Πανεπιστήμιο Πειραιώς

Μεταπτυχιακό Πρόγραμμα Σπουδών στις Διεθνείς και Ευρωπαϊκές Σπουδές

Τίτλος:

Η Ευρωπαϊκή Ένωση ως δρών ασφαλείας: Το οικοσύστημα Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης.

Φοιτητής:

Τζανάκος Δημοσθένης

Επιβλέπουσα Καθηγήτρια:

Ασδεράκη Φωτεινή

Πειραιάς, Δεκέμβριος 2024

Το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.

Υπογραφή

Περιεχόμενα

Λίστα εικόνων

Λίστα πινάκων

Συντομογραφίες

CER: Centre for European Reform
CERT-EU: The Computer Emergency Response Team for the EU institutions, bodies and agencies
CRA: Cyber Resilience Act
CVD: Coordinated Vulnerability Disclosure
DORA: Digital Operational Resilience Act
DSP: Digital service providers
ECSF- European Cybersecurity Skills Framework
EEAS: The European External Action Service is the European Union's diplomatic service
EFTA: European Free Trade Association-Ευρωπαϊκή Ζώνη Ελευθέρων Συναλλαγών
ENISA: European Union Agency for Cybersecurity
EU-CyCLONe: European Cyber Crises Liaison Organisation Network
EUIPO: European Union Intellectual Property Office
EUISS: The European Union Institute for Security Studies
GDPR: General Data Protection Regulation
ICRC: International Committee of the Red Cross
IHL: International humanitarian law
NIS/NIS2: Directive on security of network and information systems
OES: Operators of Essential Services
ΕΕ: Ευρωπαϊκή Ένωση
ΚΕΠΠΑ: Κοινή εξωτερική πολιτική και πολιτική ασφαλείας

Περίληψη

Η εργασία αναλύει τον ρόλο της Ευρωπαϊκής Ένωσης ως δρώντα ασφαλείας σε ένα γενικότερο πλαίσιο Κυβερνοασφάλειας και απαντά στα βασικά ερευνητικά μας ερωτήματα, τα οποία είναι τα εξής: Είναι η ΕΕ παγκόσμιος δρών ασφαλείας όσον αφορά στην Κυβερνοασφάλεια; Είναι αποτελεσματικό το οικοσύστημα Κυβερνοασφάλειας της ΕΕ, και αν ναι, πως ακριβώς αξιολογούμε αυτήν την αποτελεσματικότητα; Θα μελετηθούν οι ισχύουσες νομοθεσίες και από διάφορες αναφορές σε Ευρωπαϊκά εγχειρίδια θα οδηγηθούμε σε συγκεκριμένα συμπεράσματα και πορίσματα. Επίσης, θα γίνουν προτάσεις για το μέλλον και σχόλια για πιθανές βελτιώσεις. Πιο αναλυτικά, αρχικά θα γίνει μια εισαγωγή στο θέμα με αναφορές στην κατάσταση σήμερα σε θέματα Κυβερνοασφάλειας γενικότερα στα διεθνή και ευρωπαϊκά δρώμενα. Θα οριστεί δηλαδή το περιβάλλον και η κατάσταση που βρίσκεται το θέμα την χρονική στιγμή της εργασίας. Έπειτα, θα γίνει μια περιγραφή των γενικών χαρακτηριστικών και γνωρισμάτων της Κυβερνοασφάλειας και των βασικών εννοιών που την συνοδεύουν. Θα αναλυθούν όροι όπως «κυβερνοχώρος», «κυβερνητική», «κυβερνοεπίθεση», «cyber-sovereignty» και άλλα, όροι δηλαδή που είναι απαραίτητοι στην κατανόηση του θέματος και στην συνοχή της εργασίας. Στην συνέχεια και αφού έχουν περιγραφεί οι βασικές έννοιες, θα συνεχίσουμε με την απαρίθμηση των κανονισμών-ρυθμίσεων-νομολογιών από πλευράς Ευρωπαϊκής ένωσης για την Κυβερνοασφάλεια. Θα οριστεί δηλαδή το ρυθμιστικό πλαίσιο Κυβερνοασφάλειας στην Ευρώπη και θα δοθούν οι πιο πρόσφατες αποφάσεις σχετικά με το θέμα καθώς και ο τρόπος με τον οποίο έχουν εφαρμοστεί στα κράτη μέλη της Ευρωπαϊκής ένωσης και σε ποιόν βαθμό σε κάθε περίπτωση. Αμέσως μετά, θα γίνει μια λεπτομερέστερη ανάλυση των προβλημάτων που παρατηρούνται στο πεδίο της Κυβερνοασφάλειας στην ΕΕ. Από την ανάλυση αυτή θα προκύψουν οι απαντήσεις στα ερωτήματα μας, τα συμπεράσματα και τα πορίσματα των ρυθμίσεων ή της έλλειψης ρυθμίσεων από πλευράς Ευρωπαϊκής ένωσης στο ζήτημα της Κυβερνοασφάλειας για τα κράτη μέλη. Τέλος, ανάλογα με τα πορίσματα των παραπάνω, θα γίνουν σχόλια και προτάσεις βελτίωσης του πλαισίου της πολιτικής της ΕΕ απέναντι στο ζήτημα και θα επιχειρήσω μια ματιά στο μέλλον.

Κεφάλαιο 1ο: Εισαγωγή

1.1 Η συζήτηση γύρω από το θέμα (σπουδαιότητα)

Η Κοινή εξωτερική πολιτική και πολιτική ασφαλείας της ΕΕ (ΚΕΠΠΑ) έχει ως βασικό σκοπό την αποφυγή ή επίλυση διεθνών συγκρούσεων όπως επίσης και την προάσπιση της συνεργασίας της Ένωσης με άλλους παγκόσμιους οργανισμούς και κράτη. Ενσωματωμένες σε αυτόν τον ορισμό βρίσκονται και άλλες έννοιες, άρρηκτα συνδεδεμένες με την ΕΕ και τις αξίες που αυτή πρεσβεύει. Η διατήρηση της ειρήνης, η ενδυνάμωση της διεθνούς ασφάλειας, η δημοκρατία, το κράτος δικαίου, τα ανθρώπινα δικαιώματα και οι θεμελιώδεις ελευθερίες του ανθρώπου είναι μερικές από τις έννοιες που πρεσβεύει η ΕΕ μέσω της πολιτικής ασφαλείας της[1]. Για την διατήρηση όλων αυτών των χαρακτηριστικών της, η ΕΕ βασίζεται σε διεθνείς κανόνες συνεργασίας, στην διπλωματία και στον αλληλοσεβασμό μεταξύ των χωρών-μελών.

Το παγκόσμιο περιβάλλον ασφαλείας γίνεται ολοένα και πιο περίπλοκο και συνδέεται με όλο και περισσότερα νέο-εισαγόμενα χαρακτηριστικά της μοντέρνας εποχής. Νέες αντισυμβατικές απειλές για την ΕΕ και την ακεραιότητα της εμφανίζονται συνεχώς και ενισχύονται καθημερινά. Πέραν από τις ένοπλες συγκρούσεις και τους εμφυλίους πολέμους, παρατηρούμε πιά νέες μορφές πολέμου, όπως οι επιθέσεις στον κυβερνοχώρο (cyberattacks), οι υβριδικές απειλές (hybrid threats), η κυβερνοτρομοκρατία (cyberterrorism) και η παραπληροφόρηση. Η ασφάλεια λοιπόν αποκτά πια νέους ορισμούς και νέες πτυχές που δεν υπήρχαν πριν από μερικά χρόνια. Σε έναν κόσμο που όλα συνδέονται μεταξύ τους με μια ψηφιακή σφραγίδα, η ασφάλεια της ΕΕ έχει αποκτήσει πια και αποκεντρωμένο χαρακτήρα και εξαρτάται σε μεγάλο βαθμό από την ψηφιακή προστασία και τις υπηρεσίες κυβερνοασφάλειας που προσφέρει στα κράτη-μέλη της.

Πράγματι, σε μια περίοδο παγκόσμιας οικονομικής και κοινωνικής αστάθειας, η ΕΕ αναλαμβάνει ολοένα και μεγαλύτερη ευθύνη για την διατήρηση του επιπέδου ασφαλείας της και ταυτόχρονα να διευρύνει την ικανότητά της για αυτονομία σε τέτοιες ενέργειες. Αυτό βέβαια πάντα σε στενή συνεργασία με τα κράτη-μέλη, τα οποία πρέπει να συμμορφώνονται με τους κανόνες της ΕΕ. Εκτός όμως τα κράτη μέλη, σημαντικό ρόλο παίζουν και τα γεγονότα εκτός συνόρων της ΕΕ. Στον ταχέως αναπτυσσόμενο κόσμο, οι προκλήσεις ασφαλείας έχουν γίνει πολυδιάστατες και δύσκολες σε αντιμετώπιση. Τα κράτη-μέλη αδυνατούν να αντιμετωπίσουν τέτοιες προκλήσεις από μόνα τους. Ευθύνη λοιπόν της ΕΕ είναι να εκμηδενίσει αυτές τις απειλές για χάρη των κρατών-μελών και

[1] EUR-Lex. (2024). eur-lex.europa.eu. Ανάκτηση από european-union.europa.eu: https://eurlex.europa.eu/summary/chapter/foreign_and_security_policy.html?root_default=SUM_1_CODED%3D25&%3Blocale=el&locale=el

φυσικά για να διατηρήσει την ακεραιότητά της και την ασφαλή διαβίωση όλων των Ευρωπαίων πολιτών[2]. Η ασφάλεια είναι δικαίωμα όλων των πολιτών της ΕΕ και συμφέρον όλων των κρατών μελών. Και εφόσον πια η έννοια της ασφάλειας αποκτά μοντέρνες εκδοχές, όπως η Κυβερνοασφάλεια και οι υβριδικές απειλές, η ΕΕ οφείλει να δώσει προτεραιότητα σε αυτές.

Στην έκθεση της Ευρωπαϊκής Ένωσης του 2016 για την Παγκόσμια Στρατηγική, με τίτλο «Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy[3]» και μάλιστα από τον πρόλογο της τότε Υπάτου Εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας και Αντιπροέδρου της Ευρωπαϊκής Επιτροπής Federica Mogherini, γίνεται ξεκάθαρο πως ως προτεραιότητα της ΕΕ τίθεται η ασφάλεια της, με ειδική αναφορά στην Κυβερνοασφάλεια. Στην ενότητα «3: The Priorities of our External Action» και στην παράγραφο « Cyber Security» αναφέρεται:

> *Η ΕΕ θα αυξήσει την συγκέντρωσή της στην Κυβερνοασφάλεια, εξοπλίζοντας την ΕΕ και βοηθώντας τα κράτη μέλη να προστατεύσουν τον εαυτό τους από απειλές στον κυβερνοχώρο, ενώ θα διατηρεί ένα ανοιχτό, ελεύθερο και ασφαλή κυβερνοχώρο. Αυτό συνεπάγεται ενίσχυση των τεχνολογικών δυνατοτήτων που στοχεύουν στον μετριασμό των απειλών και την ανθεκτικότητα υποδομών, δικτύων και υπηρεσιών ζωτικής σημασίας και μείωση του εγκλήματος στον κυβερνοχώρο.*

Είναι κατανοητό λοιπόν πως υπάρχουν εδώ και αρκετά χρόνια εργασίες δημιουργίας προϋποθέσεων ασφαλείας και άμυνας για όλα τα κράτη-μέλη της ΕΕ και έχει ήδη σημειωθεί αρκετά μεγάλη πρόοδος. Τα προβλήματα όμως παραμένουν, μιας και υπάρχει μια συνεχής μετάλλαξη των απειλών που δέχεται η ΕΕ εκτός των συνόρων της και μια επίμονη αστάθεια εσωτερικά αλλά και στην άμεση γειτονία της. Πέραν αυτών των απειλών όμως, υπάρχουν και άλλες μεγάλες διαχρονικές προκλήσεις που επιβαρύνουν επιπλέον την κατάσταση. Η κλιματική αλλαγή, η ενεργειακή κρίση και οι έλλειψη ανθρωπιστικών επεμβάσεων σε μη-ανεπτυγμένες χώρες, είναι μερικά παραδείγματα προκλήσεων που αφορούν άμεσα τους τομείς δράσεως της Ένωσης και κατά συνέπεια καταλαμβάνουν πόρους που θα μπορούσαν να χρησιμοποιηθούν διαφορετικά, αν αυτά τα προβλήματα είχαν επιλυθεί σε νωρίτερο στάδιο[4]. Για να

---

[2]EEAS. (2024). EEAS - A Strategic Compass for Security and Defence. Ανάκτηση από www.eeas.europa.eu: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

[3]EEAS. (2016, June). Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign And Security Policy.

[4] EEAS. (2022, 12 07). EU Security, Defence and Crisis Response, A Security and Defence policy fit for the future.

μπορέσει λοιπόν η ΕΕ να αντιμετωπίσει όλα αυτά τα προβλήματα καθώς και τις απειλές ασφαλείας σε ένα συνεχώς μεταβαλλόμενο κοινωνικό και γεωπολιτικό περιβάλλον, χρειάζεται μια ισχυρή πολιτική ασφαλείας που να ενσωματώνει αποτελεσματικά και την αντιμετώπιση μοντέρνων απειλών και ιδιαιτέρως των απειλών στον κυβερνοχώρο της. Αυτό απαιτεί σίγουρα ενισχυμένες προσπάθειες και φυσικά μεγαλύτερο κεφάλαιο επενδύσεων σε καινοτόμες τεχνολογίες και καταρτισμένο προσωπικό.

Ο κόσμος αλλάζει και μαζί του αλλάζουν και τα δεδομένα της Κυβερνοασφάλειας. Η ανάγκη για συνεχή προσαρμογή στις διαρκείς αλλαγές στο παγκόσμιο τοπίο, ωθεί τους οργανισμούς, τις επιχειρήσεις αλλά και τους πολίτες, στην συνεχή πρόοδο στον τομέα της Κυβερνοασφάλειας, που φαίνεται να είναι ο μόνος τρόπος να παραμείνουμε μπροστά από τις εξελίξεις και να αποφύγουμε κινδύνους.

1.2 Σκοπός/στόχοι της εργασίας

Σκοπός της παρούσας εργασίας είναι να διερευνήσει το αν και κατά πόσο η ΕΕ μπορεί να είναι δρών ασφαλείας, σε ευρωπαϊκό και παγκόσμιο επίπεδο, όσον αφορά στην Κυβερνοασφάλεια. Για να γίνει αυτό, θα πρέπει πρώτα να γίνει περιγραφή βασικών εννοιών, όπως για παράδειγμα η έννοια του οικοσυστήματος ασφαλείας. Έτσι λοιπόν, σκοπός της εργασίας αυτής είναι επίσης να περιγράψει και να αξιολογήσει το οικοσύστημα Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης.

Επιπλέον, στην εργασία αυτή θα προσπαθήσουμε να αναγνωρίσουμε τα κενά που εμφανίζονται στην εφαρμογή και υλοποίηση της πολιτικής Κυβερνοασφάλειας της ΕΕ. Σημαντικό εδώ είναι να γίνει ξεκάθαρη η μέχρι σήμερα προσέγγιση της, ώστε να μπορέσουμε να εντοπίσουμε τα προβλήματα και να προτείνουμε βελτιώσεις για το μέλλον. Όπως αναφέραμε παραπάνω, οι μοντέρνες προκλήσεις και οι υβριδικές απειλές έχουν μετατοπίσει το περιβάλλον ασφαλείας σε χρήση περισσότερων τεχνολογικών καινοτομιών και συστημάτων και κατά συνέπεια κινούμαστε συνεχώς ένα βήμα πιο κοντά σε θέματα Κυβερνοασφάλειας παρά παραδοσιακής στρατιωτικής στρατηγικής. Είναι εξαιρετικά σημαντική πια η εφαρμογή νέας νομοθεσίας και η προσαρμογή των πολιτικών της ΕΕ στο νέο μεταβαλλόμενο και μοντέρνο περιβάλλον στο οποίο ζούμε σήμερα.

Πολύ σημαντικό ζήτημα στην παρούσα εργασία είναι επίσης να προβληματιστούμε για το μέλλον της ασφάλειας στο διαδίκτυο και να προτείνουμε δράσεις-λύσεις στα προβλήματα που σχετίζονται με αυτή. Ο ρόλος της ΕΕ στην ανάπτυξη άμεσων πολιτικών σχετικών με την Κυβερνοασφάλεια, είναι υψίστης σημασίας και κατά συνέπεια αποτελεί επίσης σκοπό και στόχο της εργασίας αυτής.

1.3 Μεθοδολογία

Σε αυτό το σημείο, θα πρέπει να ορίσουμε το θεωρητικό πλαίσιο, το που ακριβώς εντάσσεται δηλαδή η εργασία αυτή από άποψη βιβλιογραφίας. Η μεθοδολογία που θα ακολουθηθεί είναι η εξής:

- Έρευνα σε δευτερογενείς πηγές, κυρίως των Ευρωπαϊκών οργάνων και φορέων (Ευρωπαϊκή Επιτροπή, ENISA), όπου απαριθμούνται τα δεδομένα, προσδιορίζονται η αξιοπιστία και εγκυρότητα των πηγών αλλά και των ίδιων των δεδομένων και γίνεται συλλογή των χρήσιμων, για την εργασία, πληροφοριών.
- Ανάλυση δεδομένων, όπου καταχωρούνται τα δεδομένα σε ένα κείμενο και περιγράφονται με κάθε λεπτομέρεια ώστε να είναι κατανοητά, γίνεται έλεγχος των ερευνητικών υποθέσεων και τοποθετούνται όλα τα στοιχεία σε χρονολογική σειρά.
- Συσχέτιση δεδομένων, όπου τα δεδομένα που έχουν συλλεχθεί και αναλυθεί ενοποιούνται και συνδέονται μεταξύ τους.
- Συμπεράσματα, όπου γίνεται περίληψη όλων των δεδομένων που έχουν αναλυθεί και βγαίνουν λογικά αποτελέσματα από τα δεδομένα αυτά.

Στην περίπτωση της εργασίας μας λοιπόν, τα δεδομένα θα τα αναζητήσουμε από βιβλία και από το διαδίκτυο, από έγκυρες πηγές της ΕΕ και θα συλλεχθούν αυτά που είναι χρήσιμα, αυτά που σχετίζονται δηλαδή με την Κυβερνοασφάλεια ειδικότερα.

Επίσης, σημαντική πηγή βιβλιογραφίας είναι διάφορα συνέδρια σχετικού περιεχομένου (Cybersecurity skills - Building a cybersecurity workforce, Αθήνα, 20 Σεπτεμβρίου, EFTA cyberwarfare launch, cyberwarfare: international criminal justice in the 21st century, EFTA, Βρυξέλλες, 26 Οκτωβρίου, Cybersecurity research and innovation, needs and priorities, ENISA, Βρυξέλλες, 3 Νοεμβρίου, ENISA Cybersecurity Market Analysis Conference, ENISA, Βρυξέλλες, 23 Νοεμβρίου, 2022 CTI- EU Conference, ENISA, Βρυξέλλες, 7 Δεκεμβρίου, EU Cybersecurity Policy Conference, ENISA, 26 Ιανουαρίου), στα οποία παρουσιάστηκαν σημαντικά συμπεράσματα. Από τα συνέδρια αυτά αντλήσαμε λοιπόν πολλά συμπεράσματα αλλά και προτάσεις για το μέλλον, τα οποία και παρουσιάζουμε στην συνέχεια στην παρούσα εργασία.

Βασικός στόχος στην μεθοδολογία μας είναι να διερευνήσουμε το πόσο αποτελεσματικές είναι οι πολιτικές Κυβερνοασφάλειας της ΕΕ και σε τι ποσοστό έχει επιτευχθεί η εφαρμογή τους στα κράτη μέλη αλλά και τι επιρροή έχουν σε παγκόσμιο επίπεδο.

1.3.1 Το ερευνητικό ερώτημα

Τα βασικά ερευνητικά ερωτήματα, πάνω στα οποία βασίζεται η εργασία και τα οποία θα προσπαθήσουμε να απαντήσουμε, είναι τα εξής δύο:

1. Είναι η ΕΕ παγκόσμιος δρών ασφαλείας όσον αφορά στην Κυβερνοασφάλεια;
2. Είναι αποτελεσματικό το οικοσύστημα Κυβερνοασφάλειας της ΕΕ, και αν ναι, πως ακριβώς αξιολογούμε αυτήν την αποτελεσματικότητα;

Έχει δώσει η ΕΕ την αρμόζουσα σημασία στο θέμα της Κυβερνοασφάλειας ή υπάρχει ένα εμφανές κενό στην ασφάλεια που προσφέρει στην ίδια της την οργάνωση αλλά και στα κράτη-μέλη της; Συνδέεται άμεσα η Κυβερνοασφάλεια με τις πολιτικές ασφαλείας της ΕΕ ή αποτυγχάνει η ΕΕ να ενσωματώσει αποτελεσματικά την Κυβερνοασφάλεια στις πολιτικές της; Περιέχεται δηλαδή η έννοια των απειλών στον Κυβερνοχώρο στο πλαίσιο των πολιτικών ασφαλείας της ΕΕ γενικότερα ή αποσπά ελάχιστους ανεξάρτητους πόρους από τις πολιτικές ασφαλείας; Και αν δεν περιέχεται, υπάρχουν δράσεις και προσπάθειες διόρθωσης αυτού του φαινομένου;

1.3.2 Επισκόπηση βιβλιογραφίας/κριτική προσέγγιση/ διατύπωση σχολίων

Η βιβλιογραφία θα βασιστεί κυρίως σε άρθρα, δημοσιεύσεις και αναρτήσεις της Ευρωπαϊκής Ένωσης και των οργανισμών που συνεργάζονται με αυτήν ή είναι μέρος της. Παραδείγματα μερικών τέτοιων οργανισμών είναι: ENISA (The European Union Agency for Cybersecurity), CERT-EU (The Computer Emergency Response Team for the EU institutions, bodies and agencies), EEAS (The European External Action Service), EU Cyber Direct (EU Cyber Diplomacy Initiative) και EUISS (The European Union Institute for Security Studies). Οι οργανισμοί αυτοί δημοσιεύουν συχνά πρωτότυπες έρευνες και άρθρα που βοηθούν πολύ στην μελέτη θεμάτων σχετικών με την ασφάλεια και πιο συγκεκριμένα την Κυβερνοασφάλεια.

Επιπλέον, η ΕΕ δημοσιεύει ετήσιες εκθέσεις με θεματολογία σχετική με τον αντικείμενο έρευνας μας. Παραδείγματα τέτοιων εκθέσεων είναι τα: EU Global Strategy, Yearbook of European Security και Annual Report on Cybersecurity Research and Innovation Needs and Priorities. Όλα τα παραπάνω αποτελούν σημαντικά εργαλεία μελέτης και συνιστούν ένα μεγάλο μέρος της βιβλιογραφίας της εργασίας αυτής.

Υπάρχει βέβαια ένα εμφανές κενό στην εφαρμογή των πολιτικών της Ευρωπαϊκής Ένωσης σε θέματα Κυβερνοασφάλειας. Εν έτη 2023, ίσως δεν είναι απόλυτα ξεκάθαρη η άμεση ανάγκη περαιτέρω ανάπτυξης των πολιτικών Κυβερνοασφάλειας και θα έπρεπε οι πολιτικές ασφαλείας της ΕΕ να είναι μονίμως πια και άρρηκτα συνδεδεμένες με την έννοια της Κυβερνητικής και κάθε παράνομη ενέργεια κατά της ΕΕ να μεταφράζεται αυτόματα και σε προσπάθεια κυβερνοεγκλήματος (cybercrime) και σε πιο ακραίες

περιπτώσεις κυβερνοτρομοκρατίας (cyberterrorism). Δυστυχώς σήμερα δεν είναι τόσο κατανοητή η σχέση των δύο εννοιών, με αποτέλεσμα να υπάρχει συχνά καθυστέρηση στην αντιμετώπιση τέτοιων περιστατικών, όπως έχει αποδειχθεί πολλές φορές στο παρελθόν, όπως πρόσφατα με την περίπτωση της κυβερνοεπίθεσης στους μεγάλους ευρωπαϊκούς κόμβους διύλισης πετρελαίου Άμστερνταμ-Ρότερνταμ-Αμβέρσας τον Φεβρουάριο το 2022.

1.3.3 Το επιχείρημα της μελέτης/ Υποθέσεις εργασίας

Η εργασία θα βασιστεί σε δεδομένα που έχουν ήδη δημοσιευθεί από την ίδια την ΕΕ και κατά συνέπεια αποτελούν πραγματικά γεγονότα και παραδείγματα. Οι υποθέσεις δηλαδή που θα κάνουμε θα περιέχουν παραδείγματα με δεδομένα που έχουν συλλεχθεί από τις βάσεις δεδομένων της ΕΕ ή από άρθρα και δημοσιεύσεις της.

Η βασική υπόθεση εργασίας είναι πως ο τομέας της Κυβερνοασφάλειας, με ότι αυτή περιλαμβάνει, δεν είναι αρκετά συνυφασμένος με τον τομέα της ασφάλειας σε γενικό επίπεδο, της παραδοσιακής ασφάλειας όπως την ξέραμε πριν τις μοντέρνες απειλές και επιθέσεις. Αυτό είναι και το βασικό χαρακτηριστικό που θα προσπαθήσουμε να μελετήσουμε και εν τέλει να κρίνουμε εάν είναι αληθές ή ψευδές. Έπειτα, σε περίπτωση που βρεθεί πράγματι αυτό το κενό μεταξύ των δύο εννοιών, θα γίνει μια προσπάθεια προτάσεων βελτίωσης για το μέλλον.

1.3.4 Το θεωρητικό πλαίσιο και οι υποθέσεις εργασίας

Η Πολιτική ασφαλείας συνιστά αναπόσπαστο κομμάτι της εξωτερικής πολιτικής της ΕΕ. Με ένα μεγάλο σύνολο στρατιωτικών, κυρίως, αλλά και μη-στρατιωτικών δράσεων, η ΕΕ συμβάλλει σταθερά από την ίδρυση της στην Ευρωπαϊκή αλλά και παγκόσμια σταθερότητα. Δεν θα ήταν υπερβολή να πούμε ότι η πολιτικές ασφαλείας της ΕΕ έχουν παίξει επανειλημμένα στο παρελθόν ρόλο ζωτικής σημασίας σε παγκόσμιες προκλήσεις και μάλιστα σε περίοδο αναταραχών παγκοσμίου επιπέδου. Δεν είναι τυχαίο άλλωστε πως ένα από τα θεμελιώδη χαρακτηριστικά της Ένωσης είναι η διατήρηση της ειρήνης για όλους τους πολίτες της.

Μεγάλο μέρος της ζωής μας πια είναι στο διαδίκτυο. Τα τελευταία χρόνια έχει γίνει μια έντονη στροφή στον ψηφιακό κόσμο και πια πολλές από τις καθημερινές μας ενέργειες λαμβάνουν χώρα στο ίντερνετ. Εκτός όμως από απλές καθημερινές ασχολίες, ο ψηφιακός κόσμος κρύβει και απειλές με την μορφή κυβερνοεπιθέσεων. Ιδιαίτερα κατά την διάρκεια της πανδημίας, που αυξήθηκε η χρήση των ηλεκτρονικών υπηρεσιών, οι προκλήσεις αυξήθηκαν επίσης, με αποτέλεσμα η ΕΕ να καλείτε πια να αντιμετωπίσει μεγάλο αριθμό απειλών. Οι πολιτικές Κυβερνοασφάλειας της ΕΕ έχουν ως πρωταρχικό στόχο την ενίσχυση της συλλογικής ασφάλειας στον κυβερνοχώρο και τον εκμηδενισμό των κυβερνοεπιθέσεων.

Με μια πρώτη ματιά, οι δυο παραπάνω παράγραφοι ίσως να φαίνεται πως έχουν όμοιες αιτίες, όμοιες διαδικασίες και όμοια αποτελέσματα. Είναι όμως πράγματι έτσι; Είναι και οι δύο παραπάνω έννοιες όμοιες για την ΕΕ και τις πολιτικές της ή διαφέρουν σε όλα τα σημεία; Έχει η ΕΕ ίδιους τρόπους επίλυσης ή δίνει την ίδια σημασία και στα δύο; Καλούμαστε σε αυτήν την εργασία λοιπόν να βρούμε το κατά πόσο εφαρμόζονται στην πραγματικότητα οι πολιτικές Κυβερνοασφάλειας της ΕΕ και αν είναι αρκετές οι δράσεις σχετικά με την μοντέρνα έννοια της Κυβερνοασφάλειας.

1.3.5 Αναζήτηση πρωτογενών/δευτερογενών πηγών/στοιχείων/

Πρωτογενείς πηγές αποτελούν τα βιβλία, οι ιστοσελίδες, οι δημοσιεύσεις και τα άρθρα της ΕΕ και των οργάνων που συνεργάζονται με την ΕΕ ή είναι μέρος της. Επίσης, άρθρα συνεδρίων που έχουν πραγματοποιηθεί με θέμα την ασφάλεια-κυβερνοασφάλεια αποτελούν επίσης πρωτογενή πηγή.

Δευτερογενείς πηγές είναι έρευνες, δημοσιεύσεις, άρθρα και εκθέσεις ανεξάρτητων της ΕΕ ομάδων είτε ατόμων, που μελετούν το θέμα και δημοσιεύουν σχετικές πληροφορίες.

1.3.6 Τρόπος ανάλυσης

Θα γίνει συλλογή δεδομένων από βάσεις δεδομένων(π.χ. EUIPO: European Union Intellectual Property Office[5]).

Επίσης, θα χρησιμοποιηθούν εργαλεία που είναι ελεύθερα προς χρήση για όλους διαδικτυακά. Για παράδειγμα, μερικά από αυτά τα εργαλεία είναι:

- ENISA - EU Cybersecurity Institutional Map[6], ένας χάρτης που δημιούργησε η ENISA για να μπορούμε να μελετήσουμε όλα τα όργανα/οργανισμούς/οντότητες που έχουν συμμετοχή σε θέματα cybersecurity στον Ευρωπαϊκό χώρο, καθώς και τις συνδέσεις/επαφές μεταξύ τους (τα μονοπάτια επικοινωνίας τους), τον τρόπο λειτουργίας τους και τις κοινότητες που δημιουργούν, με περιγραφή και επεξήγηση για το καθένα.
- National Cybersecurity Strategies Evaluation Tool[7], επίσης ένα εργαλείο που δημιούργησε η ENISA για να βοηθήσει τα κράτη μέλη να αξιολογήσουν τις

[5]Euipo. (2024). European Union Intellectual Property Office. Ανάκτηση από https://www.euipo.europa.eu/en

[6]ENISA. (2024). Ανάκτηση από Enisa - Cybersecurity institutional map: https://www.enisa.europa.eu/login?came_from=/cybersecurity-institutional-map/results%3Froot%3Dactors

[7]ENISA. (2024). National Cybersecurity Strategies Evaluation Tool. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

στρατηγικές προτεραιότητες και τους στόχους τους που σχετίζονται με τις εθνικές στρατηγικές για την ασφάλεια στον κυβερνοχώρο.

- Cyber Diplomacy Atlas[8], που χρησιμεύει ως ένας ενιαίος διαδικτυακός χώρος για πηγές και αναλύσεις σχετικά με τις πολιτικές μεμονωμένων χωρών, περιοχών και οργανισμών.

Με βάση αυτές τις πηγές και τα εργαλεία, ο τρόπος ανάλυσης της εργασίας θα είναι ποιοτικός και επεξηγηματικός ως προς το περιεχόμενο.

[8] EU-CYBER-DIRECT. (2024). Cyber Diplomacy Atlas. Ανάκτηση από https://eucyberdirect.eu/: https://eucyberdirect.eu/atlas

Κεφάλαιο 2ο: Θεωρητικό πλαίσιο

2.1 Ορισμός έννοιας "Οικοσύστημα"

Στην ευρύτερη έννοια, ένα "οικοσύστημα" αναφέρεται σε ένα πολύπλοκο δίκτυο ή σύστημα αλληλεπίδρασης που αποτελείται από διάφορα στοιχεία, οντότητες ή συστατικά που αλληλοεπιδρούν και επηρεάζουν το ένα το άλλο εντός ενός συγκεκριμένου πεδίου ή πλαισίου[9]. Το οικοσύστημα περιλαμβάνει τις σχέσεις, τη δυναμική και τις εξαρτήσεις μεταξύ αυτών των στοιχείων, συμβάλλοντας στη συνολική λειτουργία και βιωσιμότητα του συστήματος[10].

Ουσιαστικά, ένα οικοσύστημα ενσωματώνει την αλληλεπίδραση και την αλληλεξάρτηση διαφορετικών οντοτήτων ή παραγόντων, που συχνά χαρακτηρίζονται από αμοιβαίες εξαρτήσεις, κύκλους ανατροφοδότησης και κοινές ιδιότητες. Ένα οικοσύστημα μπορεί να εκδηλωθεί σε διάφορους τομείς, όπως η τεχνολογία, οι επιχειρήσεις, η οικονομία ή οι κοινωνικοί τομείς, όπου πολλοί φορείς, πόροι και διαδικασίες αλληλοεπιδρούν και συνυπάρχουν σε ένα κοινό περιβάλλον.

Συνοπτικά, ένα οικοσύστημα αντιπροσωπεύει ένα δυναμικό και αλληλένδετο σύστημα που αποτελείται από ποικίλες οντότητες που αλληλοεπιδρούν και επηρεάζουν η μια την άλλη, βοηθώντας την λειτουργία, την πολυπλοκότητα και την προσαρμοστικότητα του συνόλου αυτού.

2.2 Ορισμός έννοιας "Οικοσύστημα Ασφαλείας"

Στο πλαίσιο της κυβερνοασφάλειας, ένα "οικοσύστημα κυβερνοασφάλειας" αναφέρεται σε ένα δυναμικό και αλληλένδετο δίκτυο παραγόντων, τεχνολογιών, πολιτικών και γενικότερα διαδικασιών που αλληλοεπιδρούν και συνεργάζονται μεταξύ τους για την αντιμετώπιση των κυβερνοαπειλών, την προστασία της ψηφιακής περιουσίας και τη διασφάλιση της ανθεκτικότητας των ψηφιακών συστημάτων και υποδομών[11].

Ένα τέτοιο οικοσύστημα περιλαμβάνει διάφορους φορείς ενδιαφέροντος, συμπεριλαμβανομένων κυβερνητικών οργάνων, ιδιωτικών επιχειρήσεων, ακαδημαϊκών ιδρυμάτων, ειδικών σε θέματα κυβερνοασφάλειας και ατομικών χρηστών, με τον καθένα από αυτούς να έχει διακριτό ρόλο στις διάφορες προσπάθειες διασφάλισης της κυβερνοασφάλειας. Επίσης, περιλαμβάνει μια ευρεία γκάμα τεχνολογιών, εργαλείων

[9] Odum, E. P. (1983). "Systems ecology: An introduction." Wiley.
[10] Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). "Resilience, adaptability and transformability in social–ecological systems." Ecology and Society, 9(2), 5.
[11] Schneider, F., & Von Solms, R. (2012). "Strategic information security: A comprehensive cyber security ecosystem.

και μεθοδολογιών με σκοπό την ανίχνευση, πρόληψη και αντιμετώπιση των κυβερνοεπιθέσεων και ευπαθειών[12].

Άλλα βασικά συστατικά ενός οικοσυστήματος κυβερνοασφάλειας είναι μηχανισμοί κοινοποίησης πληροφοριών, διαδικασίες συνεργασίας, πλατφόρμες πληροφοριών για απειλές, πρωτόκολλα αντιμετώπισης περιστατικών, νομοθετικά πλαίσια και προγράμματα ευαισθητοποίησης και εκπαίδευσης για την κυβερνοασφάλεια[13]. Αυτά τα στοιχεία αλληλοεπιδρούν μεταξύ τους για τη διευκόλυνση συντονισμένων αντιδράσεων σε κυβερνοαπειλές, την προώθηση βέλτιστων πρακτικών και την ενίσχυση του ασφαλούς κυβερνοπεριβάλλοντος.

2.3 Ορισμός έννοιας “Δρών κυβερνοασφάλειας”

Ο όρος "Δρών κυβερνοασφάλειας" αναφέρεται σε οποιαδήποτε οντότητα, είτε αυτή είναι ένα κράτος, μια οργάνωση, μια ομάδα ή ένα άτομο, που εμπλέκεται ενεργά σε κυβερνοδραστηριότητες, συμπεριλαμβανομένων, αλλά όχι περιοριστικά, της κυβερνοάμυνας, των κυβερνοεπιθέσεων, της κυβερνοκατασκοπείας και του κυβερνοεγκλήματος[14]. Αυτοί οι παράγοντες μπορούν να έχουν ποικίλα επίπεδα προθέσεων και επιρροής στο τοπίο κυβερνοασφάλειας.

Η μέτρηση των δρώντων κυβερνοασφάλειας παγκοσμίως περιλαμβάνει την αξιολόγηση αρκετών κύριων παραγόντων[15]:

1. Ικανότητες: Αυτό περιλαμβάνει τεχνική κατάρτιση, πόρους, υποδομές και εργαλεία που διατίθενται στον δρώντα για την πραγματοποίηση κυβερνοεπιχειρήσεων. Υψηλότερες ικανότητες συνήθως σημαίνουν και μεγαλύτερο δυναμικό για κυβερνοεπιθέσεις ή ικανότητες κυβερνοάμυνας.

2. Προθέσεις: Η κατανόηση των κινήτρων και των στόχων των δρώντων κυβερνοασφάλειας είναι κρίσιμη για την αξιολόγηση της συμπεριφοράς τους στον κυβερνοχώρο. Μερικοί παράγοντες μπορεί να επιδιώκουν την προστασία των δικών τους δικτύων (κυβερνοαμυντικοί παράγοντες), ενώ άλλοι μπορεί να ασχολούνται με επιθέσεις , όπως η κατασκοπεία, η αμυντική επίθεση ή ο κυβερνοπόλεμος.

[12] Rosenzweig, P., & Metzger, J. (2014). "Cybersecurity and Cyberwar: What Everyone Needs to Know

[13] Sullivan, B. J., & Goodman, M. S. (2019). "Cybersecurity Ventures

[14] Johnson, T., & Williams, A. (2019). "Understanding Cybersecurity Actors: Motivations, Tactics, and Implications." In Cybersecurity Handbook. Chapter 5: Cybersecurity Actors and Their Behavior, pp. 92-115

[15] Miller, P., & White, S. (2020). "Strengthening Global Cybersecurity Cooperation: Strategies and Best Practices." In Global Governance and Cybersecurity. Chapter 11: Global Cybersecurity Cooperation, pp. 250-273

3. Δραστηριότητες: Η ανάλυση των τύπων και της συχνότητας των κυβερνοδραστηριοτήτων που πραγματοποιούν οι δρώντες, όπως κυβερνοεπιθέσεις, ή διαρροές δεδομένων, παρέχει ενδείξεις για τη συμπεριφορά τους και την επίδρασή τους στην παγκόσμια κυβερνοασφάλεια.

Οι δρώντες κυβερνοασφάλειας παίζουν ένα σημαντικό ρόλο στην διαμόρφωση του τοπίου κυβερνοασφάλειας παγκοσμίως[16]:

1. Τοπίο απειλών: Οι δρώντες κυβερνοασφάλειας συνεισφέρουν στην διαμόρφωση του τοπίου απειλών, αναπτύσσοντας και εφαρμόζοντας νέες τεχνικές επιθέσεων, όπως για παράδειγμα το κακόβουλο λογισμικό. Οι δραστηριότητές τους αποτελούν κίνδυνο για τις κρίσιμες υποδομές, την εθνική ασφάλεια, την οικονομική σταθερότητα και το ατομικό απόρρητο σε παγκόσμιο επίπεδο.

2. Διεθνείς Σχέσεις: Οι δρώντες κυβερνοασφάλειας, ιδίως τα κράτη, εμπλέκονται σε κυβερνοεπιχειρήσεις που μπορεί να έχουν διπλωματικές, πολιτικές και οικονομικές επιπτώσεις, επηρεάζοντας τις διεθνείς σχέσεις και τη γεωπολιτική δυναμική. Οι κυβερνοεπιθέσεις μπορεί να οδηγήσουν σε ένταση, συγκρούσεις ή συνεργασία μεταξύ των εθνών.

3. Οικονομική Επίδραση: Οι κυβερνοεπιθέσεις και το κυβερνοέγκλημα μπορεί να οδηγήσουν σε οικονομικές απώλειες, κλοπή πνευματικής ιδιοκτησίας, διαταραχή της λειτουργίας των επιχειρήσεων και ζημιές στο κύρος και την φήμη επιχειρήσεων και ανθρώπων σε παγκόσμιο επίπεδο.

4. Συνεργασία για την Ασφάλεια: Η συνεργασία μεταξύ δρώντων κυβερνοασφάλειας, συμπεριλαμβανομένων κυβερνήσεων, ενδιαφερόμενων φορέων της βιομηχανίας, της ακαδημαϊκής κοινότητας και διεθνών οργανισμών, είναι απαραίτητη για την αντιμετώπιση κοινών κυβερνοαπειλών, την κοινοποίηση πληροφοριών για απειλές, την ανάπτυξη κανόνων και προτύπων, και την ενίσχυση των συλλογικών δυνατοτήτων κυβερνοασφάλειας.

Οι δρώντες κυβερνοασφάλειας συνεισφέρουν στην ανάπτυξη νέων μεθόδων ασφαλείας, στην καθιέρωση βέλτιστων πρακτικών και στην ενίσχυση των ικανοτήτων αντίδρασης σε κυβερνοεπιθέσεις. Η συνεχής και συντονισμένη προσπάθεια συμβάλλει στην αύξηση της ανθεκτικότητας του περιβάλλοντος κυβερνοασφάλειας και στη μείωση των κυβερνοαπειλών σε παγκόσμιο επίπεδο.

[16] Garcia, L., & Lee, J. (2021). "Cybersecurity and Geopolitics: Shaping the International Landscape." In International Relations in the Digital Age. Chapter 7: Cybersecurity in International Relations, pp. 145-168

Καταληκτικά, οι δρώντες κυβερνοασφάλειας σε παγκόσμιο επίπεδο περιλαμβάνουν μια ποικιλία ενεργειών που έχουν σημαντικές επιπτώσεις στο τοπίο κυβερνοασφάλειας, τις διεθνείς σχέσεις, την οικονομική σταθερότητα και την κοινωνική ευημερία[17]. Η κατανόηση και η αποτελεσματική ανταπόκριση στη συμπεριφορά των παραγόντων κυβερνοασφάλειας απαιτεί εκτενή ανάλυση, συνεργασία και συντονισμό μεταξύ των ενδιαφερόμενων φορέων σε εθνικό και διεθνές επίπεδο.

2.4 Διάφοροι τύποι διεθνών Δρώντων Κυβερνοασφάλειας

Παρακάτω ακολουθούν οι διάφοροι τύποι διεθνών δρώντων κυβερνοασφάλειας[18]:

1. Εθνικά Κράτη: Τα εθνικά κράτη είναι σημαντικοί παράγοντες στη διεθνή κυβερνοασφάλεια λόγω των πόρων, των ικανοτήτων και των στρατηγικών συμφερόντων τους. Εμπλέκονται σε κυβερνοεπιχειρήσεις για διάφορους σκοπούς, συμπεριλαμβανομένης της συλλογής πληροφοριών, της κυβερνοάμυνας και ενδεχομένως επιθετικών ενεργειών. Ορισμένα κράτη έχουν δημιουργήσει μονάδες ή οργανισμούς, υπεύθυνους για την διατήρηση της ασφάλειας του κυβερνοχώρου τους.

2. Μη-Κρατικοί Παράγοντες: Οι μη-κρατικοί παράγοντες περιλαμβάνουν μια ποικιλία εννοιών, όπως τρομοκρατικές οργανώσεις, ομάδες hacktivists, εγκληματικές ή μή συνδικαλιστικές οργανώσεις και ιδιωτικές εταιρείες κυβερνοασφάλειας. Αυτοί οι παράγοντες μπορεί να πραγματοποιούν κυβερνοεπιθέσεις για ιδεολογικούς, οικονομικούς ή πολιτικούς λόγους. Για παράδειγμα, οι ομάδες hacktivist ενδέχεται να στοχοποιούν κυβερνητικά θεσμικά όργανα ή εταιρείες για να διαμαρτυρηθούν ή να ευαισθητοποιήσουν για κοινωνικά ή πολιτικά ζητήματα.

3. Διεθνείς Οργανισμοί: Διεθνείς οργανισμοί όπως τα Ηνωμένα Έθνη (ΗΕ), το ΝΑΤΟ και η Ευρωπαϊκή Ένωση (ΕΕ) παίζουν ρόλο στον καθορισμό διεθνών κανόνων κυβερνοασφάλειας, προτύπων και συνεργασίας. Διευκολύνουν διπλωματικούς διαλόγους, προωθούν πρωτοβουλίες ενίσχυσης της κυβερνοασφάλειας και αναπτύσσουν πλαίσια για την κυβερνοάμυνα και την αντιμετώπιση περιστατικών σε παγκόσμιο επίπεδο.

4. Πολυεθνικές Εταιρείες: Οι πολυεθνικές εταιρείες λειτουργούν χωρίς συγκεκριμένα σύνορα και διαθέτουν σημαντικά δεδομένα και υποδομές που είναι ευαίσθητα στις

[17] Smith, D., & Brown, K. (2018). "Economic Consequences of Cyber Threats: Challenges and Opportunities." In The Economics of Cybersecurity. Chapter 9: Economic Impacts of Cybersecurity, pp. 200-223

[18] Johnson, T., & Williams, A. (2019). "Understanding Cybersecurity Actors: Motivations, Tactics, and Implications." In Cybersecurity Handbook, Chapter 7: Cybersecurity Actors in the International Arena

κυβερνοαπειλές. Αυτές οι εταιρείες επενδύουν σε μέτρα κυβερνοασφάλειας για την προστασία των υποδομών τους, τη συμμόρφωση με τη νομοθεσία και τη διατήρηση της εμπιστοσύνης με πελάτες και άλλα ενδιαφερόμενα μέρη. Επιπλέον, συμβάλλουν στην έρευνα, την καινοτομία και την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια.

5. Ιδρύματα Έρευνας και Ακαδημαϊκά Ιδρύματα για την Κυβερνοασφάλεια: Τα ιδρύματα έρευνας και τα πανεπιστημιακά ιδρύματα παίζουν κρίσιμο ρόλο στην προαγωγή της γνώσης, των τεχνολογιών και των πολιτικών κυβερνοασφάλειας. Διεξάγουν έρευνα για νέες πιθανές κυβερνοαπειλές, αναπτύσσουν λύσεις σχετικές με την κυβερνοασφάλεια και παρέχουν τεχνογνωσία σε κυβερνήσεις, επιχειρήσεις και διεθνείς οργανισμούς. Η συνεργασία μεταξύ των πανεπιστημίων και της βιομηχανίας είναι απαραίτητη για την αντιμετώπιση των πολύπλοκων προκλήσεων στον τομέα της κυβερνοασφάλειας.

6. Διάφοροι άλλοι μηχανισμοί/οργανώσεις και κοινωνικά όργανα: Οι κοινωνικοί οργανισμοί, συμπεριλαμβανομένων των ομάδων υπεράσπισης των ανθρωπίνων δικαιωμάτων ή οργανώσεων της κοινωνίας των πολιτών, υποστηρίζουν πολιτικές κυβερνοασφάλειας με προτεραιότητα στην ψηφιακή ελευθερία. Ενημερώνουν τους πολίτες για τις κυβερνοαπειλές, προωθούν την ενίσχυση των κανονισμών κυβερνοασφάλειας και παρακολουθούν τις κυβερνητικές ενέργειες σχετικά με την κυβερνοασφάλεια.

Αυτοί οι διάφοροι τύποι διεθνών δρώντων κυβερνοασφάλειας αλληλοεπιδρούν σε ένα πολύπλοκο οικοσύστημα, διαμορφώνοντας το παγκόσμιο τοπίο και επηρεάζοντας πολιτικές, πρακτικές και πρότυπα που ορίζουν συχνά τον κυβερνοχώρο. Η κατανόηση των ρόλων, των κινήτρων και των ικανοτήτων αυτών των παραγόντων είναι ζωτικής σημασίας για την αποτελεσματική διακυβέρνηση της κυβερνοασφάλειας και τη συνεργασία σε διεθνές επίπεδο.

2.5 Κριτήρια με τα οποία θα μπορούσε μια χώρα ή μια Ένωση Χωρών να χαρακτηριστεί ή όχι ως “δρών ασφαλείας”.

Η αξιολόγηση μιας χώρας ή μιας ένωσης χωρών ως παγκόσμιου παράγοντα στον τομέα της κυβερνοασφάλειας απαιτεί την εξέταση διαφόρων παραμέτρων και δράσεων που υποδηλώνουν την ικανότητά της να αντιμετωπίζει και να διαχειρίζεται τις κυβερνοαπειλές τόσο σε εσωτερικό όσο και σε διεθνές επίπεδο. Ένα από τα κύρια κριτήρια είναι η ανάπτυξη και η εφαρμογή αποτελεσματικών πολιτικών και στρατηγικών κυβερνοασφάλειας που να προστατεύουν τα συστήματα πληροφορικής και

επικοινωνιών της χώρας ή της ένωσης χωρών[19]. Αυτό περιλαμβάνει την εφαρμογή τεχνικών μέτρων ασφαλείας, την εκπαίδευση και ευαισθητοποίηση των πολιτών και των επιχειρήσεων σχετικά με τις κυβερνοαπειλές, καθώς και την ανάπτυξη κοινών προτύπων και πρακτικών σε εθνικό επίπεδο.

Εκτός από την εσωτερική δράση, η συμμετοχή σε διεθνείς δράσεις και φόρα αποτελεί σημαντικό κριτήριο για την αξιολόγηση του παγκόσμιου ρόλου μιας χώρας ή μιας ένωσης στον τομέα της κυβερνοασφάλειας. Αυτό περιλαμβάνει τη συμμετοχή σε διαπραγματεύσεις για διεθνείς συμφωνίες και κανονισμούς σχετικά με την κυβερνοασφάλεια, την υποστήριξη διεθνών πρωτοβουλιών για την ανάπτυξη κοινών προτύπων και την προώθηση της διακρατικής συνεργασίας για την αντιμετώπιση κοινών απειλών.

Τέλος, η ικανότητα να συνεργάζεται με άλλες χώρες και ομάδες χωρών είναι σημαντική για τον παγκόσμιο ρόλο της σε αυτόν τον τομέα. Η διαδικασία διαμερισμού πληροφοριών και εμπειρογνωμοσύνης, καθώς και η ανάπτυξη κοινών προγραμμάτων και πρωτοβουλιών για την ενίσχυση της κυβερνοασφάλειας παγκοσμίως, αποτελούν σημαντικούς παράγοντες για την αναγνώριση μιας χώρας ή μιας ένωσης ως παγκόσμιου παράγοντα κυβερνοασφάλειας.

[19] Cybersecurity and Infrastructure Security Agency (CISA). (2020). National Cyber Strategy of USA. Washington, D.C.: CISA.

Κεφάλαιο 3ο: Οι σύγχρονες προκλήσεις στην Κυβερνοασφάλεια

3.1 Κυβερνοπροκλήσεις

Ο αριθμός των κυβερνοπροκλήσεων βρίσκεται συνεχώς σε αύξηση και ενισχύεται καθημερινά από threat actors που έχουν ως σκοπό να προκαλέσουν προβλήματα (malware) στις οντότητες απέναντι στις οποίες στρέφονται[20]. Threat actors μπορούν να χαρακτηριστούν διάφοροι δρώντες που επηρεάζουν το περιβάλλον της Κυβερνοασφάλειας, αλλά πολλές φορές υπάρχει μια σύγχυση σχετικά με τον τρόπο που ορίζονται και τις διάφορες μορφές τους. Είναι σημαντικό λοιπόν να προσδιορίσουμε τους διαφορετικούς ορισμούς που υπάρχουν σχετικά με τους δρώντες Κυβερνοασφάλειας και να κατανοήσουμε τις διαφορές ή και τις ομοιότητες. Οι βασικές 3 κατηγορίες τέτοιων δρώντων είναι οι εξής: threat actors, hackers, attackers. Πρόκειται για 3 όμοιες αλλά ταυτόχρονα διαφορετικές έννοιες, που συχνά προκαλούν σύγχυση.

3.1.1 Threat Actor

Threat actor[21] (δρών απειλής): ένας παράγοντας απειλής, που ονομάζεται επίσης κακόβουλος παράγοντας, είναι μια οντότητα που είναι εν μέρει ή εξ ολοκλήρου υπεύθυνη για ένα συμβάν ασφαλείας που επηρεάζει –ή μπορεί να επηρεάσει– την ασφάλεια ενός οργανισμού.

3.1.2 Hacker

Hacker: ενώ αυτός ο όρος αρχικά αναφερόταν σε έναν έξυπνο ή έμπειρο προγραμματιστή, τώρα χρησιμοποιείται για κάποιον που μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε άλλους υπολογιστές. Ένας χάκερ μπορεί να "χακάρει" τα επίπεδα ασφαλείας ενός συστήματος υπολογιστών ή ενός δικτύου. Αυτό μπορεί να είναι κάτι απλό, όπως το να βρει τον κωδικό πρόσβασης κάποιου άλλου ή περίπλοκο, όπως το να γράψει ένα προσαρμοσμένο πρόγραμμα για να σπάσει το λογισμικό ασφαλείας άλλου υπολογιστή.

3.1.3 Attacker

Attacker: Κυβερνοεπίθεση είναι κάθε επιθετικός ελιγμός που στοχεύει συστήματα πληροφοριών υπολογιστών, δίκτυα υπολογιστών, υποδομές ή συσκευές προσωπικών υπολογιστών. Ένας attacker είναι ένα άτομο ή μια διαδικασία που επιχειρεί να αποκτήσει πρόσβαση σε δεδομένα, λειτουργίες ή άλλες περιορισμένες περιοχές του συστήματος χωρίς εξουσιοδότηση, ενδεχομένως με κακόβουλη πρόθεση. Έτσι, ένας

[20] Liaropoulos, A. N. (2017). Cyberspace Governance & State Sovereignty. Στο G. C. Bitros, & N. C. Kyriazis, Democracy and an Open-Economy World Order (σσ. 25–35). Heidelberg: Springer.

[21] Crowdstrike. (2024). Threat Actor. Ανάκτηση από www.crowdstrike.com: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/threat-actor/

attacker είναι το άτομο ή ο οργανισμός που εκτελεί αυτές τις κακόβουλες δραστηριότητες, ανεξάρτητα από τη μέθοδο που χρησιμοποιείται[22].

3.2 Μοντέρνες Κυβερνοπροκλήσεις

Έχοντας λοιπόν κατανοήσει τους δρώντες απειλής, μπορούμε να συνεχίσουμε και στον προσδιορισμό των προκλήσεων που δημιουργούνται στο κυβερνοχώρο, με πιθανή προέλευση τις προσπάθειες των δρώντων αυτών[23]. Ιδιαίτερα κατά την διάρκεια της πανδημίας του Covid-19, μια περίοδο που υποχρεωτικά όλοι παρέμειναν κλεισμένοι στα σπίτια τους, ένας μεγάλος αριθμός ανθρώπων χρησιμοποίησε σε ακόμα μεγαλύτερη καθημερινή βάση το διαδίκτυο με αποτέλεσμα να αυξηθούν και οι κυβερνοεπιθέσεις και ως επί το πλείστο οι μορφές κυβερνοπροκλήσεων. Για παράδειγμα, αναφέρουμε τις εξής:

Πίνακας 1: Μοντέρνες προκλήσεις στον Κυβερνοχώρο

Μοντέρνες προκλήσεις στον Κυβερνοχώρο(ιδιαιτέρως μετά τον Covid-19)[24]:
● *Γεωπολιτικός ανταγωνισμός για τον κυβερνοχώρο.*
● *Μεγάλη αύξηση του εγκλήματος στον κυβερνοχώρο*
● *Ασφάλεια εφοδιαστικής αλυσίδας(Supply chain security) π.χ. 5G*
● *Επεκτεινόμενη επιφάνεια επιθέσεων π.χ. IoT, νοσοκομεία, διανομή εμβολίου*
● *Απειλή από τους κβαντικούς υπολογιστές σχετικά με τα κρυπτονομίσματα*
● *Η έλευση του AI*
● *Έλλειψη δεξιοτήτων, έλλειψη εστίασης σε τεχνικές δεξιότητες ή άσχετες με το θέμα ανθρώπινες δεξιότητες όπως η οργάνωση*
● *Capacity building, ανθεκτικότητα*
● *Ευπάθεια/Τρωτότητα μικρότερων οργανισμών, SMEs*
● *Κοινή χρήση πληροφοριών, κοινή ανάλυση και γρήγορη απόκριση*

[22] Liaropoulos, A. N., Kontrafouri, C., & Zampati, M. (2020). Η επίδραση των κυβερνοεπιθέσεων στην κυβερνοασφάλεια. Κείμενο Εργασίας, Εργαστήρι Πληροφόρησης & Κυβερνοασφάλειας.
[23] Liaropoulos, A. N. (2020). A Social Contract for Cyberspace, Journal of Information Warfare, vol.19, no.2. Journal of Information Warfare.
[24] European-Commission. (2021). The Digital Economy and Society Index (DESI). Ανάκτηση από commission.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/desi

• *Εμπορευματοποίηση έρευνας και ανάπτυξης*
• *Απορρόφηση/Εκμετάλλευση*
• *Ενιαία αγορά*
• *Διπλή (Dual) χρήση*

Ο ENISA (Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών) μάλιστα, εξέδωσε στις 11 Νοεμβρίου 2022 ένα γράφημα πληροφοριών σχετικά με τις κύριες αναδυόμενες προκλήσεις του κυβερνοχώρου για το 2030, οι οποίες φαίνονται στην Εικόνα 1.

Εικόνα 1: Οι 10 αναδυόμενες προκλήσεις Κυβερνοασφάλειας για το 2030

Πηγή: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Οι 10 κυριότερες αναδυόμενες προκλήσεις Κυβερνοασφάλειας για το 2030, με βάση το γράφημα πληροφοριών του ENISA:

- *Απειλή της εφοδιαστικής αλυσίδας των εξαρτήσεων λογισμικού*
- *Προηγμένες καμπάνιες παραπληροφόρησης*
- *Άνοδος αυταρχισμού ψηφιακής επιτήρησης/απώλεια ιδιωτικότητας*
- *Ανθρώπινο λάθος και συστήματα εκμετάλλευσης παλαιού τύπου εντός κυβερνο-φυσικών οικοσυστημάτων (cyber-physical ecosystems)*
- *Στοχευμένες επιθέσεις ενισχυμένες με δεδομένα έξυπνων συσκευών*
- *Έλλειψη ανάλυσης και ελέγχου διαστημικών υποδομών και αντικειμένων*
- *Άνοδος προηγμένων υβριδικών απειλών*
- *Έλλειψη δεξιοτήτων*

- *Οι διασυνοριακοί πάροχοι υπηρεσιών ICT ως ενιαίο σημείο αποτυχίας*
- *Κατάχρηση τεχνητής νοημοσύνης*

Εικόνα 2: Μια ενδιαφέρουσα αναπαράσταση του "διαστήματος" Κυβερνοπροκλήσεων.

Πηγή: https://fortresssrm.com/the-cyber-threat-universe/

3.3 Η Κυβερνοασφάλεια στο διεθνές σύστημα δικαιοσύνης

Η EFTA (European Free Trade Association), δηλαδή η Ευρωπαϊκή Ζώνη Ελευθέρων Συναλλαγών είναι ένας οργανισμός με έτος ίδρυσης το 1960 ο οποίος ιδρύθηκε από ευρωπαϊκά κράτη τα οποία δεν ήθελαν να μπουν εξολοκλήρου στην Ευρωπαϊκή Οικονομική Κοινότητα. Στόχος αυτών των χωρών με την ίδρυση της EFTA ήταν να

προωθήσουν το ελεύθερο εμπόριο και να αναπτυχθούν οικονομικά με συνεργασία όλων των κρατών μελών.
Η EFTA λοιπόν, το 2022 διοργάνωσε μια συνοπτική συζήτηση σχετικά με το θέμα μιας προηγούμενης έκθεσης που βασίζεται στο Καταστατικό της Ρώμης του Διεθνούς Ποινικού Δικαστηρίου (ICC) για τον κυβερνοπόλεμο και τον ρόλο που μπορεί να διαδραματίσει το ICC στη ρύθμιση του πολέμου όπως εξελίσσεται στον 21ο αιώνα. Τα 4 βασικά ευρήματα αυτής της συζήτησης καθώς και προηγούμενα της έκθεσης του ICC, είναι τα εξής:

Πίνακας 2: 4 βασικά ευρήματα για το θέμα των επιθέσεων (Aggression)

4 βασικά ευρήματα για το θέμα των επιθέσεων (Aggression)
• Ένοπλες δυνάμεις, συμπεριλαμβανομένων των επιθέσεων στον κυβερνοχώρο
• Για να είναι μια κυβερνοεπίθεση επιθετική (να έχει δηλαδή την μορφή του «Aggression») υπάρχουν συγκεκριμένα κριτήρια βάσει του καταστατικού.
• Για να είσαι Ποινικά υπεύθυνος, πρέπει να είσαι σε ηγετική θέση.
• Δύσκολοι, αλλά κρίσιμοι, μη κρατικοί φορείς δεν θα εμπίπτουν στη δικαιοδοσία της ICRC (International Committee of the Red Cross)[25]

Αυτή λοιπόν είναι μια περίληψη μιας περίπλοκης συζήτησης. Υπάρχουν όμως και άλλα ενδιαφέροντα θέματα που πηγάζουν από αυτήν την έκθεση, άλλες δηλαδή πτυχές του Καταστατικού της Ρώμης, οι οποίες αξίζει να αναφερθούν και μπορεί να είναι ιδιαίτερης σημασίας για την κατανόηση άλλων παρόμοιων θεμάτων. Πιο συγκεκριμένα, η 1η παράγραφος της έκθεσης αναφέρει πως η χρήση κυβερνοεπιχειρήσεων αποτελεί μέρος μιας ένοπλης σύγκρουσης. Μπορεί όμως κάτι παρόμοιο να ισχύει και για τα εγκλήματα πολέμου; Η ερώτηση σε μια πιο απλουστευμένη μορφή θα μπορούσε να είναι ουσιαστικά η εξής: οι υπολογιστές πληρούν τις προϋποθέσεις για να ορίζονται ως αντικείμενο επιθετικότητας σύμφωνα με το Καταστατικό της Ρώμης; Τι ακριβώς αναφέρει το Καταστατικό της Ρώμης σχετικά με αυτό;

3.3.1 Crime of Aggression

Το άρθρο 8 του καταστατικού της Ρώμης (Article 8 War crimes και Article 8 bis3 Crime of aggression[26]) αναφέρει τα εξής:

1. Έγκλημα επιθετικότητας(Crime of aggression): εάν διαβάσουμε τον ορισμό, θα δούμε ότι για να διαπράξει κάποιος ένα έγκλημα επιθετικότητας, χρειάζεται πρώτα μια επιθετική πράξη όπως ορίζεται στο Καταστατικό της Ρώμης και πρέπει

[25] ICRC. (2021). International Review of the Red Cross: Humanitarian Debate, Law, Policy, Action. Digital technologies and war, Volume 102 number 913.
[26] International-Criminal-Court. (2021). Rome Statute of the ICC. Ανάκτηση από International Criminal Court, www.icc-cpi.int: https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf

να κατανοήσουμε ότι δεν πρόκειται για «δεδομένα που χαρακτηρίζονται ως αντικείμενο επιθετικότητας», λοιπόν.

2. Έγκλημα πολέμου: το ερώτημα είναι: «είναι τα δεδομένα αντικείμενο υπό τον International humanitarian law (IHL). Εδώ μπορούμε να δούμε τον ορισμό του αντικειμένου στο IHL (Άρθρο 52 AP I)[27]. Οι επιθέσεις εναντίον πολιτικών αντικειμένων απαγορεύονται βάσει του IHL. Πρόκειται λοιπόν για δεδομένα ως μη στρατιωτικό αντικείμενο και, ως εκ τούτου, προστατεύονται από το IHL (δηλαδή, οποιαδήποτε επίθεση εναντίον αυτού του πολιτικού αντικειμένου απαγορεύεται σύμφωνα με το IHL).

Η δύσκολη λέξη φαίνεται να είναι η λέξη «επίθεση» (attack). Η επίθεση λαμβάνει έναν συγκεκριμένο ορισμό σύμφωνα με το άρθρο 49 AP I. Μπορούμε να δούμε ότι είναι μια πράξη βίας κατά του αντιπάλου, επιθετική ή αμυντική. Επομένως, το ερώτημα είναι: «είναι μια εικονική επίθεση (virtual attack), πράξη βίας»; Σχετικά με αυτήν την ερώτηση, μπορεί κάποιος να μελετήσει περαιτέρω το σχετικό μέρος της έκθεσης του Συμβουλίου των Συμβούλων (The Council of Advisers)[28].

3.4 Η Κυβερνοασφάλεια εντός ΕΕ

Στο σημείο αυτό, είναι σημαντικό να προσπαθήσουμε να απαντήσουμε στο εξής ερώτημα: Γιατί χρειαζόμαστε κανονισμούς της ΕΕ για την Κυβερνοασφάλεια; Για να απαντήσουμε στο ερώτημα αυτό όμως, θα πρέπει να μελετήσουμε μερικά άλλα χαρακτηριστικά του παγκόσμιου τοπίου στο οποίο κρίνεται αναγκαία όλο και περισσότερο η εφαρμογή μέτρων Κυβερνοασφάλειας.

Όπως αναφέρει ο Ivan Bartoš (Αντιπρόεδρος της Τσεχίας για την Ψηφιοποίηση και Υπουργός Περιφερειακής Ανάπτυξης):

> *Δεν υπάρχει αμφιβολία ότι η Κυβερνοασφάλεια θα παραμείνει βασική πρόκληση για τα επόμενα χρόνια. Το διακύβευμα για τις οικονομίες μας και τους πολίτες μας είναι τεράστιο. Σήμερα, κάναμε ένα ακόμη βήμα για να βελτιώσουμε την ικανότητά μας να αντιμετωπίσουμε αυτήν την απειλή.*

[27] ICRC. (1949). Article 52 - General protection of civilian objects. Ανάκτηση από International Humanitarian Law Databases, https://ihl-databases.icrc.org/en: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52

[28] Regierung-des-Fürstentums-Liechtenstein. (2021, August). THE COUNCIL OF ADVISERS' REPORT ON THE APPLICATION OF THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT TO CYBERWARFARE. Ανάκτηση από www.regierung.li: https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

3.4.1 Η σημασία της Κυβερνοασφάλειας

Η Κυβερνοασφάλεια δεν είναι μόνο θέμα τεχνολογίας, είναι και θέμα ανθρώπων. Παρακάτω, απαριθμούνται μερικές από τις βασικές συνέπειες που έχει η έλλειψη Κυβερνοασφάλειας για τις επιχειρήσεις και στην συνέχεια στους ανθρώπους.

Ο κυβερνοχώρος θεωρείται πλέον ως η ραχοκοκαλιά της ψηφιακής κοινωνίας και της οικονομικής ανάπτυξης. Ωστόσο, τα περιστατικά ασφάλειας στον κυβερνοχώρο αυξάνονται και ενδέχεται να διαταράξουν την παροχή βασικών υπηρεσιών και να υπονομεύσουν την εμπιστοσύνη στις ψηφιακές υπηρεσίες και προϊόντα. Προωθούνται νέοι κανονισμοί της ΕΕ για τη βελτίωση της θέσης της ασφάλειας στον κυβερνοχώρο[29] και την ενίσχυση της θέσης της Ευρώπης ως ηγέτη στην ψηφιακή οικονομία.

Οι φορείς υπηρεσιών αντιμετωπίζουν πολλά προβλήματα ως αποτέλεσμα των παρακάτω παραγόντων:

- Εξελισσόμενο Περιβάλλον Απειλής
- covid19, γεωπολιτική, απειλή στον κυβερνοχώρο
- Αλλαγή Ρυθμιστικού Περιβάλλοντος (GDPR και Schrems II, Οδηγία NIS, DORA)
- Αλλαγή περιβάλλοντος πληροφορικής
- Απομακρυσμένη εργασία
- Νέα επιχειρηματικά μοντέλα
- Νέα μοντέλα πληροφορικής
- Νέες τεχνολογίες (Cloud, AI, Big data, Blockchain, Quantum…)

Συνέπειες για την επιχείρηση:

- Απώλεια χρημάτων
- Κλοπή στρατηγικών δεδομένων
- Απώλεια φήμης και εμπιστοσύνης πελατών
- Άμεσος αντίκτυπος στις ζωές των ανθρώπων: Αποκάλυψη προσωπικών πληροφοριών, Πρόσβαση σε τραπεζικά διαπιστευτήρια και χρήματα, Πρόσβαση σε προσωπικές συσκευές που μπορούν να θέσουν σε κίνδυνο την ακεραιότητα των ανθρώπων

[29] ENISA. (2024). Ανάκτηση από Enisa - Cybersecurity institutional map: https://www.enisa.europa.eu/login?came_from=/cybersecurity-institutional-map/results%3Froot%3Dactors

Κεφάλαιο 4ο: Τι έχει κάνει μέχρι στιγμής η ΕΕ για την ενίσχυση της Κυβερνοασφάλειας;

4.1 NIS2

Με στόχο την ενδυνάμωση της Κυβερνοασφάλειας στην Ευρώπη, καθώς και της αύξησης της ανθεκτικότητας όλων των ευρωπαϊκών χωρών απέναντι σε κακόβουλα λογισμικά και κυβερνοεπιθέσεις, το συμβούλιο υιοθετεί νέα νομοθεσία σε συνέχεια της προηγούμενης έκδοσης της, το NIS Directive. Η νέα αυτή νομοθεσία, που ονομάζεται NIS2, αντικαθιστά την προηγούμενη σε θέματα ασφάλειας συστημάτων και πληροφοριών, και αυτό για βελτίωση της αντίδρασης (incident response capacities) στον δημόσιο αλλά και στον ιδιωτικό τομέα.

Ο βασικότερος σκοπός της νέας αυτής νομοθεσίας είναι η καλύτερη διαχείριση κρίσεων και η συνεργασία μεταξύ των κρατών μελών, κάτι που μπορούμε επίσης να αξιολογήσουμε χρησιμοποιώντας το εργαλείο Cyber Diplomacy Atlas[30]. Θέτει τις βάσεις για σωστότερο «risk management» αλλά και «reporting» σε βασικούς τομείς τους οποίους αγγίζει η Κυβερνοασφάλεια, όπως οι μεταφορές, η ενέργεια, η υγεία και άλλα. Για να επιτευχθούν αυτά, φυσικά η "ντιρεκτίβα" NIS2 ορίζει τους κανόνες και τους μηχανισμούς με βάση τους οποίους θα πρέπει να λειτουργήσει μια οντότητα, είτε αυτή είναι ένα κράτος-μέλος είτε είναι ένας οργανισμός ή μια διοικητική αρχή. Για να υπάρξει όμως εναρμόνιση στους κανόνες και στους μηχανισμούς, απαιτείται συνεργασία και επικοινωνία μεταξύ των κρατών-μελών και των διάφορων αρχών και επιχειρήσεων.

Ταυτόχρονα όμως, η "ντιρεκτίβα" ορίζει και κυρώσεις αλλά και άλλες μορφές επιλύσεων των διαφορών, ώστε να εξασφαλίσει την επιτυχία της και την σωστή εφαρμογή αυτών που ορίζει. Επίσης, εγκαθιδρύει και επίσημα πια το EU-CyCLONe (European Cyber Crises Liaison Organisation Network) το οποίο κατά κύριο λόγο αφορά την διαχείριση κρίσεων μεγάλου μεγέθους[31]. Ουσιαστικά το NIS2 αποτελεί μια προέκταση της πρώτης έκδοσης του NIS και αυτό αποδεικνύεται σε διάφορα επίπεδα. Για παράδειγμα, καλύπτονται πια μεσαίες και μεγάλες οντότητες, οι οποίες με το παλιό NIS εξαρτιούνταν εντελώς από το κράτος-μέλος στο οποίο υπαγόντουσαν, από την άποψη πως το κράτος-μέλος ήταν αυτό που καθόριζε ποιες οντότητες θα έπρεπε να τηρούν τα κριτήρια και τους μηχανισμούς

[30] EU-CYBER-DIRECT. (2024). Cyber Diplomacy Atlas. Ανάκτηση από https://eucyberdirect.eu/: https://eucyberdirect.eu/atlas

[31] Askoxylakis, I. (2019, June 3). https://www.enisa.europa.eu/events/past#b_start=0. Ανάκτηση από ENISA: https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf

που προτείνονταν. Αυτή η αλλαγή ονομάζεται «size-cap rule». Με αυτόν τον τρόπο, εισάγεται και για πρώτη φορά η έννοια της «αναλογικότητας» (proportionality).

Άλλες αλλαγές αναφέρουν πως η ντιρεκτίβα NIS2 δεν αφορά οντότητες που δραστηριοποιούνται στους τομείς εθνικής ασφάλειας, δημόσιας ασφάλειας και επιβολής του νόμου. Τονίζεται επίσης πως δικαστήρια, τράπεζες και εθνικά Κοινοβούλια εξαιρούνται από τα μέτρα και τους μηχανισμούς της αναθεωρημένης ντιρεκτίβας., η οποία όμως θα αφορά δημόσιες διοικητικές υπηρεσίες και σε εθνικό και σε τοπικό επίπεδο. Για να ενισχυθούν αυτές οι αλλαγές, εισάγεται επιπλέον μια μορφή τομεακής νομοθεσίας (σε επίπεδο ξεχωριστών τομέων δηλαδή). Για παράδειγμα θα υπάρχει πλήρης εναρμόνιση με το DORA (Digital Operational Resilience Act), που ασχολείται με την ψηφιακή ανθεκτικότητα για τον χρηματοπιστωτικό τομέα, και το CER (Centre for European Reform) που ασχολείται με νομικά θέματα και θα είναι ο συνδετικός κρίκος μεταξύ του NIS2 και των λοιπών νομοθεσιών.

4.1.1 Πρωτοτυπίες του NIS2 έναντι στο NIS

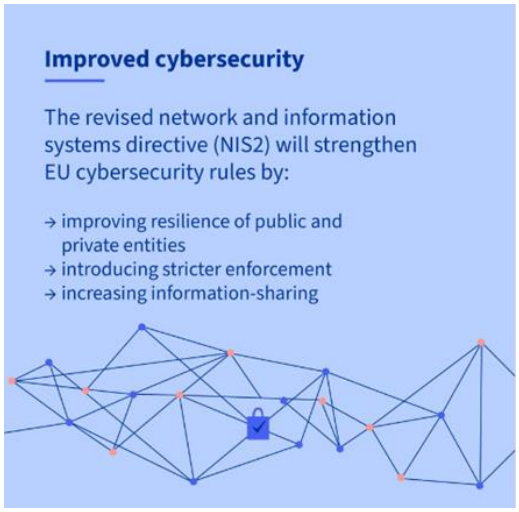
Η βασική πρωτοτυπία της νέας ντιρεκτίβας NIS2 έναντι στην παλαιότερη έκδοσή της, NIS, έγκειται στα επόμενα βήματα που προτείνονται. Τα κράτη μέλη θα έχουν 21 μήνες, αφού τεθεί η ντιρεκτίβα σε ισχύ, για να ενσωματώσουν τα μέτρα και τους μηχανισμούς που ορίζονται στην εθνική τους νομοθεσία.

Εικόνα 3: Το διευρυμένο πεδίο του NIS2 σε περισσότερους τομείς

Πηγή: NIS INVESTMENTS, https://www.enisa.europa.eu/publications/nis-investments-2022

Ο αυξημένος αριθμός επιθέσεων στον κυβερνοχώρο απαιτεί αμεσότερη και εντονότερη αντίδραση από την μεριά της ΕΕ. Οι νέοι κανονισμοί που προάγονται από την οδηγία NIS 2, θα βοηθήσουν σε αυτήν την διαδικασία και θα ενισχύσουν το έργο της ΕΕ στον τομέα της Κυβερνοασφάλειας. Επίσης, πέραν από την ΕΕ, θα υποστηρίξουν και την ανάπτυξη ικανοτήτων αντίδρασης τόσο των δημόσιων όσο και των ιδιωτικών φορέων της Ευρώπης. Πρόκειται για αναπόσπαστο κομμάτι ευρύτερων δράσεων για την δημιουργία ανθεκτικότητας της ΕΕ έναντι των φυσικών και ψηφιακών κινδύνων[32].

Εικόνα 4: Οι βασικές αλλαγές που φέρνει η οδηγία NIS2



Πηγή: NIS INVESTMENTS, https://www.enisa.europa.eu/publications/nis-investments-2022

4.2 ENISA

Ο ENISA, κατόπιν 8-μηνης άσκησης (από τον Μάρτιο έως τον Αύγουστο του 2022) σε συνεργασία με το "ENISA Foresight Expert Group", το "CSIRTs Network" και τους ειδικούς από το "EU CyCLONe", προσδιόρισε και κατηγοριοποίησε μερικές προκλήσεις που πρόκειται να εμφανιστούν ή να αποτελέσουν σημαντικό πρόβλημα ως το 2030. Σε συνέχεια αυτών των αποτελεσμάτων, ο ENISA οργάνωσε το "Threat Identification Workshop" , με σκοπό να βρει λύσεις σε αυτές τις προκλήσεις.

[32] Council-of-the-EU-and-the-European-Council. (2022, November 28). EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation. Ανάκτηση από www.consilium.europa.eu: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

Ο εκτελεστικός διευθυντής του ENISA, Juhan Lepassaar δήλωσε:

> *"Ο μετριασμός των μελλοντικών κινδύνων δεν μπορεί να αναβληθεί ή να αποφευχθεί. Αυτός είναι ο λόγος για τον οποίο οποιαδήποτε επίγνωση για το μέλλον είναι το καλύτερο σχέδιο ασφαλείας. Όπως λέει και η παροιμία: "η πρόληψη είναι καλύτερη από τη θεραπεία". Είναι ευθύνη μας να λάβουμε όλα τα δυνατά μέτρα εκ των προτέρων για να διασφαλίσουμε ότι θα αυξήσουμε την ανθεκτικότητά μας με την πάροδο των ετών για ένα βελτιωμένο τοπίο Κυβερνοασφάλειας το 2030 και μετά".*

Από τα αποτελέσματα της 8μηνης αυτής ασκήσεως, καταλαβαίνουμε πως οι προκλήσεις που παρουσιάζονται πιθανά στο μέλλον ποικίλουν σε χαρακτηριστικά και περιλαμβάνουν και πολλά από τα σημερινά προβλήματα. Σε κάθε περίπτωση, φαίνεται πως τα σημερινά προβλήματα θα παραμείνουν στην ατμόσφαιρα χωρίς ιδιαίτερες αλλαγές σε μέγεθος, παρά μόνο σε χαρακτήρα. Οι νέες τεχνολογίες και η αύξηση σε εξαρτήσεις από αυτές θα παίξουν σημαντικό ρόλο στις αλλαγές που θα λάβουν χώρα από τώρα ως το 2030. Οι παράγοντες αυτοί, γίνεται άμεσα κατανοητό πως είναι καθοριστικής σημασίας για το μέλλον και για αυτό προσθέτουν και επιπλέον βαρύτητα στην 8μηνη άσκηση του ENISA. Ταυτόχρονα όμως, την κάνουν και πιο πολύπλοκη. Για αυτούς τους λόγους, τα αποτελέσματα που παρουσιάζονται σε αυτού του είδους τις έρευνες είναι χρήσιμα εργαλεία κατανόησης των προβλημάτων και προσπάθειας επίλυσης τους, όπως επίσης και κίνητρα για όλους τους stakeholders για ένα καλύτερο μέλλον. Ουσιαστικά, με τις εργασίες που ξεκίνησαν με την πρώτη έκθεση «Foresight on Emerging and Future Cybersecurity Challenges», ο ENISA προσπαθεί να βελτιώσει την ανθεκτικότητα της ΕΕ σε θέματα Κυβερνοασφάλειας, αυξάνοντας την ευαισθητοποίηση σχετικά με μελλοντικές απειλές και προτείνοντας αντίμετρα που μπορούν να χρησιμοποιήσουν τα κράτη μέλη της ΕΕ και γενικότερα τα ενδιαφερόμενα μέρη.

4.2.1 Cybersecurity Incident Response Teams ή CSIRT network

Ιδρύθηκε με το Directive on Network and Information Security Systems (NIS Directive - Οδηγία για τα Συστήματα Ασφάλειας Δικτύων και Πληροφοριών) το 2016. Οι Ομάδες Αντιμετώπισης Συμβάντων Κυβερνοασφάλειας (CSIRT network) περιλαμβάνουν τους διορισμένους CSIRT και CERT-EU των κρατών μελών της ΕΕ. Σε αυτή τη διαδικασία, η Ευρωπαϊκή Επιτροπή λειτουργεί ως παρατηρητής. Ο ρόλος του ENISA είναι να υποστηρίζει το δίκτυο CSIRT, να συντονίζει τα διάφορα συμβάντα κατόπιν αιτήματος των ενδιαφερόμενων και να τους υποστηρίζει διοικητικά. Με την σειρά του, σκοπός του δικτύου CSIRT είναι να βελτιώσει την διαχείριση συμβάντων διασυνοριακού χαρακτήρα

και να ορίσει τον τρόπο με τον οποίο μπορεί κάποιος να ανταποκριθεί σε συγκεκριμένα περιστατικά με συντονισμένο τρόπο.

4.2.2 EU Cyber Crisis Liaison Network ή EU CyCLONE

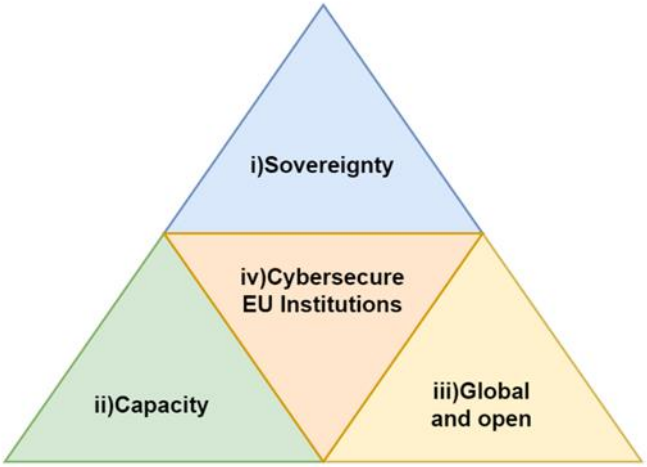
Παρουσιάστηκε κατά τη δεύτερη έκδοση του Blue Olex το 2020[33]. Σκοπός του είναι να δημιουργήσει συνεργατικό πνεύμα των διορισμένων εθνικών υπηρεσιών και αρχών, αρμόδιων για τη διαχείριση κρίσεων στον κυβερνοχώρο και να αποτελέσει συνδετικό κρίκο μεταξύ του EU CSIRT Δικτύου (σε τεχνικό επίπεδο) και του πολιτικού επιπέδου της Ε.Ε. Το EU CyCLONe (Ευρωπαϊκό Δίκτυο Οργανισμού Διασύνδεσης Κρίσεων στον Κυβερνοχώρο) ιδρύθηκε επίσημα με την αναθεωρημένη Οδηγία NIS (NIS Directive).

Όπως αναφέρει το EUs cybersecurity strategy for the Digital Decade (16.12.2020), υπάρχουν 3 όργανα/μέσα πολιτικών Κυβερνοασφάλειας, ή αλλιώς οι 3 πυλώνες: Ρυθμιστική, επενδυτική, πολιτική πρωτοβουλία.

- Ανθεκτικότητα, τεχνολογική κυριαρχία (sovereignty) και ηγεσία (leadership) (αναθεωρημένη οδηγία για την ασφάλεια δικτύων και συστημάτων πληροφοριών NIS2, cybersecurity shield CSIRT SOC, Secure communication infrastructure, quantum NG Mobile IPv6 DNS, Κέντρο ικανοτήτων και δίκτυο κέντρων συντονισμού CCCN, αναβάθμιση εργατικού δυναμικού της ΕΕ)
- Δημιουργία επιχειρησιακής ικανότητας για αποτροπή και αντίδραση (πλαίσιο διαχείρισης κρίσεων στον κυβερνοχώρο, ατζέντα για το έγκλημα στον κυβερνοχώρο, cyber intelligence των κρατών μελών, πλαίσιο πολιτικής για την άμυνα στον κυβερνοχώρο).
- Συνεργασία για την προώθηση ενός παγκόσμιου και ανοιχτού κυβερνοχώρου (ηγεσία της ΕΕ σε πρότυπα, κανόνες και πλαίσια σε φορείς τυποποίησης, προώθηση του multistakeholderism μοντέλου διακυβέρνησης του Διαδικτύου, ατζέντα ανάπτυξης ικανοτήτων στον κυβερνοχώρο/ cyber capacity building agenda, eu cyber dialogue and diplomacy network)

[33]EU-CyCLONe. (2020, September 29). Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe). Ανάκτηση από ENISA: https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

Εικόνα 5: Η στρατηγική της ΕΕ για την Ψηφιακή Δεκαετία



Πηγή: Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

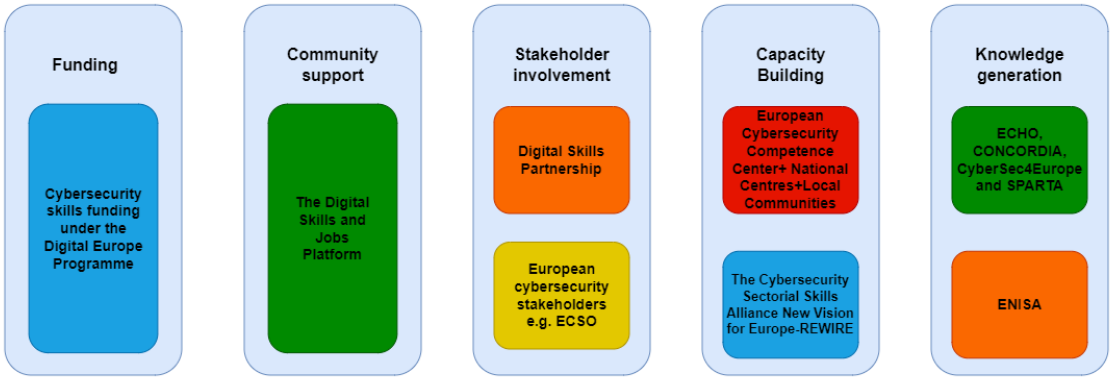
Επίσης μπορούμε να δούμε και μια συσχέτιση εννοιών που υπάρχουν γύρω από το πεδίο των ευρωπαϊκών πολιτικών. Για να κατανοήσουμε καλύτερα το παρακάτω σχήμα που αποδεικνύει αυτή τη συσχέτιση, ας αναφέρουμε ενδεικτικά μερικά παραδείγματα τέτοιων εννοιών. Οι δεξιότητες στον κυβερνοχώρο στο τοπίο της πολιτικής Κυβερνοασφάλειας της ΕΕ, οι διάφορες χρηματοδοτήσεις, η δημιουργία γνώσης για τη συμμετοχή των ενδιαφερομένων, η υποστήριξη της κοινότητας για την ανάπτυξη ικανοτήτων συμμετοχής των ενδιαφερομένων.

Εικόνα 6: Οι ευρωπαϊκές πολιτικές και διάφοροι δρώντες που επιδρούν πάνω τους.

Πηγή: Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Ας δούμε με περισσότερη λεπτομέρεια μερικούς από τους δρώντες που αναφέρονται στο παρακάτω σχήμα.

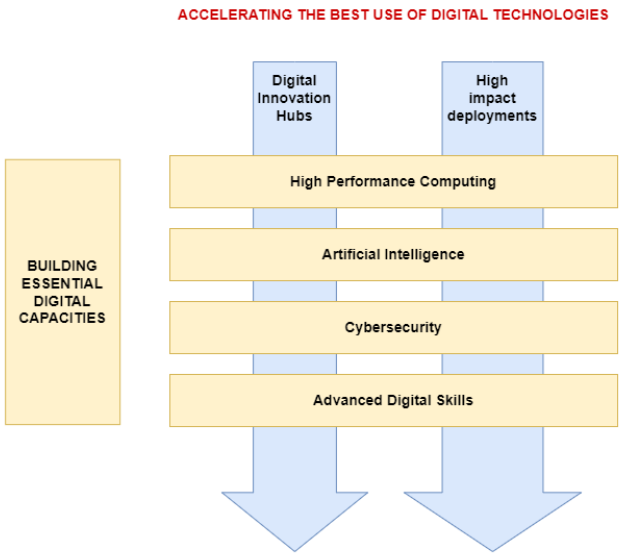
Εικόνα 7: Οι δρώντες που επιδρούν στο περιβάλλον Ευρωπαϊκών πολιτικών Κυβερνοασφάλειας.



Πηγή: Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Σε συνέχεια των στοιχείων που παρουσιάστηκαν εδώ, θα μπορούσαμε να μελετήσουμε και την δομή του προγράμματος Digital Europe, το οποίο σχετίζεται άμεσα με το πεδίο των Ευρωπαϊκών πολιτικών, όπως αυτό παρουσιάστηκε παραπάνω. Για βασικούς στρατηγικούς τομείς, όπως αυτοί που αναφέρονται στην παρακάτω εικόνα, το πρόγραμμα παραμένει οπτικά απλό και κινείται, όπως στο σχήμα, από πάνω προς τα κάτω.

Εικόνα 8: η δομή του προγράμματος Digital Europe.



Πηγή: Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Βασικός στόχος, όπως φαίνεται και στην Εικόνα 8, είναι η επιτάχυνση της βέλτιστης χρήσης των ψηφιακών τεχνολογιών. Βασικοί τομείς, όπως η ασφάλεια στον κυβερνοχώρο, δέχονται ιδιαίτερη υποστήριξη στην εφαρμογή της σχετικής νομοθεσίας της ΕΕ.

4.3 EU Cyber Competence Centre and Network of NCCs (Κέντρο κυβερνοαρμοδιότητας της ΕΕ και Δίκτυο NCC)

Έπειτα, υπάρχει και το Ευρωπαϊκό κέντρο ικανοτήτων και Δίκτυο NCC/ EU Cyber Competence Centre and Network of NCCs (κονδύλια για τον κυβερνοχώρο στο πλαίσιο της Ψηφιακής Ευρώπης και του Horizon Europe 2021-2027, συντονισμός του Δικτύου και της Κοινότητας για την προώθηση της τεχνολογικής ατζέντας)

- Δίκτυο εθνικών κέντρων συντονισμού (οικοδόμηση εθνικών ικανοτήτων και σύνδεση με υπάρχουσες πρωτοβουλίες, τα εθνικά κέντρα συντονισμού ενδέχεται να λάβουν χρηματοδότηση και να μεταβιβάσουν οικονομική υποστήριξη)
- Κοινότητα ικανοτήτων (μεγάλη, ανοιχτή και ποικιλόμορφη ομάδα ενδιαφερομένων για την ασφάλεια στον κυβερνοχώρο, από τον ιδιωτικό και δημόσιο τομέα)

Το Ευρωπαϊκό Κέντρο Ικανοτήτων για την Κυβερνοασφάλεια (ECCC), σε συνεργασία με το Δίκτυο Εθνικών Κέντρων Συντονισμού, θα δημιουργήσει μια ισχυρή κοινότητα γνώσεων για την ασφάλεια στον κυβερνοχώρο για να διευκολύνει τη συνεργασία και την ανταλλαγή εμπειρογνωμοσύνης και ικανοτήτων μεταξύ όλων των σχετικών ενδιαφερομένων, ιδίως των ερευνητικών και βιομηχανικών κοινοτήτων, καθώς και ως δημόσιες αρχές.

Αυτό το οικοσύστημα θα πρέπει να ενισχύσει τις ικανότητες της κοινότητας της γνώσης, να προστατεύσει την οικονομία και την κοινωνία μας από επιθέσεις στον κυβερνοχώρο, να διατηρήσει την αριστεία στην έρευνα και να ενισχύσει την ανταγωνιστικότητα της ευρωπαϊκής βιομηχανίας στον τομέα της Κυβερνοασφάλειας.
Στόχος είναι η συγκέντρωση και ο καλύτερος συντονισμός των επενδύσεων έρευνας, τεχνολογίας και βιομηχανικής ανάπτυξης στον τομέα της ασφάλειας στον κυβερνοχώρο στην Ένωση, πέρα από τα σύνορα μη στρατιωτικών και αμυντικών οργανώσεων.

Το ECCC θα βοηθήσει στην διαχείριση των κεφαλαίων που προβλέπονται για την ασφάλεια στον κυβερνοχώρο στο πλαίσιο της Digital Europe και του Horizon Ευρώπη 2021-2027 και παράλληλα στα εξής:

- διευκόλυνση και βοήθεια στο συντονισμό του Δικτύου και της Κοινότητας για την προώθηση της ατζέντας της τεχνολογίας στον κυβερνοχώρο,
- υποστήριξη κοινών επενδύσεων από την ΕΕ, τα κράτη μέλη και τη βιομηχανία και υποστήριξη της ανάπτυξης προϊόντων και λύσεων.

Αντίστοιχα, το Network of National Coordination Centres (NCCs), που ορίζεται από τα κράτη μέλη ως εθνικό σημείο επαφής, θα έχει τα εξής χαρακτηριστικά:

- Στόχος: ανάπτυξη εθνικών ικανοτήτων και σύνδεση με υφιστάμενες πρωτοβουλίες.
- Μπορεί να λάβει χρηματοδότηση, μπορεί να μεταβιβάσει οικονομική υποστήριξη.

Η βασική ιδέα είναι να υπάρχει ένα NCC ανά κράτος μέλος, ώστε να δημιουργηθεί μια κοινότητα αρμοδιότητας με τα εξής χαρακτηριστικά:

- Μια μεγάλη, ανοιχτή και ποικιλόμορφη ομάδα ενδιαφερόμενων μερών στον τομέα της Κυβερνοασφάλειας από την έρευνα και τον ιδιωτικό και δημόσιο τομέα
- Παρέχει πληροφορίες για τις δραστηριότητες του κέντρου ικανοτήτων στα προγράμματα
- Αποστολή του είναι η στρατηγική αυτονομία και παγκόσμια ανταγωνιστικότητα
- Στόχοι του η αντοχή στον κυβερνοχώρο, η γνώση και οι υποδομές, ένα χωρίς αποκλεισμούς, ανθεκτικό οικοσύστημα ενδιαφερόμενων, προώθηση της έρευνας, της καινοτομίας, της ανάπτυξης, στρατηγική ατζέντα για έρευνα, καινοτομία, ανάπτυξη, προγράμματα χρηματοδότησης της ΕΕ, εθελοντικές εθνικές συνεισφορές, συνεργασία, συντονισμός

4.4 Coordinated Vulnerability Disclosure: Towards a Common EU Approach

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) παρουσίασε και δημοσίευσε μια νέα έκθεση που μελετά τις προσδοκίες των κρατών μελών αλλά και των βιομηχανικών φορέων, για τους στόχους που θέτει η NIS2. Αναλύει τις νομικές και τεχνικές προκλήσεις που πηγάζουν από τέτοιου είδους πρωτοβουλίες και προτάσεις. Η συνεργασία μεταξύ του ENISA και της Ομάδας Συνεργασίας της NIS ανοίγει τον δρόμο για γόνιμη συνεργασία και επικοινωνία μεταξύ των κρατών μελών της ΕΕ, τα οποία θα πρέπει να θεσπίσουν τις εθνικές τους πολιτικές CVD (**Coordinated Vulnerability Disclosure**[34]). Η συνεργασία αυτή θα έχει βασικό στόχο τη διαχείριση τρωτών σημείων, τις ειδικές διαδικασίες και τις σχετικές αρμοδιότητες.

Η νέα αυτή έκθεση του ENISA (European Union Agency for Cybersecurity) ερευνά το πως αναπτύσσονται αρμονικά εθνικές πρωτοβουλίες Κυβερνοασφάλειας εντός της ΕΕ. Με την νέα ντιρεκτίβα NIS2 που υιοθετήθηκε στις 16 Γενάρη 2023, όλα τα κράτη μέλη οφείλουν να έχουν καθορισμένες πολιτικής αντιμετώπισης κυβερνοπροκλήσεων (οι οποίες ονομάζονται στην ντιρεκτίβα «Vulnerabilities disclosure policies») και μάλιστα να τις έχουν υιοθετήσει πλήρως έως τις 17 οκτωβρίου 2024. Πολλές από αυτές τις πολιτικές έχουν ήδη ληφθεί υπόψιν, ή θα έπρεπε θεωρητικά να είναι μέρος των πολιτικών των κρατών μελών ήδη από την παρουσία του **Cyber Resilience Act (CRA)**. Με αυτήν την έρευνα/έκθεση λοιπόν, η ENISA προσπαθεί ουσιαστικά να κατανοήσει τον τρόπο με τον

[34] ENISA. (2023, February 16). Coordinated Vulnerability Disclosure: Towards a Common EU Approach. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/news/coordinated-vulnerability-disclosure-towards-a-common-eu-approach/

οποίο θα μπορούσε να υπάρξει μια πλήρως οργανωμένη και αρμονική επικοινωνία μεταξύ των κρατών μελών σε θέματα πολιτικών και αποφάσεων Κυβερνοασφάλειας. Η έρευνα αυτή θα γίνει σε συζήτηση μεταξύ του ανθρωπίνου δυναμικού της ENISA που ηγείται του project και του NIS cooperation group.

Μια γρήγορη ματιά στην έκθεση αυτή φανερώνει τα παρακάτω:

- Μια εθνική ή ευρωπαϊκή **CVD (Coordinated Vulnerability Disclosure)** πολιτική είναι αυτή που θα ωθήσει οργανισμούς να έχουν ως πρώτο τους μέλημα τις πρακτικές διαχείρισης ευπάθειας και ασφάλειας (vulnerability management and security practices).

- Οι υπεύθυνοι χάραξης πολιτικής (policy makers) οφείλουν από εδώ και στο εξής να έχουν συνεχώς υπόψη τους τα θέματα και τα standards των CVD πολιτικών.

- Είναι επιτακτική η ανάγκη πια για συνεργασία σε διάφορες νομοθεσίες, όχι μόνο σε εθνικό επίπεδο, αλλά και σε διεθνικό πια επίπεδο, καθώς και μεταξύ της βιομηχανίας και του δημόσιου τομέα, ώστε να επιτευχθεί όσο το δυνατόν περισσότερη αρμονία και λιγότερη αστοχία σε τέτοια θέματα.

Ταυτόχρονα, υπάρχουν και εμπόδια που μπαίνουν μπροστά στους ερευνητές που προσπαθούν να μελετήσουν τα σημεία τρωτότητας των εθνικών και ευρωπαϊκών πολιτικών. Η έκθεση της ENISA αναφέρεται και σε αυτές τις προκλήσεις για τους ερευνητές, που όπως αναφέρεται ένα αόριστο και ασαφές ή ανύπαρκτο πλαίσιο πολιτικής CVD προκαλεί αβεβαιότητα στην γνώση του θέματος, κάτι το οποίο εμποδίζει την απρόσκοπτη δουλειά των ερευνητών και τους βάζει σε κίνδυνο να χάσουν εν μέρει την επαγγελματική τους αξιοπιστία.

4.5 Cyber Resilience Act (CRA)

Ο νόμος Cyber Resilience Act (CRA) είναι μια νομοθεσία που πρότεινε η Ευρωπαϊκή επιτροπή στις 15 Σεπτεμβρίου το 2022, για να βελτιώσει το επίπεδο Κυβερνοασφάλειας και ανθεκτικότητας (resilience) της ΕΕ, μέσω κοινών προτύπων ψηφιοποίησης της. Τα κύρια στοιχεία της πρότασης CRA είναι τα εξής:

- Επιβολή κυρώσεων (συμπεριλαμβανομένων προστίμων έως 15 000 000 ευρώ).
- Σε εξαιρετικές περιπτώσεις, η Ευρωπαϊκή Επιτροπή μπορεί να απαιτήσει από τον Οργανισμό Κυβερνοασφάλειας της ΕΕ (ENISA) να πραγματοποιήσει μια αξιολόγηση και ανάλογα με τα ευρήματα της αξιολόγησης αυτής, να αποφασίσει περιοριστικά μέτρα ή άλλες ενέργειες για να εξασφαλίσει την συμμόρφωση, κάτι που είναι δυνατό σε επίπεδο ΕΕ μέσω εκτελεστικής πράξης (και κατόπιν διαβουλεύσεων με τα κράτη μέλη).

4.6 Εθνικές πρωτοβουλίες

Πέραν των οργανισμών και των προγραμμάτων που αναφέρθηκαν παραπάνω, αξίζει να αναφέρουμε και μερικές εθνικές αρχές κρατών-μελών της ΕΕ που ασχολούνται με θέματα Κυβερνοασφάλειας. Στον παρακάτω πίνακα λοιπόν, βλέπουμε παραδείγματα εθνικών δράσεων και προγράμματα σχετικά με την Κυβερνοασφάλεια και την Διακυβέρνηση στον Κυβερνοχώρο[35].

Πίνακας 3: Εθνικές δράσεις και προγράμματα σχετικά με την Κυβερνοασφάλεια και την Διακυβέρνηση στον Κυβερνοχώρο

Εθνικές δράσεις και προγράμματα σχετικά με την Κυβερνοασφάλεια και την Διακυβέρνηση στον Κυβερνοχώρο		
ΧΩΡΑ	**ΟΡΓΑΝΙΣΜΟΣ/ΑΡΧΗ**	**ΙΣΤΟΣΕΛΙΔΑ**
Ισπανία	Εθνικό Ινστιτούτο Κυβερνοασφάλειας , incibe instituto nacional de cibersecuridad	https://www.incibe.es/
Ελλάδα	Greece National Cyber Security Authority – Ministry of Digital Governance (NCSA)	https://mindigital.gr/
Πορτογαλία	Portugal (situational context-national and european networks-c-academy) Centro Nacional de Cibersegurança (CNCS)	https://www.cncs.gov.pt/
Γαλλία	France CFSSI-ANSSI Centre de Formation à la Sécurité des Systèmes d'Information	https://www.ssi.gouv.fr/agence/contacts/cfssi/
Γερμανία	Germany BSI Federal Office for information Security	https://www.bsi.bund.de/EN/Home/home_node.html

[35] ENISA. (2024). National Cybersecurity Strategies Evaluation Tool. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

Κεφάλαιο 5ο: Συζήτηση και Προβλήματα

5.1 Λόγοι για τους οποίους μπορεί η ΕΕ να χαρακτηριστεί ως "δρών ασφαλείας".

Στο Κεφάλαιο 1 τίθενται τα βασικά ερευνητικά ερωτήματα, πάνω στα οποία βασίζεται η εργασία:

1. Είναι η ΕΕ παγκόσμιος δρών ασφαλείας όσον αφορά στην Κυβερνοασφάλεια;
2. Είναι αποτελεσματικό το οικοσύστημα Κυβερνοασφάλειας της ΕΕ, και αν ναι, πως ακριβώς αξιολογούμε αυτήν την αποτελεσματικότητα;

Για να απαντήσουμε λοιπόν στα παραπάνω ερωτήματα, η Ευρωπαϊκή Ένωση (ΕΕ) μπορεί να αναγνωριστεί ως ένας σημαντικός συμμετέχων στον παγκόσμιο χώρο της κυβερνοασφάλειας με βάση αρκετά κριτήρια. Καταρχάς, η ΕΕ έχει θεσπίσει ένα ισχυρό κανονιστικό πλαίσιο, που εκδηλώνεται σε διάφορους περίπλοκους κανονισμούς και οδηγίες, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Αυτοί οι κανόνες υπογραμμίζουν τη δέσμευση της ΕΕ στην αντιμετώπιση των κυβερνοαπειλών και την προστασία των ψηφιακών υποδομών.

Επιπλέον, η ΕΕ έχει διαμορφώσει μια καλά ορισμένη και συντονισμένη στρατηγική κυβερνοασφάλειας, καθιστώντας εμφανές ότι αναγνωρίζει την κυβερνοασφάλεια ως έναν παγκόσμιο προβληματισμό. Αυτή η στρατηγική περιλαμβάνει μέτρα για την ενίσχυση των δυνατοτήτων κυβερνοασφάλειας, την προώθηση του κοινού χώρου πληροφοριών και την συνεργασία με διεθνείς εταίρους.

Ένα βασικό στοιχείο της διεθνούς επιρροής της ΕΕ στον τομέα της κυβερνοασφάλειας είναι η ενεργός της συμμετοχή σε διεθνείς συνεργασίες. Η ΕΕ συνεργάζεται με άλλες χώρες και διεθνείς οργανισμούς σε διάφορες πρωτοβουλίες κυβερνοασφάλειας, συμβάλλοντας στις συλλογικές προσπάθειες αντιμετώπισης των προκλήσεων κυβερνοασφάλειας. Αυτή η συνεργατική προσέγγιση είναι εμφανής μέσω της συνεργασίας με χώρες εκτός της ΕΕ, της συμμετοχής σε παγκόσμια fora κυβερνοασφάλειας και των κοινών προσπαθειών αντιμετώπισης των κυβερνοαπειλών.

Επιπλέον, η ΕΕ επιδεικνύει τη δέσμευσή της στην παγκόσμια σταθερότητα της κυβερνοασφάλειας παρέχοντας υποστήριξη και βοήθεια σε θέματα κατάρτισης σε άλλες χώρες. Αυτό περιλαμβάνει διάφορες πρωτοβουλίες όπως προγράμματα εκπαίδευσης, τεχνική βοήθεια και κοινοποίηση γνώσης για την ενίσχυση των σχετικών τους ικανοτήτων.

Η επένδυση της ΕΕ σε έρευνα και ανάπτυξη σχετικά με τεχνολογίες κυβερνοασφάλειας συμβάλλει επίσης στη θέση της ως ενεργού παράγοντα στην αντιμετώπιση νέων

απειλών. Αυτή η καινοτομία στις πρακτικές της κυβερνοασφάλειας συμβάλλει σημαντικά στον προσδιορισμό των κανόνων κυβερνοασφάλειας παγκοσμίως.

Η θέσπιση αποτελεσματικών μηχανισμών αντιμετώπισης και συντονισμού σε περίπτωση περιστατικών κυβερνοεπιθέσεων ή κυβερνοαπειλών είναι ένα άλλο στοιχείο της προσπάθειας της ΕΕ στον τομέα της κυβερνοασφάλειας. Αυτό περιλαμβάνει τον συντονισμό με τα κράτη μέλη, την κοινοποίηση πληροφοριών για απειλές και τις κοινές αντιδράσεις σε τέτοια περιστατικά τόσο σε περιφερειακό/εθνικό όσο και σε παγκόσμιο επίπεδο.

Επιπλέον, η ΕΕ προωθεί τη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα για την αντιμετώπιση προκλήσεων. Η διευκόλυνση της συνεργασίας και της κοινοποίησης πληροφοριών μεταξύ των δημοσίων και ιδιωτικών φορέων αντικατοπτρίζει την αναγνώριση της ΕΕ για την ανάγκη συνεργασίας για την ενίσχυση της κυβερνοασφάλειας.

Τέλος, η ΕΕ συμμετέχει ενεργά σε διπλωματικές προσπάθειες για την προώθηση υπεύθυνης συμπεριφοράς στον κυβερνοχώρο, συμμετέχοντας σε διπλωματικές πρωτοβουλίες για την καθιέρωση κανόνων υπεύθυνης συμπεριφοράς κρατών. Αυτές οι ενέργειες συνολικά υπογραμμίζουν τον σημαντικό ρόλο της ΕΕ στον προσδιορισμό παγκοσμίων κανόνων και πλαισίων σε θέματα κυβερνοασφάλειας.

5.2 Προβλήματα

Το αβέβαιο γεωπολιτικό περιβάλλον που επικρατεί εν έτη 2023 είναι αυτό που πυροδοτεί και επιταχύνει τις απειλές και τις επιθέσεις στον κυβερνοχώρο. Η επιρροή της επίθεσης της Ρωσίας στην Ουκρανία είναι απόδειξη ακριβώς αυτού και γίνεται αισθητή από όλους τους πολίτες παγκοσμίως. Τέτοια γεγονότα προκαλούν απορίες και αμφισβητήσεις σχετικά με την ισχύ της ΕΕ και της αποτελεσματικότητάς της να αντιμετωπίσει τέτοιου είδους απειλές. Για παράδειγμα, συχνά τον τελευταίο καιρό έρχεται στην σκέψη των ερευνητών ή των ενδιαφερόμενων σε τέτοια θέματα, η εξής ερώτηση: Γιατί το ΝΑΤΟ είναι τόσο πιο δυνατό, εάν το συγκρίνουμε με την ισχύ της ΕΕ; Η απάντηση, αν κάποιος αναρωτηθεί, δεν φαίνεται να είναι και τόσο δύσκολη. Σε πολλές περιπτώσεις, οι συμμαχίες υπόσχονται στρατιωτική υποστήριξη εάν υπάρχει μέλος που απειλείται, μια επίσημη δέσμευση γνωστή ως αμοιβαία ασφάλεια. Ο πυρήνας της δύναμης του ΝΑΤΟ προέρχεται από το άρθρο 5 της ιδρυτικής της συνθήκης — μια δέσμευση που μια επίθεση κατά μία χώρα μέλος θα θεωρηθεί επίθεση σε ολόκληρη τη συμμαχία. Ο λόγος που το ΝΑΤΟ είναι τόσο ισχυρό είναι επειδή υπάρχει αμοιβαία ασφάλεια. Αυτό πρακτικά σημαίνει ότι αν μια χώρα δεχθεί επίθεση, τότε όλες οι χώρες δέχονται επίθεση. Θα έπρεπε λοιπόν κάτι τέτοιο να ισχύει και για τις πολιτικές Κυβερνοασφάλειας της ΕΕ που μέχρι τώρα δεν έχει μεριμνήσει για κάτι τέτοιο η ΕΕ.

Από το περιεχόμενο της παραπάνω παραγράφου μάλιστα, θα μπορούσε ίσως να προκύψει μια τρίτη ερευνητική ερώτηση στην εργασία μας, η ερώτηση της «κυβερνοκυριαρχίας» (cyber sovereignty) της Ευρωπαϊκής Ένωσης στο παγκόσμιο τοπίο κυβερνοασφάλειας. Σε μια προσπάθεια ορισμού το όρου «κυβερνοκυριαρχία», θα μπορούσαμε να γράψουμε το εξής: Η έννοια της "κυβερνοκυριαρχίας" αναφέρεται στην ικανότητα ενός κράτους να διαχειρίζεται και να προστατεύει τον κυβερνοχώρο του, συμπεριλαμβανομένων των δικτύων, των συστημάτων και των δεδομένων του, από εξωτερικές απειλές και επιθέσεις. Αυτό περιλαμβάνει την ανάπτυξη και την εφαρμογή πολιτικών, κανονισμών και τεχνολογιών που διασφαλίζουν την ασφάλεια και την ακεραιότητα των ψηφιακών υποδομών και των πληροφοριών του κράτους. Η κυβερνοκυριαρχία είναι κρίσιμη για την εθνική ασφάλεια και την προστασία της ιδιωτικότητας των πολιτών[36].

Η συζήτηση αυτή και η απάντηση του ερωτήματος «Είναι η Ευρωπαϊκή Ένωση ένα cyber sovereign state;», είναι συμπληρωματική της δεύτερης ερευνητικής μας ερώτησης σχετικά με την αποτελεσματικότητα του οικοσυστήματος κυβερνοασφάλειας της Ε.Ε. Αυτό σημαίνει πως απαντώντας την δεύτερη ερευνητική μας ερώτηση, ουσιαστικά ξεκινάμε να απαντάμε εν μέρει την ερώτηση περί cyber sovereignty της ΕΕ. Η απάντηση σε αυτήν την νέα ερώτηση είναι όμως πιο πολύπλοκη και απαιτεί μια νέα συζήτηση και ανάλυση, μιας και πρέπει να οριστούν και τεθούν νέα κριτήρια αξιολόγησης. Σε οποιαδήποτε περίπτωση όμως, η προσπάθεια ανάλυσης και αξιολόγησης της ΕΕ ως cyber sovereign state μας οδηγεί στο να ανακαλύψουμε και να κατανοήσουμε τα προβλήματα και τις αδυναμίες της ΕΕ στο τοπίο της κυβερνοασφάλειας. Παρακάτω λοιπόν, αναλύουμε μερικά από τα προβλήματα που παρατηρήσαμε σχετικά με την κυβερνοασφάλεια στην ΕΕ και που θα μπορούσαν να αποτελέσουν κριτήρια αξιολόγησης της ως cyber sovereign state, σε πιθανή μελλοντική συζήτηση και ανάλυση.

5.2.1 Η πανδημία του Covid

Η πανδημία του Covid-19 ώθησε αναγκαστικά μερικές χώρες στην ανάπτυξη ψηφιακών συστημάτων και στην δημιουργία προγραμμάτων εκπαίδευσης, που προσέφεραν στους Ευρωπαίους τουλάχιστον τις ελάχιστες αναγκαίες γνώσεις για την λειτουργία βασικών τέτοιων συστημάτων[37]. Ενώ ώθησε τον κόσμο στον αποκλεισμό στο σπίτι, ταυτόχρονα βοήθησε και στην ιδέα της συνδεσιμότητας, στις ψηφιακές υποδομές και σε έναν

[36] Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? Journal of Information Warfare, vol. 12, no. 2, 19-26

[37] Χειλά, Ε. (2020). COVID-19 και η «επόμενη μέρα» - Γεωπολιτική, Οικονομία, Διεθνείς θεσμοί. Πειραιάς: Εκδόσεις Πανεπιστημίου Πειραιώς.

ψηφιακά εκπαιδευμένο πληθυσμό, προάγοντας έτσι και την ψηφιακή ενασχόληση και το ταλέντο σε ψηφιακά θέματα από μικρή ηλικία[38].

5.2.2 Το "Skills gap"

Η Ευρώπη υστερεί στην ανάπτυξη ψηφιακών δεξιοτήτων, λέει αξιωματούχος της ΕΕ. Οι προσπάθειες της Επιτροπής να γεμίσουν το κενό των ψηφιακών δεξιοτήτων μέχρι το 2030, κάτι το οποίο αποτελεί βασικό στόχο της στο τοπίο της ψηφιακής ανάπτυξης, φαίνεται να περιπλέκονται από την έλλειψη επενδύσεων καθώς και την αδυναμία επικράτησης της δια βίου μάθησης σε αυτόν τον τομέα.

> *"Σύμφωνα με τη Eurostat, το 2021, το 54% των ατόμων στην ΕΕ ηλικίας 16 έως 74 ετών είχαν τουλάχιστον βασικές συνολικές ψηφιακές δεξιότητες, αλλά ο αριθμός αυτός έφερε μεγάλη ποικιλία – από το 79% στην Ολλανδία και τη Φινλανδία έως το 28% στη Ρουμανία. Επιπλέον, το ποσοστό αυτό πέφτει στο 26% όταν εξετάζουμε άτομα με πιο προηγμένες ψηφιακές δεξιότητες."*[39]

Πρόκειται για ένα ζήτημα που πρέπει να αντιμετωπιστεί άμεσα μέσω της εκπαίδευσης. Είναι αναγκαία η δημιουργία ενός συνεκτικού και αποτελεσματικού οικοσυστήματος ψηφιακής εκπαίδευσης, το οποίο να μπορεί να αναπτύσσει τις δεξιότητες των νέων, αλλά ταυτόχρονα να συντηρεί ένα διαρκές υψηλό επίπεδο σε ποιότητα και ποσότητα συμμετεχόντων. Αυτή η διαδικασία βέβαια δυσκολεύει εξαιτίας των συνεχών αλλαγών που συμβαίνουν στην τεχνολογία και στον ψηφιακό κόσμο. Επίσης, παρατηρείται χαμηλό επίπεδο στην πρόσληψη πληροφορίας από τους Ευρωπαίους ενήλικες. Πιο συγκεκριμένα, το 2021, μόνο το 10.8% των ενηλίκων στην Ευρώπη πήρε μέρος σε εκπαιδευτικά προγράμματα ή σεμινάρια (με τα μεγαλύτερα ποσοστά να εμφανίζονται σε Σουηδία, Φινλανδία και Κάτω Χώρες)[40]. Η αιτιολογία αυτού του φαινομένου φαίνεται να κρύβεται στο κόστος των προγραμμάτων αυτών, καθώς και στην ποιότητα τους. Και αυτός είναι ακόμα ένας λόγος που η εκπαίδευση χρειάζεται στήριξη από την ΕΕ ώστε να καταφέρουν περισσότεροι ενήλικες να έχουν πρόσβαση σε προγράμματα και στην

[38]Bora. (2023). Cybersecurity Marketing in 2023: 12 Industry Experts Look Ahead. Ανάκτηση από Bora, welcometobora.com: https://welcometobora.com/resources/cybersecurity-marketing-industry-experts-look-ahead/

[39]Ellena, S. (2023, March 29). Europe lagging behind on digital skills development, says EU official. Ανάκτηση από Euractiv.com: https://www.euractiv.com/section/economy-jobs/news/europe-lagging-behind-on-digital-skills-development-says-eu-official/

[40] European-Commission. (2023). Three EU targets to set the ambition for 2030. Ανάκτηση από Publications Office of the European Union: https://op.europa.eu/webpub/empl/european-pillar-of-social-rights/en/#chapter2

γνώση. Ταυτόχρονα, η παραδοσιακή εκπαίδευση οφείλει να προσαρμοστεί στις συνεχείς αλλαγές και στην αγορά και να αποκτήσει έναν πιο μοντέρνο χαρακτήρα.

5.2.3 Επενδύσεις

Η βιομηχανία ζητά την κλιμάκωση των επενδύσεων σε ψηφιακές δεξιότητες εν μέσω έλλειψης και αναγνωρίζει την σημασία των επενδύσεων στην κάλυψη του κενού των ψηφιακών δεξιοτήτων. Οι επενδύσεις στις ψηφιακές δεξιότητες και στην εκπαίδευση αυτών θα είναι καθοριστικής σημασίας για το μέλλον της Ευρώπης στον εν λόγω τομέα. Μόνο με σωστή οικονομική στήριξη θα καταφέρει η Ευρώπη να πετύχει τον στόχο που έχει θέσει για το 2030, όπως αναφέραμε νωρίτερα. Οι στόχοι αυτοί, πέρα από τα άμεσα οφέλη όπως η δημιουργία καταρτισμένου προσωπικού και η διατήρηση ενός καλού επιπέδου ψηφιακών γνώσεων εντός ΕΕ, θα φέρει επίσης και άλλα, πιο έμμεσα οφέλη. Το σημαντικότερο αυτών ίσως να είναι η οικονομική ανάπλαση της ΕΕ σε θέματα παγκόσμιας αγοράς, βιομηχανίας και καινοτομίας, έμμεσα αποτελέσματα δηλαδή της ανάπτυξης των ψηφιακών δεξιοτήτων των Ευρωπαίων. Αυτό συμβαίνει γιατί όσο προχωράει η τεχνολογία, τόσο αυξάνονται οι ανάγκες για καταρτισμένο προσωπικό και ταυτόχρονα όλο και μεγαλώνει το κενό αυτό της ειδίκευσης σε ψηφιακά θέματα[41].

> *"Καθώς τώρα όλα ψηφιοποιούνται –χώρες, εταιρείες και ιδιώτες– νομίζω ότι γίνεται ακόμη πιο σαφές ότι η έλλειψη τέτοιων ταλέντων και η πρόσβαση σε αυτά τα ταλέντα, δημιουργεί ένα τεράστιο κενό και η Ευρώπη ίσως ξεχωρίζει αρνητικά από αυτή την άποψη", δήλωσε στο EURACTIV ο Kenneth Fredriksen, εκτελεστικός αντιπρόεδρος για την Κεντρική Ανατολική Ευρώπη και τη Σκανδιναβία της Huawei, στην πρόσφατη σύνοδο κορυφής Huawei Talent Summit στο Ελσίνκι."*

5.2.4 Το "Skills gap" μέσα από τα μάτια της Επιτροπής

Μεγάλο θέμα συζήτησης λοιπόν για την Επιτροπή τα τελευταία χρόνια είναι η ενίσχυση των δεξιοτήτων Κυβερνοασφάλειας στην Ευρώπη για ένα μελλοντικά ασφαλές οικοσύστημα Κυβερνοασφάλειας της ΕΕ. Με άλλα λόγια, το ζήτημα του «skills gap» και τρόποι επίλυσής του.

> *Το ζήτημα αυτό αποκτά ξαφνικά καινούρια δυναμική, μετά από τον πόλεμο στην Ουκρανία. Αυτό είναι εμφανές πια, καθώς και οι Υπουργοί εξωτερικών αποφασίζουν να μιλήσουν και να αναφερθούν στο θέμα «Cyber».*

Αυτά είναι μερικά από αυτά που τόνισε η κα. Σπανού κατά την διάρκεια της διάλεξης της στο EU Cybersecurity Policy Conference που διοργάνωσε η ENISA στις Βρυξέλλες στις 26

[41] Euractiv. (2021, December 14). Industry calls for scaling up investment in digital skills amid shortage. Ανάκτηση από Euractiv.com: https://www.euractiv.com/section/digital/news/industry-calls-for-scaling-up-investment-in-digital-skills-amid-shortage/

Ιανουαρίου 2023. Μεταξύ άλλων, η κα. Σπανού, Επικεφαλής του Συμβουλίου του Αντιπροέδρου Σχινά, είπε τα παρακάτω:

> *Εντελώς νέα αξία μετά τον πόλεμο στην Ουκρανία. Οι Υπουργοί Εσωτερικών μιλούν επιτέλους για τον κυβερνοχώρο. Πολύς κόσμος, σε ιδιωτικούς τομείς, στην αγορά. Πρόκειται για ανθρώπους που δεν έχουμε, άλλο ένα σημαντικό κενό. Επαγγελματίες στον κυβερνοχώρο που να λαμβάνουν πραγματικά υπόψη τις προτάσεις και τα ψηφίσματα της επιτροπής (όπως το NIS κ.λπ). Δεν είναι μόνο οι δεξιότητές στην πληροφορική αλλά και σε άλλους τομείς σπουδών, κοινωνικούς και διεθνείς. Το να παραμένει σταθερό το ανθρώπινο δυναμικό και να μην μειώνεται είναι επίσης πολύ σημαντικό, ώστε να έχουμε τον αριθμό των θέσεων εργασίας που απαιτούνται.*
>
> *Το European Cyber Skills Academy γίνεται πραγματικότητα το 2023. Δεν θα υπονομεύσει τα υπάρχοντα πράγματα, θα είναι αυτό που θα αναθεωρήσει τα πάντα και θα είναι μακροπρόθεσμο. Θα έχει μια συνέχεια, επαγγελματίες που ξεκινούν συνεχώς. Βραχυπρόθεσμα: ένα σώμα κυβερνο-πρακτορείων, καθηγητές που θα κληθούν να βοηθήσουν σε μια κρίση στον κυβερνοχώρο. Οι λειτουργικές ικανότητες της ENISA να ενισχυθούν με αυτόν τον τρόπο στην περίπτωση μιας κρίσης. Πρέπει όμως να βρούμε έναν τρόπο να πιστοποιούμε και άτομα από τον ιδιωτικό τομέα ώστε να μπορούμε να τα χρησιμοποιήσουμε και εμείς. Υπάρχοντες καθηγητές να βοηθήσουν ή να αποκτήσουμε νέους για να παραμείνουν ενεργοί για πολλά χρόνια ακόμα. Μακροπρόθεσμα: να χρησιμοποιήσουμε προγράμματα εκπαίδευσης για να φέρουμε τους νέους να σπουδάσουν και να γίνουν αυτοί οι καθηγητές. Τα ερωτήματα εδώ είναι: Πώς να εκπαιδεύσουμε καθηγητές ιδιωτικά και πώς τους φέρνουμε στην ακαδημία; Με την απάντηση θα υπάρξουν έτοιμοι καθηγητές να εργαστούν στον τομέα αυτόν.*
>
> *Να υπάρξει οικονομική στήριξη για περισσότερες τοπικές ακαδημίες. Θα είναι ένα είδος ομπρέλας για τους πολίτες κάθε χώρας. Το πρόβλημα μέχρι στιγμής είναι ότι τα χρήματα είναι διάσπαρτα και ασυντόνιστα. Έτσι, το πρόγραμμα θα προσπαθήσει να οργανώσει όλον αυτόν τον τομέα συζήτησης και θα αποτελέσει μια συστημική προσέγγιση για τη δημιουργία μιας ομπρέλας.*

5.3 Συζήτηση

5.3.1 Ακαδημία δεξιοτήτων Κυβερνοασφάλειας (Cybersecurity Skills Academy)

Η Ευρωπαϊκή Επιτροπή στις 18 Απριλίου 2023 έθεσε σε λειτουργία την Ακαδημία δεξιοτήτων Κυβερνοασφάλειας (Cybersecurity Skills Academy). Με αυτόν τον τρόπο θα προσπαθήσει να μειώσει όσο περισσότερο γίνεται το κενό που υπάρχει στην Ευρώπη σε θέματα δεξιοτήτων και ειδίκευσης σε θέματα Κυβερνοασφάλειας. Επίσης, επιτυγχάνεται

έτσι αύξηση της ευαισθητοποίησης των πολιτών, καθώς μέσω της ακαδημίας , διαδίδεται περαιτέρω το θέμα της Κυβερνοασφάλειας στην κοινωνία των πολιτών. Επίσης, βελτιώνεται κατά πολύ η ανθεκτικότητα της ΕΕ απέναντι σε κυβερνοεπιθέσεις και περιστατικά που θέτουν σε κίνδυνο τον διαδικτυακό κόσμο της ΕΕ και όχι μόνο.

> *500 εκατομμύρια ειδικοί στον τομέα της Κυβερνοασφάλειας λείπουν για τα επόμενα χρόνια. Χρειαζόμαστε τον κόσμο για να πραγματοποιήσουμε συγκεκριμένες πράξεις. Η ακαδημία έχει στόχο να επιταχύνει τις προσπάθειές μας. Είναι ένα ενιαίο σημείο εισόδου για ευκαιρίες εκπαίδευσης και χρηματοδότησης στον τομέα της Κυβερνοασφάλειας.*

ανακοίνωσε ο Αντιπρόεδρος της Επιτροπής Μαργαρίτης Σχοινάς[42]. [Κέντρο Πολυμέσων του Ευρωπαϊκού Κοινοβουλίου / Frédéric MARVAUX]

Η ακαδημία αυτή είναι μέρος του 2023 European Year of Skills[43], μιας πρωτοβουλίας της Ευρωπαϊκής Επιτροπής να προωθήσει την ανάπτυξη δεξιοτήτων σε θέματα Κυβερνοασφάλειας στην ΕΕ. Σκοπός λοιπόν είναι να επανοριστούν οι αναγκαίες γνώσεις και δεξιότητες και να επανδρωθούν εκ νέου οι οργανισμοί και οι επιχειρήσεις με νέους ειδικευμένους στον τομέα του διαδικτύου και της ασφάλειάς του. Όπως έχει αναφερθεί επανειλημμένως από την Επιτροπή, καθώς και σε αυτήν την εργασία, υπάρχει μια εμφανής έλλειψη (Cyber gap, όπως το ονομάζει η Επιτροπή) σε ταλέντα και γνώσεις γύρω από την Κυβερνοασφάλεια. Πράγματι, η Ευρώπη βρίσκεται σε άμεση ανάγκη ειδικευόμενων για να εργαστούν για την διασφάλιση την ασφάλειας της. Δεν μιλάμε βέβαια μόνο για γνώστες των θεωριών συμμόρφωσης με τους νόμους, αλλά και για IT specialists που θα μπορούν να ανταποκριθούν στις αυξημένες απαιτήσεις των περιστατικών κυβερνοεπιθέσεων που δέχεται η Ευρώπη από χώρες όπως η Ρωσία ή η Κίνα. Μόνο με μεγαλύτερο αριθμό τέτοιων ειδικών θα καταφέρει η Ευρώπη να ανταπεξέλθει πραγματικά στον συνεχώς αυξανόμενο αριθμό επιθέσεων και η ακαδημία είναι ίσως ο καλύτερος τρόπος να σιγουρευτούμε πως θα τα καταφέρουμε.

> *"Η Κυβερνοασφάλεια είναι μια αυξανόμενη ανησυχία για όλους. Ωστόσο, εξακολουθεί να υπάρχει περιορισμένη κατανόηση για το πώς να προστατευτούμε στην πράξη – η περιορισμένη συγκέντρωση εμπειρογνωμόνων, η μακροχρόνια εμπειρία διαχείρισης κινδύνων για την ασφάλεια στον κυβερνοχώρο και η*

[42]Euractiv. (2023, April 19). EU seeks to bridge cyber-skills gap with new 'academy'. Ανάκτηση από Euractiv.com: https://www.euractiv.com/section/cybersecurity/news/eu-seeks-to-bridge-cyber-skills-gap-with-new-academy/

[43]European-Commission. (2023). European Year of Skills 2023. Ανάκτηση από commission.europa.eu: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-year-skills-2023_en

συνεχώς εξελισσόμενη τεχνολογία και το τοπίο απειλών έχουν δημιουργήσει ένα κενό"

δήλωσε η Iva Tasheva, επικεφαλής της Κυβερνοασφάλειας στην εταιρεία συμβούλων CYEN, στην EURACTIV.

Η ακαδημία, που όπως είπαμε είναι μια πρωτοβουλία της Επιτροπής, θα προσπαθήσει να μειώσει την έλλειψη της Ευρώπης σε καταρτισμένο προσωπικό και αυτό θα το καταφέρει μέσω ειδικής εκπαίδευσης καθώς και μέσω προγραμμάτων κατάρτισης.

'Πρωτοβουλίες όπως η EU Cybersecurity Skills Academy είναι βήματα προς τη σωστή κατεύθυνση από τους υπεύθυνους χάραξης πολιτικής για τη μείωση του χάσματος ψηφιακών δεξιοτήτων μέσω της εκπαίδευσης και της κατάρτισης σε όλες τις ηλικίες. Αυτή είναι μια τεράστια πολύπλευρη πρόκληση που απαιτεί τη συγκέντρωση όλων των ενδιαφερομένων στο τραπέζι.'

δήλωσε στο EURACTIV ο Chris Gow, επικεφαλής δημόσιας πολιτικής της ΕΕ στη Cisco.

Για να κατανοήσουμε περισσότερο την λειτουργία της Ακαδημίας, θα πρέπει να δούμε τα βασικά χαρακτηριστικά της ως δράση. Ποιοι είναι λοιπόν οι βασικοί πυλώνες πάνω στους οποίους βασίζεται η λειτουργία της ακαδημίας;

Οι 4 βασικοί πυλώνες της EU Cybersecurity Skills Academy:

1) Εκπαιδευτικά προγράμματα για κατάρτιση των συμμετεχόντων σε θέματα Κυβερνοασφάλειας.
2) Πιστοποιήσεις και δυνατότητες υποτροφιών.
3) Stakeholders και ο ρόλος τους στην ανάπτυξη των δεξιοτήτων των συμμετεχόντων.
4) Ανάπτυξη μεθοδολογίας για έλεγχο της ανάπτυξης της αγοράς και της ανάγκης καταρτισμένου προσωπικού.

5.3.2 Ο Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας (DESI- Digital Economy and Society Index)

Ο Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας (**DESI- Digital Economy and Society Index**) είναι ένας δείκτης που μετρά, σε διάρκεια ενός χρόνου, το κατά πόσο επιτυγχάνονται οι στόχοι που θέτει η Ευρωπαϊκή Ένωση και τα όργανα της στα κράτη-μέλη. Για το έτος 2022 λοιπόν, ο DESI έδειξε ότι η εισβολή της Ρωσίας στην Ουκρανία "*καθιστά την εφαρμογή καινοτόμων ψηφιακών λύσεων, τεχνολογιών και υποδομών που*

βασίζονται στις αξίες και τις αρχές της ΕΕ, καθώς και την ενίσχυση της Κυβερνοασφάλειας, ακόμη πιο σχετική"[44].

Είναι ένα πρόβλημα που αγγίζει όλους τους δρώντες αλλά μόνο οι μεγάλες επιχειρήσεις έχουν προς το παρόν την οικονομική δυνατότητα και την τεχνογνωσία να έχουν μεγάλες και ικανές ομάδες Κυβερνοασφάλειας, αφήνοντας τις μικρομεσαίες επιχειρήσεις ευάλωτες σε επιθέσεις και πειράματα. Έτσι, ακόμα ένας καινούργιος όρος εμφανίζεται στο παγκόσμιο λεξιλόγιο, η λεγόμενη Κυβερνο-φτώχεια (Cyberpoverty), για την οποία ήδη γίνεται συζήτηση και προκαλείται ανησυχία από τους policymakers για την επίλυσή της. Κοινή γνώμη πια πως το να παίρνονται αποφάσεις που υποστηρίζονται από κενούς οργανισμούς ή ανύπαρκτο προσωπικό, δεν είναι η λύση στο πρόβλημα. Εδώ είναι λοιπόν που έρχεται να δώσει την απάντηση στο πρόβλημα η Ακαδημία.

5.3.3 Οι στόχοι για το 2030

Οι στόχοι τους οποίους έχει θέσει η επιτροπή μέχρι το τέλος αυτής της δεκαετίας είναι ξεκάθαροι και μετρήσιμοι: 80% των ενήλικων Ευρωπαίων πολιτών να έχουν τις βασικές ικανότητες του ψηφιακού κόσμου , όπως επίσης και 20 εκατομμύρια εργαζόμενοι, ειδικευμένοι στην τεχνολογία πληροφορίας και επικοινωνιών (Information and communications technology-ICT). Αυτοί οι στόχοι είναι πράγματι επιτεύξιμοι, αρκεί να τεθεί σε άμεση ισχύ η λειτουργία της ακαδημίας αλλά και όλων των εκπαιδευτικών προγραμμάτων που αυτή θα προσφέρει. Σημαντικό είναι οι προσπάθειες αυτές να επικεντρωθούν σε ηλικίες κάτω των 30 χρονών, ώστε να είναι πιθανότερο οι γνώσεις που θα μεταδοθούν να μπορέσουν να διατηρηθούν σε βάθος χρόνου. Νέοι και νέες που θα αποκτήσουν αυτές τις γνώσεις μέχρι το 2030, είναι πολύ πιθανό πως θα βρουν με αυτό τον τρόπο την πρώτη τους δουλειά στον τομέα της ασφάλειας του κυβερνοχώρου και θα συμβάλλουν επίσης δυναμικά στην μελλοντική ανάπτυξη του χώρου και γιατί όχι στην μετέπειτα εκπαίδευση καινούργιου ανθρώπινου δυναμικού. Όπως έχουμε αναφέρει ήδη, στόχος και ταυτόχρονα πρόκληση αυτής της νέας πρωτοβουλίας της Επιτροπής, είναι να αυξήσει τον αριθμό των τεχνικά καταρτισμένων ανθρώπων του χώρου, να βελτιώσει τις γνώσεις των πολιτών και να μειώσει το κενό που υπάρχει σε θέματα Κυβερνοασφάλειας στην Ευρώπη. Η εκπαίδευση παραμένει βασικό εργαλείο της ΕΕ, είναι όμως ταυτόχρονα και εθνικό καθήκον να επιτευχθούν οι παραπάνω στόχοι μέχρι το τέλος του 2030.

[44]European-Commission. (2022). Digital Economy and Society Index (DESI)

5.3.4 Ευρωπαϊκό πλαίσιο δεξιοτήτων για την ασφάλεια στον κυβερνοχώρο (ECSF-European Cybersecurity Skills Framework)

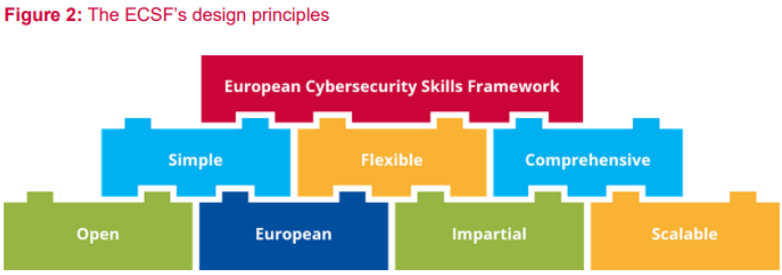
Πρόκειται για ένα ανοιχτό ευρωπαϊκό εργαλείο για την οικοδόμηση κοινής κατανόησης των προφίλ επαγγελματικών ρόλων στον κυβερνοχώρο και κοινών χαρτογραφήσεων με τις κατάλληλες δεξιότητες και ικανότητες που απαιτούνται[45].

Για να κατανοήσουμε το κενό που υπάρχει σε θέματα Κυβερνοασφάλειας της ΕΕ, θα πρέπει πρώτα να κατανοήσουμε τα κενά που έχουν οι νέοι επαγγελματίες του κλάδου.

Κενά και έλλειψη δεξιοτήτων στον κυβερνοχώρο:
- Μη καλυμμένες θέσεις
- Δεξιότητες που δεν αποκτήθηκαν
- οι απαιτούμενες δεξιότητες συνεχώς αυξάνονται
- Σχηματίστηκαν επαγγελματίες;

Με αυτό το πλαίσιο προσπαθεί η ΕΕ να δημιουργήσει μια κοινή κατανόηση των ρόλων, των δεξιοτήτων και των γνώσεων, να διευκολύνει την αναγνώριση δεξιοτήτων στον κυβερνοχώρο, να υποστηρίξει τον σχεδιασμό εκπαιδευτικών προγραμμάτων που σχετίζονται με τον κυβερνοχώρο.

Εικόνα 9: Οι βασικές αρχές του ECSF

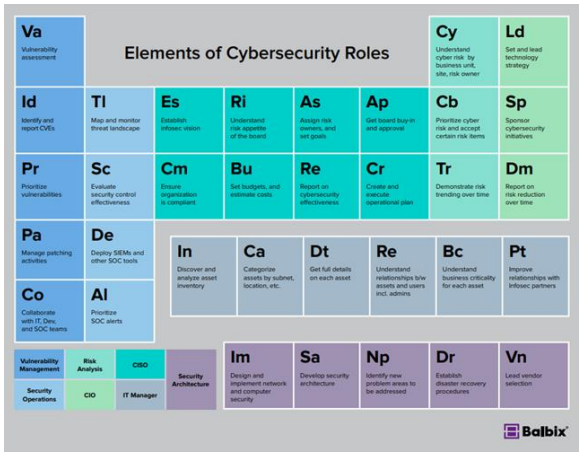


Πηγή: European Cybersecurity Skills Framework, https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Με βάση τα παραπάνω, θα μπορούσε να επιτευχθεί το μέγιστο στην κατανομή των ρόλων του προσωπικού που ασχολείται με την Κυβερνοασφάλεια, τόσο σε θεωρητικό, όσο και σε τεχνικό επίπεδο.

[45] ENISA. (2022, September). European Cybersecurity Skills Framework (ECSF). Ανάκτηση από enisa.com: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Εικόνα 10: Τα «χημικά στοιχεία» των ρόλων Κυβερνοασφάλειας



Πηγή: https://www.balbix.com/insights/what-is-cyber-security-posture/

Κεφάλαιο 6ο: Συμπεράσματα

6.1 Τα οφέλη του ECSF

Συνεχίζοντας με το ECSF, ας μιλήσουμε για τα οφέλη του από διαφορετικές μεριές και οπτικές. Το ECSF είναι χρήσιμο στα εξής:

6.1.1 Τα οφέλη από την μεριά της οργάνωσης

- Ανάπτυξη στρατηγικής Κυβερνοασφάλειας, οργανωτική δομή και σχεδιασμός ανθρώπινου δυναμικού
- Προσδιορισμός θέσεων εργασίας, προφίλ ρόλων, αναγκών πρόσληψης και άλλων τύπων προδιαγραφών
- Ταυτοποίηση και αξιολόγηση υποψηφίων
- Εκτέλεση ρόλων Κυβερνοασφάλειας και ανάλυση κενού δεξιοτήτων και πρόβλεψη αναγκών σε ατομικό, ομαδικό ή οργανωτικό επίπεδο, καθορίζει σχέδια ανάπτυξης και εκπαίδευσης σε επίπεδο ατόμου, ομάδας ή οργανισμού
- Χρήση μιας κοινής και ρεαλιστικής γλώσσας για διαγωνισμούς Cybersecurity

6.1.2 Τα οφέλη από την μεριά των παρόχων μάθησης

- Σχεδιασμός εκπαιδευτικών προγραμμάτων και προγραμμάτων σπουδών
- Συνεργασία μεταξύ ιδρυμάτων και βελτίωση της κινητικότητας των προγραμμάτων μάθησης, π.χ. διευρωπαϊκά προγράμματα για όλους
- Προώθηση των μαθησιακών προσφορών και να ευαισθητοποίηση
- Αποτελέσματα εύρεσης θέσεων σε πραγματικό περιβάλλον εργασίας
- Διενέργεια διαδικασιών αξιολόγησης και αναγνώρισης
- Παροχή επαγγελματικού προσανατολισμού στους μαθητές

6.1.3 Τα οφέλη από την μεριά των policy makers και των legal stakeholders:

Πρόκειται για ένα επαγγελματικό και εύκολα προσβάσιμο εργαλείο που βοηθά στα εξής:

- Κατανόηση των τομέων Κυβερνοασφάλειας
- Τόνωση του σχεδιασμού προτεραιότητας και ανάπτυξης ικανοτήτων για την ασφάλεια στον κυβερνοχώρο
- Χαρτογράφηση πολλαπλών πρωτοβουλιών για την ασφάλεια στον κυβερνοχώρο
- Υποστήριξη πολιτικών πρωτοβουλιών που βασίζονται στην ανάλυση δεδομένων

Εικόνα 11: Τα 5 βήματα της εφαρμογής του ESCF.

Πηγή: European Cybersecurity Skills Framework, European Cybersecurity Skills Framework User Manual.pdf

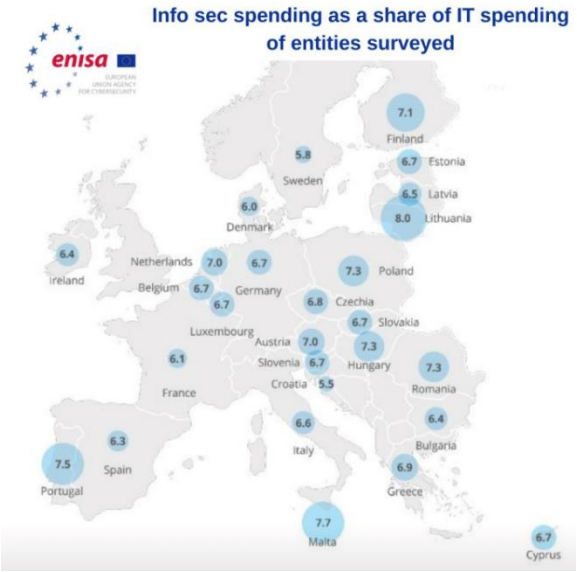
Ένας βασικός οδηγός 5 βημάτων για την επιτυχία της εφαρμογής του ESCF

1. Ανάλυση του περιβάλλοντος-στόχου
2. Προσδιορισμός συγκεκριμένων στόχων
3. Επιλογή κατάλληλων εξαρτημάτων
4. Προσαρμογή επιλεγμένων στοιχείων
5. Εφαρμογή προσαρμοσμένων εξαρτημάτων

6.2 NIS2 και Επενδύσεις

Η έκθεση του ENISA για τις επενδύσεις σχετικά με την οδηγία NIS ανέλυσε περισσότερους από 1000 φορείς ή οντότητες σχετικές με Κυβερνοασφάλεια και δείχνει το ποσοστό του προϋπολογισμού IT που αφιερώνεται στην Κυβερνοασφάλεια σε κάθε χώρα της Ε.Ε.

Εικόνα 12: οι επενδύσεις των χωρών της ΕΕ σε μονάδες.



Πηγή: https://www.enisa.europa.eu/publications/nis-investments-2022

Αυτή η έκθεση είναι ουσιαστικά μια τρίτη έκδοση της έκθεσης NIS Investments του ENISA. Στην έκθεση αυτή, ο ENISA έχει συλλέξει δεδομένα που σχετίζονται με φορείς εκμετάλλευσης βασικών υπηρεσιών (OES) και παρόχους ψηφιακών υπηρεσιών (DSP) που ορίζονται στην οδηγία της Ευρωπαϊκής Ένωσης για την ασφάλεια δικτύων και συστημάτων πληροφοριών (NIS). Δείχνει τον τρόπο με τον οποίο οι φορείς αυτοί χρησιμοποιούν τους προϋπολογισμούς τους και επενδύουν στον τομέα της Κυβερνοασφάλειας και πώς αυτές οι επενδύσεις έχουν επηρεαστεί από την Οδηγία NIS. Παρουσιάζονται οι τάσεις της παγκόσμιας αγοράς Κυβερνοασφάλειας μέσω δεδομένων που παρατηρούνται παγκοσμίως αλλά και στην ΕΕ, και με αυτόν τον τρόπο υπάρχει καλύτερη κατανόηση της κατάστασης. Η έκδοση αυτή της έκθεσης περιέχει δεδομένα που συλλέχθηκαν από 1080 OES (operators of essential services) και DSPs (digital service providers) και από τα 27 κράτη μέλη της ΕΕ και τα δεδομένα που παρέχονται βοηθούν στην σύγκριση και στον προσδιορισμό των τάσεων από έτος σε έτος.

Οι ερωτήσεις που προκύπτουν από αυτού του είδους τις έρευνες είναι οι εξής: Είναι αρκετές οι επενδύσεις της ΕΕ στον τομέα της Κυβερνοασφάλειας[46]; Είναι αρκετά τα χρήματα για να πληρούνται τα νέα πρότυπα Κυβερνοασφάλειας; Αν ναι, είναι αρκετές οι επενδύσεις σε όλους τους τομείς, όπως για την πρόοδο σε τεχνικά κομμάτια του Cyber ή

[46]ENISA. (2022, November 23). Cybersecurity Investments in the EU: Is the Money Enough to Meet the New Cybersecurity Standards? Ανάκτηση από enisa.europa.eu: https://www.enisa.europa.eu/news/cybersecurity-investments-in-the-eu-is-the-money-enough-to-meet-the-new-cybersecurity-standards

παραμένουν οι επενδύσεις μόνο σε θεωρητικούς τομείς όπως το regulations και policies κομμάτι;

Ο Εκτελεστικός Διευθυντής του ENISA, Juhan Lepassaar, δήλωσε:

> *"Η ανθεκτικότητα των κρίσιμων υποδομών και τεχνολογιών μας στην ΕΕ θα εξαρτηθεί σε μεγάλο βαθμό από την ικανότητά μας να κάνουμε στρατηγικές επενδύσεις. Είμαι βέβαιος ότι έχουμε την ικανότητα και τις δεξιότητες που μας οδηγούν για να πετύχουμε τον στόχο μας, που είναι να διασφαλίσουμε ότι θα έχουμε τους επαρκείς πόρους στη διάθεσή μας για να αναπτύξουμε περαιτέρω τις ικανότητές μας στον τομέα της Κυβερνοασφάλειας…."*

Στόχος της οδηγίας NIS (οδηγίας για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών) είναι η επίτευξη κοινής κατεύθυνσης για όλα τα κράτη μέλη σε θέματα Κυβερνοασφάλειας και ταυτόχρονα ένα υψηλό επίπεδο επιτυχίας αυτής. Η οδηγία NIS έχει 3 βασικούς πυλώνες λειτουργίας και ο ένας από αυτούς είναι η εφαρμογή της διαχείρισης κινδύνου και αναφορών (risk management and reporting obligations) για το OES και το DSP. Οι OES (Operators of Essential Services) προσφέρουν βοήθεια και βασικές υπηρεσίες σε τομείς ενέργειας με στρατηγική σημασία (ηλεκτρισμός, πετρέλαιο και φυσικό αέριο), σε θέματα μεταφορών (αεροπορικές, σιδηροδρομικές, υδάτινες και οδικές), σε τραπεζικές υποδομές, υποδομές χρηματοπιστωτικών αγορών, στην υγεία, στην παροχή και διανομή πόσιμου νερού και σε ψηφιακές υποδομές (σημεία ανταλλαγής Διαδικτύου, πάροχοι υπηρεσιών συστήματος ονομάτων τομέα, μητρώα ονομάτων τομέα ανωτάτου επιπέδου) (Internet exchange points, domain name system service providers, top-level domain name registries). Οι DSP (digital service providers) έχουν ισχύ σε περιβάλλοντα του διαδικτύου, όπως για παράδειγμα σε διαδικτυακές αγορές, ηλεκτρονικές μηχανές αναζήτησης και υπηρεσίες cloud.

Η έκθεση λοιπόν NIS Investments του ENISA, εξετάζει με ποιόν τρόπο οι φορείς εκμετάλλευσης επενδύουν στην Κυβερνοασφάλεια και πως έπειτα συμμορφώνονται στους στόχους της οδηγίας NIS. Επίσης, μέσω της έκθεσης, γίνεται και μια επισκόπηση της κατάστασης σε διάφορα θέματα άμεσου ενδιαφέροντος, όπως η το πως στελεχώνεται η ασφάλεια της πληροφορικής, η ασφάλεια στον κυβερνοχώρο και πως οργανώνεται η ασφάλεια πληροφοριών σε OES και DSP.

6.2.1 Παράμετροι της ανάλυσης

Η ανάλυση της έκθεσης περιλαμβάνει και αφορά περισσότερους από 1000 φορείς από τα 27 κράτη μέλη της ΕΕ. Τα αποτελέσματα της αποδεικνύουν ότι το ποσοστό του προϋπολογισμού της πληροφορικής που αφιερώνεται στην Ασφάλεια Πληροφοριών (IS) είναι χαμηλότερο από αυτό του περασμένου έτους. Πιο συγκεκριμένα, το ποσοστό

μειώθηκε από 7,7% σε 6,7%. Πρόκειται για γενικούς δείκτες που δείχνουν την ασφάλεια των πληροφοριών σε ένα ιδιαιτέρως πολύπλοκο περιβάλλον που καθορίζεται από πολλά, στρατηγικά ή μη, χαρακτηριστικά. Για παράδειγμα, μακροοικονομικά απρόοπτα όπως ο COVID19 μπορεί να έχουν επηρεάσει τα μέσα αποτελέσματα.

6.2.2 Βασικά αποτελέσματα της ανάλυσης

Κύριοι παράγοντες επηρεασμού του προϋπολογισμού για την ασφάλεια των πληροφοριών είναι προφανώς η οδηγία NIS, άλλες νομοθεσίες που ίσως δημοσιεύονται παράλληλα και επίσης το περιβάλλον απειλών. Τα πρώτα και κυριότερα αποτελέσματα της ανάλυσης είναι τα εξής:

- Η υγεία και οι τράπεζες είναι οι τομείς που πλήττονται εντονότερα, σε σχέση με άλλους τομείς, σε περίπτωση σοβαρών περιστατικών απειλής στον κυβερνοχώρο, με το μέσο άμεσο κόστος ενός περιστατικού σε αυτούς τους τομείς να ανέρχεται σε 300.000 ευρώ.
- Η ασφάλεια στον κυβερνοχώρο (insurance in cyberspace) μειώθηκε κατά 13% το 2021 και έτσι έφτασε στο πολύ χαμηλό 30% σε σύγκριση με το 2020.
- Μόνο το 5% των ΜΜΕ είναι συνδρομητές στην ασφάλεια στον κυβερνοχώρο.

Αξίζει επίσης να γίνει και μια σύντομη αναφορά στα βασικά αποτελέσματα σχετικά με τους τομείς Υγείας και Ενέργειας, που φαίνεται να έχουν επηρεαστεί έντονα από τις εξελίξεις των τελευταίων χρόνων, και ιδιαίτερα από την πανδημία του Covid-19

6.2.3 Υγεία

Ο COVID-19 φαίνεται να έχει επηρεάσει σε πολύ μεγάλο βαθμό τις επενδύσεις σε θέματα Κυβερνοασφάλειας και μάλιστα σε παγκόσμιο επίπεδο. Αυτό θα σκεφτόταν κανείς πως οφείλεται στο γεγονός πως πολλά νοσοκομεία αναζητούν τεχνολογίες για την επέκταση των υπηρεσιών υγειονομικής περίθαλψης και σε κάλυψη προβλημάτων του κυβερνοχώρου. Παρόλα αυτά, οι έλεγχοι σχετικά με την Κυβερνοασφάλεια παραμένουν κορυφαία προτεραιότητα για τις επενδύσεις, καθώς το 55% των φορέων υγείας αναζητά αυξημένη χρηματοδότηση για εργαλεία Κυβερνοασφάλειας.

6.2.3 Ενέργεια

Οι φορείς εκμετάλλευσης πετρελαίου και φυσικού αερίου φαίνεται να δίνουν ξεκάθαρα προτεραιότητα στην Κυβερνοασφάλεια. Αυτό αποδεικνύεται από το γεγονός πως οι επενδύσεις αυξάνονται και φτάνουν σε ποσοστό το 74%. Ο ενεργειακός τομέας παρουσιάζει μια τάση στις επενδύσεις, οι οποίες μετατοπίζονται από τις παλαιού τύπου υποδομές και τα κέντρα δεδομένων προς τις υπηρεσίες cloud.

6.3 Το μέλλον του Κυβερνοχώρου

Το μέλλον του Κυβερνοχώρου είναι σύνθετο και το AI το κάνει ακόμα πιο πολύπλοκο. Οι νέες πολιτικές δεν είναι τρόπος να προχωρήσουμε μπροστά, έχουμε ήδη αρκετές πολιτικές και πρέπει να τις εφαρμόσουμε. Ο εντοπισμός του προβλήματος είναι το πρώτο βήμα. Όλες οι τεχνολογίες που αναπτύσσονται είναι σχεδόν ανεξάρτητες των πολιτικών που εισάγονται σε αυτόν τον τομέα.

Ένας τομέας που πρέπει να συζητήσουμε περισσότερο σε επίπεδο ΕΕ είναι η καινοτομία. Υπάρχουν ήδη εθνικές στρατηγικές καινοτομίας, και χώρες όπως η Κίνα, η Αυστραλία, οι ΗΠΑ καθώς επίσης και καινοτόμες βιομηχανίες όπως η nasa, η amazon, η google, που εξελίσσονται συνεχώς με σκοπό να είναι πάντα μπροστά από τις εξελίξεις. Τέτοια παραδείγματα είναι που μπορούν να κατευθύνουν και την ΕΕ και να μας κάνουν να αναρωτηθούμε: Τι κάνουν αυτοί οι δρώντες και πως μπορούμε να προσαρμόσουμε στις πολιτικές της ΕΕ με όμοια κατεύθυνση; Η καινοτομία μπορεί να γίνει διαχειρίσιμη για να έχει ξεκάθαρο στόχο. Το χρειαζόμαστε, γιατί πρέπει να ξέρουμε τι θέλουμε να κάνουμε και που θέλουμε να φτάσουμε.

Αυτό που παρατηρούμε ότι λείπει για την σωστή εφαρμογή και επιτυχία της καινοτομίας είναι τα εξής:

- Συμφωνημένο λεξιλόγιο.
- Ένα πεδίο εφαρμογής
- Ένα οικοσύστημα για τη δημιουργία μιας συγκεκριμένης νοοτροπίας. (Κόμβος καινοτομίας άμυνας)
- Διακυβέρνηση (παρόμοια ή ίδια για όλους)
- Αληθοφανείς προσδοκίες

Πράγματι, τα μέσα καινοτομίας θα πρέπει να έχουν ως πιθανότητα την αποτυχία. Που θα πρέπει να επικεντρωθούμε όμως, εκτός από τα παραπάνω πεδία που φαίνεται να λείπουν από την σημερινή καινοτομία της ΕΕ; Την ερώτηση αυτή θα προσπαθήσουμε να την απαντήσουμε στο επόμενο κεφάλαιο.

Στην συνέχεια, μια άλλη παρατήρηση για το μέλλον της Κυβερνοασφάλειας στην ΕΕ είναι οι κυρώσεις και η εποπτεία (supervision) που οφείλουν να αλλάζουν και να προσαρμόζονται συνεχώς ανάλογα με την κάθε περίσταση και σοβαρότητα του γεγονότος. Η έλλειψη ικανότητας επισκόπησης των καταστάσεων δημιουργεί όμως πρόβλημα σε αυτό. Θα πρέπει να βρεθεί μια ισορροπία και σε οποιαδήποτε περίπτωση απαραίτητο είναι να κατανοήσουμε τις ανάγκες και να αντιμετωπίσουμε την κατάσταση αναλόγως.

Ως προς τις απαιτήσεις ασφαλείας; Πώς μπορούμε να τις μεταφράσουμε; Τρία είναι τα βασικά αποτελέσματα σχετικά με τις απαιτήσεις ασφαλείας που έχει η ΕΕ το 2023:

1) Το επίπεδο των απειλών είναι υψηλό. Οι επιτιθέμενοι αποδεικνύουν ότι κατέχουν ικανότητες κατασκοπείας.

2) Τα θύματα: από ότι παρατηρούμε, οι πρώτοι και ευκολότεροι στόχοι είναι οι μικρομεσαίες επιχειρήσεις - τα msme (Micro, Small & Medium Enterprises).

3) Λιγότερα περιστατικά συμβαίνουν σε λιγότερο προστατευμένες οντότητες. Αυτό συμβαίνει γιατί οι λιγότερο προστατευμένες οντότητες έχουν μικρότερο ενδιαφέρον συνήθως για τους κακόβουλους χρήστες. Επίσης, πολλές επιθέσεις συμβαίνουν λόγω τρωτών σημείων που είναι γνωστά.

Τα συστήματα καινοτομίας όμως που έχει η ΕΕ, εστιάζουν μόνο σε ένα μέρος του προβλήματος. Η υλοποίηση των λύσεων για τα προαναφερθέντα προβλήματα και ελλείψεις δεν είναι πάντα δυνατή μέσω της καινοτομίας. Οι Κυβερνήσεις των κρατών μελών ή τα όργανα της ΕΕ, φαίνεται πως δεν επιλέγουν τους σωστούς ανθρώπους για να στελεχώσουν τις ομάδες εργασίας που θα επιλύσουν τα προβλήματα και θα μειώσουν τις ελλείψεις. Με συγκεκριμένη νοοτροπία και με σωστή χρηματοδότηση όμως θα μπορούσαν να επιτευχθούν περισσότερα.

Πρέπει επίσης να ακούμε την αγορά, όχι μόνο την καινοτομία. Οι τελικοί χρήστες των συστημάτων Κυβερνοασφάλειας, οι εγγυητές ασφαλείας (εταιρείες που αναπτύσσουν λογισμικά και συστήματα Κυβερνοασφάλειας) και επίσης η βιομηχανία είναι μέρος της αγοράς αυτής. Πώς μπορούμε να μοιραστούμε δεδομένα μεταξύ μας και να πειραματιστούμε μαζί τους; Χτίζοντας το οικοσύστημα καινοτομίας στον κυβερνοχώρο στην Ευρώπη ίσως να μπορέσουμε να το πετύχουμε. Ο σκοπός θα είναι να βελτιώσουμε τη θέση που βρισκόμαστε τώρα, τη θέση της ΕΕ στον κόσμο της Κυβερνοασφάλειας σε παγκόσμιο επίπεδο. Σε αυτό το κομμάτι είναι σημαντική η χρήση μιας “τριπλέτας” χαρακτηριστικών, γνωστών στον ψηφιακό κόσμο και στην Κυβερνοασφάλεια. Πρόκειται για το **Triple S:** sociotechnical - sustainability – sovereignty[47].

6.3.1 Εφαρμογή της NIS2

Πέραν των όσων έχουμε προαναφέρει για την οδηγία NIS2 στα παραπάνω κεφάλαια, σημαντική είναι η συμμετοχή του ιδιωτικού τομέα για τον κυβερνοχώρο για να βοηθήσει στην εφαρμογή NIS, να υποστηρίξει δηλαδή την στρατηγική της ΕΕ για το μέλλον. Η

[47]Askoxylakis, I. (2019, June 3). https://www.enisa.europa.eu/events/past#b_start=0. Ανάκτηση από ENISA: https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf

επιχειρηματική πλευρά αυτής της ιδέας είναι να χρησιμοποιηθούν όσα περισσότερα εργαλεία και μέσα γίνεται. Για να δημιουργήσουμε δηλαδή δυνατότητες σε μερικά σημεία της Κυβερνοασφάλειας, στα οποία ξεκινάμε από το μηδέν. Ωστόσο, πρέπει να γίνει πολλή δουλειά σε επίπεδο ΕΕ μεταξύ των κρατών μελών και της ENISA ή άλλων φορέων.

Ποια είναι η όμως η πρωτοτυπία του NIS2; Έχουμε δει πολλά από αυτά τα ψηφίσματα, άλλα με μικρότερη και άλλα με μεγαλύτερη επιρροή στην κοινή γνώμη ή στην κοινωνία γενικότερα. Το NIS μπαίνει όμως σε εθνικό επίπεδο. Αυτό βέβαια προσθέτει πολλές προκλήσεις. Ο προϋπολογισμός είναι επιτέλους διαθέσιμος για υλοποίηση. Αλλά εξακολουθεί να εστιάζει πολύ στην ανίχνευση και την πρόληψη. Οι κατευθυντήριες γραμμές έρχονται σε μορφή προτροπής και έτσι το κομμάτι της πρόληψης θα είναι πιο εστιασμένο. Επίσης έρχονται πολλές αλλαγές και για τον ιδιωτικό τομέα, όπου θα έχουμε πια και ανταλλαγή πληροφοριών μεταξύ των κρατών μελών και ιδιωτικού τομέα και επικοινωνία και συνεργασία ιδιωτικού και δημόσιου τομέα.

Η συνεργασία είναι πράγματι βασικό θέμα. Ο ιδιωτικός τομέας όμως; Πως θα καταφέρει να μπει έντονα στο παιχνίδι της Κυβερνοασφάλειας σε Ευρωπαϊκό επίπεδο; Απαιτούνται μέτρα στον κυβερνοχώρο από ιδιώτες και υπάρχει ήδη μια ενθάρρυνση από την ΕΕ να εισαχθεί ο ιδιωτικός τομέας πιο αποφασιστικά. Υπάρχουν κάποιες συγκρούσεις συμφερόντων μεταξύ τους, αλλά πρέπει να υπάρχει επικοινωνία και μία από τις βασικές προκλήσεις θα είναι να δημιουργηθεί ένα περιβάλλον όπου όλοι οι οργανισμοί θα μπορούν να εκφέρουν άποψη.

Ένα άλλο θέμα είναι οι εθνικές στρατηγικές στον κυβερνοχώρο. Θα υπάρξουν κατευθυντήριες γραμμές από την ΕΕ; Πώς θα εναρμονιστούν όσο το δυνατόν περισσότερο οι εθνικές στρατηγικές; Ίσως ένα πρώτο βήμα είναι να ξεκινήσουν πιο ουσιαστικές συζητήσεις με ομάδες συνεργασίας της ΕΕ για τις προτεραιότητες και τα βήματα που πρέπει να ακολουθηθούν. Παράλληλα, εθνικές ομάδες μπορούν να αποτελέσουν σύνδεσμο για επικοινωνία μεταξύ κράτους-μέλους και ΕΕ. Οι ομάδες αυτές θα μπορούσαν να είναι ομάδες ειδικών για το μέλλον της Κυβερνοασφάλειας σε εθνικό επίπεδο.

Εν συνεχεία, θα υπάρξει κάποια επιβολή προστίμου ή άλλης ποινής για να συμμορφωθούν οι εταιρείες; Η ντιρεκτίβα NIS2 αναφέρει πως εξαρτάται από το έθνος να συμμορφωθεί/συμμορφώσει. Προτείνει επίσης ένα πλαίσιο ενίσχυσης με τα ελάχιστα εργαλεία που βοηθούν στην επίβλεψη και την επιβολή. Είναι μια πιο εναρμονισμένη προσέγγιση για όλους τους φορείς και αποτελεί μια πιο περίπλοκη προσέγγιση για τις εθνικές αρχές. Το ένστικτο που προκύπτει από τη NIS2 λοιπόν δεν είναι να υπάρχει ο φόβος της τιμωρίας, αλλά να υπάρχει θέληση συμμόρφωσης ή υιοθέτησης των μέτρων.

Δεν έχει αξία να υπάρχουν απαιτήσεις που να αποδεικνύουν απλά κανόνες και υποχρεώσεις πράξεων και δράσεων. Το ζητούμενο είναι να υπάρχει διάλογος, να μιλάμε την ίδια γλώσσα. Από τη μια πλευρά, πρέπει να υπάρχει επίβλεψη. Από την άλλη, οι εταιρείες συνηθίζουν σε κυρώσεις και άλλα μέσα συμμόρφωσης στους κανόνες. Πρέπει λοιπόν να υπάρχει ισορροπία και εμπιστοσύνη μεταξύ των stakeholders. Άρα δεν υπάρχει συγκεκριμένη διαδρομή που να είναι προδιαγεγραμμένη για όλες τις εθνικές στρατηγικές.

Πρέπει να κάνουμε λόγο όμως και για την εποπτεία. Τα μέτρα των εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο επιβάλλουν την ενεργοποίηση μιας κεντρικής ομάδας επιθεώρησης (που υποστηρίζεται από ταμεία Ανάκτησης και Ανθεκτικότητας - Recovery and Resilience funds). Υπό τον όρο του αριθμού των οντοτήτων που θα εποπτεύονται, η προσέγγιση είναι πολύ πιθανό να είναι κλιμακωτή. Επίσης οι εθνικές στρατηγικές θα πρέπει να επιβάλλουν την υιοθέτηση εθνικής πολιτικής Κυβερνοασφάλειας και συντονισμένης αντίδρασης απέναντι σε τρωτότητες (vulnerabilities). Αυτό βέβαια θα αποτελεί μια πολύπλοκη αλληλεπίδραση με το εθνικό ποινικό δίκαιο, αλλά χάριν στην ευρωπαϊκή δραστηριότητα σχετικά με την Κυβερνοασφάλεια και φυσικά το σκέλος της συνεργασίας στο πλαίσιο του NIS2, θα μπορούσε να επιφέρει μια πιο ολοκληρωμένη ροή.

Από όλα τα παραπάνω προκύπτουν πολλά ερωτήματα σχετικά με την εποπτεία. Για παράδειγμα, ποιες θα είναι οι συνέπειες της μη συμμόρφωσης;

Πιθανές απαντήσεις στην παραπάνω ερώτηση θα μπορούσαν να είναι οι εξής:

1) Πρόστιμα έως και Χ% (ανάλογα με ποια νομοθεσία) του συνολικού ετήσιου κύκλου εργασιών της εταιρείας
2) Περιοδικές χρηματικές ποινές έως και Χ% του μέσου ημερήσιου τζίρου
3) Μπορούν να επιβληθούν πρόσθετα ένδικα μέσα μετά από έρευνα και έλεγχο (ανάλογα με το αδίκημα που διαπράχθηκε)
4) Εάν είναι απαραίτητο και ως έσχατη επιλογή, μπορούν να επιβληθούν μη οικονομικά ένδικα μέσα. Αυτά μπορεί να περιλαμβάνουν συμπεριφορικές και δομικές θεραπείες, π.χ. η εκποίηση (τμημάτων) μιας επιχείρησης.

6.3.2 Το μέλλον της Κυβερνοασφάλειας στην αγορά

Αφού συζητήσαμε λοιπόν τα αποτελέσματα της NIS2 στο μέλλον της Κυβερνοασφάλειας, ας κλείσουμε αυτό το κεφάλαιο με μερικά σχόλια σχετικά με την αγορά. Τι λείπει λοιπόν στην αγορά και γενικότερα στην σκέψη της κοινωνίας ως προς την ασφάλεια; Φαίνεται πως υπάρχει έλλειψη συνείδησης στον κυβερνοχώρο και χρειαζόμαστε περισσότερη κατανόηση σε θέματα ασφάλειας. Χρειαζόμαστε μια προσέγγιση βασισμένη στον άμεσο

κίνδυνο, όπου όλοι οι δρώντες γνωρίζουν καλά όλα τα ρίσκα που υπάρχουν και αντιδρούν σωστά για το καλό των πολιτών αλλά και της ΕΕ. Απαιτείται συνεργασία σε όλα τα επίπεδα. Οι ευρωπαϊκές κυβερνήσεις αναλαμβάνουν ενέργειες για την ενίσχυση της ευρωπαϊκής συνείδησης και σε ατομικό αλλά και σε κοινοτικό επίπεδο. Σημεία αποκλεισμού όμως σε αυτό το θέμα είναι τα εξής:

- το κόστος και η πολυπλοκότητα των απαιτούμενων/προτεινόμενων μέτρων
- έλλειψη δεξιοτήτων λήψης αποφάσεων για την αξιολόγηση της ποιότητας σύνθετων προϊόντων ασφαλείας και υπηρεσιών, π.χ.τεχνική, οργανωτική και νομική τεχνογνωσία
- αδυναμία σωστής λήψης των 3 βημάτων: τεχνογνωσία-υλοποίηση-ολοκλήρωση
- έλλειψη πιστοποιήσεων από άτομα με ρόλους λήψης αποφάσεων.

Από τα παραπάνω καταλαβαίνουμε πως η συνεργασία είναι η μόνη λύση. Οι στρατηγικές όπως η ασφάλεια και ο σχεδιασμός της είναι καλοπροαίρετες, αλλά αποτυγχάνουν λόγω έλλειψης ειδικευμένων στην πληροφορική και της απουσίας μετάδοσης σωστών πληροφοριών από τους ίδιους σε άλλους δρώντες τους οποίους αφορά άμεσα η ασφάλεια. Έπειτα, οι επενδύσεις στον κυβερνοχώρο αποτελούν το πολύ το 1% των συνολικών επενδύσεων, αλλά η ασφάλεια στον κυβερνοχώρο είναι μια υποχρεωτική απαίτηση που πρέπει να διασφαλίζεται καθολικά και από όλους τους δρώντες ταυτόχρονα και με συνεργασία.

Στις παραπάνω σκέψεις θα προσπαθήσουμε να ρίξουμε περισσότερο φως στο κεφάλαιο 6 της εργασίας αυτής, όπου θα γίνουν προτάσεις για το μέλλον.

Κεφάλαιο 7ο: Προτάσεις

Σε αυτό το καταληκτικό κεφάλαιο θα προσπαθήσουμε να κάνουμε μερικές προτάσεις για το μέλλον, που να αφορούν την Κυβερνοασφάλεια, όχι μόνο σε Ευρωπαϊκό επίπεδο, αλλά και σε παγκόσμιο και ταυτοχρόνως συλλογικό, όχι μόνο ατομικό.

7.1 Γενικά

Μια πρώτη σκέψη την οποία αναφέραμε και σε προηγούμενο κεφάλαιο είναι η ύπαρξη μιας τυπικής αναφοράς για όλους, να δημιουργηθεί δηλαδή ένα συγκεκριμένο πλαίσιο για όλα τα κράτη μέλη και επιταχυνθεί με αυτόν τον τρόπο η συνεργασία έχοντας τα ίδια σημεία αναφοράς και την ίδια ατζέντα. Η πρόταση λοιπόν είναι να υπάρξει μια κοινή ευρωπαϊκή επαγγελματική γλώσσα για την ασφάλεια στον κυβερνοχώρο για όλους, όπου θα υπάρχει κοινή πλεύση σε θέματα εργασίας, επιλογής καριέρας, στρατηγικής ενδυνάμωσης, δημιουργίας κοινότητας Κυβερνοασφάλειας και τέλος δεξιοτήτων.

Για την δημιουργία μιας Ευρώπης ασφαλούς κυβερνοχώρου, χρειάζεται μια σειρά από δράσεις που να έχουν άμεσο αντίκτυπο σε αυτόν. Χρειάζεται προώθηση πολιτικών σε συγκεκριμένες κατηγορίες Κυβερνοασφάλειας και φυσικά υποστήριξη οικονομική και νομική σε αυτές. Χρειάζονται ενεργοί δρώντες, οι οποίοι λείπουν αυτή την στιγμή, που θα καταφέρουν να εφαρμόσουν όλες αυτές οι δεξιότητες που αναφέραμε σε προηγούμενο κεφάλαιο. Χρειάζεται μια κοινότητα που θα παίρνει μέρος πιο ενεργά στην λήψη αποφάσεων και στην εφαρμογή των μέτρων που προτείνονται. Η κοινότητα αυτή με άλλα λόγια θα πρέπει να συμπεριληφθεί περισσότερο στο παγκόσμιο παιχνίδι Κυβερνοασφάλειας και να φτάσει σε επίπεδο παραδείγματα άλλων κοινοτήτων, όπως αυτά του Καναδά ή της Αυστραλίας. Χρειάζονται περισσότερα προγράμματα μάθησης και εκπαίδευσης, με χρήση ενός οικονομικά αποδοτικότερου τρόπου εκπαίδευσης του προσωπικού, με συνεχή ανανέωση εκπαιδευτικού προσωπικού, και όχι μόνο εφάπαξ προσωπικό. Χρειάζεται συμμετοχή εθνικών φορέων και εθνικών συστημάτων για την σωστή εκπαίδευση των ανθρώπων, από τα πρώτα ακαδημαϊκά έτη ενός φοιτητή ως τα πιο προχωρημένα χρόνια μεταπτυχιακής εκπαίδευσης.

Για όλα τα παραπάνω όμως χρειάζονται κυρίως πόροι, ώστε να επιτευχθεί συντονισμός όλων αυτών των δράσεων. Η ύπαρξη πόρων μαζί με την καινοτομία μπορούν πράγματι να επιφέρουν πολλά θετικά στην Ευρωπαϊκή Κυβερνοασφάλεια.

Επιπλέον, περί καινοτομίας και ανάπτυξης της αγοράς Κυβερνοασφάλειας, απαιτούνται τα παρακάτω:

- Αυτονομία κάθε κράτους μέλους στις πολιτικές Κυβερνοασφάλειας.
- Εκπαίδευση: ο ανθρώπινος παράγοντας είναι βασικός παράγοντας για την ασφάλεια στον κυβερνοχώρο.

- Ψηφιακός αλφαβητισμός (Digital literacy), πρέπει να υπάρχει εκπαίδευση σε θέματα Κυβερνοασφάλειας και γενικότερα πληροφορικής.

Σχετικά με το τελευταίο σημείο, πράγματι η ευρωπαϊκή προσέγγιση συγκεντρώνεται κυρίως σε πολιτικό επίπεδο, αλλά θα πρέπει να συμφιλιωθούμε και με τα τεχνικά θέματα και να αφήσουμε λίγο στην άκρη τα πολιτικά, σε επίπεδο διακυβέρνησης δηλαδή. Θα μπορούσαμε να υλοποιήσουμε κάτι που να έρχεται πιο κοντά στην εκπαίδευση και τον ψηφιακό αλφαβητισμό στην Ευρώπη, ώστε να προσεγγίσουμε περισσότερο και τους πολίτες. Δεν πρόκειται για εκπαίδευση μόνο των ειδικών, αλλά όλων των πολιτών γενικότερα, καθώς όλοι πρέπει να συμμετέχουν σε αυτή την προσπάθεια.

Ως προς την καινοτομία επίσης, μπορούμε να θέσουμε και τα παρακάτω ερωτήματα:

- Δεδομένου του κύματος καινοτομιών τα τελευταία χρόνια, μπορούμε να έχουμε περισσότερες; Μπορεί η κοινωνία και η βιομηχανία να υποστηρίξει την συνεχή καινοτομία και να την ακολουθεί βήμα-βήμα;
- Στήριξη της καινοτομίας: ποια μέτρα πρέπει να πάρουμε για να την στηρίξουμε και να την αναπτύξουμε;
- Υποσχόμενες τεχνολογίες; Υπάρχουν; Αν ναι, γιατί ίσως να προέρχονται από έξω από την ΕΕ?
- Πώς μπορούμε να συνδυάσουμε την τεχνητή νοημοσύνη και τον κυβερνοχώρο; Είναι το AI μια τεχνολογία που μπορεί να εκμεταλλευτεί η ΕΕ και να πάρει προβάδισμα στην παγκόσμια Κυβερνοασφάλεια;
- Θα μπορούσαμε να δημιουργήσουμε ένα κύμα “Open Innovation”, με ανοιχτές ιδέες και διάφορες κοινότητες που συνεργάζονται μεταξύ τους;

Στα παραπάνω θα μπορούσε να βοηθήσει η έρευνα σε έργα χρηματοδοτούμενα από την ΕΕ, οι σχετικές ρυθμίσεις που να συμβαδίζουν με τους νόμους. Αναφέραμε βέβαια σε προηγούμενο κεφάλαιο πως πια έχουμε τόσους πολλούς νόμους που καταλήγουμε να τους ξεχνάμε ή να μην τους εφαρμόζουμε τελικά. Για αυτόν τον λόγο, να υπενθυμίσουμε την ανάγκη ουσιαστικών λύσεων και την πραγματοποίηση δράσεων, παρά την συνεχή παραγωγή νομοθεσιών που φαίνεται να μην προσφέρουν όσο θα έπρεπε στο τελικό αποτέλεσμα.

Για να κατανοήσουμε καλύτερα το νόημα της παραπάνω φράσης, θα μπορούσαμε να θέσουμε την παρακάτω ερώτηση σε ειδικούς σε θέματα Κυβερνοασφάλειας αλλά και σε απλούς πολίτες: Αν σας έδιναν προϋπολογισμό και σας έλεγαν να δώσετε προτεραιότητα

μόνο σε έναν τομέα το 2023, σε ποια δραστηριότητα μάρκετινγκ θα επικεντρώνατε τον χρόνο και τον προϋπολογισμό σας;

Με βάση πολλά άρθρα και συνεντεύξεις από το διαδίκτυο, οι εξής τομείς ίσως είναι οι πιο σημαντικοί για την Κυβερνοασφάλεια και την αγορά της το 2023:

- Προώθηση της γνώσης (awareness), με την οποία οι άνθρωποι θα αποκτήσουν αυτοπεποίθηση και βεβαιότητα.
- Προώθηση της μάθησης, με κοινούς στόχους και ιδέες, όπου όλοι μοιράζονται τις εμπειρίες τους για το κοινό καλό.
- Δημιουργία μακροχρόνιων σχέσεων οι οποίες να βασίζονται σε κοινές αξίες και στην εμπιστοσύνη μεταξύ των stakeholders.
- Καλλιέργεια ενσυναίσθησης και συμπόνιας

Τα παραπάνω μπορεί να αποτελούν βασικές και σχετικά απλές ιδέες, αλλά είναι και πολύ σημαντικά θέματα στο τοπίο της Κυβερνοασφάλειας, καθώς χωρίς αυτά δεν θα επιτευχθούν οι στόχοι της ΕΕ για το 2030. Είναι θέματα που δεν αγγίζουν μόνον τους ανθρώπους που θέλουν να ειδικευθούν στην ασφάλεια του διαδικτύου, αλλά τροφοδοτούν πολλούς άλλους τομείς ανάπτυξης για τις εταιρείες, από το μάρκετινγκ περιεχομένου έως την ανάπτυξη προϊόντων και όχι μόνο.

7.2 Προτάσεις για την Κυβερνοασφάλεια στην αγορά

Η ανάλυση της εξέλιξης της αγοράς Κυβερνοασφάλειας είναι ένα απαραίτητο βήμα για τον εντοπισμό των βασικών τάσεων, των βασικών παικτών στην αγορά και την ικανοποίηση των απαιτήσεων ασφάλειας των πολιτών. Αν και η αγορά της Κυβερνοασφάλειας έχει εξεταστεί στο παρελθόν, το πεδίο εφαρμογής των αναλύσεων εξακολουθεί να είναι σε χαμηλά επίπεδα. Σε αυτό το σημείο λοιπόν, θα προσπαθήσουμε να αναφερθούμε επιγραμματικά στην συζήτηση μεταξύ των ενδιαφερομένων με σκοπό την ανταλλαγή εμπειριών και γνώσεων, στον εντοπισμό των προκλήσεων και βέλτιστων πρακτικών, και στην παρουσίαση νέων ιδεών στον τομέα της αγοράς Κυβερνοασφάλειας.

Στην συζήτηση περί αγοράς Κυβερνοασφάλειας και της ανάπτυξής της, θα μπορούσαμε να επικεντρωθούμε στα εξής:

- Κύριες τάσεις στην αγορά Κυβερνοασφάλειας τόσο από την πλευρά της ζήτησης όσο και από την πλευρά της προσφοράς.
- κύριοι μοχλοί και προκλήσεις για την ανάπτυξη της βιομηχανίας και των υπηρεσιών Κυβερνοασφάλειας

- κύριοι παράγοντες και προκλήσεις για την προώθηση και την εφαρμογή μέτρων Κυβερνοασφάλειας
- προβλεπόμενος αντίκτυπος των ευρωπαϊκών νομοθεσιών Κυβερνοασφάλειας στην αγορά.

Για να απαντήσει βέβαια κάποιος στα παραπάνω, θα πρέπει να μελετηθούν οι προκλήσεις, να γίνει εξαγωγή συμπερασμάτων, να βρεθούν τα κενά της αγοράς και των τομέων έρευνας. Όλες αυτές οι σκέψεις θα λέγαμε πως στηρίζονται σε 3 βασικούς πυλώνες: ικανότητα, διαχείριση κινδύνων, νοοτροπία συνεργασίας και υποστήριξης.

Βασισμένοι στο παραπάνω, θα λέγαμε πως βασικό ζήτημα είναι πως οι οικονομικοί φορείς θα πρέπει να ακολουθούν τους κανόνες που θέτει η Επιτροπή. Αυτό ακριβώς είναι που εννοούμε με την νοοτροπία συνεργασίας, σε συνδυασμό με σωστές υποδομές και την ενίσχυση της διαφάνειας όλων των μερών. Αλλά δεν πρέπει να υποτιμούμε την προσπάθεια που πρέπει να καταβληθεί στα ζητήματα του κυβερνοχώρου σε τεχνικό επίπεδο, παρόλο που υπάρχουν τόσες πολλές πολιτικές. Θα πρέπει δηλαδή να δοθεί εξίσου σημασία σε τεχνικά ζητήματα, στις υποδομές και στην κατάρτιση των νέων επαγγελματιών, όπως έχουμε αναφέρει και σε άλλα κεφάλαια.

Επίσης, σημαντικές προκλήσεις στην ανάπτυξη της αγοράς της Κυβερνοασφάλειας, είναι οι επενδύσεις. Πράγματι, φαίνεται να υπάρχει ένα κενό στις επενδύσεις στον κυβερνοχώρο. Μια πρόταση είναι η δημιουργία μιας πλατφόρμας επενδύσεων στον κυβερνοχώρο. Αυτό ταυτοχρόνως θα δώσει και μια νέα πνοή στην Ψηφιακή Ευρώπη και στο κέντρο ανταγωνισμού της. Θα μπορούσε για παράδειγμα να γίνει μια συνεργασία μεταξύ κρατών-μελών και ακαδημαϊκού κόσμου, και γιατί όχι μέσω του Δικτύου εθνικών κέντρων και άλλων ιδρυμάτων της ΕΕ (enisa). Προτείνεται δηλαδή μια νέα ευρωπαϊκή πλατφόρμα επενδύσεων στον κυβερνοχώρο για τη βελτίωση της πρόσβασης του κλάδου σε χρηματοδότηση και επιχειρηματικά κεφάλαια, καθώς και κινητοποίηση περισσότερων επενδύσεων της ΕΕ στην ασφάλεια στον κυβερνοχώρο. Να γίνονται συλλογικές επενδύσεις, τόσο δημόσιες όσο και ιδιωτικές.

Τα κύρια συμπεράσματα από τα παραπάνω δεν είναι πολύπλοκα. Αρχικά, χρειαζόμαστε τους κανονισμούς αλλά εκτός από αυτό χρειαζόμαστε συνεργασία, εφαρμογή και προσαρμογή όλων των δρώντων. Στο εξής, πρέπει τα κράτη μέλη και τα ενδιαφερόμενα μέρη γενικότερα να εφαρμόσουν πράγματι τις πολιτικές που προτείνονται από την ΕΕ και να συμμορφωθούν με τους κανονισμούς. Όλα τα ενδιαφερόμενα μέρη μπορούν και πρέπει να εμπλακούν. Ο καθένας μπορεί να προσθέσει αξία στο θέμα, ώστε να μην χάσουμε την ευκαιρία να είμαστε ανταγωνιστικοί στην αγορά. Περισσότερη

συμμόρφωση θα επιφέρει καλύτερα ποσοστά επιτυχούς εφαρμογής της ασφάλειας στην Ευρώπη. Δεν χρειάζεται να είμαστε αντίπαλοι ή ανταγωνιστές. Το ίδιο ισχύει και για την συνεργασία μεταξύ της ΕΕ και των παγκόσμιων οντοτήτων ίσως ή άλλων χωρών. Είναι ένα παγκόσμιο θέμα που πρέπει να βρίσκεται σε παγκόσμιο πλαίσιο και δεν χρειάζεται να αποτελεί πρόβλημα ή να μας ορίζει αντιπάλους με άλλες χώρες. Στην συνέχεια, οι χρηματοδοτήσεις και επενδύσεις δεν επαρκούν. Κατά συνέπεια, κλειδί είναι η συνεργασία, η συνεργασία δημόσιου και ιδιωτικού τομέα. Είναι απόλυτα συνυφασμένη με το οικοσύστημα του κυβερνοχώρου.

7.3 Συνοπτικά

Είναι λοιπόν προφανές πως οι αυξημένες επιθέσεις στον κυβερνοχώρο απαιτούν ισχυρότερη απάντηση από την Ε.Ε. Οι νέοι κανονισμοί θα ενισχύσουν το έργο της ΕΕ στον τομέα της Κυβερνοασφάλειας και θα ενισχύσουν τις ικανότητες αντίδρασης τόσο των δημόσιων όσο και των ιδιωτικών φορέων. Η οδηγία NIS2 αποτελεί μέρος ευρύτερων δράσεων για την δημιουργία ανθεκτικότητας της ΕΕ έναντι των φυσικών και ψηφιακών κινδύνων. Γίνονται συνεχώς μελέτες των μελλοντικών και αναδυόμενων προκλήσεων που θα επηρεάσουν την ασφάλεια τα επόμενα 3-5 χρόνια και παρουσιάζονται τα ανάλογα αποτελέσματα, ενώ ταυτόχρονα προτείνονται νέα μέτρα. Έτσι, με γοργούς ρυθμούς επίσης γίνεται ανάπτυξη στρατηγικών λήψης αποφάσεων, έτσι ώστε η ηγεσία να μπορεί να σχεδιάσει μια στρατηγική που να μπορεί να διαχειριστεί μελλοντικές προκλήσεις τα επόμενα 3-5 χρόνια.

Υπάρχουν βέβαια, όπως έχουμε αναφέρει ξανά, ανάγκες και προτεραιότητες για τον R&D (research and development) τομέα στον κυβερνοχώρο και για την αξιολόγηση του κενού μεταξύ της υπάρχουσας συγκέντρωσης δυνάμεων στην έρευνα και της απαιτούμενης μελλοντικής συγκέντρωσης με βάση τις αλλαγές στο τοπίο τα επόμενα 5 χρόνια. Σε αυτό θα συνεισφέρει αρκετά η πρόοδος της συνεργασίας των επιχειρήσεων για να ληφθούν υπόψη και οι παράγοντες μεταβολής στους μηχανισμούς και στις σχέσεις συνεργασίας. Θα πρέπει για αυτόν τον λόγο να υπάρξει προσδιορισμός προτεραιοτήτων πολιτικής για το μέλλον με βάση τις αναδυόμενες προκλήσεις που μπορεί να καθορίσουν το μέλλον στον κυβερνοχώρο.

Τέλος, κύριο θέμα ανησυχίας για το 2030 θα πρέπει να γίνει η ευπάθεια/τρωτότητα (vulnerability). Σχετικά με αυτό το θέμα θα μπορούσε να ενεργοποιηθεί ένας μηχανισμός αντιμετώπισης των τρωτοτήτων. Η ΕΕ οφείλει και πρέπει να δουλέψει σκληρά πάνω σε αυτό. Τους βασικούς τρόπους με τους οποίους μπορεί αυτό να επιλυθεί τους αναφέραμε παραπάνω (κατάρτιση νέων ειδικευόμενων, επενδύσεις κλπ). Η ιδιωτική βιομηχανία επίσης θα πρέπει να συνεισφέρει σημαντικά σε αυτό. Ως σήμερα, υπάρχουν πράγματι ενέργειες αποκάλυψης ευπάθειας (Disclosure vulnerability). Αυτός ο όρος σημαίνει με

απλά λόγια πως εάν μοιραστούμε με άλλους τα τρωτά σημεία μας, κάνουμε τους άλλους πιο ασφαλείς. Η Κυβερνοασφάλεια για μια ιδιωτική επιχείρηση αντιμετωπίζεται ως επιπλέον κόστος, επομένως τα διοικητικά συμβούλια προσπαθούν να το ελαχιστοποιήσουν. Δεν χρειάζεται να ισχύει το ίδιο όμως και για την ΕΕ. Ακόμα και για τις ιδιωτικές επιχειρήσεις, η αντίδραση απέναντι στα κόστη Κυβερνοασφάλειας θα έπρεπε να είναι διαφορετική. Θα πρέπει να καταλάβουμε ότι το κόστος αυτό θα μετατραπεί σε μακροπρόθεσμο κέρδος, για μια ιδιωτική επιχείρηση αλλά κυριότερα για την ΕΕ. Για αυτόν τον λόγο, θα μπορούσαμε να αναπτύξουμε τις γνώσεις μας σχετικά με το αντικείμενο ώστε να μετατρέψουμε τον τομέα της Κυβερνοασφάλειας σε κάτι πιο κερδοφόρο. Αυτό βέβαια απαιτεί να ξοδέψουμε περισσότερα χρήματα σε δράσεις που δεν υπήρχαν νωρίτερα, όπως τα awareness trainings και τα Cybersecurity compliance certificates.

Βιβλιογραφία

Askoxylakis, I. (2019, June 3). *https://www.enisa.europa.eu/events/past#b_start=0.* Ανάκτηση από ENISA: https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf

Bora. (2023). *Cybersecurity Marketing in 2023: 12 Industry Experts Look Ahead.* Ανάκτηση από Bora, welcometobora.com: https://welcometobora.com/resources/cybersecurity-marketing-industry-experts-look-ahead/

CISA. (2020). *CISA 2020 Year in Review*. Ανάκτηση από www.cisa.gov: https://www.cisa.gov/resources-tools/resources/cisa-2020-year-review

Council-of-the-EU-and-the-European-Council. (2022, November 28). *EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation*. Ανάκτηση από www.consilium.europa.eu: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

Crowdstrike. (2024). *Threat Actor*. Ανάκτηση από www.crowdstrike.com: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/threat-actor/

EEAS. (2016, June). Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign And Security Policy.

EEAS. (2022, 12 07). EU Security, Defence and Crisis Response, A Security and Defence policy fit for the future.

EEAS. (2024). *EEAS - A Strategic Compass for Security and Defence.* Ανάκτηση από www.eeas.europa.eu: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

Ellena, S. (2023, March 29). *Europe lagging behind on digital skills development, says EU official.* Ανάκτηση από Euractiv.com: https://www.euractiv.com/section/economy-jobs/news/europe-lagging-behind-on-digital-skills-development-says-eu-official/

ENISA. (2020, June). *A TRUSTED AND CYBER SECURE EUROPE.* Ανάκτηση από enisa.europa.eu: https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

ENISA. (2022, November 23). *Cybersecurity Investments in the EU: Is the Money Enough to Meet the New Cybersecurity Standards?* Ανάκτηση από enisa.europa.eu: https://www.enisa.europa.eu/news/cybersecurity-investments-in-the-eu-is-the-money-enough-to-meet-the-new-cybersecurity-standards

ENISA. (2022, September). *European Cybersecurity Skills Framework (ECSF).* Ανάκτηση από enisa.com: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

ENISA. (2022, May 12). *Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation Needs and Priorities.* Ανάκτηση από enisa.europa.eu: https://www.enisa.europa.eu/publications/research-and-innovation-brief

ENISA. (2023, February 16). *Coordinated Vulnerability Disclosure: Towards a Common EU Approach.* Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/news/coordinated-vulnerability-disclosure-towards-a-common-eu-approach/

ENISA. (2024). Ανάκτηση από Enisa - Cybersecurity institutional map: https://www.enisa.europa.eu/login?came_from=/cybersecurity-institutional-map/results%3Froot%3Dactors

ENISA. (2024). *National Cybersecurity Strategies Evaluation Tool*. Ανάκτηση από www.enisa.europa.eu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

EU-CYBER-DIRECT. (2024). *Cyber Diplomacy Atlas*. Ανάκτηση από https://eucyberdirect.eu/: https://eucyberdirect.eu/atlas

EU-CyCLONe. (2020, September 29). *Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe).* Ανάκτηση από ENISA: https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

Euipo. (2024). *European Union Intellectual Property Office*. Ανάκτηση από https://www.euipo.europa.eu/en

Euractiv. (2021, December 14). *Industry calls for scaling up investment in digital skills amid shortage.* Ανάκτηση από Euractiv.com: https://www.euractiv.com/section/digital/news/industry-calls-for-scaling-up-investment-in-digital-skills-amid-shortage/

Euractiv. (2023, April 19). *EU seeks to bridge cyber-skills gap with new 'academy'.* Ανάκτηση από Euractiv.com: https://www.euractiv.com/section/cybersecurity/news/eu-seeks-to-bridge-cyber-skills-gap-with-new-academy/

EUR-Lex. (2024). *eur-lex.europa.eu*. Ανάκτηση από european-union.europa.eu: https://eurlex.europa.eu/summary/chapter/foreign_and_security_policy.html?root_default=SUM_1_CODED%3D25&%3Blocale=el&locale=el

European-Commission. (2021). *The Digital Economy and Society Index (DESI).* Ανάκτηση από commission.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/desi

European-Commission. (2022). Digital Economy and Society Index (DESI).

European-Commission. (2023). *European Year of Skills 2023.* Ανάκτηση από commission.europa.eu: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-year-skills-2023_en

European-Commission. (2023). *Three EU targets to set the ambition for 2030.* Ανάκτηση από Publications Office of the European Union: https://op.europa.eu/webpub/empl/european-pillar-of-social-rights/en/#chapter2

Fiott, D., & Zeiss, M. (2021, October 11). *Yearbook of European Security 2021.* Ανάκτηση από iss.europa.eu: https://www.iss.europa.eu/content/yearbook-european-security-2021

Fortinet. (2022). *Cyber Threat Predictions for 2022.* Ανάκτηση από www.fortinet.com: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/wp-threat-prediction-2022.pdf

François Delerue, A. G. (2022, July 12). *International Law and Cybersecurity Governance.* Ανάκτηση από eucyberdirect.eu: https://eucyberdirect.eu/research/international-law-and-cybersecurity-governance

Gallagher, C. H. (2018). *Classifying Cyber Events: A .* Maryland: Center for International and Security Studies at Maryland.

Garcia, L. &. (2021). Cybersecurity and Geopolitics: Shaping the International Landscape.

Giantas, D., & Liaropoulos, A. N. (2019). *Cybersecurity in the EU: Threats, Frameworks and future perspectives.* Laboratory of Intelligence & Cyber-Security.

ICRC. (1949). *Article 52 - General protection of civilian objects.* Ανάκτηση από International Humanitarian Law Databases, https://ihl-databases.icrc.org/en: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52

ICRC. (2021). *International Review of the Red Cross: Humanitarian Debate, Law, Policy, Action. Digital technologies and war, Volume 102 number 913.*

International-Criminal-Court. (2021). *Rome Statute of the ICC.* Ανάκτηση από International Criminal Court, www.icc-cpi.int: https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf

Johnson, T. &. (2019). Understanding Cybersecurity Actors: Motivations, Tactics, and Implications.

Johnson, T., & Williams, A. (2019). *Understanding Cybersecurity Actors: Motivations, Tactics, and Implications." In Cybersecurity Handbook. Chapter 5: Cybersecurity Actors and Their Behavior, pp. 92-115.*

Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? *Journal of Information Warfare, vol. 12, no. 2*, 19-26.

Liaropoulos, A. (2023). The Geopolitics of 5G and EU Digital Sovereignty. Στο M. A. Ferrag, I. Kantzavelou, Leandros Maglaras, & H. Janicke, *Hybrid Threats, Cyberterrorism & Cyberwarfare* (σσ. 22-39). CRC Press.

Liaropoulos, A. N. (2017). Cyberspace Governance & State Sovereignty. Στο G. C. Bitros, & N. C. Kyriazis, *Democracy and an Open-Economy World Order* (σσ. 25–35). Heidelberg: Springer.

Liaropoulos, A. N. (2020). *A Social Contract for Cyberspace, Journal of Information Warfare, vol.19, no.2.* Journal of Information Warfare.

Liaropoulos, A. N. (2023). Digitizing the Battlefield. Στο A. Gruszczak, & S. Kaempf, *Routledge Handbook of the Future of Warfare* (σσ. 308-318). London: Routledge.

Liaropoulos, A. N., Kontrafouri, C., & Zampati, M. (2020). *Η επίδραση των κυβερνοεπιθέσεων στην κυβερνοασφάλεια.* Κείμενο Εργασίας, Εργαστήρι Πληροφόρησης & Κυβερνοασφάλειας.

Miller, P., & White, S. (2020). *Strengthening Global Cybersecurity Cooperation: Strategies and Best Practices." In Global Governance and Cybersecurity. Chapter 11: Global Cybersecurity Cooperation, pp. 250-273.*

Odum, E. (1983). *System's ecology: An introduction.* Wiley.

Pande, D. J. (2017). *Introduction to Cyber Security.* Uttarakhand: Uttarakhand Open University.

Regierung-des-Fürstentums-Liechtenstein. (2021, August). *THE COUNCIL OF ADVISERS' REPORT ON THE APPLICATION OF THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT TO CYBERWARFARE.* Ανάκτηση από www.regierung.li: https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

Rosenzweig, P., & Metzger, J. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.*

Schneider, F., & Von Solms, R. (2012). *Strategic information security: A comprehensive cyber security ecosystem.*

Smith, D., & Brown, K. (2018). Economic Consequences of Cyber Threats: Challenges and Opportunities.

Sullivan, B. J., & Goodman, M. S. (2019). *Cybersecurity Ventures.*

Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). *Resilience, adaptability and transformability in social–ecological systems.* Ecology and Society.

Λιαρόπουλος, Α. (2022). *Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις.* Εκδόσεις Παπαζήση.

Λιαρόπουλος, Α. (2023). *Κυβερνοχώρος και Παγκόσμια Τάξη.* Εκδόσεις Παπαζήση.

Λιαρόπουλος, Α. (2024). Θεωρία Διεθνών Σχέσεων και Κυβερνοχώρος. Στο Μ. Κοππά, & Π. Τσάκωνας, *Θεωρία και Πράξη στις Διεθνείς Σχέσεις* (σσ. σελ.101-116). Εκδόσεις Παπαζήση.

Χειλά, Ε. (2020). COVID-19 και η «επόμενη μέρα» - Γεωπολιτική, Οικονομία, Διεθνείς θεσμοί. Πειραιάς: Εκδόσεις Πανεπιστημίου Πειραιώς.