, Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση
23. ΕΕ L. 135 Κανονισμός (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ
24. COM/2001/0298, Ανακοίνωση από την Επιτροπή προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών - Ασφάλεια δικτύων και πληροφοριών: Πρόταση ευρωπαϊκής πολιτικής
25. ΕΕ L 2001_149_R_0001_01, 2001/413/ΔΕΥ: Απόφαση-πλαίσιο του Συμβουλίου, της 28ης Μαΐου 2001, για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών
26. ΕΕ L 201, Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
27. ΕΕ L 77, Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών
28. COM/2006/0251, Ανακοινωση της Επιτροπης στο Συμβουλιο, στο Ευρωπαϊκο Κοινοβουλιο, στην Ευρωπαϊκη Οικονομικη και Κοινωνικη Επιτροπη και στην Επιτροπη των Περιφερειων - Στρατηγική για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων»
29. ΕΕ L 345, Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008 , σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους
30. ΕΕ L 313, Οδηγία 2009/149/ΕΚ της Επιτροπής, της 27ης Νοεμβρίου 2009 , για την τροποποίηση της Οδηγίας 2004/49/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και

του Συμβουλίου όσον αφορά τους κοινούς δείκτες ασφάλειας και τις κοινές μεθόδους υπολογισμού του κόστους ατυχήματος
31. 2009/C 321/01, Ψήφισμα του Συμβουλίου, της 18ης Δεκεμβρίου 2009, για μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών
32. COM/2010/0245, Ανακοίνωση της Επιτροπής της 19ης Μαΐου 2010, προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, σχετικά με το Ψηφιακό Θεματολόγιο για την Ευρώπη.
33. COM/2010/521, Πρόταση, Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον Ευρωπαϊκό Οργανισμό για την ασφάλεια Δικτύων και Πληροφοριών (ENISA)
34. COM/2010/0171, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών για ένα χώρο ελευθερίας, ασφάλειας και δικαιοσύνης στην υπηρεσία των πολιτών της Ευρώπης Σχέδιο δράσης για την εφαρμογή του προγράμματος της Στοκχόλμης
35. COM/2010/0673 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο Η στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη
36. ΕΕ L 70, Απόφαση της Επιτροπής της 16ης Μαρτίου 2011 για την έγκριση σχεδίων που υποβλήθηκαν από τρίτες χώρες σύμφωνα με το άρθρο 29 της οδηγίας 96/23/ΕΚ του Συμβουλίου
37. COM/2012/0140, Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, Αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο
38. COM/2012/0529, Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους
39. COM/2012/0784, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών. Ψηφιακό θεματολόγιο για την Ευρώπη. Οδηγώντας την Ευρώπη στη ψηφιακή ανάπτυξη.
40. ΕΕ L 218, Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013 , για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου
41. COM/2010/521, Πρόταση της Επιτροπής, στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)
42. COM/2013/0027, Πρόταση της Επιτροπής, στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση.
43. JOIN/2013/1, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών. Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο
44. ΕΕ L 93, Στρατηγική για την ασφάλεια στον κυβερνοχώρο της ΕΕ: ένας ανοιχτός, ασφαλής και προστατευμένος κυβερνοχώρος. Ψήφισμα του Ευρωπαϊκού

Κοινοβουλίου της 12ης Σεπτεμβρίου 2013 σχετικά με μια στρατηγική για την ασφάλεια στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο
45. https://www.sas.com/el_gr/insights/big-data/internet-of-things.html
46. https://ec.europa.eu/greece/news/20190626_3_el_el
47. https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-stin-eyropaiki-enosi-hrisimes-plirofories-me-aformi-ti-nea-praxi-gia-tin
48. ΕΕ L, 129Ι, ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2019/797 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της,
49. https://ec.europa.eu/commission/presscorner/detail/el/IP_19_2891
50. https://www.nato.int/docu/review/2007/issue2/Greek/art6.html
51. JOIN/2013/1, κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκη Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο
52. http://www.epset.gr/el/content/ypologistiko-nefos-cloud-computing
53. COM/2019/353, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το ΣΥΜΒΟΥΛΙΟ Δέκατη ένατη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας

Βιβλιογραφία (Ξενόγλωσση)

1. Ulysses goes CyberSpace... Warren St. McCulloch, A Heterarchy of Values Determined by the Topology of Nervous Nets, Abdruck in: Embodiments of Mind, Warren St. McCulloch, MIT Press, Cambridge Mass. 1970
2. David J. Betz and Tim Stevens, Cybersecurity and the State, IISS, UK,
3. Nils Melzer, Cyberwarfare and International Law, Unidir Resources, 2011
4. https://www.nsa.gov/
5. https://powerpolitics.eu/
6. http://www.economist.com/node/16478792
7. https://gdpr.report/news/2019/04/29/cyber-attacks-reported-by-61-of-us-and-european-firms-over-past-year/
8. https://www.rathenau.nl/en/digital-society/cyberspace-without-conflict/cyber-attacks-cyber-espionage
9. 2007 Cyber Attacks on Estonia, Cyber Operations, 2007, NATO, StratCom, COE
10. https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html
11. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
12. https://en.wikipedia.org/wiki/Backdoor_(computing)
13. http://www.enet.gr/?i=news.el.article&id=181298
14. SWD(2017) 295 final, Commission Staff Working Document Assessment of the EU2013 cybersecurity strategy, 13.09.2017
15. Review of Cyber Hygiene practices, Δεκέμβριος 2016, ENISA
16. https://www.enisa.europa.eu/topics/cyber-exercises/trainings/cyber_exercises
17. https://csirtsnetwork.eu/
18. https://www.europol.europa.eu/el/about-europol
19. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
20. http://publications.europa.eu/resource/cellar/15306167-9a7e-4022-9f02-ce742f9d7850.0009.02/DOC_1
21. https://cert.europa.eu/cert/plainedition/en/cert_about.html

22. https://www.consilium.europa.eu/el/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/
23. https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
24. https://www.nato.int/cps/en/natohq/official_texts_24470.htm?mode=pressrelease
25. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5388/shaping-of-a-common-security-and-defence-policy-_en
26. https://eeas.europa.eu/headquarters/headquarters-homepage/15917/nato-and-eu-press-ahead-with-cooperation-on-cyber-defence_en
27. https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
28. http://www.europarl.europa.eu/cmsdata/121581/ST_15283_2016_INIT_EN.pdf
29. https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf
30. http://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf
31. https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx
32. https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem
33. ENISA Threat Landscape Report 2018, ETL 2018, Ιανουάριος 2019, www.enisa.europa.eu
34. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month/ecsm-2019