ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2024-2025

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Δήμα Έλσας (Α.Μ.: ΜΔΙ 2313)

«Η εξέλιξη της πολιτικής/ νομοθεσίας της ΕΕ στον τομέα της κυβερνοασφάλειας»

‘’The evolution of EU cybersecurity policy/legislation.’’

Επιβλέπουσα καθηγήτρια

Κα. Ευαγγελία Μήτρου

Αθήνα, Μάρτιος 2026.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία εξετάζει τη θεσμική προσέγγιση της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας, με ιδιαίτερη έμφαση στη σημασία της προστασίας κρίσιμων υποδομών και θεμελιωδών δικαιωμάτων. Αρχικά, αποσαφηνίζονται οι βασικές έννοιες του κυβερνοχώρου και της κυβερνοασφάλειας, μέσα από την εξέλιξή τους στη σύγχρονη ψηφιακή πραγματικότητα. Ιδιαίτερη σημασία δίνεται στην αλλαγή στρατηγικής της ΕΕ μετά το 2013, οπότε η κυβερνοασφάλεια αντιμετωπίζεται όχι μόνο ως παράγοντας της ενιαίας αγοράς, αλλά και ως εργαλείο προστασίας της πολιτικής σταθερότητας και της κοινωνικής συνοχής.

Η ανάλυση επικεντρώνεται στη θεσμική συγκρότηση και στις κύριες ευρωπαϊκές πρωτοβουλίες, όπως η ίδρυση των CSIRTs και του ENISA, καθώς και στη συμβολή οργανισμών όπως το CERT-EU και το Europol-EC3. Παρουσιάζεται ο ρόλος των Διωκτικών Αρχών (LE) και η σύνδεσή τους με μηχανισμούς κυβερνοασφάλειας, μέσω της ανταλλαγής πληροφοριών και της τεχνικής υποστήριξης. Επιπλέον, διερευνάται η στρατηγική συνεργασία με διεθνείς εταίρους, όπως το NATO και η INTERPOL, στο πλαίσιο ενίσχυσης της ψηφιακής ανθεκτικότητας και της διακρατικής ασφάλειας.

Η εργασία εξετάζει επίσης τη σταδιακή θεσμική εδραίωση του πλαισίου κυβερνοασφάλειας μέσω Οδηγιών και Κανονισμών, την αλληλεπίδραση με τον GDPR και άλλες ρυθμίσεις, και καταλήγει στη σημασία της νομοθετικής εξέλιξης ως αναγκαίου εργαλείου προστασίας της ενιαίας ψηφιακής αγοράς, των χρηστών και της δημοκρατικής τάξης εντός της ΕΕ.

ABSTRACT

This paper examines the institutional approach of the European Union in the field of cybersecurity, with particular emphasis on the importance of protecting critical infrastructures and fundamental rights. Initially, the key concepts of cyberspace and cybersecurity are clarified through their evolution in the contemporary digital reality. Special attention is given to the strategic shift of the EU after 2013, when cybersecurity began to be regarded not only as a factor of the single market but also as a tool for protecting political stability and social cohesion.

The analysis focuses on the institutional framework and the main European initiatives, such as the establishment of CSIRTs and ENISA, as well as the contribution of organizations like CERT-EU and Europol-EC3. The role of Law Enforcement Authorities (LE) and their connection with cybersecurity mechanisms, through information exchange and technical support, is also presented. Moreover, the strategic cooperation with international partners, such as NATO and INTERPOL, is explored within the context of enhancing digital resilience and cross-border security.

The paper further investigates the gradual institutional consolidation of the cybersecurity framework through Directives and Regulations, the interaction with the GDPR and other regulations, and concludes on the significance of legislative development as a necessary tool for protecting the unified digital market, users, and democratic order within the EU.

Στη μητέρα μου.

1. ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ.

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΠΡΩΙΜΗ ΑΝΑΠΤΥΞΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ.

Η ταχύτατη εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών έχει καταστήσει την κυβερνοασφάλεια ζήτημα πρώτης προτεραιότητας για τις σύγχρονες κοινωνίες. Η ολοένα αυξανόμενη εξάρτηση από ψηφιακές υποδομές και υπηρεσίες, σε συνδυασμό με την πολυπλοκότητα των ψηφιακών απειλών, δημιουργεί νέες ανάγκες προστασίας των δικτύων, των δεδομένων και των κρίσιμων λειτουργιών του δημόσιου και ιδιωτικού τομέα. Η διασφάλιση της εμπιστοσύνης των πολιτών και των επιχειρήσεων στο ψηφιακό περιβάλλον προϋποθέτει όχι μόνο τεχνολογικές λύσεις, αλλά και ένα σταθερό, αναλογικό και αποτελεσματικό νομοθετικό πλαίσιο. Η Ευρωπαϊκή Ένωση, αναγνωρίζοντας τη διασυνοριακή φύση των κυβερνοαπειλών, αναπτύσσει σταδιακά μια συνεκτική στρατηγική για την ενίσχυση της ψηφιακής ανθεκτικότητας. Η νομοθεσία για την κυβερνοασφάλεια αποτελεί πλέον αναπόσπαστο μέρος του ευρωπαϊκού δικαίου, επιδιώκοντας τη ρύθμιση κρίσιμων τομέων, την εναρμόνιση των υποχρεώσεων των κρατών μελών και την ενίσχυση της συνεργασίας σε επίπεδο θεσμών και φορέων.

«Η Κυβερνοασφάλεια αποτελεί κοινή ευθύνη» (Bay, 2016). Στην Ευρωπαϊκή Ένωση, από νωρίς έγινε αντιληπτή της έννοιας της ασφάλειας των ψηφιακών συστημάτων και η ανάγκη για συνεργασία μεταξύ των κρατών-μελών, των λοιπών οργανισμών αλλά και με τρίτους φορείς. Έτσι, μέσα από συνεχείς προσπάθειες αμοιβαιότητας και συνεργατικότητας εμφανίστηκαν και οι πρώιμες πρωτοβουλίες για την στοχοθέτηση ενός επαρκούς επιπέδου κυβερνοασφάλειας (Τάσσης, 2024, σ. 78–92), το οποίο θα αναλυθεί στην πορεία του κειμένου. Για να γίνουν κατανοητά όλα όσα θα ακολουθήσουν, θα πρέπει να δοθεί μία ανάλυση των εννοιών της «Κυβερνοασφάλειας», της «Κυβερνοαπειλής» και του «Κυβερνοχώρου», έννοιες οι οποίες έχουν συχνά χρησιμοποιηθεί από πολιτικούς, μελετητές, μυθιστοριογράφους και λοιπούς. Παρακάτω, παρατίθενται οι ορισμοί της «κυβερνοασφάλειας» και του «κυβερνοχώρου».

1.2. Τι είναι ο Κυβερνοχώρος;

Ο ορισμός της Κυβερνοασφάλειας δεν είναι σαφής και απολύτως κατανοητός εάν δεν δοθεί, πρωτίστως, ο ορισμός του Κυβερνοχώρου. Ο όρος υφίσταται πολλές δεκαετίες, ήδη από το 1940, όταν επινοήθηκε από τον καθηγητή μαθηματικών του MIT Norbert Weiner ο όρος «κυβερνητική». Αρχαιοελληνική ήταν η προέλευση καθώς το επίθετο «κυβερνητικός» σήμαινε τον ικανό να πιλοτάρει και η χρήση αφορούσε την φουτουριστική ιδέα ότι θα εφευρεθεί ένα υπολογιστικό σύστημα το οποίο θα είναι αυτορρυθμιζόμενο και θα λειτουργεί αποκλειστικά με ανατροφοδότηση πληροφοριών (Bay,2016). Έκτοτε, έχει χρησιμοποιηθεί αρκετές φορές σε μυθιστορηματικό πλαίσιο, όπως από τον Vernor Vinge, ο οποίος είναι συγγραφέας επιστημονικής φαντασίας και πρώην καθηγητής πληροφορικής (Bay,2016). Μάλιστα, θεωρείται από τους πλέον πρωτοπόρους στη διαμόρφωση της σύγχρονης αντίληψης για τον Κυβερνοχώρο. Μέσα σε αυτό το πλαίσιο, ο όρος έχει πλέον οικειοποιηθεί από το δημόσιο κοινό και την επιστημονική κοινότητα, αποκτώντας μία θέση και στο διαδικτυακό λεξικό Oxford English Dictionary. Ειδικότερα, κατά τον ορισμό που δίνεται στο εν λόγω λεξικό, ο Κυβερνοχώρος αποτελεί «Το νοητό περιβάλλον στο οποίο πραγματοποιείται η επικοινωνία μέσω δικτύων υπολογιστών» (Moore and Pym, 2015). Κατά την επιστημονική κοινότητα, ωστόσο, έχει γίνει εμφανές πως ο όρος έχει βιώσει μία εξέλιξη με την πρόοδο και την ενίσχυση της πολυπλοκότητας των ψηφιακών συστημάτων και την τεχνολογική πρόοδο.

Σύμφωνα με τους Craigen, Diakun-Thibault, & Purse, "(Craigen, Diakun-Thibault and Purse, 2014), , ο όρος ‘’cyber’’ αποτελεί ένα όρο πρόθεμα, ο οποίος αναφέρεται στα ηλεκτρονικά δίκτυα επικοινωνίας και την, κατά την λογοτεχνική οπτική, εικονική πραγματικότητα. Ο όρος προέρχεται από τον όρο ‘Cybernics’, ο οποίος αφορούσε ένα γενικότερο πλαίσιο επικοινωνίας είτε της μηχανής είτε του ανθρώπου (Bay,2016) Όπως εξηγούν περαιτέρω οι προαναφερόμενοι ερευνητές, ο κυβερνοχώρος αποτελεί ένα διαρκώς εξελισσόμενο περιβάλλον τεχνολογικών υποδομών, κανόνων, ιδεών και λογισμικών, το οποίο δέχεται ποικίλες επιρροές, αναγκάζοντάς τον να προσαρμόζεται συνεχώς.

1.3. Τι ορίζεται ως Κυβερνοασφάλεια;

Ο όρος «Κυβερνοασφάλεια», σε γλωσσικό επίπεδο, είναι σχετικά νέος. Όπως έχει αναλυθεί, μέχρι πρότινος επικρατούσε ο όρος «Κυβερνοχώρος» και, επομένως ο όρος «Κυβερνοασφάλεια» ξεκίνησε να χρησιμοποιείται από επαγγελματίες και ειδικούς του τεχνολογικού χώρου, ώστε να εκφράσει ανησυχίες και προβληματισμούς που αφορούν την κατάσταση στον Κυβερνοχώρο. Στην καθομιλουμένη η «Κυβερνοασφάλεια» ορίζεται από το Oxford English Dictionary ως «Η κατάσταση κατά την οποία κάποιος ή κάτι προστατεύεται απέναντι στην εγκληματική ή μη εξουσιοδοτημένη χρήση ηλεκτρονικών δεδομένων, ή τα μέτρα τα οποία λαμβάνονται για την επίτευξη αυτής της προστασίας», ορισμό τον οποίο ενστερνίζεται και ο ENISA (ENISA, 2015). Ωστόσο, σε ένα σύγχρονο τεχνολογικό και επιχειρηματικό περιβάλλον, ο όρος θα πρέπει να διευρυνθεί, ώστε να καλύπτει και λοιπούς τομείς οι οποίοι απαιτούν προσοχή ώστε να επιτευχθεί ένα ασφαλές ψηφιακό περιβάλλον. Για παράδειγμα, ο ορισμός που δίνεται από το Oxford English Dictionary αφήνει κάποια κενά καθώς, καλύπτει τις περιπτώσεις της μη εξουσιοδοτημένης και εγκληματικής-κακής χρήσης των πληροφοριών αφήνει, όμως ακάλυπτες τις περιπτώσεις των λειτουργικών σφαλμάτων ή των ανθρώπινων λαθών. Σύμφωνα με τα παραπάνω, ο όρος διευρύνεται, όταν πραγματοποιείται χρήση του από φορείς τυποποίησης και οργανισμούς, οι οποίοι ορίζουν κανόνες για την διαμόρφωση τυποποιημένων προδιαγραφών, ώστε να επιτευχθεί η ασφάλεια των υπηρεσιών. Οι κύριοι φορείς τυποποίησης, σε παγκόσμιο επίπεδο είναι ο ISO (International Organization for Standardization, ο IEC (International Electrotechnical Commission), ITU (International Telecommunication Union), IEEE (Institute of Engineering Task Force) και NIST (National Institute of Standards and Technology). Ένας από τους πλέον περιεκτικούς και λειτουργικούς ορισμούς παρέχεται από τον ISO/IEC (ISO/IEC, 2022). Σύμφωνα με τον εν λόγω ορισμό, η έννοια της ασφάλειας συναρτάται πρωτίστως με την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα της πληροφορίας. Εντούτοις, ο ίδιος οργανισμός υιοθετεί έναν ευρύτερο προσδιορισμό της ασφάλειας των ΤΠΕ, περιλαμβάνοντας και επιμέρους διαστάσεις όπως η μη αποποίηση ευθύνης, η λογοδοσία, η αυθεντικότητα και η αξιοπιστία των πληροφοριακών πόρων.

Να σημειωθεί πως ο ENISA, παρόλο που δεν αποτελεί φορέα τυποποίησης, συμβάλλει σημαντικά στην προώθηση προτύπων και βέλτιστων πρακτικών στον χώρο της κυβερνοασφάλειας στην Ευρώπη. Σύμφωνα με την έκθεση του ENISA(ENISA, 2015) στην πραγματικότητα δε δύναται η υιοθέτηση ενός ορισμού για την Κυβερνοασφάλεια, με την παραδοσιακή μορφή με την οποία δημιουργούμε ορισμούς. Αυτό οφείλεται στο γεγονός ότι ο όρος καλύπτει ένα ευρύ φάσμα εννοιών και για αυτό, δεν είναι δυνατόν να δοθεί ένας ορισμός ο οποίος να περιβάλλει το πλήρες εύρος των θεμάτων που εμπίπτουν στην Κυβερνοασφάλεια.

Η Οδηγία NIS 1 είχε εισαγάγει έναν «νομοθετικό ορισμό» για την «ασφάλεια συστημάτων δικτύου και πληροφοριών». Ειδικότερα, η ασφάλεια συστημάτων δικτύου και πληροφοριών αφορά «την ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών·» (Άρθρο 4, σημείο 2). Παρατηρούμε πως η Οδηγία δεν κάνει αναφορά στην έννοια της «Κυβερνοασφάλειας».

Επιπρόσθετα, η Πράξη για την Κυβερνοασφάλεια (Κανονισμός 2019/881) ορίζει την «κυβερνοασφάλεια» ως «τις δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων»(Κανονισμός (ΕΕ) 2019/881, 2019, άρθρο 2), ενώ ως «κυβερνοαπειλή» «κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλο τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα» (Κανονισμός (ΕΕ) 2019/881, 2019, άρθρο 2). Πρόκειται για μία αξιοσημείωτη εξέλιξη καθώς, στο πεδίο της προστασίας εντάσσονται,πέραν του «κυβερνοχώρου»,πλέον και τα «πρόσωπα». Αντιλαμβανόμαστε, λοιπόν, πως τέτοιες απειλές μπορούν να επηρεάσουν δυσμενώς, όχι μόνο τους χρήστες των συστημάτων δικτύου και πληροφοριών αλλά και λοιπά άτομα όπως είναι πελάτες, οι οποίοι βασίζονται σε αυτά τα συστήματα, προμηθευτές σε εταιρείες ή

οργανισμούς που απειλούνται και, γενικότερα οποιοσδήποτε μπορεί να επηρεαστεί μέσω της διαρροής προσωπικών δεδομένων ή της διακοπής των υπηρεσιών. Ο ορισμός που δίνεται στον Κανονισμό 2019/881 ενσωματώθηκε και στον Κανονισμό 2555/2022 για την Κυβερνοασφάλεια. Ειδικότερα, στο άρθρο 6 σημείο 3 αναφέρεται ως «κυβερνοασφάλεια: η κυβερνοασφάλεια όπως ορίζεται στο άρθρο 2 σημείο 1. του Κανονισμού (ΕΕ) 2019/881.

Εν κατακλείδι, η έννοια της ασφάλειας συνιστά έναν δυναμικά εξελισσόμενο όρο, του οποίου το περιεχόμενο μεταβάλλεται παράλληλα με την πρόοδο της τεχνολογίας. Στο πλαίσιο αυτό, η Ένωση επιδίωξε την υιοθέτηση ενός κοινού και γενικώς αποδεκτού ορισμού της κυβερνοασφάλειας, ικανού να αποτυπώσει επαρκώς τους συλλογικούς στόχους των κρατών-μελών. Ο ENISA επεσήμανε ότι, μολονότι η καθιέρωση ενός ενιαίου ορισμού θα συνέβαλε στην προαγωγή της σαφήνειας και της νομικής ασφάλειας, τα εμπλεκόμενα μέρη και οι αρμόδιοι φορείς χάραξης πολιτικής διατηρούν η δυνατότητα να επιλέγουν τον ορισμό που εξυπηρετεί καλύτερα τις ειδικές ανάγκες και το εκάστοτε ρυθμιστικό ή επιχειρησιακό πλαίσιο εντός του οποίου δραστηριοποιούνται.

1.4. Η κρισιμότητα κατοχύρωσης ενός ενιαίου πλαισίου κυβερνοασφάλειας.

Σε επίπεδο Ευρωπαϊκής Ένωσης, σημειώθηκε μία βασική αλλαγή στην αντίληψη ως προς την κυβερνοασφάλεια. Έτσι, ενώ μέχρι το 2013 η Ευρωπαϊκή Ένωση θεωρούσε την Κυβερνοασφάλεια κατά κύριο λόγο ως έναν παράγοντα για τη λειτουργία της ενιαίας αγοράς μέσω της διασφάλισης ασφαλούς λειτουργίας των συστημάτων δικτύου και πληροφοριών, ώστε αυτά να στηρίζουν αποτελεσματικά την οικονομική δραστηριότητα και την εμπορική συναλλαγή εντός της ενιαίας αγοράς, ιδίως από το 2017, η έμφαση μετατοπίστηκε αλλού. Ιδιαίτερη σημασία, απέκτησε η πολιτική ακεραιότητα της Ένωσης και των κρατών-μελών της. Η σημασία αυτή αντανακλάται και στο γεγονός ότι η κυβερνοασφάλεια έχει πλέον καταστεί αντικείμενο κανονιστικής παρέμβασης και ρύθμισης (Μήτρου,2021). Η ρύθμιση αυτή εκδηλώνεται με τρεις κύριες κατηγορίες παρεμβάσεων:

1. Εισαγωγή σαφών και νομικά δεσμευτικών υποχρεώσεων για τη λήψη μέτρων ασφάλειας.

2. Υιοθέτηση και οργάνωση μηχανισμών και εργαλείων για την επιβολή και εφαρμογή αυτών των υποχρεώσεων.

3. Διεύρυνση της ποινικής προστασίας που προβλέπεται σε περιπτώσεις επιθέσεων κατά πληροφοριακών συστημάτων.

Η κατοχύρωση της κυβερνοασφάλειας συνιστά θεμελιώδη προτεραιότητα για την Ευρωπαϊκή Ένωση, καθώς αφορά άμεσα την ανθεκτικότητα των κρίσιμων υποδομών, την προστασία των θεμελιωδών δικαιωμάτων των πολιτών και τη διατήρηση της δημοκρατικής σταθερότητας. Κρίσιμοι τομείς όπως, οι μεταφορές, η ενέργεια, η υγεία και ο χρηματοοικονομικός κλάδος, εξαρτώνται, ολοένα και περισσότερο, από τις ψηφιακές τεχνολογίες, για την απρόσκοπτη λειτουργία των βασικών τους δραστηριοτήτων. Αν και η ψηφιοποίηση δημιουργεί πολλαπλά οφέλη και δυνατότητες επίλυσης διαρθρωτικών προκλήσεων, ταυτόχρονα, καθιστά την ευρωπαϊκή οικονομία και την κοινωνία πιο ευάλωτες σε κυβερνοαπειλές.

Οι κυβερνοαπειλές, καθώς και το κυβερνοέγκλημα, παρουσιάζουν εντεινόμενη έξαρση στην ευρωπαϊκή επικράτεια, τόσο σε αριθμό περιστατικών, όσο και σε πολυπλοκότητα, γεγονός το οποίο εγείρει σοβαρές προκλήσεις για τη διατήρηση της ασφάλειας και της εμπιστοσύνης τον ψηφιακό χώρο. Η κατάσταση αναμένεται να επιδεινωθεί περαιτέρω στο μέλλον, δεδομένου ότι ο αριθμός των διασυνδεδεμένων συσκευών διεθνώς προβλέπεται να υπερδιπλασιαστεί, σχεδόν από 15,9 δισεκατομμύρια το 2023 σε, άνω των 32 δισεκατομμυρίων, μέχρι το 2030 (Council of the European Union, 2024). Η εντατικοποίηση της ψηφιακής διασύνδεσης, σε συνδυασμό με την ευρεία χρήση έξυπνων συστημάτων, ενισχύει τη σημασία της ανάπτυξης στιβαρών και προληπτικών μηχανισμών κυβερνοασφάλειας.

Η κυβερνοασφάλεια, σε αυτό το πλαίσιο, λειτουργεί ως καθοριστικός μηχανισμός προστασίας των δικτύων, των πληροφοριακών συστημάτων, των χρηστών, αλλά και όλων, όσοι ενδέχεται να επηρεαστούν από κακόβουλες ψηφιακές επιθέσεις. Η ενίσχυση της ασφάλειας στον κυβερνοχώρο δεν αποτελεί, απλώς, μία τεχνική πρόκληση, αλλά, στρατηγικό στόχο, ο οποίος συνδέεται με την οικοδόμηση εμπιστοσύνης προς τα ψηφιακά εργαλεία και υπηρεσίες, ενισχύοντας

την ενεργό συμμετοχή των πολιτών στον ψηφιακό μετασχηματισμό (Council of the European Union, 2024).

Ανταποκρινόμενη στις αυξανόμενες προκλήσεις, η Ευρωπαϊκή Ένωση έχει επιδείξει ισχυρή πολιτική βούληση ώστε να «θωρακίσει» το ψηφιακό χώρο της ήδη από το 2013 με την υιοθέτηση της Πράξης για την Κυβερνοασφάλεια (5526/2013), η οποία καταργείται με την υιοθέτηση του Κανονισμού (ΕΕ) 2019/881, γνωστός και ως 'Cybersecurity Act'. Παράλληλα, τον Ιούλιο του 2016 υιοθετήθηκε η Οδηγία (ΕΕ) 2016/1148 σχετικά με τα μέτρα για υψηλό κοινό επίπεδο Ασφάλειας Συστημάτων Δικτύου και πληροφοριών στη Ευρωπαϊκή Ένωση, γνωστή ως NIS 1, σε μία προσπάθεια αυτοτελούς ρύθμισης της ασφάλειας των δικτύων και τηλεπικοινωνιών. Αξίζει να σημειωθεί ότι, τον Δεκέμβριο του 2024 το Συμβούλιο της Ευρωπαϊκής Ένωσης έκανε δεκτό έναν νέο κανονισμό τον "Cyber Solidarity Act (EU Regulation 2025/38)" ο οποίος θα αφορά την αλληλεγγύη στον κυβερνοχώρο, σε μία προσπάθεια διαρκούς εξέλιξης και προστασίας.

Επιγραμματικά, η ασφάλεια του ψηφιακού περιβάλλοντος διασφαλίζει την αποτροπή της ανεξέλεγκτης συλλογής προσωπικών δεδομένων και της παραπληροφόρησης, συμβάλλοντας αποφασιστικά στην προάσπιση των δημοκρατικών αξιών. Η κυβερνοασφάλεια, συνεπώς, δεν περιορίζεται σε ένα τεχνικό ή επιχειρησιακό εργαλείο, αλλά, αποτελεί αναγκαία προϋπόθεση για τη διατήρηση της ασφάλειας, της ελευθερίας και της εμπιστοσύνης στην ενιαία ψηφιακή αγορά.

1.5.Στόχοι Της Εργασίας.

Η παρούσα εργασία εξετάζει τη θεσμική και κανονιστική προσέγγιση της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας. Ιδιαίτερη έμφαση δίνεται στις βασικές έννοιες και απαιτήσεις που απορρέουν από το ενωσιακό πλαίσιο, καθώς και στον ρόλο των ενδιαφερόμενων οργανισμών στη διαμόρφωση και την ερμηνεία της εφαρμογής του. Μέσα από την κριτική ανάλυση των σύγχρονων νομοθετικών εξελίξεων και των θεσμικών δυναμικών που τις συνοδεύουν, επιδιώκεται η κατανόηση του τρόπου με τον οποίο η Ευρωπαϊκή Ένωση επιχειρεί να

διαμορφώσει ένα κοινό επίπεδο προστασίας στον κυβερνοχώρο, λαμβάνοντας υπόψη τις τεχνολογικές, οικονομικές και πολιτικές προκλήσεις που εγείρονται.

Η μεθοδολογική προσέγγιση της εργασίας βασίζεται στη συστηματική ανάλυση του ενωσιακού πλαισίου και τη συγκριτική επισκόπηση των σχετικών θεσμικών εξελίξεων, με αξιοποίηση τόσο πρωτογενών όσο και δευτερογενών πηγών. Μέσα από τη μελέτη επιστημονικών άρθρων και νομοθετικών κειμένων, επιχειρείται η ανάλυση των βασικών νομοθετημάτων καθώς και των προκλήσεων που διαμορφώνουν το πεδίο της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Η εργασία δομείται σε κεφάλαια, που παρουσιάζουν σταδιακά το θεωρητικό υπόβαθρο, το θεσμικό και κανονιστικό πλαίσιο, καθώς και τις προοπτικές μελλοντικής εξέλιξης της ενωσιακής πολιτικής στον τομέα αυτό.

Βασικοί στόχοι της παρούσας εργασίας αποτελούν η χαρτογράφηση της υφιστάμενης νομοθεσίας της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια και η συγκριτική ανάλυσή της με προγενέστερες ρυθμίσεις, προκειμένου να αναδειχθεί η εξέλιξη του σχετικού θεσμικού πλαισίου. Εξετάζονται, επίσης οι υποχρεώσεις οι οποίες απορρέουν από το εν λόγω πλαίσιο για τα κράτη μέλη, καθώς και οι προκλήσεις τις οποίες αντιμετωπίζουν κατά την εφαρμογή του. Κεντρικό άξονα της εργασίας αποτελεί η μελέτη της Οδηγίας για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Directive) και, κυρίως, της αναθεωρημένης πλέον μορφής της NIS2, στην οποία και δίνεται ιδιαίτερη έμφαση καθώς το βασικότερο νομοθετικό εργαλείο της Ένωσης για την ενίσχυση της κυβερνοασφάλειας.

Παράλληλα, αναλύεται η διασταύρωση της εν λόγω Οδηγίας με τον Γενικό Κανονισμό της Προστασίας των Δεδομένων (GDPR), ενώ, εξετάζεται και η σύνδεση με άλλες κρίσιμες ρυθμιστικές πράξεις, όπως ο Κανονισμός DORA, οι οποίες συναρθρώνονται σε ένα ευρύτερο πλαίσιο ψηφιακής ανθεκτικότητας. Επιπροσθέτως, πραγματοποιείται σύγκριση του ευρωπαϊκού πλαισίου με αντίστοιχες νομοθεσίες άλλων, παγκόσμιων δρώντων, όπως των Ηνωμένων Πολιτειών της Αμερικής και της Λαϊκής Δημοκρατίας της Κίνας. Τέλος, επιδιώκεται η διατύπωση προτάσεων και η συζήτηση πιθανών πρακτικών εφαρμογής, οι οποίες θα μπορούσαν να συμβάλλουν στη βελτίωση και αποτελεσματικότερη εφαρμογή

του ευρωπαϊκού νομοθετικού πλαισίου στον τομέα της κυβερνοασφάλειας.

2. ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

ΘΕΣΜΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΦΟΡΕΙΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

2.1.Βασικές Αρχές

Η Ευρωπαϊκή Ένωση έχει αναπτύξει ένα συνεκτικό πλαίσιο πολιτικών και νομοθετικών μέτρων, όσον αφορά τον τομέα της Κυβερνοασφάλειας. Βασικός στόχος αποτελεί η προστασία των κρατών-μελών, των επιχειρήσεων καθώς και των πολιτών από κυβερνοαπειλές. Τον Δεκέμβριο του 2020, η Ευρωπαϊκή Επιτροπή και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) παρουσίασαν μία νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια (European Commission, 2020), σε μία προσπάθεια προστασίας από τις νέες απειλές, οι οποίες ανακύπτουν παράλληλα με τον ψηφιακό μετασχηματισμό της κοινωνίας. Ακρογωνιαίος λίθος της νέας αυτής στρατηγικής αποτελεί η έννοια της ανθεκτικότητας, στο πλαίσιο διασφάλισης της ασφαλούς λειτουργίας των κρίσιμων υποδομών και δικτύων, εντός της Ευρωπαϊκής Ένωσης. Για να επιτευχθεί πραγματική ανθεκτικότητα, δεν αρκεί μόνο η προστασία από επιθέσεις ή βλάβες, αλλά, απαιτείται μία ολιστική προσέγγιση, η οποία περιλαμβάνει και την ικανότητα προσαρμογής, ανάκαμψης και διατήρησης της λειτουργίας σε περιόδους κρίσης (European Commission, 2020). Η ενίσχυση της ασφάλειας των κρίσιμων υποδομών αφορά όχι μόνο την τεχνολογική θωράκιση των συστημάτων, αλλά και τη διασφάλιση της ορθής λειτουργίας, συντήρησης και ενημέρωσης των υποδομών αυτών, προκειμένου να ελαχιστοποιηθεί η έκθεση σε κινδύνους και να βελτιωθεί η ανθεκτικότητα σε ανεπιθύμητα περιστατικά.

Στο πλαίσιο αυτό, η Ευρωπαϊκή Επιτροπή προτείνει τη μεταρρύθμιση των κανόνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών μέσω της αναθεωρημένης NIS2, με στόχο την αύξηση του επιπέδου κυβερνοανθεκτικότητας στους κρίσιμους δημόσιους και ιδιωτικούς τομείς. Οι τομείς αυτοί περιλαμβάνουν νοσοκομεία, κέντρα δεδομένων, ενεργειακούς τομείς, δημόσιες διοικήσεις, ερευνητικά κέντρα και άλλες κρίσιμες υποδομές και υπηρεσίες. Η προστασία αυτών

κρίνεται απαραίτητη ώστε να παραμείνουν αδιαπέραστες σε ένα περιβάλλον μονίμων εξελίξεων και τεχνολογικών μεταβολών.

Επιπλέον, η Επιτροπή προωθεί τη δημιουργία ενός πανευρωπαϊκού δικτύου κέντρων επιχειρήσεων ασφάλειας, όπως προβλέπεται από την Cyber Solidarity Act[1] τα οποία θα υποστηρίζονται από τεχνολογίες τεχνητής νοημοσύνης. Ειδική έμφαση δίνεται στη στήριξη των μικρών και μεσαίων επιχειρήσεων, οι οποίες εντάσσονται σε κόμβους ψηφιακής καινοτομίας. Παράλληλα, ενισχύονται οι προσπάθειες για την ανάπτυξη και αναβάθμιση των δεξιοτήτων του εργατικού δυναμικού, στον τομέα της κυβερνοασφάλειας. Σημαντική είναι η ενίσχυση των επενδύσεων στην έρευνα και την καινοτομία, με στόχο την δημιουργία ενός ανοιχτού και ανταγωνιστικού περιβάλλοντος, στον τομέα της κυβερνοασφάλειας. Είναι κρίσιμο να τονιστεί πως η πρόληψη είναι απαραίτητη για τη μείωση της πιθανότητας εκδήλωσης κυβερνοαπειλών. Η πρόληψη βασίζεται σε ένα διαρκές και δυναμικό σύστημα παρακολούθησης, αξιολόγησης και ανταλλαγής πληροφοριών σχετικά με τις κυβερνοαπειλές, παλαιότερες και νεότερες.

Η ενίσχυση της ανθεκτικότητας και της πρόληψης δεν μπορεί να επιτευχθεί χωρίς τη συνδρομή των κρατών-μελών. Αντιθέτως, η διευρυμένη συνεργασία και ο συντονισμός σε ενωσιακό και τοπικό επίπεδο αποτελούν κρίσιμες προϋποθέσεις για την αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων. Μέσω της ανταλλαγής βέλτιστων πρακτικών, της κοινής αξιολόγησης απειλών και της συνεργασίας σε επίπεδο ανταπόκρισης, τα κράτη ενδυναμώνουν τις συλλογικές τους δυνατότητες, μειώνοντας έτσι το συνολικό επίπεδο κινδύνου. Για να διασφαλιστεί η άμεση και αποτελεσματική αντίδραση, δημιουργούνται μηχανισμοί έγκαιρης προειδοποίησης και γρήγορης απόκρισης σε περιστατικά κυβερνοεπιθέσεων. Αυτοί οι μηχανισμοί επιτρέπουν την ταχεία αναγνώριση και απομόνωση απειλών, προλαμβάνοντας την εξάπλωση των επιθέσεων και μειώνοντας τις αρνητικές συνέπειες για την κοινωνία και την οικονομία. Βεβαίως, η

[1] «….ανήγγειλε μια πρωτοβουλία αλληλεγγύης της ΕΕ στον κυβερνοχώρο με στόχο την ενίσχυση των κοινών ικανοτήτων ανίχνευσης, την αντίληψη της κατάστασης και την αντίδραση της ΕΕ μέσω της προώθησης της ανάπτυξης υποδομής κέντρων επιχειρήσεων ασφάλειας της ΕΕ («SOC»), την στήριξη της σταδιακής δημιουργίας εφεδρείας στον τομέα της κυβερνοασφάλειας σε επίπεδο ΕΕ με υπηρεσίες από αξιόπιστους ιδιωτικούς παρόχους και την δοκιμή κρίσιμων οντοτήτων για πιθανά τρωτά σημεία με βάση εκτιμήσεις κινδύνου της ΕΕ.».

ενσωμάτωση των κανονισμών και των οδηγιών από τα κράτη-μέλη, μέσω της εγχώριας νομοθεσίας, διασφαλίζει την ομαλή εφαρμογή των κανόνων κυβερνοασφάλειας. Η τήρηση αυτών των κανόνων δεν αποτελεί απλά νομική υποχρέωση, αλλά αναγκαία προϋπόθεση για την αποτελεσματική διαχείριση κινδύνων. Σε περίπτωση μη συμμόρφωσης, ορίζεται ένα σαφές πλαίσιο ποινών το οποίο λειτουργεί αποτρεπτικά και ενισχύει τη νομοθετική επιβολή, δημιουργώντας έτσι ένα συνεκτικό και λειτουργικό σύστημα ασφάλειας, σε ευρωπαϊκό επίπεδο.

Επιπρόσθετα, η παιδεία και η κατάρτιση σε θέματα κυβερνοασφάλειας είναι απαραίτητες προϋποθέσεις για την ενίσχυση της ανθεκτικότητας και της πρόληψης. Η ανάπτυξη βασικών δεξιοτήτων και γνώσεων σε όλα τα επίπεδα, από το ευρύ κοινό έως τους επαγγελματίες, συμβάλλει στην έγκαιρη αναγνώριση κινδύνων και στην υιοθέτηση σωστών πρακτικών ασφαλείας. Επιπλέον, η εκπαίδευση προωθεί την ψύχραιμη και συντονισμένη διαχείριση περιστατικών, περιορίζοντας, έτσι τις ζημίες που προκύπτουν στο πλαίσιο των κυβερνοεπιθέσεων.

Σε ένα γενικότερο πλαίσιο, οι βασικές αρχές του θεσμικού πλαισίου της Ευρωπαϊκής Ένωσης, στον τομέα της Κυβερνοασφάλειας, επικεντρώνονται στην ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και των δικτύων, ώστε να διασφαλιστεί η προστασία των κρίσιμων υποδομών και της ψηφιακής επιχειρηματικότητας. Κεντρική θέση στο πλαίσιο αυτό κατέχει η πολυεπίπεδη διακυβέρνηση και ο συντονισμός μεταξύ των κρατών-μελών και των ευρωπαϊκών θεσμών (Porcedda, 2021). Η πολυεπίπεδη διακυβέρνηση (Multilevel Governance-MLG) αφορά κάθε συντονισμένη δράση μεταξύ της Ευρωπαϊκής Ένωσης, των κρατών-μελών και των τοπικών και περιφερειακών τους αρχών, στοχεύοντας στη χάραξη και τη συντονισμένη υλοποίηση των πολιτικών της Ε.Ε. (Coopenergy Consortium, 2015). Η συνεργασία αυτή αποσκοπεί στην καλύτερη διαχείριση των κινδύνων, την ενίσχυση της ανταλλαγής πληροφοριών και την υλοποίηση κοινών στρατηγικών, προκειμένου να ενδυναμωθεί η ικανότητα των κρατών-μελών να ανταπεξέρχονται σε κυβερνοαπειλές. Τέλος, η προστασία των θεμελιωδών δικαιωμάτων και, ειδικότερα, των προσωπικών δεδομένων, αποτελεί μία από τις κύριες αρχές του θεσμικού πλαισίου. Η προστασία της ιδιωτικότητας και των δικαιωμάτων των πολιτών στον ψηφιακό χώρο θεωρούνται θεμελιώδεις για

τη διασφάλιση της δημοκρατικής σταθερότητας και της εμπιστοσύνης των πολιτών στις ψηφιακές τεχνολογίες (European Commission, 2017). Η ΕΕ επιδιώκει να εξισορροπήσει την ανάγκη για ενίσχυση της κυβερνοασφάλειας με την προστασία των θεμελιωδών δικαιωμάτων, εξασφαλίζοντας ότι οι πολιτικές ασφαλείας δεν παραβιάζουν τις ελευθερίες των ατόμων. Συνολικά, αυτές οι αρχές διασφαλίζουν την «ώριμη» προσπάθεια για αποτελεσματικότητα και συνεκτικότητα όσον αφορά το θεσμικό πλαίσιο της ΕΕ για την κυβερνοασφάλεια, προωθώντας την ανάγκη για ασφάλεια των δικτύων και των πληροφοριακών συστημάτων και ενισχύοντας την ανθεκτικότητα της Ευρωπαϊκής Ένωσης απέναντι στα διαρκώς αυξανόμενες κυβερνοαπειλές.

2.2. Ο ρόλος της ΕΕ στην προστασία των κρατών-μελών.

Η Ευρωπαϊκή Ένωση διαδραματίζει έναν καθοριστικό ρόλο στην προστασία των κρατών-μελών της από το κυβερνοέγκλημα ενισχύοντας τη συνεργασία, παρέχοντας τεχνική υποστήριξη και δημιουργώντας ένα ισχυρό νομοθετικό πλαίσιο. Μεταξύ των κυρίων δράσεών της είναι η θέσπιση ενός ισχυρού νομοθετικού πλαισίου, το οποίο περιλαμβάνει Οδηγίες και Κανονισμούς. Οι Οδηγίες που καθορίζουν το νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης είναι η Οδηγία NIS Directive, η οποία αντικαταστάθηκε από τη NIS 2 καθώς και η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών,"Directive on attacks against information systems", η οποία καθιερώνει την ποινικοποίηση επιθέσεων όπως το hacking, το malware και τα botnets. Οι κανονισμοί που ενισχύουν το νομοθετικό πλαίσιο είναι ο Κανονισμός (ΕΕ) 2019/881 καθώς και ο Γενικός Κανονισμός Προστασίας των Προσωπικών Δεδομένων (ΕΕ) 2016/679, ο οποίος διασφαλίζει την προστασία των προσωπικών δεδομένων από κακόβουλες επιθέσεις.

Παράλληλα, η ΕΕ υποστηρίζει τα κράτη-μέλη μέσω οργανισμών, οι οποίοι παρέχουν βοήθεια και συντονισμό στην αντιμετώπιση των κυβερνο-απειλών. Ο σπουδαιότερος οργανισμός σε αυτόν τον τομέα θεωρείται ο ENISA (Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια), ο οποίος παρέχει στρατηγικές, τεχνική υποστήριξη και κατευθυντήριες οδηγίες για την ενίσχυση της κυβερνοασφάλειας, σε εθνικό και τοπικό επίπεδο. Ένας οργανισμός με εξίσου σημαντική δράση είναι

και ο Europol-EC3 (European Cybercrime Centre), στόχος του οποίου αποτελεί ο συντονισμός και η ενίσχυση των ερευνών για το κυβερνοέγκλημα και, ως εκ τούτου, η προστασία των ευρωπαίων πολιτών, των επιχειρήσεων και των κυβερνήσεων από το ηλεκτρονικό έγκλημα. Για το λόγο αυτό, ο οργανισμός συνεργάζεται με τις κυβερνήσεις και τις εταιρείες, για την εξάρθρωση εγκληματικών δικτύων. Τέλος, τον ρόλο της άμεσης και έγκαιρης προειδοποίησης για κυβερνοεπιθέσεις στους θεσμούς της ΕΕ και στα κρατικά δίκτυα έχει αναλάβει η Ομάδα Αντιμετώπισης Κυβερνοεπιθέσεων της ΕΕ-CERT-EU.

Την ίδια στιγμή, η ΕΕ συνεργάζεται στενά και με διεθνείς οργανισμούς για την προστασία ενάντια στο Κυβερνοέγκλημα (π.χ. Συνεργασία με το ΝΑΤΟ), συνάπτει συμφωνίες με τρίτες χώρες όπως οι Η.Π.Α., ο Καναδάς και η Ιαπωνία για την καταπολέμηση του διεθνούς κυβερνοεγκλήματος και πραγματοποιεί εκστρατείες ενημέρωσης για την κυβερνοασφάλεια και τους κινδύνους που αυτή ενέχει, εκπαιδεύοντας πολίτες και επιχειρήσεις σε θέματα προστασίας από κυβερνοεπιθέσεις (Porcedda, 2021). Τέλος, η ΕΕ στηρίζει τις προσπάθειες για την ανάπτυξη λύσεων στα θέματα της κυβερνοασφάλειας, μέσω χρηματοδοτικών προγραμμάτων όπως το πρόγραμμα Horizon Europe & Digital Europe και το Ευρωπαϊκό Κέντρο Ψηφιακής Καινοτομίας. Η ΕΕ συνεχώς ενισχύει τις πολιτικές και τις στρατηγικές με σκοπό την εξασφάλιση της προστασίας των κρατών-μελών από το κυβερνοέγκλημα, καθώς οι κυβερνοαπειλές εξελίσσονται διαρκώς. Ο στόχος της ΕΕ είναι η δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος για τους πολίτες, τις επιχειρήσεις και τις κυβερνήσεις.

2.3. Οργανισμοί και Φορείς της ΕΕ.

2.3.1 ENISA (European Union Agency for Cybersecurity)

Ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια (ENISA) αποτελεί ένα όργανο της Ευρωπαϊκής Ένωσης με νομική προσωπικότητα (Άρθρο 38). Ο οργανισμός ιδρύθηκε το 2004, με έδρα το Ηράκλειο Κρήτης. Τα γραφεία διασύνδεσης βρίσκονται στην Αθήνα και τις Βρυξέλλες. Το ελληνικό κράτος, ως κράτος-μέλος υποδοχής, θα πρέπει να φροντίζει ώστε να επικρατούν οι βέλτιστες συνθήκες για την «εύρυθμη και αποδοτική λειτουργία του ENISA»(Ευρωπαϊκό

Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 18). Ο οργανισμός συστάθηκε δυνάμει του Κανονισμού (ΕΕ) 526/2013 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, ο οποίος αντικαταστάθηκε από τον Κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου του 2019. Έτσι, ο σκοπός και ο τρόπος λειτουργίας του ENISA ορίζονται, πλέον από τον Κανονισμό (ΕΕ) 2019/881. Βασικός στόχος του είναι η επίτευξη ενός κοινού υψηλού επιπέδου Κυβερνοασφάλειας (Άρθρο 3) σε όλη την Ευρωπαϊκή Κοινότητα (ENISA, 2024), μέσω της ενίσχυσης της ανάγκης για μία συνεπή εφαρμογή του νομικού πλαισίου (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 24), με έμφαση στην αποτελεσματική εφαρμογή της Οδηγίας (ΕΕ) 2016/1148. Επιπρόσθετα, ο ρόλος του Οργανισμού είναι επικουρικός (Άρθρο 5). Οι εξειδικευμένοι επιστήμονες, οι οποίοι στελεχώνουν τον Οργανισμό μπορούν να εγγυηθούν για την συλλογή και προώθηση ανεξάρτητων και υψηλού επιπέδου συμβουλών και οδηγιών στα Κράτη-Μέλη και στους Ευρωπαϊκούς Οργανισμούς Κυβερνοασφάλειας (Άρθρο 4 και 11). Ο ENISA επιδιώκει την παροχή, στους πολίτες και στις επιχειρήσεις, αξιολόγησης των επιπέδων διασφάλισης για τις ψηφιακές λύσεις, καθώς και ενίσχυση της εμπιστοσύνης στις εφοδιαστικές αλυσίδες, μέσω μηχανισμών όπως η πιστοποίηση, στο πλαίσιο του Ευρωπαϊκού Πλαισίου Πιστοποίησης Κυβερνοασφάλειας (The European Cybersecurity Certification Group, 2025).

Παράλληλα, ο ENISA στοχεύει στην υλοποίηση ενός ασφαλούς ψηφιακού περιβάλλοντος σε όλη την ΕΕ, όπου ευρωπαϊκές και εθνικές δημόσιες αρχές, όπως και επιχειρήσεις θα μπορούν να ανταποκρίνονται στις ρυθμιστικές απαιτήσεις, μέσω της χρήσης πιστοποιημένων λύσεων. Αυτό μπορεί να επιτευχθεί μέσω της συμβολής του στην ανάπτυξη και την επικαιροποίηση των στρατηγικών που έχουν υιοθετηθεί, στο πλαίσιο της ασφάλειας των ψηφιακών συστημάτων δικτύου και πληροφοριών, της προώθησης των εν λόγω στρατηγικών και της παρακολούθησης της προόδου ως προς την υλοποίησή τους (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 26). Για τον σκοπό αυτόν, συγκεντρώνει και αναλύει εθνικές εκθέσεις από της CSIRTs και την CERT-EU, συμβάλλοντας στη δημιουργία κοινών διαδικασιών και ορολογίας, για την

ανταλλαγή πληροφοριών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 31). Παράλληλα, ο ENISA συμβάλλει στην αντιμετώπιση διασυνοριακών περιστατικών μεγάλης κλίμακας, διευκολύνοντας την ανταλλαγή τεχνικών λύσεων και υποστηρίζοντας την επιχειρησιακή συνεργασία μεταξύ των κρατών-μελών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 32).

Τέλος, ο ENISA παρέχει στα κράτη μέλη κατάρτιση στον τομέα της εκπαίδευσης και ευαισθητοποίησης των πολιτών, στον τομέα της κυβερνοασφάλειας (Άρθρο 4 και 10). Η υποστήριξη αυτή περιλαμβάνει τη δημιουργία ενός δικτύου εθνικών σημείων επαφής για θέματα εκπαίδευσης στον τομέα της κυβερνοασφάλειας, καθώς ανάπτυξη μιας ειδικής πλατφόρμας κατάρτισης. Το δίκτυο αυτό θα μπορούσε να ενταχθεί στο ήδη υπάρχον δίκτυο εθνικών συνδέσμων και να αποτελέσει τη βάση για καλύτερο συντονισμό των σχετικών δράσεων, σε εθνικό επίπεδο (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 27). Το έργο του ENISA πρέπει να αξιολογείται τακτικά και με ανεξάρτητο τρόπο. Η αξιολόγηση αυτή θα πρέπει να εξετάζει κατά πόσο ο Οργανισμός επιτυγχάνει τους στόχους του, αν ακολουθεί αποτελεσματικές πρακτικές εργασίας και αν τα καθήκοντά του, ιδίως εκείνα που σχετίζονται με την επιχειρησιακή συνεργασία εντός της Ευρωπαϊκής Ένωσης, παραμένουν επίκαιρα και ουσιώδη. Επιπλέον, θα πρέπει να αποτιμάται η επίδραση, η αποδοτικότητα και η αποτελεσματικότητα του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας. Σε περίπτωση που γίνει αναθεώρηση, η Ευρωπαϊκή Επιτροπή οφείλει να εξετάσει πως μπορεί να ενισχυθεί ο ρόλος του ENISA ως βασικού φορέα παροχής συμβουλών και τεχνογνωσίας. Θα πρέπει, επίσης να μελετήσει εάν μπορεί να του ανατεθεί υποστηρικτικός ρόλος στην αξιολόγηση προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ, οι οποίες προέρχονται από τρίτες χώρες και δεν συμμορφώνονται με τους κανόνες της ΕΕ, όταν αυτά εισάγονται στην Ένωση (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019, αιτιολογική σκέψη 108).

2.3.2. CERT-EU (Computer Emergency Response Team) και CSIRTs.

Οι CERTs (Computer Security Incident Response Teams) αποτελούν ομάδες αντιμετώπισης περιστατικών ασφάλειας πληροφοριών. Οι CERTs δημιουργήθηκαν σε μία προσπάθεια επιτυχούς ανταπόκρισης στις ελλείψεις ασφαλείας κατά τον αρχικό σχεδιασμό του Διαδικτύου. Ο ρόλος τους είναι να ανιχνεύουν, να αναλύουν και να ανταποκρίνονται σε περιστατικά Κυβερνοασφάλειας, όπως επιθέσεις hacking, malware κλπ. Στην Ευρωπαϊκή Ένωση ιδρύθηκε το δίκτυο CSIRTs, το οποίο τέθηκε σε εφαρμογή κατ' ακολουθία της Οδηγίας NIS2 (European Union, 2022, Άρθρο 10) και αποτελείται από τα εθνικά CSRISTs των κρατών-μελών, το CERT-EU (CSIRT των θεσμών της ΕΕ καθώς και τον οργανισμό ENISA, ο οποίος παρέχει την καθοδήγηση και την υποστήριξη στο δίκτυο αυτό). Κάθε κράτος-μέλος μπορεί να συστήσει μία ή περισσότερες ομάδες αντιμετώπισης περιστατικών ασφαλείας και οφείλει να φροντίζει ώστε κάθε ομάδα να διαθέτει τους κατάλληλους πόρους, ώστε να μπορεί να επιτελεί αποτελεσματικά το έργο που της έχει ανατεθεί. (Οδηγία 2022/2555, άρθρο 10). Μάλιστα, τα κράτη-μέλη μπορούν να ζητούν τη συνδρομή του ENISA για την ανάπτυξη των ομάδων τους (Οδηγία 2022/2555, άρθρο 10). Οι ομάδες CSIRTs μπορούν να συνεργάζονται και, ανάλογα την περίπτωση, να ανταλλάσσουν σχετικές πληροφορίες.

Σύμφωνα με το άρθρο 11 της Οδηγίας NIS 2, οι CSIRTs οφείλουν να λειτουργούν σύμφωνα με ορισμένες βασικές προδιαγραφές. Θα πρέπει, λοιπόν, να διατηρούν μία συνεχή διαθεσιμότητα μεταξύ των διαύλων επικοινωνίας τους, αποφεύγοντας την εξάρτηση από ένα και μόνο μέσο και παρέχοντας εναλλακτικές επιλογές για επικοινωνία με τρίτους, ανά πάσα στιγμή. Οι τρόποι επικοινωνίας θα πρέπει να είναι σαφώς καθορισμένοι και γνωστοποιημένοι στα αρμόδια μέλη και συνεργάτες. Οι εγκαταστάσεις τους, καθώς και τα υποστηρικτικά πληροφοριακά τους συστήματα, θα πρέπει να βρίσκονται σε ασφαλή περιβάλλοντα. Παράλληλα, είναι απαραίτητο να διαθέτουν ένα αποδοτικό σύστημα διαχείρισης και δρομολόγησης αιτημάτων, το οποίο επιτρέπει την αποτελεσματική υλοποίηση των αρμοδιοτήτων τους. Η προστασία της εμπιστευτικότητας και της αξιοπιστίας των δραστηριοτήτων τους αποτελεί βασική αρχή λειτουργίας. Επιπλέον, πρέπει να είναι επαρκώς στελεχωμένες με κατάλληλα εκπαιδευμένο προσωπικό, ώστε να

διασφαλίζεται η αδιάλειπτη παροχή των υπηρεσιών τους. Τέλος, πρέπει να διαθέτουν πλεονάζοντα συστήματα και εφεδρικό χώρο εργασίας, ώστε να εξασφαλίζεται η επιχειρησιακή συνέχεια, ακόμη και σε περιόδους κρίσης.

Μάλιστα, στο πλαίσιο περαιτέρω ενίσχυσης της κυβερνοασφάλειας εντός της Ευρωπαϊκής Ένωσης, η Οδηγία NIS2 προβλέπει τη δημιουργία ενός συντονισμένου μηχανισμού γνωστοποίησης ευπαθειών, με στόχο τη διασφάλιση τα έγκαιρης και αποτελεσματικής αντιμετώπισης κινδύνων, οι οποίοι προκύπτουν από ευπάθειες σε υπηρεσίες ΤΠΕ. Σύμφωνα με το άρθρο 12§1, κάθε κράτος μέλος οφείλει να αναθέσει σε μία από τις CSIRTs συντονιστικό ρόλο για την εν λόγω διαδικασία. Η CSIRT, η οποία ορίζεται, λειτουργεί ως αξιόπιστος διαμεσολαβητής μεταξύ των προσώπων, τα οποία αναφέρουν την ευπάθεια, και των κατασκευαστών ή παρόχων των υπηρεσιών παρέχοντας στήριξη, συντονισμό και διαχείριση της επικοινωνίας. Επιπλέον, η εν λόγω CSIRT διασφαλίζει τη δυνατότητα ανώνυμης αναφοράς από φυσικά ή νομικά πρόσωπα καθώς και την προστασία της ανωνυμίας τους (Άρθρο 12§1)[2]. Στην περίπτωση που μία ευπάθεια δύναται να επηρεάσει οντότητες περισσοτέρων κρατών-μελών, προβλέπεται η δυνατότητα της συνεργασίας μεταξύ των διαφόρων ομάδων απόκρουσης, οι οποίες έχουν αναλάβει συντονιστικό ρόλο σε κάθε ενδιαφερόμενο κράτος, μέσω του δικτύου CSIRT. Παράλληλα, ο ENISA έχει την αρμοδιότητα να αναπτύσσει και να διατηρεί μία ευρωπαϊκή βάση δεδομένων ευπαθειών, σε συνεργασία με την Ομάδα Συνεργασίας (Άρθρο 12§2).[3] Η βάση αυτή έχει ως στόχο την παροχή, στις ενδιαφερόμενες οντότητες της δυνατότητας για εθελοντική δημοσιοποίηση δημοσίως γνωστών ευπαθειών, συνοδευόμενων από αρχείο πληροφοριών, το οποίο καταδεικνύει τη σοβαρότητα και την έκταση του προβλήματος, καθώς και για τη διαθεσιμότητα διορθωτικών παρεμβάσεων ή καθοδήγησης για τον περιορισμό των κινδύνων.

[2] «Τα κράτη μέλη διασφαλίζουν ότι τα φυσικά ή νομικά πρόσωπα μπορούν να αναφέρουν ανώνυμα, εφόσον ζητηθεί, ευπάθειες στην CSIRT στην οποία έχει ανατεθεί ο συντονισμός…».

[3] «Ο ENISA αναπτύσσει και διατηρεί, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας, ευρωπαϊκή βάση δεδομένων ευπαθειών…».

Η αποτελεσματική εφαρμογή των υποχρεώσεων, οι οποίες απορρέουν από την Οδηγία, προϋποθέτει στενή συνεργασία, σε εθνικό επίπεδο. Το άρθρο 13§1[4] προβλέπει ότι οι αρμόδιες αρχές και οι CSIRTs του ίδιου κράτους-μέλους οφείλουν να συνεργάζονται μεταξύ τους. Επιπρόσθετα, διασφαλίζεται ότι οι CSIRTs ή οι αρμόδιες αρχές κρίνονται υπεύθυνες για τη λήψη αναφορών σχετικά με σοβαρά περιστατικά (Άρθρο 13§2[5]), καθώς και περιστατικά, κυβερνοαπειλές και «παρολίγον» περιστατικά, όπως αυτά ορίζονται στα άρθρα 23 και 30 της ίδιας Οδηγίας. Παράλληλα, οι αρμόδιοι φορείς υποχρεούνται να ενημερώνουν τα ενιαία σημεία επαφής (Single Points of Contact – SPOC), τις συγκεκριμένες, δηλαδή αρχές οι οποίες λειτουργούν ως δίαυλοι για την επικοινωνία με τα υπόλοιπα κράτη μέλη, σχετικά με τις κοινοποιήσεις αυτές, ώστε να διασφαλίζεται η κεντρική συλλογή και η κατάλληλη διαχείριση των σχετικών δεδομένων, σε εθνικό επίπεδο (13§3).[6]

Για την ενίσχυση της διακρατικής εμπιστοσύνης και της στρατηγικής συνεργασίας μεταξύ των κρατών-μελών, συστήνεται η Ομάδα Συνεργασίας, όπως ορίζεται στο άρθρο 14§1 της Οδηγίας NIS2.[7] Η ομάδα αυτή αποτελεί βασικό εργαλείο στην προσπάθεια ανταλλαγής πληροφοριών και βέλτιστων πρακτικών, μεταξύ των κρατών-μελών, ενώ λειτουργεί στη βάση διετών πρακτικών εργασιών, κατ'άρθον 14§2.[8] Η σύνθεσή της περιλαμβάνει εκπροσώπους των κρατών-μελών, της Ευρωπαϊκής Επιτροπής και του ENISA, ενώ συμμετέχουν η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ως παρατηρητής), οι Ευρωπαϊκές Εποπτικές Αρχές

[4] «Εφόσον πρόκειται για διακριτές οντότητες, οι αρμόδιες αρχές, το ενιαίο σημείο επαφής και οι CSIRT του ίδιου κράτους μέλους συνεργάζονται μεταξύ τους για τους σκοπούς της τήρησης των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.…».

[5] «Τα κράτη μέλη διασφαλίζουν ότι οι CSIRT ή, κατά περίπτωση, οι αρμόδιες αρχές τους λαμβάνουν αναφορές σοβαρών περιστατικών σύμφωνα με το άρθρο 23, καθώς και περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών σύμφωνα με το άρθρο 30.…».

[6] «Κάθε κράτος μέλος μεριμνά ώστε οι CSIRT του ή, κατά περίπτωση, οι αρμόδιες αρχές του να ενημερώνουν τα ενιαία σημεία επαφής τους για κοινοποιήσεις περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών που υποβάλλονται σύμφωνα με την παρούσα οδηγία.…».

[7] «Για την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, καθώς και την ενίσχυση της πίστης και της εμπιστοσύνης, συστήνεται Ομάδα Συνεργασίας.…»)

[8] «Η Ομάδα Συνεργασίας εκτελεί τα καθήκοντά της βάσει διετών προγραμμάτων εργασιών τα οποία αναφέρονται στην παράγραφο 7.…».

και λοιπές αρμόδιες αρχές κατά περίπτωση, κατ'άρθον 14§3.[9] Όπου κρίνεται σκόπιμο στην Ομάδα μπορεί να συμμετάσχουν και μέλη του Ευρωπαϊκού Κοινοβουλίου ή άλλων ενδιαφερόμενων μερών.

Η CERT-EU (Computer Emergency Response Team for the EU Institutions, Bodies and Agencies), συγκεκριμένα, αποτελεί την ομάδα άμεσης αντιμετώπισης περιστατικών Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης, με έδρα τις Βρυξέλλες, το οποίο προστατεύει τα θεσμικά όργανα, τους οργανισμούς και διάφορες περαιτέρω υπηρεσίες της Ευρωπαϊκής Ένωσης από κυβερνοεπιθέσεις. Για να το επιτύχουν αυτό, οι ειδικοί IT, οι οποίοι στελεχώνουν την ομάδα, φροντίζουν να συλλέξουν, να διαχειριστούν, να αναλύσουν και να μοιραστούν πληροφορίες για τα θεσμικά όργανα, τους φορείς και τις υπηρεσίες της ΕΕ σχετικά με απειλές, τρωτά σημεία και περιστατικά που αφορούν μη διαβαθμισμένες υποδομές ΤΠΕ. Η ομάδα αυτή φροντίζει να συντονίσει, επίσης, τις αντιδράσεις σε περιστατικά, σε διοργανικό και θεσμικό επίπεδο, για παράδειγμα, παρέχοντας ή συντονίζοντας την παροχή εξειδικευμένης επιχειρησιακής βοήθειας (CERT-EU, no date).

Για να επιτύχει την αποστολή της η CERT-EU συνεργάζεται στενά με τους θεσμούς της Ευρωπαϊκής Ένωσης, όπως είναι η Ευρωπαϊκή Επιτροπή, το Ευρωπαϊκό Κοινοβούλιο και η Ευρωπαϊκή Κεντρική Τράπεζα. Συλλέγει και αναλύει δεδομένα απειλών από εσωτερικές και εξωτερικές πηγές, εκδίδει οδηγίες ασφαλείας και προειδοποιήσεις για νέες κυβερνοαπειλές και συμμετέχει σε ευρωπαϊκές και διεθνείς επιχειρήσεις κυβερνοασφάλειας. Η συνεργασία της CERT-EU με άλλους φορείς είναι κρίσιμη για την αποτελεσματική αντιμετώπιση των κυβερνοαπειλών. Συνεργάζεται με την ENISA για στρατηγική καθοδήγηση, με το Europol-EC3 (European Cybercrime Centre), για την ποινική διερεύνηση κυβερνοεγκλήματος και με τα εθνικά CSIRTs των κρατών-μελών για τη διαχείριση διασυνοριακών επιθέσεων. Η σημασία της CERT-EU, καθώς και των λοιπών ομάδων CSIRTs των κρατών-μελών, έγκειται στο γεγονός ότι αποτελούν κεντρικό πυλώνα κυβερνοασφάλειας της ΕΕ, διασφαλίζοντας την ακεραιότητα των

[9] «Η Ομάδα Συνεργασίας απαρτίζεται από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης συμμετέχει στις δραστηριότητες της ομάδας συνεργασίας ως παρατηρητής. Οι Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) και οι αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554 μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας σύμφωνα με το άρθρο 47 παράγραφος 1 του εν λόγω κανονισμού.....…».

δεδομένων, των συστημάτων και των λειτουργιών των θεσμικών της οργάνων και των κρατών-μελών της προστατεύοντάς τα από σύγχρονες και εξελιγμένες κυβερνοαπειλές.

2.3.3.Συνεργασία με τις Διωκτικές Αρχές των κρατών-μελών.

Στον τομέα της Κυβερνοασφάλειας, οι διωκτικές αρχές[10] συνεργάζονται με τις ομάδες CSRISTs για την καταπολέμηση του Κυβερνοεγκλήματος και την προστασία των κρίσιμων υποδομών από απειλές στον Κυβερνοχώρο (ENISA, 2022). Η συνεργασία αυτή επικεντρώνεται στην ανταλλαγή πληροφοριών και την ανάπτυξη μηχανισμών πρόληψης και απόκρισης σε κυβερνοεπιθέσεις, με στόχο την έγκαιρη ανίχνευση, διαχείριση και αποτροπή κυβερνοεγκλήματος. Σε περιπτώσεις μαζικών ή κρίσιμων κυβερνοεπιθέσεων, ενεργοποιούνται ευρωπαϊκοί και διεθνείς μηχανισμοί για τη διαχείριση της απειλής, ώστε να επιτευχθεί ταχεία αντίδραση και συντονισμένη δράση μεταξύ των αρμοδίων φορέων. Οι επιθέσεις αυτού του είδους απαιτούν διεθνή συνεργασία, καθώς συχνά προέρχονται από διακρατικά δίκτυα κυβερνοεγκληματιών, γεγονός που καθιστά αναγκαία τη συμμετοχή διαφόρων φορέων ασφαλείας και επιβολής του νόμου.

Η Europol EC3 αποτελεί το βασικό κέντρο συνεργασίας για την καταπολέμηση του κυβερνοεγκλήματος στην Ευρώπη. Το κέντρο αυτό υποστηρίζει τις διωκτικές αρχές των κρατών-μελών της ΕΕ, προσφέροντας τεχνική και επιχειρησιακή βοήθεια στη διερεύνηση σοβαρών κυβερνοεγκλημάτων. Παράλληλα, συντονίζει δράσεις με διεθνείς οργανισμούς, όπως η INTERPOL και το FBI για την αντιμετώπιση εγκληματικών δικτύων στον κυβερνοχώρο. Μέσω της συνεργασίας του με τα CSIRTs και άλλους φορείς ασφαλείας, το Europol EC3 συμβάλλει στην πρόληψη, ανίχνευση και καταστολή των ψηφιακών απειλών, ενισχύοντας την ανθεκτικότητα της Ευρωπαϊκής Ένωσης απέναντι σε κυβερνοεπιθέσεις.

Η συνεργασία μεταξύ των ομάδων αντιμετώπισης περιστατικών ασφαλείας υπολογιστών (CSIRTs) και των υπηρεσιών επιβολής του νόμου (LE) αποτελεί το κλειδί για την εύρεση τέτοιων πληροφοριών και την καταπολέμηση του

[10] Ο όρος 'Law Enforcement' αναφέρεται στις Διωκτικές Αρχές κάθε κράτους-μέλους, οι οποίες είναι υπεύθυνες για την τήρηση του νόμου, την πρόληψη του εγκλήματος και τη διερεύνηση παραβιάσεων (Vagianos, 2024).

εγκλήματος στον κυβερνοχώρο. Όπως αναφέρεται στο σημείωμα του Συμβουλίου της 31ης Μαΐου 2017 Cybersecurity-Information from the Επιτροπής (Συμβούλιο, ΕΕ, 2017), «Τα συμπεράσματα που εξήχθησαν από την επίθεση WannaCry (Mohurle and Patil, 2017) περιλαμβάνουν την ανάγκη συνεργασίας των CSIRT, των αρχών LE και του ιδιωτικού τομέα και η ανάγκη για LE αρχές να διαθέτουν τα κατάλληλα εργαλεία για τη διερεύνηση τέτοιου είδους εγκλημάτων και τη δίωξη των εγκληματιών».

2.3.4. Συνεργασία με τρίτους φορείς (Interpol, NATO).

Η ενίσχυση της συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και τρίτων φορέων, όπως το NATO και η INTERPOL, αποτελεί κρίσιμη στρατηγική για την κυβερνοασφάλεια και την κυβερνοάμυνα (Lawspot.gr, 2024). Η αυξανόμενη πολυπλοκότητα των κυβερνοαπειλών καθιστά αναγκαία τη διαμόρφωση ενός κοινού πλαισίου δράσης, ενισχύοντας την ανταλλαγή πληροφοριών, την ανάπτυξη ψηφιακών ικανοτήτων και τη συντονισμένη αντιμετώπιση κυβερνοεπιθέσεων.

Στις 2 Σεπτεμβρίου 2023, υψηλόβαθμοι αξιωματούχοι της ΕΕ και του NATO συναντήθηκαν στην έδρα του NATO για να αποτιμήσουν τις πρόσφατες εξελίξεις και να διερευνήσουν νέες δυνατότητες συνεργασίας στην κυβερνοασφάλεια και την κυβερνοάμυνα (Lawspot.gr, 2024). Στις συνομιλίες υψηλού επιπέδου συμμετείχαν η Benedikta von Seherr-Thoß, Διευθύνουσα Σύμβουλος της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης και ο David van Weel, Αναπληρωτής Γενικός Γραμματέας του NATO (EEAS, 2023). Ο επιθετικός πόλεμος της Ρωσίας κατά της Ουκρανίας έχει επιταχύνει την εμφάνιση ενός περίπλοκου τοπίου κυβερνοαπειλών, χαρακτηρισμένου από μεγαλύτερη αστάθεια και αυξημένες επιθέσεις σε οικονομικά, κοινωνικά και στρατηγικά συστήματα. Οι κυβερνοεπιθέσεις που προέρχονται από αυταρχικά καθεστώτα υπονομεύουν την παγκόσμια ασφάλεια και την οικονομική σταθερότητα, καθιστώντας τη συνεργασία μεταξύ των συμμάχων πιο κρίσιμη από ποτέ. Η Benedikta von Seherr-Thoß τόνισε τη σημασία της εναρμόνισης των στρατηγικών της ΕΕ και του NATO, καθώς τα περισσότερα κράτη μέλη της ΕΕ είναι επίσης μέλη του NATO. Η Lorena Boix Alonso, Διευθύντρια για την Ψηφιακή Κοινωνία και την Κυβερνοασφάλεια στη Γενική Διεύθυνση Επικοινωνιακών Δικτύων της Ευρωπαϊκής Επιτροπής, υπογράμμισε ότι η

συνεργασία μεταξύ των δύο οργανισμών είναι ζωτικής σημασίας για την ανθεκτικότητα απέναντι σε κυβερνοαπειλές (EEAS, 2023). Σύμφωνα με τη στρατηγική πυξίδα της Ευρωπαϊκής Ένωσης και την Πολιτική για την Κυβερνοάμυνα, η ΕΕ και το ΝΑΤΟ θα συνεχίσουν να εργάζονται για την ενίσχυση της κοινής επίγνωσης της κατάστασης, την ανάπτυξη ψηφιακών ικανοτήτων και την πρόληψη, αποτροπή και αντιμετώπιση κυβερνοεπιθέσεων.

Παράλληλα, η ΕΕ συνεργάζεται στενά με την INTERPOL για την αντιμετώπιση του κυβερνοεγκλήματος και την καταπολέμηση εγκληματικών δικτύων που δραστηριοποιούνται στον κυβερνοχώρο. Η συνεργασία μεταξύ των κρατών-μελών και των ευρωπαϊκών οργανισμών στην αντιμετώπιση του κυβερνοεγκλήματος εκφράζεται μέσα από τρεις βασικούς άξονες (European Commission, 2021). Πρώτον, η ανταλλαγή πληροφοριών μεταξύ των υπηρεσιών επιβολής του νόμου αποτελεί κρίσιμο εργαλείο για την παρακολούθηση, την έγκαιρη ανίχνευση και την ανάλυση κυβερνοεγκληματικών δραστηριοτήτων. Η διαρκής και συστηματική ροή δεδομένων και ευρημάτων μεταξύ εθνικών και υπερεθνικών αρχών ενισχύει σημαντικά τη δυνατότητα εντοπισμού και κατανόησης των τεχνικών και των μεθόδων, οι οποίες χρησιμοποιούνται από τους δράστες. Δεύτερον, η διεξαγωγή κοινών επιχειρήσεων αποτελεί ουσιώδες μέσο στην προσπάθεια εξάρθρωσης εγκληματικών δικτύων καθώς και την αποτροπή οργανωμένων κυβερνοεπιθέσεων. Τέτοιες επιχειρήσεις συχνά, υπό τον εντοπισμό της Europol και του European Cybersecurity Centre (EC3), επιτρέπουν τη συγκέντρωση και αξιοποίηση επιχειρησιακών πόρων και πληροφοριών από πολλαπλές εθνικές υπηρεσίες, ενισχύοντας την αποτελεσματικότητα της αντίδρασης σε κυβερνοαπειλές. Τρίτον, η εκπαίδευση και η ανάπτυξη ικανοτήτων των εθνικών αρχών αποτελεί πυλώνα για τη μακροπρόθεσμη ενίσχυση της ανθεκτικότητας έναντι του κυβερνοεγκλήματος. Μέσω της παροχής εξειδικευμένης τεχνογνωσίας, της διάθεσης προηγμένων εργαλείων και της υλοποίησης στοχευμένων προγραμμάτων κατάρτισης, οργανισμοί όπως η ENISA και η Europol ενισχύουν την επιχειρησιακή ετοιμότητα των κρατών-μελών και συμβάλλουν στη δημιουργία ενός συνεκτικού και αποτελεσματικού ευρωπαϊκού πλαισίου πρόληψης και καταστολής του κυβερνοεγκλήματος.

3. ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

ΤΥΠΟΛΟΓΙΑ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΕΠΙΤΑΚΤΙΚΟΤΗΤΑ ΛΗΨΗΣ ΜΕΤΡΩΝ.

3.1. Κλιμάκωση των κυβερνοεγκλημάτων και επιτακτική ανάγκη για Δράση.

Η αρχή της ψηφιακής εποχής, η οποία δεν έχει αυστηρά καθορισμένη ημερομηνία αλλά τοποθετείται γύρω στα τέλη του 20ου αιώνα, επέφερε ποικίλες προκλήσεις. Μία εξ αυτών αποτελεί και η προσπάθεια διασφάλισης της ασφάλειας στον κυβερνοχώρο καθώς και της ιδιωτικότητας αφού, η έλλειψη ρυθμιστικών πλαισίων άφηνε περιθώρια για καταχρήσεις. Οι εταιρείες δεν γνώριζαν πως θα μπορούσαν να προστατεύσουν σωστά τα πολυάριθμα δεδομένα τους, καθιστώντας τα εύκολο στόχο για τους επίδοξους hackers. Τα περιστατικά κυβερνοασφάλειας αυξάνονται σταθερά, με τις συνέπειες να είναι ολοένα και πιο σοβαρές. Ενδεικτικά, το ποσοστό των επιχειρήσεων στην ΕΕ οι οποίες υπέστησαν ζημία από περιστατικά ασφαλείας ΤΠΕ αυξήθηκε από 12% το 2018 σε 22% το 2021, σύμφωνα με δεδομένα της Eurostat (Vandezande, 2024). Η επιπτώσεις κυμαίνονται από τη διακοπή εργασιών έως την απώλεια δεδομένων και τη διαρροή εμπιστευτικών πληροφοριών, ενώ οι κακόβουλες επιθέσεις παρουσιάζουν σημαντική κλιμάκωση τα τελευταία έτη.

Κατά τη δεύτερη δεκαετία του 21ου αιώνα σημειώθηκαν σημαντικές εξελίξεις αφορώσες το πεδίο της ασφάλειας πληροφοριών, συστημάτων και δικτύων. Ειδικότερα, το 2001, η Ευρωπαϊκή Ένωση προσχώρησε στη Σύμβαση της Βουδαπέστης για τα εγκλήματα στον κυβερνοχώρο (Convention on Cybercrime) και επιδιώκει την εναρμόνιση των εθνικών ποινικών νομοθεσιών των κρατών στον τομέα της εγκληματικότητας στον κυβερνοχώρο. Η νομοθεσία επικεντρώνεται στην προστασία των κρίσιμων υποδομών, όπως οι τράπεζες, οι τηλεπικοινωνίες και οι εταιρείες τεχνολογίας. Από το 2013 και μετά, οι κυβερνοεπιθέσεις αυξήθηκαν δραματικά. Η κυβερνοασφάλεια έπαψε να αποτελεί απλώς ένα εργαλείο ομαλής εξέλιξης της ενιαίας αγοράς. Αντιθέτως, έκτοτε αντιμετωπίζεται ως πυλώνας της ευρωπαϊκής ασφάλειας και άμυνας. Κάτω από αυτές τις συνθήκες, το 2013 η Ευρωπαϊκή Ένωση παρουσίασε την πρώτη της στρατηγική για την κυβερνοασφάλεια με τίτλο «Στρατηγική της Ευρωπαϊκής Ένωσης για την

Κυβερνοασφάλεια: Ασφαλές και Αξιόπιστο Ψηφιακό Περιβάλλον». Η επιδίωξη της κυβερνοασφάλειας ενέχει, εκτός από το κομμάτι λήψης προληπτικών μέτρων ασφαλείας, και τη ρύθμιση του κυβερνοεγκλήματος. Στην πραγματικότητα αποτελούν αλληλένδετες πτυχές της σύγχρονης ψηφιακής πραγματικότητας. Η κυβερνοασφάλεια αποσκοπεί στην προστασία των συστημάτων πληροφορικής, των δεδομένων και των επικοινωνιών από κακόβουλες ενέργειες ενώ, η ρύθμιση του κυβερνοεγκλήματος επικεντρώνεται στη νομική αντιμετώπιση των παράνομων δραστηριοτήτων οι οποίες λαμβάνουν χώρα στο διαδίκτυο. Έτσι, γίνεται φανερό πως η ύπαρξη ενός ισχυρού πλαισίου κυβερνοασφάλειας αποτελεί αναγκαία προϋπόθεση για τον αποτελεσματικό εντοπισμό, την πρόληψη και την καταστολή του κυβερνοεγκλήματος. Αφενός, η κυβερνοασφάλεια παρέχει τα τεχνικά εργαλεία και τις μεθόδους οι οποίες καθιστούν δυνατή την ανίχνευση και την απόκρουση ψηφιακών επιθέσεων. Αφετέρου, η ρύθμιση του κυβερνοεγκλήματος διασφαλίζει ότι οι επιτιθέμενοι υπόκεινται σε έννομες συνέπειες, αποθαρρύνοντας, έτσι, την τέλεση εγκληματικών πράξεων(Vandezande, 2024). Η θεσμική συνεργασία μεταξύ τεχνολογικών φορέων και νομοθετικών αρχών είναι απαραίτητη ώστε να καλυφθούν τα κενά που υπάρχουν μεταξύ της τεχνολογικής και της νομικής προσέγγισης. Ειδικά σε ένα διασυνοριακό περιβάλλον, η εναρμόνιση των ρυθμιστικών πλαισίων και η διακρατική συνεργασία καθίστανται κρίσιμες.

Εν τέλει, η επιδίωξη της κυβερνοασφάλειας χωρίς ταυτόχρονη και δυναμική ρύθμιση του κυβερνοεγκλήματος καθίσταται ανεπαρκής καθώς απουσιάζει ο αποτρεπτικός και κατασταλτικός μηχανισμός. Από την άλλη πλευρά, η ρύθμιση του κυβερνοεγκλήματος, χωρίς τις κατάλληλες τεχνολογικές υποδομές και τους μηχανισμούς της κυβερνοασφάλειας είναι πρακτικά αδύνατη. Επομένως, οι δύο αυτές συνιστώσες θα πρέπει να λειτουργούν παράλληλα, σε ένα πλαίσιο θωράκισης της ψηφιακής ασφάλειας.

3.2. Κυβερνοέγκλημα: Ορισμός.

Το κυβερνοέγκλημα αποτελεί έναν σύνθετο και εξελισσόμενο φαινόμενο, το οποίο δεν περιορίζεται σε έναν αυστηρά καθορισμένο ορισμό. Ανατρέχοντας στο παρελθόν, από νωρίς έγιναν προσπάθειες να δοθεί ένας σαφής και

εμπεριστατωμένος ορισμός του κυβερνοεγκλήματος. Από τους πρώτους στο εν λόγω εγχείρημα υπήρξε ο Donn Parker (1976), επιστήμων πληροφορικής, ο οποίος, αρχικά εισήγαγε τον όρο «κατάχρηση υπολογιστών», αναφερόμενος σε κάθε σκόπιμη ενέργεια η οποία θα μπορούσε να προκαλέσει ζημία στο θύμα, επιφέροντας όφελος στο δράστη, με τη συμμετοχή υπολογιστικών συστημάτων (Vagianos, 2024). Πρότεινε τέσσερις βασικές κατηγορίες: τον υπολογιστή ως αντικείμενο, ως περιβάλλον, ως εργαλείο ή ως «σύμβολο» εξαπάτησης. Οι θεμελιώδεις αυτές διακρίσεις αποτέλεσαν τη βάση για τη μεταγενέστερη εννοιολόγηση των ψηφιακών εγκλημάτων. Σε μία μεταγενέστερη προσπάθεια αναπλαισίωσης των παραπάνω εννοιών, το 2007, ο επιστήμονας Robert Taylor πρότεινε μία επικαιροποιημένη τετραμερή κατηγοριοποίηση: α. ο υπολογιστής ως στόχος επίθεσης, β. ως εργαλείο για την τέλεση αδικημάτων, γ. ως βοηθητικό μέσο, δ. ως κρίσιμη συνιστώσα εγκλημάτων, τα οποία στρέφονται κατά της ίδιας της ψηφιακής υποδομής (Vagianos, 2024). Παράλληλα, ο ερευνητής Majid Yar υποστήριξε, το 2006 ότι, το κυβερνοέγκλημα δε συνιστά ενιαίο όρο, αλλά, ένα φάσμα παράνομων ή, έστω, κοινωνικώς αποδοκιμαστέων δραστηριοτήτων, στις οποίες τα πληροφοριακά και επικοινωνιακά μέσα παίζουν καίριο ρόλο (Vagianos, 2024). Ο σύγχρονος ορισμός, ορμώμενος από προγενέστερες σκέψεις και παρατηρήσεις ορίζει ότι, το σύνολο της παραβατικής συμπεριφοράς το οποίο, σε κάποιο στάδιο της εκτέλεσης, περιλαμβάνει τη χρήση τεχνολογικών εργαλείων στοιχειοθετεί το ηλεκτρονικό έγκλημα. Η εξέλιξη του ηλεκτρονικού εγκλήματος, με τη χρήση του διαδικτύου στοιχειοθετεί το κυβερνοέγκλημα (Mavridis, 2015). Η Διεθνής Οργάνωση Τυποποίησης (ISO) ορίζει το κυβερνοέγκλημα ως «τη διάπραξη εγκληματικών ενεργειών στον κυβερνοχώρο» (International Organization for Standardization, 2023) ενώ, ευρύτερα θεωρείται ως μία νέα μορφή διάπραξης παραδοσιακών εγκλημάτων, με ψηφιακά μέσα. Τέτοια εγκλήματα, για παράδειγμα, αποτελούν η κλοπή ταυτότητας, η απάτη (μέσω της χρήσης ηλεκτρονικού υπολογιστή), η κλοπή χρεωστικής-πιστωτικής κάρτας και τα λοιπά (Vagianos, 2024). Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο χρησιμοποιεί τον όρο έγκλημα στον κυβερνοχώρο για να αναφερθεί σε αδικήματα που κυμαίνονται από εγκληματική δραστηριότητα κατά των

δεδομένων έως την παραβίαση περιεχομένου και πνευματικών δικαιωμάτων. Ιδιαίτερη ανησυχία προκαλούν οι ψηφιακές μορφές σεξουαλικής κακοποίησης, όπως είναι ο διαδικτυακός εκβιασμός και η παιδική πορνογραφία, οι οποίες ευνοούνται από την εξάπλωση των κοινωνικών δικτύων και την ευκολία παραγωγής και διακίνησης παράνομου υλικού.

Παρά την πρόοδο, η οποία έχει σημειωθεί, δεν υφίσταται ακόμη ένας ενιαίος ορισμός για το κυβερνοέγκλημα, σε διεθνές επίπεδο. Οργανισμοί, όπως η Interpol επισημαίνουν τη διάκριση μεταξύ τεχνολογικά προηγμένων επιθέσεων σε υπολογιστικά συστήματα και παραδοσιακών εγκλημάτων, που, απλώς, διευκολύνονται από την τεχνολογία, όπως είναι οι οικονομικές απάτες και η παιδική πορνογραφία.

3.2.1. Τύποι Κυβερνοεγκλημάτων:

Μπορούμε να κατηγοριοποιήσουμε του τύπους Κυβερνοεγκλημάτων σε τρεις βασικές κατηγορίες: α. Τα Κυβερνοεγκλήματα κατά τα οποία στοχοποιείται ένας συγκεκριμένος υπολογιστής, β. Αυτά, για την διάπραξη των οποίων απαραίτητη προϋπόθεση είναι η χρήση ηλεκτρονικού υπολογιστή και γ. αυτά κατά τα οποία η χρήση ηλεκτρονικού υπολογιστή διευκολύνει την εκτέλεσή τους (Vagianos, 2024).
Στην πρώτη κατηγορία, ένας υπολογιστής ή ένα πληροφοριακό σύστημα αποτελεί τον στόχο μιας συγκεκριμένης Κυβερνοεπίθεσης. Κάποιοι βασικοί τύποι τέτοιων επιθέσεων αποτελούν:

Hacking or Cracking:

Ο όρος αυτός αναφέρεται σε έγκλημα στον υπολογιστή ενός χρήστη, με σκοπό την παραβίαση ευαίσθητων και προσωπικών δεδομένων. Ο εγκληματίας, αρκετά εξοικειωμένος με υπολογιστικά περιβάλλοντα, χρησιμοποιεί διάφορα εργαλεία για να εισέλθει στον υπολογιστή, χωρίς τη συγκατάθεση του ιδιοκτήτη. Ο χάκερ έχει πρόσβαση και επιτίθεται από μια απομακρυσμένη τοποθεσία (Kaspersky, 2021).

Malicious Software (Malware):

Το malware αποτελεί ένα κακόβουλο λογισμικό το οποίο θεωρείται μία από τις πιο κοινές απειλές στον Κυβερνοχώρο. Δημιουργείται από τον κυβερνογκληματία με αποκλειστικό σκοπό να εισχωρήσει και να υποκλέψει ή να βλάψει τα δεδομένα του υπολογιστή ενός χρήστη. Ως κακόβουλο λογισμικό μπορεί να θεωρηθεί κάποιος ιός

(virus), σκουλήκια (worms) και δούρειοι ίπποι (Trojan Horses)[11]. Το κακόβουλο αυτό λογισμικό χρησιμοποιείται από τους hackers για την επίτευξη κάποιου οικονομικού κέρδους, για επίδειξη δύναμης ή για την μετάδοση ενός πολιτικού μηνύματος (Wadhwa and Arora, 2017).

Spyware (Κατασκοπευτικό Λογισμικό) :

Πρόγραμμα κατασκοπείας το οποίο εισχωρεί στο υπολογιστικό σύστημα και καταγράφει κρυφά τις κινήσεις του χρήστη. Πρόσβαση σε τέτοιου είδους λογισμικά μπορεί να δοθεί με το άνοιγμα, για παράδειγμα, ενός διαδικτυακού συνδέσμου (link) το οποίο έχει αποσταλεί μέσω e-mail και κλασικό παράδειγμα τέτοιου λογισμικού νοείται το λογισμικό υποκλοπής κωδικών καρτών τραπέζης (Wadhwa and Arora, 2017).

Ransomware (Λογισμικό Λύτρων):

Το λογισμικό αυτό προσβάλλει τον υπολογιστή και μπλοκάρει την πρόσβαση στον χρήστη έως ότου πληρωθούν τα λύτρα που ζητούνται. Στην ουσία, πραγματοποιείται κρυπτογράφηση των δεδομένων, το οποίο οδηγεί στην απόρριψη της ορθής πρόσβασης. Το λογισμικό αυτό είναι ιδιαίτερα επικίνδυνο καθώς μπορεί να προσβάλλει νοσοκομεία, δημόσιες δομές, μικρές, μεσαίες και επιχειρήσεις-κολοσσούς, θέτοντας σε κίνδυνο τεράστια βάση δεδομένων, αρκετά εκ των οποίων μπορεί να συγκαταλέγονται στην κατηγορία των ευαίσθητων δεδομένων(Wadhwa and Arora, 2017).

Adware:

Κακόβουλο λογισμικό το οποίο εμφανίζει ανεπιθύμητες διαφημίσεις στους χρήστες. Μέσω διαφόρων αναδυόμενων παραθύρων ανακατευθύνει τον χρήστη σε ύποπτες ιστοσελίδες και παρακολουθεί τη δραστηριότητα περιήγησης ώστε να

[11] 'Trojan Horse: A Trojan horse program presents itself as a useful computer program, while it actually causes havoc and damage to your computer. Increasingly, Trojans are the first stage of an attack and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot. Unlike viruses and worms, Trojan horses cannot spread by themselves [7]. They are often delivered to a victim through an email message where it masquerades as an image or joke, or by a malicious website, which installs the Trojan horse on a computer through vulnerabilities in web browser. After it is installed, the Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds, such as downloading spyware, while the victim continues with their normal activities.'

εμφανίζονται στοχευμένες διαφημίσεις ή να πωληθούν δεδομένα σε τρίτους χρήστες (Wadhwa and Arora, 2017).

BotNets:

Αποτελεί ένα δίκτυο από μολυσμένους υπολογιστές ή άλλες συσκευές οι οποίες έχουν μολυνθεί με κακόβουλο λογισμικό (bot malware). Αυτές οι συσκευές, οι οποίες ονομάζονται bots ή zombies, ελέγχονται από έναν hacker ή cybercriminal, επονομαζόμενος ως botmaster ή bot herder. Οι χρήστες των μολυσμένων συσκευών δε γνωρίζουν ότι οι συσκευές τους αποτελούν μέρος του botnet και χρησιμοποιούνται για κακόβουλες ενέργειες(Wadhwa and Arora, 2017).

SQL injection:

Αποτελεί έναν τύπο κυβερνοεπίθεσης μέσω της εισαγωγής ενός κακόβουλου λογισμικού SQL στο υπολογιστικό σύστημα μιας βάσης δεδομένων. Ο σκοπός είναι, σαφώς, η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του υπολογιστή(Wadhwa and Arora, 2017).

Denial of Service (DoS or DDoS):

Μία επίθεση αυτού του χαρακτήρα έχει ως σκοπό το μπλοκάρισμα και την παύση λειτουργίας μίας συσκευής ή ενός δικτύου, με σκοπό την παρεμπόδιση της πρόσβασης από τους χρήστες. Ο τρόπος με τον οποίο οι επιτιθέμενοι το επιτυγχάνουν αυτό είναι μέσω της διαρκούς αποστολής μηνυμάτων και ειδοποιήσεων ή στέλνοντας πληροφορίες οι οποίες οδηγούν στον «κρασάρισμα» του συστήματος(Wadhwa and Arora, 2017).

Βεβαίως, οι κυβερνοεπιθέσεις δεν μπορούν να συντελεστούν μόνο μέσω της εισχώρησης κακόβουλου λογισμικού αλλά και μέσω της απόσπασης πληροφοριών και ευαίσθητων δεδομένων, με τη χρήση ηλεκτρονικών συστημάτων, όπως προαναφέρθηκε. Έτσι, με την χρήση υπολογιστή ως μέσο για την τέλεση κυβερνοεπιθέσεων μπορεί να επιτευχθεί ηλεκτρονική απάτη, phishing, pharming και η κλοπή ταυτότητας (Wadhwa and Arora, 2017).

3.2.2. Παραδείγματα Κυβερνοεπιθέσεων:

WannaCry Ransomware**:**

Τον Μάιο του 2017, μία ομάδα hackers, εκμεταλλευόμενη μία αδυναμία-ευπάθεια των Windows, επ ονόματι ‘EternalBlue’, η οποία διέρρευσε από hackers με την

ονομασία ‘Shadow Brokers’, εισέβαλε σε υπολογιστικά συστήματα με εγκατεστημένο το λογισμικό Windows, σε παγκόσμια κλίμακα, προκαλώντας μαζικό χάος και διαρροή δεδομένων. Παρόλο που η Microsoft κατόρθωσε να κυκλοφορήσει εγκαίρως μία ενημερωμένη έκδοση ασφαλείας, πολλοί χρήστες δεν την εγκατέστησαν. Η επίθεση αυτή έλαβε τεράστιες διαστάσεις καθώς κατάφερε να διακόψει τις λειτουργίες πολλών κρατικών ιδρυμάτων αλλά και επιχειρήσεων. Ως μηχανισμός αντίδρασης ανακαλύφθηκε ο «Μηχανισμός Θανάτου» από έναν ειδικό ασφαλείας, ωστόσο αρκετοί είχαν ήδη προβεί στην καταβολή των λύτρων που είχαν ζητηθεί. Η επίθεση αυτή κατάφερε να επηρεάσει πάνω από 230.000 υπολογιστές σε όλο τον κόσμο. Το κόστος της ζημίας, παγκοσμίως, υπολογίζεται ότι ανήλθε γύρω στα 4 δισεκατομμύρια δολάρια ενώ, παράλληλα, η επίθεση ανέδειξε το υπάρχον ζήτημα των απαρχαιωμένων συστημάτων (Europol, 2017).

The HSBC Bank phishing in India:

Σε αυτή την επίθεση, κυβερνοεγκληματίες δημιούργησαν ένα ψεύτικο αντίγραφο της επίσημης ιστοσελίδας της Τραπεζας HSBC, με σκοπό την εξαπάτηση των υπαλλήλων της μέσω phishing. Ο στόχος τους ήταν να τους πείσουν να εισάγουν τα στοιχεία σύνδεσης τους (όνομα και κωδικός πρόσβασης) σε αυτή την ψεύτικη σελίδα. Για να το πετύχουν έστειλαν 120 ψεύτικα emails σε υπαλλήλους της τράπεζας (Vagianos, 2024). Τα emails αυτά περιείχαν έναν ψεύτικο σύνδεσμο, ο οποίος φαινόταν αξιόπιστος και ενημέρωναν τους παραλήπτες ότι υπήρχε κίνδυνος παραβίασης των λογαριασμών τους. Το μήνυμα ισχυριζόταν ότι το τμήμα IT της Τράπεζας είχε εντοπίσει ύποπτη δραστηριότητα και πως, για λόγους ασφαλείας, κάποιες υπηρεσίες είχαν απενεργοποιηθεί προσωρινά. Για να επαναφέρουν τους λογαριασμούς τους οι εργαζόμενοι κλήθηκαν να συνδεθούν με τα τελευταία στοιχεία σύνδεσής τους στην ψεύτικη σελίδα. Μόλις το έκαναν έλαβαν μήνυμα ότι η ενεργοποίηση είχε ολοκληρωθεί με επιτυχία. Στην πραγματικότητα, με αυτόν τον χειρισμό, οι hackers απέκτησαν πρόσβαση στους λογαριασμούς τους. Ως αποτέλεσμα, το 44% των υπαλλήλων έπεσαν στην παγίδα και έδωσαν τις εμπιστευτικές πληροφορίες που ζητήθηκαν, επιτρέποντας στους hackers να

αποκτήσουν πρόσβαση στα συστήματα της τράπεζας (Vagianos, 2024). Τέτοιες επιθέσεις είναι ιδιαίτερα διαδεδομένες και συχνά βασίζονται στην εμπιστοσύνη και την άγνοια των θυμάτων, τα οποία πείθονται να αποκαλύψουν προσωπικά δεδομένα μέσω emails ή άλλων μέσων ανταλλαγής μηνυμάτων.

3.3. Συμπέρασμα

Συνοψίζοντας, το κυβερνοέγκλημα με τις πολλαπλές μορφές και εκφάνσεις του αναδεικνύεται σε μία από τις σημαντικότερες προκλήσεις της σύγχρονης ψηφιακής εποχής. Οι οικονομικές του διαστάσεις είναι ιδιαίτερα ανησυχητικές καθώς το μέσο κόστος μιας παραβίασης δεδομένων άγγιξε τα 4,35 εκατομμύρια δολάρια το 2022 (Vagianos, 2024). Η αυξανόμενη συχνότητα και πολυπλοκότητα των επιθέσεων, σε συνδυασμό με την κλιμάκωση των συνεπειών τους, καθιστούν εμφανές ότι το ζήτημα ξεπερνά τα στενά όρια της τεχνολογίας. Τα δεδομένα αυτά καταδεικνύουν όχι μόνο τη συνεχή επιδείνωση του φαινομένου αλλά και την επιτακτική ανάγκη για την ανάπτυξη αποτελεσματικών στρατηγικών πρόληψης και αντιμετώπισης, σε εθνικό, ευρωπαϊκό αλλά και σε διεθνές επίπεδο.

4. ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ.

ΘΩΡΑΚΙΣΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΕ-ΚΥΡΙΑ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ.

4.1. Πρώιμες θεσμικές ρυθμίσεις.

Οι πρώτες κανονιστικές παρεμβάσεις της Ευρωπαϊκής Ένωσης στον τομέα της ψηφιακής ασφάλειας εστιάζουν τόσο στη διασφάλιση της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες όσο και στη διαμόρφωση ενός στρατηγικού πλαισίου για την ενίσχυση της κυβερνοασφάλειας. Ενδεικτικά, σημαντικό ρόλο διαδραμάτισαν η Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ePrivacy Directive) και η πρώτη Στρατηγική της ΕΕ για την Κυβερνοασφάλεια, το 2013.

Η Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αποτέλεσε μία από τις πρώτες στοχευμένες παρεμβάσεις της ΕΕ στον τομέα της ψηφιακής ιδιωτικότητας. Ήρθε να συμπληρώσει την Οδηγία 95/46/ΕΚ (Data Protection Directive), εστιάζοντας ειδικά στις ηλεκτρονικές επικοινωνίες. Βασικός στόχος ήταν η ενίσχυση της εμπιστευτικότητας των επικοινωνιών και η προστασία των χρηστών απέναντι σε κινδύνους όπως η μη εξουσιοδοτημένη παρακολούθηση, η αποθήκευση δεδομένων κίνησης και θέσης αλλά και η αθέμιτη εμπορική χρήση των προσωπικών δεδομένων (European Commission, 2002).

Ιδιαίτερη σημασία δόθηκε στη ρύθμιση τεχνολογιών όπως τα cookies, τα οποία αποτέλεσαν κομβικό σημείο για την διαδικτυακή διαφήμιση και την παρακολούθηση χρηστών, καθώς και στην καταπολέμηση του ανεπιθύμητου ηλεκτρονικού ταχυδρομείου. Η Οδηγία τροποποιήθηκε με την 2009/136/ΕΚ, εισάγοντας την απαίτηση για «ενημερωμένη συγκατάθεση» στη χρήση cookies, ετοιμάζοντας το έδαφος για την μετέπειτα ενίσχυση του πλαισίου, με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων.[12]

[12] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο (2009). Οδηγία 2009/136/ΕΚ της 25ης Νοεμβρίου 2009 για την τροποποίηση της Οδηγίας 2002/22/ΕΚ σχετικά με την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά τα δίκτυα και τις υπηρεσίες ηλεκτρονικών επικοινωνιών, της Οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τομέα των ηλεκτρονικών επικοινωνιών και του Κανονισμού (ΕΚ) αριθ.

Η Στρατηγική της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (2013) αποτέλεσε το πρώτο ολοκληρωμένο πλαίσιο πολιτικής της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο. Στόχος της ήταν η ενίσχυση της ανθεκτικότητας των κρατών-μελών και των κρίσιμων υποδομών της Ένωσης, απέναντι σε κυβερνοαπειλές, καθώς και η προώθηση ενός ασφαλούς και αξιόπιστου περιβάλλοντος για την ψηφιακή οικονομία. Η στρατηγική επικεντρώθηκε σε τρεις βασικούς άξονες, οι οποίοι αφορούσαν την ενίσχυση της συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών-μελών και των θεσμικών οργάνων της Ένωσης, την προώθηση αποτελεσματικών πολιτικών και κανονιστικών πλαισίων για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων και την ανάπτυξη ικανοτήτων και δεξιοτήτων στον τομέα της κυβερνοασφάλειας, μέσω έρευνας και ευαισθητοποίησης των χρηστών (European Commission, 2013). Η Στρατηγική του 2013, έτσι, «χάραξε» το δρόμο για την υιοθέτηση της NIS Directive (2016/1148/ΕΕ) και στη διαμόρφωση ενιαίων κανόνων και προτύπων για την προστασία των κρίσιμων υποδομών και των ψηφιακών υπηρεσιών της ΕΕ. Παράλληλα, ενίσχυσε τη συνεργασία με τον ιδιωτικό τομέα, ενθαρρύνοντας κοινές πρακτικές διαχείρισης κινδύνων και ανταλλαγής καλών πρακτικών μεταξύ κρατών, φορέων και επιχειρήσεων.

4.2. Οδηγία NIS (1148/2016) για την Κυβερνοασφάλεια.

Από τις σημαντικότερες νομοθετικές ρυθμίσεις, οι οποίες έχουν ψηφιστεί κατά την τελευταία εικοσαετία στον τομέα της κυβερνοασφάλειας, είναι η Οδηγία 2016/1148 NIS (Network Information Systems), η οποία εκδόθηκε στις 6 Ιουλίου του 2016 και εστιάζει στην προστασία των Δικτύων και των πληροφοριακών συστημάτων

2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών για την επιβολή της προστασίας των καταναλωτών. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 337, σσ. 11–36. Ιδιαίτερα, στο Άρθρο 5(3) αναφέρεται: «Τα κράτη μέλη μεριμνούν ώστε η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία.»

(Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2016). Η εν λόγω Οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη τον Δεκέμβριο του 2018, με τον Νόμο 4577/2018. Ακολούθως, με την Υπουργική Απόφαση 1027/2019 ρυθμίστηκαν επιμέρους ζητήματα που ανέκυψαν κατά την εφαρμογή της σε εθνικό επίπεδο.

Η σπουδαιότητα της εν λόγω Οδηγίας έγκειται, ακριβώς, στο γεγονός ότι αποτέλεσε την πρώτη ολοκληρωμένη, δεσμευτική νομοθεσία καθώς, τα κράτη-μέλη είχαν την υποχρέωση να ενσωματώσουν την Οδηγία αυτή στο εθνικό τους δίκαιο (Tassis, 2024). Παράλληλα, αποτέλεσε την πρώτη οριζόντια νομοθετική πράξη (Markopoulou, Papakonstantinou and de Hert, 2019) σε επίπεδο Ευρωπαϊκής Ένωσης, η οποία καθόρισε βασικές αρχές και στόχευσε στη διαμόρφωση ενός κοινού επιπέδου κυβερνοασφάλειας σε κρίσιμους τομείς, όπως είναι η ενέργεια, οι μεταφορές, ο χρηματοπιστωτικός κλάδος και η υγειονομική περίθαλψη και, επιπρόσθετα, ο Κανονισμός (ΕΕ) 2019/881 εισήγαγε τα συστήματα πιστοποίησης στον τομέα της Κυβερνοασφάλειας (Markopoulou, Papakonstantinou and de Hert, 2019).

4.2.1. Στόχοι και προβλέψεις της Οδηγίας.

Η Οδηγία 2016/1148 στόχευε στην ενίσχυση της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων σε όλη την Ευρώπη, επηρεάζοντας κυρίως δύο κλάδους παροχής υπηρεσιών. Οι κλάδοι αυτοί διακρίνονται στους φορείς παροχής βασικών υπηρεσιών (Operators of Essential Services-OES) οι οποίοι προσφέρουν υπηρεσίες κρίσιμες για τη διατήρηση βασικών κοινωνικών και οικονομικών δραστηριοτήτων, των οποίων η λειτουργία εξαρτάται από πληροφοριακά συστήματα και τους παρόχους ψηφιακών υπηρεσιών (Schmitz-Berndt and Anheier, 2020).Παραδείγματα παρόχων βασικών υπηρεσιών αποτελούν η ενέργεια, οι μεταφορές, η υγεία, η ύδρευση κλπ.. Επέβαλε στα κράτη-μέλη την υποχρέωση καθορισμού, ανά τομέα και υποτομέα, των οντοτήτων που εμπίπτουν στην έννοια του φορέα βασικής υπηρεσίας, με βάση τρία σωρευτικά κριτήρια: α. η παρεχόμενη υπηρεσία να είναι ουσιώδης για τη συνέχιση κρίσιμων κοινωνικών ή/και οικονομικών δραστηριοτήτων, β. η παροχή της να εξαρτάται από τη διαθεσιμότητα και την αξιοπιστία συστημάτων δικτύου και πληροφοριών και γ. ένα ενδεχόμενο συμβάν να μπορεί να προκαλέσει σημαντική διαταραχή στη λειτουργία της

υπηρεσίας (European Commission, 2016).[13] Αργότερα, με την αντικατάσταση της Οδηγίας από τη NIS 2, επέρχονται και τροποποιήσεις αφορώσες την κατηγοριοποίησης των κλάδων παροχής υπηρεσιών. Στην ελληνική έννομη τάξη, ο ορισμός των εν λόγω φορέων πραγματοποιήθηκε με την υπ'αριθμόν 1027/08.10.2019 απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης.

Επιπλέον, ιδρύθηκε ένα Δίκτυο Ομάδων Απόκρισης σε Συμβάντα Ασφαλείας Πληροφοριακών Συστημάτων (CSIRT)[14],το οποίο ενίσχυσε τη διακρατική επιχειρησιακή συνεργασία και προωθούσε την έγκαιρη και αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπίθεσης. Το Δίκτυο αυτό διατηρήθηκε και ενισχύθηκε και με την υιοθέτηση της NIS2. Η Οδηγία έθετε, επιπρόσθετα, σαφείς υποχρεώσεις ασφάλειας και γνωστοποίησης, τόσο για τους φορείς εκμετάλλευσης βασικών υπηρεσιών όσο και για τους παρόχους ψηφιακών υπηρεσιών, οι οποίοι δραστηριοποιούνται στην επιγραμμική αγορά, με σκοπό την πρόληψη και την αντιμετώπιση απειλών στον κυβερνοχώρο.

4.2.2. Συμμόρφωση και Κυρώσεις.

Ο ευρωπαίος νομοθέτης απέδιδε, όπως ειπώθηκε παραπάνω, δεσμευτικό χαρακτήρα στην απαίτηση συμμόρφωσης, προβλέποντας σαφές πλαίσιο εποπτείας και επιβολής. Στην περίπτωση των φορέων εκμετάλλευσης βασικών υπηρεσιών, τα κράτη-μέλη υποχρεούνταν να εξοπλίσουν τις αρμόδιες αρχές με τις αναγκαίες εξουσίες ελέγχου και τις κατάλληλες απαιτήσεις πληροφόρησης, για την τεκμηρίωση της εφαρμογής πολιτικών ασφαλείας.[15] Επιπρόσθετα, προβλεπόταν η δυνατότητα έκδοσης δεσμευτικών οδηγιών, για την αποκατάσταση διαπιστωμένων

[13] European Union (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, pp. 1–30 (Αιτιολογική Σκέψη υπ'αριθμ. 20).

[14] European Union (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, pp. 1–30 (Άρθρο 9).

[15] European Union (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, pp. 1–30 (Άρθρο 15§1 και 2).

ελλείψεων.[16] Στην Ελλάδα, η αρμοδιότητα αυτή ανατέθηκε στην Εθνική Αρχή Κυβερνοασφάλειας, σύμφωνα με το άρθρο 10 παρ.2 του Νόμου 4577/2018.

Αναφορικά με τους παρόχους ψηφιακών υπηρεσιών, η εποπτική παρέμβαση προβλεπόταν σε μεταγενέστερο στάδιο και υπό την προϋπόθεση τεκμηριωμένης μη συμμόρφωσης.[17] Ωστόσο, ακόμη και στην περίπτωση αυτή, η αρμόδια αρχή διέθετε την εξουσία απαίτησης πληροφόρησης και επιβολής των κατάλληλων μέτρων συμμόρφωσης. Ο νόμος 4577/2018 ορίζει ότι, η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς αρμόδιους φορείς, είναι υπεύθυνη για την αξιολόγηση της επάρκειας των μέτρων τα οποία λαμβάνονται για την πρόληψη και την αντιμετώπιση των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων.[18] Στο εσωτερικό ελληνικό δίκαιο, οι επιταγές της εν λόγω Οδηγίας ενσωματώθηκαν με τον Νόμο 4377/2018, ο οποίος εισήγαγε διοικητικά πρόστιμα, ως μορφή κύρωσης (European Commission, 2016). Συγκεκριμένα, σύμφωνα με το άρθρο 15 του εν λόγω νόμου, ο Υπουργός Ψηφιακής Διακυβέρνησης, κατόπιν εισήγησης της Εθνικής Αρχής της Κυβερνοασφάλειας, δύνατο να επιβάλλει κυρώσεις σε φυσικά ή νομικά πρόσωπα. Οι κυρώσεις αυτές αφορούσαν:

- σε περιπτώσεις μη έγκαιρης ή μη επαρκούς γνωστοποίησης περιστατικών που είχαν σημαντική επίπτωση στη συνέχιση παροχής βασικών υπηρεσιών, προβλεπόταν η επιβολή προστίμου έως δεκαπέντε χιλιάδες (15.000) ευρώ. Σε περιπτώσεις υποτροπής, το ανώτατο όριο του προστίμου ανερχόταν στις διακόσιες χιλιάδες (200.000) ευρώ.
- σε περιπτώσεις παράλειψης λήψης κατάλληλων και αναλογικών τεχνικών ή οργανωτικών προληπτικών μέτρων για την ασφάλεια των δικτύων και

[16] European Union (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, pp. 1–30 (Άρθρο 15§3).

[17] European Union (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, pp. 1–30 (Άρθρο 17§1 και 2).

[18] European Union (2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, pp. 1–30 (Άρθρο 11§1).

των συστημάτων πληροφοριών, το ανώτατο διοικητικό πρόστιμο οριζόταν σε πενήντα χιλιάδες (50.000) ευρώ, με ταυτόχρονη έκδοση σύστασης συμμόρφωσης και προειδοποίηση για επιβολή βαρύτερων κυρώσεων· ενώ, σε περίπτωση υποτροπής, μπορούσε να επιβληθεί πρόστιμο έως διακόσιες χιλιάδες (200.000) ευρώ.

- στην περίπτωση μη παροχής πληροφοριών που ζητούνταν κατά τη διάρκεια ελέγχου ή διερεύνησης περιστατικού κυβερνοασφάλειας ή καθυστέρησης στην παροχή τους χωρίς επαρκή αιτιολόγηση, δύνατο να επιβληθεί πρόστιμο έως πενήντα χιλιάδες (50.000) ευρώ, ενώ για επαναλαμβανόμενη παραβίαση το ύψος του προστίμου δύνατο να φτάσει τις διακόσιες χιλιάδες (200.000) ευρώ.

Όπως θα αναλυθεί και σε επόμενο κεφάλαιο, η NIS 2 θα εισάγει ένα αυστηρότερο κανονιστικό πλαίσιο, με σαφώς υψηλότερα πρόστιμα, επιδιώκοντας την ενίσχυση της αποτελεσματικότητας της εποπτείας και την εξασφάλιση της υιοθέτησης ουσιαστικών μέτρων κυβερνοασφάλειας, μειώνοντας τη ανομοιομορφία που δημιουργούσε η NIS. Επιπλέον, η νέα Οδηγία ενισχύει τη διαφάνεια και την αναλογικότητα στην επιβολή κυρώσεων, ενώ προβλέπει και τη δυνατότητα συνδυασμού διοικητικών προστίμων με άλλα μέτρα συμμόρφωσης, ώστε να επιτυγχάνεται πλήρης συμμόρφωση με τις υποχρεώσεις των οργανισμών.

4.2.3. Συμπέρασμα

Η Οδηγία NIS συνιστά την πρώτη ουσιαστική θεσμική απάντηση της Ευρωπαϊκής Ένωσης σε ένα διαρκώς επιδεινούμενο πρόβλημα όπως είναι αυτό της κυβερνοασφάλειας. Παρόλο η Οδηγία επέτρεπε ευελιξία και χρόνο προσαρμογής στα κράτη-μέλη, γεγονός το οποίο θα μπορούσε να θεωρηθεί μειονέκτημα υπό το πρίσμα της ανάγκης για άμεση και εναρμονισμένη δράση, προσέφερε, τελικά, μία ισορροπημένη και ρεαλιστική προσέγγιση. Το πλαίσιο της Οδηγίας προέβλεπε τη δημιουργία αρμοδίων αρχών, σε εθνικό επίπεδο, καθώς και μηχανισμούς διασυνοριακής συνεργασίας. Στο πλαίσιο της ενσωμάτωσης της Οδηγίας NIS στις εθνικές νομοθεσίες των κρατών-μελών, η Ευρωπαϊκή Ένωση παρείχε χρηματοδότηση ύψους τριάντα οχτώ εκατομμυρίων ευρώ, μέσω του Προγράμματος «Συνδέοντας την Ευρώπη», έως και το 2020 (European Commission, 2018). Η χρηματοδότηση αυτή είχε ως στόχο την ενίσχυση των εθνικών ομάδων αντιμετώπισης περιστατικών ασφάλειας περιφερειακών συστημάτων (CSIRTs),

καθώς και άλλων συναφών φορέων. Σκοπός ήταν να εξοπλιστούν τα κράτη με τις κατάλληλες υποδομές, εργαλεία και μηχανισμούς, προκειμένου να μπορούν να ανταποκρίνονται αποτελεσματικά στις αυξανόμενες απειλές στον κυβερνοχώρο. Επιπρόσθετα, αντανακλά και την ανάγκη για σεβασμό στις διαφοροποιήσεις των κρατών-μελών σε επίπεδο τεχνολογικής ωριμότητας και οικονομικών δυνατοτήτων. Τέλος, η Οδηγία θα πρέπει να γίνει αντιληπτή ως η απαρχή της ευρωπαϊκής στρατηγικής για την κυβερνοασφάλεια, ακολουθώντας τη Στρατηγική του 2013. Αντιπροσωπεύει την ευρωπαϊκή απάντηση σε παγκόσμιες εξελίξεις, ενώ, αναδεικνύει κρίσιμα ζητήματα τα οποία επηρεάζουν κάθε απόπειρα διαμόρφωσης συνολικής στρατηγικής ασφάλειας στον κυβερνοχώρο.

4.3. CYBERSECURITY ACT (ΕΕ 2019/881)

4.3.1. Υιοθέτηση και γενικοί ορισμοί.

Ο Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, γνωστός και ως Cybersecurity Act, αποτελεί μια από τις σημαντικότερες νομοθετικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας. Υιοθετήθηκε στις 17 Απριλίου 2019 και τέθηκε σε ισχύ 27 Ιουνίου του ίδιου έτους, με σκοπό να ενισχύσει την κυβερνοανθεκτικότητα των κρατών-μελών, να ενδυναμώσει τον ρόλο του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια (ENISA) και να καθιερώσει για πρώτη φορά ένα ενιαίο ευρωπαϊκό πλαίσιο πιστοποίησης προϊόντων, υπηρεσιών και διεργασιών στον τομέα της κυβερνοασφάλειας. Ο Κανονισμός είναι δεσμευτικός στο σύνολό του και άμεσα εφαρμόσιμος στα κράτη-μέλη, γεγονός που ενισχύει τη νομική του βαρύτητα.[19] Με τον Κανονισμό, η Ένωση υιοθετεί μια περισσότερο συντονισμένη και συνεκτική προσέγγιση απέναντι στις αυξανόμενες κυβερνοαπειλές, θέτοντας νομικές βάσεις για την εδραίωση εμπιστοσύνης στον ψηφιακό κόσμο.

[19] (*European Union, 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, pp.15–69,* άρθρο 69 «…Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος…..»)

Στον Κανονισμό 2019/881, ο όρος «Κυβερνοασφάλεια»[20] ορίζεται ως οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων. Αντίστοιχα, ως «κυβερνοαπειλή»[21] προσδιορίζεται κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλο τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα. Οι ορισμοί αυτοί αποτελούν θεμέλιο για την κατανόηση του νέου ευρωπαϊκού πλαισίου κυβερνοασφάλειας και επανεμφανίζονται ενισχυμένοι και στην Οδηγία NIS2.

4.3.2. Νομοθετική διαδικασία και Διαβουλεύσεις.

Η διαμόρφωση του Cybersecurity Act υπήρξε αποτέλεσμα εντατικής νομοθετικής διαδικασίας στο Ευρωπαϊκό Κοινοβούλιο και άλλους θεσμούς της ΕΕ, με σημαντική συμμετοχή διαφόρων επιτροπών. Η Επιτροπή Έρευνας και Ενέργειας (ITRE) ανέλαβε την κύρια ευθύνη του φακέλου. Η Επιτροπή Εσωτερικής Αγοράς και Προστασίας Καταναλωτών (IMCO), ως συνδεδεμένη Επιτροπή, σύμφωνα με τον Κανονισμό 54 των Κανόνων Διαδικασίας του Κοινοβουλίου, καθώς και οι Επιτροπές Προϋπολογισμών (BUDG), Εξωτερικών Υποθέσεων (AFET) και Ελευθεριών κλήθηκαν για απόψεις. Ωστόσο, η επιτροπή AFET αποφάσισε να μη δώσει γνώμη για την πρόταση (European Parliament, 2018).

Η διαδικασία ξεκίνησε με την παρουσίαση της πρότασης και της εκτίμησης αντικτύπου από την Ευρωπαϊκή Επιτροπή, στις 12 Οκτωβρίου του 2017 στην

[20] (*European Union, 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, pp.15–69,* άρθρο 2 (…«κυβερνοασφάλεια»: οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων…)

[21] (*European Union, 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, pp.15–69,* άρθρο 2 («κυβερνοαπειλή»: κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα,…)

Επιτροπή IMCO και στις 22 Ιανουαρίου του 2018 στην Επιτροπή ITRE, η οποία είχε ήδη πραγματοποιήσει δημόσια ακρόαση για το θέμα, τον Νοέμβριο του 2017. Οι Επιτροπές εξέδωσαν τις απόψεις τους στις 16 Μαρτίου και 23 Απριλίου 2018, αντίστοιχα. Η IMCO εξέδωσε την απόφασή της στις 22 Μαΐου του 2018, υπογραμμίζοντας τη σημασία ενίσχυσης των αρμοδιοτήτων του ENISA και της συμμετοχής των ενδιαφερομένων μερών. Η έκθεση της ITRE, η οποία εγκρίθηκε στις 10 Ιουλίου του 2018 με 56 ψήφους υπέρ, 5 κατά και 1 αποχή, υποστήριξε τη δημιουργία ενός πλαισίου πιστοποίησης Κυβερνοασφάλειας και τη νέα εντολή για την ENISA (European Parliament, 2018). Η έκθεση πρότεινε τη διεύρυνση του ρόλου του ENISA στον τομέα της εκπαίδευσης στον κυβερνοχώρο και την ενίσχυση της συνεργασίας μεταξύ των κρατών-μελών, για την ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια. Αναγνώρισε τη σημασία της ανάπτυξης πιστοποιήσεων για τη Συνδεσιμότητα Διαδικτύου (IoT), δεδομένων των αυξανόμενων απειλών από τις συνδεδεμένες συσκευές. Η απόφαση για τη διαδικασία διαπραγμάτευσης με το Συμβούλιο και την Επιτροπή ήταν θετική και επιβεβαιώθηκε από την Ολομέλεια του Κοινοβουλίου τον Σεπτέμβριο του 2018. Οι διαπραγματεύσεις συνεχίστηκαν με τη Συμφωνία του Συμβουλίου στις 25 Μαΐου του 2018 και της θέσης σε ισχύ του, στις 8 Ιουνίου του 2018. Τον Σεπτέμβριο του 2018, η συμφωνία μεταξύ των θεσμών επιτεύχθηκε και εγκρίθηκε από την Επιτροπή ITRE τον Ιανουάριο του 2019 (European Parliament, 2018).

4.3.3. Αναθεώρηση του ρόλου του ENISA και πιστοποιήσεις ασφαλείας.

Στο πλαίσιο, λοιπόν ενίσχυσης της κυβερνοανθεκτικότητας προτάθηκε και η αναβάθμιση του ρόλου του οργανισμού ENISA. Πρωτίστως, αναλαμβάνει έναν ηγετικό ρόλο στην ανάπτυξη ευρωπαϊκών σχημάτων πιστοποίησης στον τομέα της κυβερνοασφάλειας (Άρθρο 4{6} και 8), σε συνεργασία με τις εθνικές αρχές ενώ, στηρίζει και τις προσπάθειες ως προς την ανάπτυξη κοινών ευρωπαϊκών πλαισίων και τεχνικών προτύπων (standardization), στον τομέα των τεχνολογιών πληροφορικής και επικοινωνιών. Παράλληλα, παρέχει συστηματική υποστήριξη στην Ευρωπαϊκή Επιτροπή και τα κράτη-μέλη, όσον αφορά τον σχεδιασμό και την εφαρμογή πολιτικών στον τομέα της κυβερνοασφάλειας, ειδικά σε κρίσιμους τομείς

υποδομών, όπως αυτή ορίζονται στην οδηγία NIS. (Άρθρο 4{2}, 5 και 9) Επιπρόσθετα, ο ENISA ενισχύει τις εθνικές ικανότητες μέσω παροχής τεχνογνωσίας ενώ, δρα ως κόμβος πληροφόρησης για την Ευρωπαϊκή Ένωση, στον συγκεκριμένο κλάδο. (Άρθρο 4{1} και 6). Τέλος, διαδραματίζει κομβικό ρόλο ως προς τη διαχείριση των ομάδων CSIRTs, σε ευρωπαϊκό επίπεδο, και στη συντονισμένη απόκριση σε κυβερνοεπιθέσεις μεγάλης κλίμακας. (Άρθρο 6 και 7).

Ένα κρίσιμο ζήτημα, το οποίο ανακύπτει για τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ), όπως προβλέπεται στο νομικό πλαίσιο της Οδηγίας NIS, αφορά την ανάγκη πιστοποίησης και διαπίστευσης των αρμόδιων φορέων, ως προς τη συμμόρφωσή τους με τις απαιτήσεις της εφαρμοστέας νομοθεσίας για την ασφάλεια των δικτύων και συστημάτων πληροφορικής (Tassis, 2024). Στο πλαίσιο αυτό, ο ως άνω Κανονισμός καθιερώνει ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας, το οποίο προβλέπει τη θέσπιση κοινών ευρωπαϊκών συστημάτων αξιολόγησης της συμμόρφωσης προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ, με συγκεκριμένες απαιτήσεις ασφάλειας (European Parliament, 2018). Σκοπός του συστήματος είναι να διασφαλίσει τη διαθεσιμότητα, ακεραιότητα καθώς και την εμπιστευτικότητα των δεδομένων, καθόλη τη διάρκεια της ύπαρξής τους. (Άρθρο 46 {2}). Το πεδίο εφαρμογής του πλαισίου καλύπτει τρεις κατηγορίες: τα προϊόντα (υλικό και λογισμικό), τις υπηρεσίες και τις διαδικασίες. Το πλαίσιο εισάγει ένα μηχανισμό για την ανάπτυξη, την έγκριση και την εφαρμογή ευρωπαϊκών συστημάτων πιστοποίησης, τα οποία αξιολογούν τη συμμόρφωση των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών σε συγκεκριμένες απαιτήσεις, κατά τη διάρκεια του πλήρους κύκλου ζωής τους (European Parliament, 2018).

Η νομοθεσία ορίζει σαφώς τους στόχους ασφαλείας οι οποίοι θα πρέπει να επιτυγχάνονται (Άρθρο 51) τα επίπεδα διασφάλισης (Άρθρο 52) και το ελάχιστο περιεχόμενο των συστημάτων πιστοποίησης (Άρθρο 54). Επιπρόσθετα, προβλέπεται η σταδιακή ανάπτυξη των συστημάτων μέσα από τέσσερις φάσεις: από τη διαμόρφωση του «Κυλιόμενου προγράμματος εργασίας» μέχρι την εφαρμογή σε εθνικό επίπεδο (Μήτρου Λ., 2021). Η πιστοποίηση ενώ είναι κατά βάση εθελοντική (Άρθρο 56), δύναται να καθίσταται υποχρεωτική όπου ορίζεται από την ένωσή την εθνική νομοθεσία. Αξιοσημείωτη είναι η δυνατότητα

«αυτο-αξιολόγησης της συμμόρφωσης» (Άρθρο 53), για προϊόντα χαμηλού κινδύνου, επιπέδου «βασικού» ασφαλείας, υπό την αποκλειστική ευθύνη των κατασκευαστών ή παρόχων, με την προϋπόθεση σαφούς ενημέρωσης και διαφάνειας προς τους τελικούς χρήστες. Στις 31 Ιανουαρίου 2024, η Ευρωπαϊκή Επιτροπή εξέδωσε εκτελεστικό κανονισμό για το σύστημα πιστοποίησης κυβερνοασφάλειας της ΕΕ, βάση κοινών κριτηρίων (EUCC). Το σύστημα αυτό αποτελεί το πρώτο εγκεκριμένο σε επίπεδο ΕΕ και ευθυγραμμίζεται πλήρως με το σχέδιο το οποίο εκπόνησε ο ENISA, με τη συνδρομή ειδικής ομάδας εργασίας. Το EUCC, αν και εθελοντικό, αναμένεται να αποτελέσει το πρότυπο για τα επόμενα συστήματα που θα θεσπιστούν. Η εφαρμογή του EUCC εντάσσεται στο γενικότερο ευρωπαϊκό πλαίσιο πιστοποίησης που επιδιώκει την ενίσχυση της Κυβερνοασφάλειας, μέσω ενός συνεκτικού συνόλου κανόνων, τεχνικών απαιτήσεων και διαδικασιών, αναγνωρισμένων σε ολόκληρη την ΕΕ. Παρότι προαιρετικό, επιτρέπει στους παρόχους προϊόντων ΤΠΕ να επιλέξουν μια κοινώς αποδεκτή ευρωπαϊκή διαδικασία αξιολόγησης και πιστοποίησης. Κατά την περίοδο μετάβασης εξακολουθούν να ισχύουν τα εθνικά συστήματα πιστοποίησης, ωστόσο οι φορείς μπορούν να διαπιστευθούν σύμφωνα με το νέο σύστημα. Ο ENISA είναι υπεύθυνος για τη δημοσίευση των σχετικών πιστοποιητικών καθώς και των υποστηρικτικών υλικών, στον ειδικό ιστότοπό του (Khurshid et al., 2022). Επιπρόσθετα, κάθε σύστημα πιστοποίησης θα πρέπει να διαμορφώνεται με τρόπο που να επιτυγχάνει τουλάχιστον τους βασικούς στόχους ασφάλειας, όπως είναι η προστασία των δεδομένων από μη εξουσιοδοτημένη, η αποφυγή αλλοίωσης ή απώλειας των δεδομένων, η πρόσβαση σε αυτά μόνο από εξουσιοδοτημένα άτομα ή συστήματα, η καταγραφή και ιχνηλάτηση ενεργειών, η τεκμηρίωση γνωστών τρωτών σημείων καθώς και η εξασφάλιση ότι τα προϊόντα ΤΠΕ παρέχονται χωρίς γνωστές ευπάθειες και με δυνατότητα ασφαλούς αναβάθμισης (Khurshid et al., 2022). Η προσέγγιση αυτή αναδεικνύει ότι, τα κριτήρια ένταξης των οργανισμών στους ΦΕΒΥ εντάσσονται σε ένα ευρύτερο πλαίσιο διασφάλισης της ανθεκτικότητας των κρίσιμων υποδομών. Η πιστοποίηση, υπό αυτή την έννοια, αποτελεί ουσιαστικό παράγοντα για την επίτευξη των επιδιωκόμενων επιπέδων ασφαλείας.

Ο ρόλος του ENISA ως προς την κατοχύρωση των πιστοποιήσεων ασφαλείας είναι κεντρικός (Άρθρο 49 και 50) καθώς, αναλαμβάνει τη συλλογή απαιτήσεων, τον συντονισμό των ενδιαφερομένων, τη διαμόρφωση των υποψηφίων σχημάτων πιστοποίησης και τη συνεργασία με την Ευρωπαϊκή Επιτροπή και τους λοιπούς φορείς. Σε εθνικό επίπεδο(Άρθρο 57 και 58), τα κράτη μέλη ορίζουν εθνικές αρχές πιστοποίησης με αρμοδιότητα την εποπτεία της εφαρμογής και τη συμμόρφωση με τους κανόνες του πλαισίου, ιδιαίτερα σε περιπτώσεις αυτοαξιολόγησης. Τέλος, το πλαίσιο διασφαλίζει τη συμβατότητα με το ενωσιακό δίκαιο, όπως επισημαίνεται στην αιτιολογική σκέψη υπ'αριθμόν 74[22], στην οποία διευκρινίζεται ότι δε θίγονται υφιστάμενοι κανόνες πιστοποίησης, όπως αυτοί του Γενικού Κανονισμού Προστασίας των Προσωπικών Δεδομένων. Η πιστοποίηση δεδομένων εντός του ΓΚΠΔ αποσκοπεί στη δημιουργία μηχανισμών οι οποίοι επιτρέπουν την αποτελεσματική αξιολόγηση και επικοινωνία των επιπέδων προστασίας προσωπικών δεδομένων από τα προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ, ενισχύοντας την εμπιστοσύνη των υποκειμένων των δεδομένων (Khurshid et al., 2022).

4.3.4. Συμπέρασμα

Η Συμφωνία-Πράξη η οποία επιτεύχθηκε συνετέλεσε στη δημιουργία ενός εναρμονισμένου ευρωπαϊκού πλαισίου πιστοποίησης κυβερνοασφάλειας και ενίσχυσε ενεργά τον ρόλο και τις αρμοδιότητες του ENISA. Μέσω της εισαγωγής κοινών προτύπων αξιολόγησης και ασφάλειας, η Πράξη προάγει την εναρμόνιση

[22] (*European Union, 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, pp.15–69, αιτιολογική σκέψη 74:* «Οι διατάξεις του παρόντος κανονισμού δεν θα πρέπει να θίγουν το ενωσιακό δίκαιο που προβλέπει συγκεκριμένους κανόνες για την πιστοποίηση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Πιο συγκεκριμένα, ο κανονισμός (ΕΕ) 2016/679 περιλαμβάνει διατάξεις για τη θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων, προκειμένου να αποδεικνύεται η συμμόρφωση με τον εν λόγω κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Αυτοί οι μηχανισμοί πιστοποίησης και οι σφραγίδες και τα σήματα προστασίας των δεδομένων θα πρέπει να επιτρέπουν στα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Ο παρών κανονισμός ισχύει με την επιφύλαξη της πιστοποίησης των πράξεων επεξεργασίας των δεδομένων δυνάμει του κανονισμού (ΕΕ) 2016/679, μεταξύ άλλων όταν τέτοιες πράξεις βρίσκονται ενσωματωμένες σε προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ.»

των εθνικών συστημάτων, διευκολύνοντας την αμοιβαία αναγνώριση πιστοποιήσεων και ενισχύοντας την ασφάλεια της ψηφιακής αγοράς, σε ενωσιακό επίπεδο. Επιπρόσθετα, η ευελιξία του θεσμικού πλαισίου εξασφαλίζει την προσαρμοστικότητα του θεσμού στις, διαρκώς εξελισσόμενες, τεχνολογικές και επιχειρησιακές συνθήκες. Η Πράξη προάγει, επίσης τη συνεργασία μεταξύ των ευρωπαϊκών και εθνικών φορέων, ενισχύοντας την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας και συμβάλλοντας στη διασφάλιση της εμπιστοσύνης των χρηστών. Συνολικά, θα λέγαμε πως ενσωματώνει καινοτόμες προσεγγίσεις, προωθώντας ένα περιβάλλον ψηφιακής εμπιστοσύνης και ανθεκτικότητας, θεμελιώδη για την επίτευξη των ευρύτερων στρατηγικών στόχων της Ευρωπαϊκής Ένωσης, στον ψηφιακό μετασχηματισμό.

4.4. Οδηγία NIS 2 (ΕΕ 2022/2555).

Η Οδηγία NIS κατόρθωσε να επιβάλλει ένα κοινό επίπεδο Κυβερνοασφάλειας, σε επιχειρήσεις απαραίτητων υπηρεσιών και σε επιχειρήσεις ψηφιακών υπηρεσιών στην Ευρωπαϊκή Ένωση. Ωστόσο, όπως αργότερα διαπιστώθηκε, η μεταφορά και ενσωμάτωση της Οδηγίας στην Ευρωπαϊκή Ένωση αποδείχθηκε αρκετά αποκλίνουσα ανάμεσα στα Κράτη-μέλη. Το γεγονός αυτό είχε ως αποτέλεσμα ένα άνισο πεδίο ανταγωνισμού και ανεπαρκή ετοιμότητα των κρατών-μελών απέναντι σε νέες και εξελισσόμενες προκλήσεις στον κυβερνοχώρο.

Τα ως άνω επέφεραν την κατάργηση της εν λόγω Οδηγίας, από τις 18 Οκτωβρίου του 2024 και την αντικατάστασή της με μία νέα Οδηγία, η οποία αποκαλείται NIS2 Directive (EU) 2022/2555. Η Οδηγία NIS2 βασίζεται στη NIS, ωστόσο, επεκτείνει το πεδίο εφαρμογής της ώστε να καλύπτει περισσότερους τομείς και οργανισμούς. Για την υιοθέτησή της η Ευρωπαϊκή Ένωση ακολούθησε την τυπική διαδικασία. Αρχικά, η πρόταση πέρασε για εξέταση από την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας του Ευρωπαϊκού Κοινοβουλίου[23]. Στη συνέχεια, το Συμβούλιο της Ευρωπαϊκής Ένωσης διαμόρφωσε τη θέση του στις 3 Δεκεμβρίου του 2021. Μετά από διαπραγματεύσεις οι δύο θεσμοί κατέληξαν σε

[23] Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας (Ευρωπαϊκό Κοινοβούλιο), 2024

προσωρινή συμφωνία, στις 13 Μαΐου του 2022, η οποία και επικυρώθηκε από το Κοινοβούλιο και το Συμβούλιο τον Νοέμβριο του 2022. Η Οδηγία τέθηκε και επισήμως σε ισχύ τον Ιανουάριο του 2023 με παράλληλη υποχρέωση των κρατών-μελών για ενσωμάτωση στο εθνικό δίκαιο εντός της προθεσμίας των 21 μηνών, δηλαδή έως της 17 Οκτωβρίου του 2024.

Να σημειωθεί πως αμφότερες οι Οδηγίες βασίζονται στο Άρθρο 114 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), η οποία αποτελεί και τη νομική βάση για την εναρμόνιση των νομοθεσιών των κρατών-μελών, με στόχο την εγκαθίδρυση και τη λειτουργία της εσωτερικής αγοράς. Η νέα πρόταση ενισχύει τις απαιτήσεις ασφαλείας, καλύπτει κινδύνους στην εφοδιαστική αλυσίδα, απλοποιεί τις υποχρεώσεις αναφοράς και εισάγει αυστηρότερη εποπτεία και επιβολή, συμπεριλαμβανομένων αυστηρότερων εναρμονισμένων κυρώσεων σε όλη την Ευρωπαϊκή Ένωση.

Η αναθεωρημένη Οδηγία, λοιπόν, εισάγει σημαντικές μεταρρυθμίσεις, διευρύνοντας το φάσμα των υπόχρεων φορέων και επαναπροσδιορίζοντας τον τρόπο κατηγοριοποίησής τους. Ειδικότερα, προτείνεται η αντικατάσταση των «φορέων βασικών υπηρεσιών» (Operations of Essential Services-OESs) και των «παρόχων ψηφιακών υπηρεσιών» (Digital Service Providers-DSPs), όπως αυτοί προβλέπονταν στην πρότερη Οδηγία NIS, με δύο νέες κατηγορίες, τους βασικούς-ουσιώδεις φορείς (Ees) και τους σημαντικούς φορείς (IEs) (Άρθρο 3).[24] Κατ'αυτόν τον τρόπο, η NIS2 επεκτείνει σημαντικά το πεδίο εφαρμογής της προηγούμενης Οδηγίας, καλύπτοντας πλέον ένα ευρύτερο φάσμα κρίσιμων τομέων όπως είναι η υγειονομική περίθαλψη, η παραγωγή εμβολίων, τα ερευνητικά κέντρα, η βιομηχανία ιατρικών συσκευών καθώς και η διαστημική υποδομή (European Commission, 2020). Ταυτόχρονα, στο πεδίο εντάσσονται και φορείς ψηφιακής υποδομής, όπως είναι οι (δημόσιοι) πάροχοι υπηρεσιών cloud, τα δίκτυα παράδοσης περιεχομένου, οι φορείς εμπιστοσύνης και τα δημόσια δίκτυα

[24] European Union. (2022) *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, Άρθρο 3 «Για τους σκοπούς της παρούσας οδηγίας, οντότητες του τύπου που αναφέρεται στα Παραρτήματα I ή II, οι οποίες δεν πληρούν τα κριτήρια για να χαρακτηριστούν ως ουσιώδεις οντότητες σύμφωνα με την παράγραφο 1 του παρόντος άρθρου, θεωρούνται σημαντικές οντότητες.» Official Journal of the European Union, L333, pp. 80–152.

ηλεκτρονικών επικοινωνιών (European Commission, 2020). Η διεύρυνση του πεδίου εφαρμογής της οδηγίας, ώστε να καλύπτει σχεδόν τον διπλάσιο αριθμό τομέων συνεπάγεται ότι ένας πολύ μεγάλος αριθμός οργανισμών θα υπάγεται πλέον στις διατάξεις της. Υπολογίζεται ότι, περισσότεροι από 160.000 φορείς σε ολόκληρη την Ευρωπαϊκή Ένωση θα επηρεαστούν από το νέο κανονιστικό πλαίσιο (Vandezande, 2023). Παρά το γεγονός ότι αυτή η αύξηση της εμβέλειας μπορεί να θεωρηθεί ιδιαίτερα εκτεταμένη, η συνεχώς εντεινόμενη απειλή του κυβερνοεγκλήματος και των κυβερνοεπιθέσεων καθιστά αδικαιολόγητο τον περιορισμό ενός τόσο θεμελιώδους πλαισίου, σε περιορισμένους μόνο τομείς. Υπό αυτό το πρίσμα, η διεύρυνση την οποία εισάγει η NIS2 συνιστά ένα απολύτως αναμενόμενο και ορθολογικό εξελικτικό στάδιο, το οποίο ενδέχεται να αποτελέσει προάγγελο για την περαιτέρω γενίκευση του πλαισίου με σκοπό την εφαρμογή του σε όλους τους οργανισμούς (Vandezande, 2023).

Η διαφοροποίηση μεταξύ ουσιωδών και σημαντικών φορέων προορίζεται να αντικατοπτρίζει το επίπεδο κινδύνου και τον βαθμό κρισιμότητας κάθε οντότητας. Οι ουσιώδεις φορείς υπόκεινται σε προληπτική εποπτεία (ex ante), ενώ οι σημαντικοί σε εκ των υστέρων (ex post) εποπτεία (Άρθρο 31). Επιπρόσθετα, η οργάνωση επισημαίνει την ανάγκη για σαφείς και περιοριστικές οριοθετήσεις των υπόχρεων φορέων, με στόχο την αποφυγή επικαλύψεων και την αποτροπή πολλαπλών χαρακτηρισμών, για την ίδια επιχείρηση (Vandezande, 2023). Προτείνεται επίσης, όταν οι εσωτερικές λειτουργίες των επιχειρήσεων δεν προσφέρονται ως υπηρεσίες προς τρίτους, να εξαιρούνται ρητώς από το πεδίο εφαρμογής της Οδηγίας. Περιλαμβάνει, δηλαδή, όλες τις μεσαίες και μεγάλες επιχειρήσεις καθώς και μικρότερες, εφόσον κρίνονται κρίσιμες για την κοινωνία ή την οικονομία, μέσω των υπηρεσιών ή προϊόντων που αυτές παρέχουν. Ενσωματώνει, επίσης ρυθμίσεις για την ασφάλεια στην εφοδιαστική αλυσίδα, υποχρεώσεις διακυβέρνησης κινδύνου και ενισχυμένες διαδικασίες αναφοράς περιστατικών, εντός αυστηρών χρονοδιαγραμμάτων.

4.4.1. Υποχρεώσεις των κρατών-μελών.

Η Οδηγία NIS2 διευρύνει το θεσμικό πλαίσιο των εθνικών στρατηγικών κυβερνοασφάλειας, μεταβαίνοντας από τον περιορισμένο στόχο της προστασίας των δικτύων και των συστημάτων πληροφορίας σε μια πιο συνολική προσέγγιση. Σε αντίθεση με την προηγούμενη Οδηγία, η οποία εστίαζε κυρίως στην τεχνική διάσταση της ασφάλειας, η NIS 2 απαιτεί από τα κράτη-μέλη την ανάπτυξη εθνικών στρατηγικών οι οποίες καλύπτουν ένα ευρύτερο φάσμα πολιτικών και θεσμικών ρυθμίσεων (Vandezande, 2023). Η αλλαγή αυτή επιδιώκει να αντιμετωπίσει τις ελλείψεις, οι οποίες είχαν εντοπιστεί στο πλαίσιο εφαρμογής της αρχικής οδηγίας, όπου το επίπεδο ποιότητας και πληρότητας των εθνικών στρατηγικών παρουσίαζε έντονες διαφοροποιήσεις.

Ειδικότερα, η NIS 2 εισάγει πιο συγκεκριμένες κατευθύνσεις ως προς το ελάχιστο περιεχόμενο των στρατηγικών, καθιστώντας υποχρεωτική τη συμπερίληψη πολιτικών που αφορούν κρίσιμους τομείς, όπως η κυβερνοασφάλεια της εφοδιαστικής αλυσίδας, γνωστοποίηση ευπαθειών και η ανάπτυξη μηχανισμών ανταλλαγής πληροφοριών. Παράλληλα, προβλέπει την καθιέρωση πλαισίου διακυβέρνησης που αποσαφηνίζει τους ρόλους και τις αρμοδιότητες των εμπλεκόμενων φορέων, καθώς και τη δημιουργία μηχανισμών συντονισμού μεταξύ των αρμόδιων αρχών. Επιπλέον, με τη δυνατότητα υποβολής των στρατηγικών σε αξιολογήσεις από ομότιμους, δηλαδή από ειδικούς του ίδιου ή παρόμοιου επιστημονικού πεδίου, καλλιεργείται μία διαδικασία διακρατικής συνεργασίας και ανταλλαγής καλών πρακτικών.

Συνολικά, η NIS2 σηματοδοτεί μία σαφή μετατόπιση από την αποσπασματική τεχνική προστασία σε μία ολιστική θεώρηση της κυβερνοασφάλειας, σε εθνικό επίπεδο (Vandezande, 2023). Η καθιέρωση ελάχιστων απαιτήσεων και η ενίσχυση της συνεργασίας, τόσο εντός των κρατών μελών όσο και μεταξύ τους, αποσκοπεί στη διαμόρφωση ενός συνεκτικού και λειτουργικού πλαισίου το οποίο θα εξασφαλίζει υψηλότερο επίπεδο ανθεκτικότητας απέναντι σε κυβερνοαπειλές. Μέσω αυτών των μεταρρυθμίσεων, η οδηγία επιδιώκει όχι μόνο την ενίσχυση της εθνικής ετοιμότητας, αλλά και τη σύγκλιση των στρατηγικών προσεγγίσεων εντός

της Ευρωπαϊκής Ένωσης, διασφαλίζοντας,έτσι, μία πιο ομοιογενή και ισχυρή συλλογική άμυνα απέναντι στις σύγχρονες κυβερνοπροκλήσεις.

4.4.2. Υποχρεώσεις των οντοτήτων υπό την Οδηγία NIS2.

Η αναθεωρημένη Οδηγία διευρύνει σημαντικά το φάσμα των υποχρεώσεων για τις υπόχρεες οντότητες, καθιερώνοντας πιο αυστηρές απαιτήσεις σε ζητήματα διαχείρισης κινδύνου, κρυπτογράφησης, πιστοποίησης, αναφοράς περιστατικών και κοινοποίησης ευπαθειών (DSA Cyprus, 2024). Το άρθρο 21 επιβάλλει την υιοθέτηση τεχνικών, επιχειρησιακών και οργανωτικών μέτρων για την ολιστική διαχείριση των κινδύνων, οι οποίοι συνδέονται με την ασφάλεια δικτύων και συστημάτων πληροφορίας. Η εφαρμογή αυτής της προσέγγισης πρέπει να λαμβάνει υπόψη τις ιδιαιτερότητες κάθε οργανισμού, ευθυγραμμισμένη, ταυτόχρονα, με διεθνή και ευρωπαϊκά πρότυπα. Ιδιαίτερα σημαντικό αναδεικνύεται ο ρόλος του ENISA,τόσο στη διαμόρφωση τεχνικών και μεθολογικών κατευθυντηρίων γραμμών, όσο και στην υποστήριξη της Ευρωπαϊκής Επιτροπής ως προς την έκδοση εκτελεστικών πράξεων, που εξειδικεύουν τις απαιτήσεις το άρθρου 21 (Vandezande, 2023).

Η Οδηγία αποδίδει, επίσης, βαρύνουσα σημασία στην πιστοποίηση κυβερνοασφάλειας, καθιστώντας πλέον δυνατή την επιβολή υποχρεωτικής πιστοποίησης για προϊόντα, υπηρεσίες ή διαδικασίες, βάσει ευρωπαϊκών σχημάτων πιστοποίησης, που θεσπίζονται στον Κανονισμό 2019/881. Η ρύθμιση αυτή αποσκοπεί στην ενίσχυση της εμπιστοσύνης, ενδέχεται όμως να προκαλέσει αυξημένο κανονιστικό και οικονομικό βάρος, με πιθανές επιπτώσεις στην καινοτομία. Παράλληλα, το άρθρο 23 εισάγει αυστηρά χρονοδιαγράμματα για την αναφορά περιστατικών: αρχική ειδοποίηση εντός 24 ωρών, ενδιάμεση ενημέρωση στις 72 ώρες και τελική αναφορά-έκθεση το αργότερο ένα μήνα μετά την κοινοποίηση του συμβάντος. Αν και τα συγκεκριμένα χρονικά όρια ενισχύουν την ταχύτητα ανταπόκρισης, έχουν διατυπωθεί αμφιβολίες για τη ρεαλιστικότητα εφαρμογής τους, ιδίως λόγω της ασάφειας γύρω από τον ορισμό του «σημαντικού περιστατικού».

Σε αυτό το πλαίσιο, κρίνεται κρίσιμη η συμμετοχή του ENISA για την παροχή ερμηνευτικών οδηγιών που εξασφαλίζουν ενιαία και αναλογική εφαρμογή, σε ευρωπαϊκό επίπεδο. Σε συνεργασία με τον ENISA, σύμφωνα με το άρθρο 7, τα

κράτη-μέλη καλούνται να θεσπίσουν φορείς αρμόδιους για τη διαχείριση κοινοποίησης ευπαθειών, στηριζόμενοι σε διεθνώς αναγνωρισμένα πρότυπα όπως τα ISO/IEC 29147 και 30111 (European Union Agency for Cybersecurity (ENISA), 2025). Επιπλέον, το άρθρο 29 καθορίζει το πλαίσιο για την ανταλλαγή πληροφοριών, απειλών και ευπαθειών, δίνοντας έμφαση στη διασφάλιση εμπιστευτικότητας και στην προστασία επαγγελματικών μυστικών. Η συμμετοχή σε αυτούς τους μηχανισμούς βασιζεται σε κίνητρα και οχι σε αυστηρές υποχρεώσεις, με σκοπό την ενίσχυση της εμπιστοσύνης μεταξύ των εμπλεκόμενων φορέων και εποπτικών αρχών.

4.4.3 Εποπτεία και επιβολή Κυρώσεων

Η Οδηγία NIS 2 καθιερώνει ένα αυστηρότερο και εναρμονισμένο πλαίσιο για την εποπτεία και την επιβολή μέτρων στον τομέα της κυβερνοασφάλειας, αποσκοπώντας στη διασφάλιση της συμμόρφωσης των ουσιωδών-βασικών και σημαντικών οντοτήτων. Σύμφωνα με το άρθρο 32, οι αρμόδιες αρχές διαθέτουν τη δυνατότητα να διενεργούν τόσο προληπτικούς όσο και εκ των υστέρων ελέγχους, περιλαμβανομένων επιθεωρήσεων, ελέγχων ασφαλείας και αξιολόγησης τεκμηρίωσης. Η επιβολή κυρώσεων ρυθμίζεται στο άρθρο 34, το οποίο παρέχει στις εποπτικές αρχές εξουσία επιβολής διορθωτικών μέτρων, αναστολής ή διακοπής δραστηριοτήτων, καθώς και διοικητικών προστίμων. Η κλιμάκωση των κυρώσεων βασίζεται στη σοβαρότητα και τη διάρκεια της παράβασης αλλά και στο βαθμό συνεργασίας της οντότητας. Το άρθρο 35 ορίζει τα ανώτατα όρια των διοικητικών προστίμων: για τις ουσιώδεις οντότητες έως 10 εκατομμύρια ευρώ ή 2% του ετήσιου κύκλου εργασιών παγκοσμίως και, για τις σημαντικές οντότητες έως 7 εκατομμύρια ευρώ ή 1,4% του αντίστοιχου κύκλου εργασιών.

Παράλληλα, εισάγεται η δυνατότητα επιβολής περιοδικών χρηματικών ποινών, ώστε να διασφαλίζεται η συμμόρφωση και η άμεση παύση παραβάσεων, σε αντίθεση με τα «παραδοσιακά» πρόστιμα τα οποία αποδεικνύονται συχνά λιγότερο αποτελεσματικά (Vandezande, 2023). Η διαχείριση της κυβερνοασφάλειας θα πρέπει να προσαρμόζεται ανάλογα με το επίπεδο κινδύνου, το μέγεθος του οργανισμού, το κόστος εφαρμογής των μέτρων και την πιθανή σοβαρότητα και επιρροή των συμβάντων. Η Ευρωπαϊκή Επιτροπή διατηρεί την αρμοδιότητα να θεσπίζει

υποχρεώσεις πιστοποίησης και να εκδίδει εκτελεστικές πράξεις που καθορίζουν συγκεκριμένες τεχνικές απαιτήσεις, λαμβάνοντας υπόψη τις τελευταίες τεχνολογικές εξελίξεις και τα υπάρχοντα ευρωπαϊκά και διεθνή πρότυπα. Επιπλέον, απαιτείται η εκτέλεση εκτιμήσεων κινδύνου για κρίσιμες υπηρεσίες, πληροφοριακά συστήματα ή αλυσίδες εφοδιασμού ΤΠΕ, ώστε να διασφαλίζεται η αποτελεσματική πρόληψη και αντιμετώπιση πιθανών απειλών, προάγοντας, έτσι, ένα υψηλό επίπεδο ασφάλειας σε ολόκληρο το ψηφιακό περιβάλλον (DSA Cyprus, 2024). Η αναλογικότητα και η σαφήνεια στην εφαρμογή των κυρώσεων αποτελούν κρίσιμες προϋποθέσεις ενώ, το άρθρο 33 θεμελιώνει εγγυήσεις δίκαιης διοικητικής διαδικασίας, κατοχυρώνοντας το δικαίωμα ακρόασης και ένδικης προσφυγής για τις οντότητες που υπόκεινται σε εποπτικά μέτρα και κυρώσεις.

Η ενίσχυση των εποπτικών μηχανισμών αποσκοπεί όχι μόνο στην ομοιογενή εφαρμογή της οδηγίας σε ευρωπαϊκό επίπεδο, αλλά και στη δημιουργία ενός αξιόπιστου πλαισίου λογοδοσίας και υπευθυνότητας, το οποίο θα ενδυναμώσει την ανθεκτικότητα της Ένωσης απέναντι στις αυξανόμενες απειλές στον κυβερνοχώρο. Στο επόμενο κεφάλαιο θα εξεταστεί ο Νόμος 5160/2024, μέσω του οποίο οι προαναφερθείσες διατάξεις ενσωματώνονται στην ελληνική έννομη τάξη, αποτυπώνοντας τις υποχρεώσεις και τις απαιτήσεις που επιβάλλει η Οδηγία στους οργανισμούς παροχής κρίσιμων και ψηφιακών υπηρεσιών.

4.4.4. Συμπεράσματα

Η μετάβαση από το περιορισμένο πλαίσιο της NIS1 σε ένα πιο ευρύ και αυστηρό σύστημα, επιτρέπει την καλύτερη κάλυψη κρισιμων τομέων και επιχειρήσεων, ενώ, η καθιέρωση υψηλότερων και εναρμονισμένων κυρώσεων ενισχύει την πίεση για συμμόρφωση. Ειδικότερα, η NIS2 εισάγει σημαντικές αλλαγές σε σχέση με την NIS1. Το πεδίο εφαρμογής της διευρύνεται, καλύπτοντας πλέον 18 τομείς (έναντι μόλις 7 της προγενέστερης Οδηγίας) και, περιλαμβάνει περισσότερες επιχειρήσεις, κυρίως μεσαίου και μεγάλου μεγέθους. Ο προηγούμενος διαχωρισμός μεταξύ «φορέων εκμετάλλευσης βασικών υπηρεσιών» και «παρόχων ψηφιακών υπηρεσιών» καταργείται, εισάγοντας πλέον τις κατηγορίες «βασικές» και «σημαντικές» οντότητες. Μία ακόμη ουσιαστική διαφορά αφορά το πλαίσιο κυρώσεων. Στη NIS1, οι κυρώσεις καθορίζονταν σε εθνικό επίπεδο, χωρίς ενιαία

προσέγγιση και χωρίς σαφές ανώτατο όριο προστίμων. Έτσι, επιτυγχάνεται εναρμόνιση του καθεστώτος κυρώσεων σε όλη την ΕΕ. Αν και η πλήρη εφαρμογή βρίσκεται ακόμη σε εξέλιξη, η Ελλάδα δείχνει να επενδύει ουσιαστικά στη θωράκιση του ψηφιακού περιβάλλοντος, εδραιώνοντας τη θέση της σε ένα πιο ανθεκτικό και ασφαλές ευρωπαϊκό κυβερνοχώρο.

Η NIS 2 αποτελεί, επομένως, ένα σημαντικό βήμα προς την κατεύθυνση της ενιαίας ευρωπαϊκής ψηφιακής ανθεκτικότητας. Η εναρμονισμένη εφαρμογή της Οδηγίας από τα κράτη-μέλη θεωρείται κρίσιμη, προκειμένου να αποφευχθεί ο κατακερματισμός του ρυθμιστικού πλαισίου και να διασφαλιστεί η ουσιαστική προστασία κρίσιμων ψηφιακών και φυσικών υποδομών (Vandezande, 2023) . Η επιτυχία της θα εξαρτηθεί σε μεγάλο βαθμό από τη σαφήνεια και την πληρότητα των εθνικών ρυθμίσεων, την ενίσχυση των αρμόδιων εποπτικών αρχών καθώς και την ενεργό συνεργασία τόσο μεταξύ των κρατών-μελών όσο και μεταξύ δημοσίου και ιδιωτικού τομέα.

Παράλληλα, απαιτείται η ανάπτυξη κοινής ευρωπαϊκής κουλτούρας ασφάλειας, η συνεχής ανταλλαγή πληροφοριών και βέλτιστων πρακτικών καθώς και η καλλιέργεια εμπιστοσύνης μεταξύ όλων των εμπλεκόμενων φορέων. Η εφαρμογή της Οδηγίας δεν θα πρέπει να περιοριστεί σε τυπική συμμόρφωση αλλά, να λειτουργήσει ως μοχλός για τη συνολική αναβάθμιση του επιπέδου κυβερνοασφάλειας στην Ένωση.

4.5. (ΕΕ) 2016/679-Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου του 2018, αποτελεί τον αυστηρότερο Κανονισμό για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Στόχος του αποτελεί η ενίσχυση των δικαιωμάτων των ατόμων, όσον αφορά τα προσωπικά τους δεδομένα, και η εξασφάλιση της διαφάνειας στον τρόπο με τον οποίο οι οργανισμοί συλλέγουν, επεξεργάζονται και αποθηκεύουν αυτά τα δεδομένα. Ο GDPR ενσωματώνει την Οδηγία 95/46/ΕΚ και έχει ως βασικό σκοπό την εναρμόνιση των νόμων προστασίας των προσωπικών δεδομένων στην ΕΕ και την ενίσχυση της

προστασίας των ατόμων. Βασίζεται στη Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) και έχει εφαρμογή σε όλα τα κράτη-μέλη της ΕΕ, καθώς και σε οποιονδήποτε οργανισμό εκτός ΕΕ, όπου επεξεργάζονται δεδομένα προσωπικού χαρακτήρα πολιτών της Ευρωπαϊκής Ένωσης.

4.5.1. Αλληλεπίδραση ΓΚΠΔ και Οδηγίας NIS στο σύγχρονο τοπίο κυβερνοαπειλών.

Η Οδηγία NIS2 και ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων επιδιώκουν, αμφότεροι, την προστασία δεδομένων γεγονός που αντανακλά τη σημασία τόσο των προσωπικών όσο και των εταιρικών δεδομένων στη διαδικασία λήψης αποφάσεων. Παρότι μοιράζονται κοινούς στόχους, η προσέγγισή τους διαφοροποιείται ως προς το πεδίο εφαρμογής και της κανονιστικές προτεραιότητες.

Ένα από τα πιο χαρακτηριστικά σημεία σύνδεσης του GDPR και της Οδηγίας NIS2 αποτελεί η υποχρέωση κοινοποίησης περιστατικών παραβίασης δεδομένων στην αρμόδια αρχή (Zuiderveen Borgesius et al., 2023), η οποία ειδικεύεται σε θέματα παραβιάσεων, είτε πρόκειται για ζητήματα κυβερνοασφάλειας είτε για θέματα παραβιάσεων προσωπικών δεδομένων. Όπως προβλέπεται από την Οδηγία NIS2, κάθε κράτος μέλος της ΕΕ ορίζει μία αρχή με τεχνογνωσία σχετικά με ζητήματα κυβερνοασφάλειας, η οποία έχει ως αποστολή να διασφαλίζει ότι οι οντότητες συμμορφώνονται με τις σχετικές απαιτήσεις. Αντίστοιχα, στον ΓΚΠΔ, κάθε κράτος-μέλος διαθέτει εποπτική αρχή με σκοπό την άμεση ανταπόκριση σε περιστατικά παραβίασης δεδομένων, τον μετριασμό των επιπτώσεων αλλά και τη διενέργεια ερευνών, σε συνεργασία με άλλες αρχές της ΕΕ, σε διασυνοριακές υποθέσεις. Στην Ελλάδα, ο ρόλος αυτός ανατίθεται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στην οποία μπορούν να απευθύνονται πολίτες για καταγγελίες, ενημέρωση ή συμμετοχή σε δράσεις συμμορφωσης (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, 2023). Για θέματα που άπτονται της NIS2, αρμόδια αρχή είναι η Εθνική Αρχή Κυβερνοασφάλειας, η οποία είναι επιφορτισμένη με τη χάραξη στρατηγικής, την υιοθέτηση κατάλληλων τεχνικών και οργανωτικών μέτρων καθώς και τον έλεγχο της συμμόρφωσης των οντοτήτων, μέσω επιθεωρήσεων. Σημαντικό είναι να τονιστεί ότι η NIS2 δεν αποκλείει τη συμπληρωματική εφαρμογή του ΓΚΠΔ αλλά λειτουργεί συμπληρωματικά.

Στο πλαίσιο του Κανονισμού, η υποχρέωση γνωστοποίησης παραβιάσεων προσωπικών δεδομένων διαφοροποιείται, με βάση τον βαθμό κινδύνου ο οποίος προκύπτει για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Έτσι, ο Κανονισμός καθορίζει τρία επίπεδα παραβιάσεων με αντίστοιχες υποχρεώσεις εκ μέρους του υπευθύνου επεξεργασίας. Αρχικά, λοιπόν, έχουμε την κατηγορία παραβίασης χωρίς εκτιμώμενο κίνδυνο (no-risk breaches). Σε περιπτώσεις όπου μία παραβίαση κρίνεται απίθανο να οδηγήσει σε οποιονδήποτε κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, δεν υφίσταται κάποια υποχρέωση γνωστοποίησης ούτε προς την εποπτική αρχή ούτε ως προς τα υποκείμενα. Το άρθρο 33 ΓΚΠΔ ορίζει ρητά ότι η γνωστοποίηση στην αρμόδια εποπτική αρχή απαιτείται μόνο όταν υφίσταται κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.[25] Ωστόσο, αν, εκ των υστέρων, αποδειχθεί ότι η κρυπτογράφηση ήταν ευάλωτη, τότε, η παραβίαση ενδέχεται να αποκτήσει επικινδυνότητα, καθιστώντας υποχρεωτική τη γνωστοποίησή της. Το παραπάνω υπογραμμίζει τη σημασία της τεκμηρίωσης όλων των περιστατικών παραβίασης, ανεξαρτήτως αρχικής εκτίμησης, όπως άλλωστε επιτάσσει και ο ίδιος ο Κανονισμός.

Εν συνεχεία, η κατηγοριοποίηση συνεχίζεται με τις παραβιάσεις κανονικού κινδύνου (normal-risk breaches) (Zuiderveen Borgesius et al., 2023). Όταν η εξαίρεση για παραβιάσεις χωρίς κίνδυνο δεν εφαρμόζεται, ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει την παραβίαση στην αρμόδια εποπτική αρχή, εντός της προθεσμίας των 72 ωρών, από τη στιγμή που αυτή έχει γίνει αντιληπτή. Η υποχρέωση αυτή εισάγεται στο άρθρο 33 του Κανονισμού. Σε περίπτωση καθυστέρησης πέραν του προβλεπόμενου χρονικού ορίου, ο υπεύθυνος θα πρέπει να αιτιολογήσει την καθυστέρηση. Αν και η προθεσμία των 72 ωρών θεωρείται ιδιαίτερα περιοριστική, συγκριτικά με προθεσμίες άλλων χωρών όπως των Η.Π.Α (όπου συχνά προβλέπονται προθεσμίες των 30 έως 60 ωρών), εντούτοις, η πρόωρη γνωστοποίηση μπορεί να προκαλέσει προβλήματα όταν απαιτείται περισσότερος

[25] «Σύμφωνα με το άρθρο 33(1) του GDPR, "…εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων…..» European Union, 2016. *General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. Article 33(1). [online] *Official Journal of the European Union*, L119, pp.1–88.

χρόνος για τη διερεύνηση του περιστατικού (Zuiderveen Borgesius et al., 2023). Για τον λόγο αυτό, ο ΓΚΠΔ επιτρέπει την υποβολή γνωστοποίησης σε δύο φάσεις: μία αρχική ενημέρωση εντός του χρονικού πλαισίου, και, εν συνεχεία, συμπληρωματικές λεπτομέρειες, όπου αυτές καθίστανται διαθέσιμες. Σημειώνεται πως κάθε παραβίαση δεδομένων θα πρέπει να κοινοποιείται χωριστά στις αρμόδιες αρχές των κρατών-μελών όπου διαμένουν τα επηρεαζόμενα υποκείμενα των δεδομένων. Η κοινοποίηση πραγματοποιείται σύμφωνα με το πλαίσιο εξουσιοδότησης που έχει θέσει ο υπεύθυνος επεξεργασίας για τον εκπρόσωπό του και παραμένει υπό την πλήρη ευθύνη του υπεύθυνου επεξεργασίας (EDPB, 2023).

Η τρίτη κατηγορία αφορά τις παραβιάσεις υψηλού κινδύνου (high-risk breaches) (Zuiderveen Borgesius et al., 2023). Στην περίπτωση που μία παραβίαση ενέχει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας οφείλει να προχωρήσει σε άμεση ενημέρωση, όχι μόνο της εποπτικής αρχής, αλλά και των ίδιων των υποκειμένων των δεδομένων, σύμφωνα με το άρθρο 34 του Κανονισμού. Οι συνέπειες μιας τέτοιας παραβίασης μπορεί να είναι κρίσιμες. Ξεκινούν από απάτη ταυτότητας και οικονομική ζημία έως βλάβη της φήμης και περαιτέρω προσβολές της ιδιωτικής ζωής. Οι παραβιάσεις οι οποίες αφορούν «ειδικές κατηγορίες δεδομένων», όπως είναι, για παράδειγμα, οι πληροφορίες για την υγεία, τις πολιτικές απόψεις, τις θρησκευτικές πεποιθήσεις και τον σεξουαλικό προσανατολισμό, θεωρούνται ιδιαιτέρως ευαίσθητες και άρα υψηλού κινδύνου. Η Επιτροπή Προστασίας Δεδομένων τονίζει, πλέον, την ανάγκη αξιολόγησης παραγόντων όπως είναι η φύση, η ευαισθησία, ο όγκος των δεδομένων αλλά και, η σοβαρότητα των ενδεχόμενων συνεπειών για τα άτομα (EDPB, 2023). Σημειώνεται πως, ακόμη και αν ο υπεύθυνος επεξεργασίας δεν προχωρήσει σε γνωστοποίηση προς τα υποκείμενα των δεδομένων, η εποπτική αρχή έχει τη δυνατότητα να τον υποχρεώσει σε σχετική ενέργεια.[26] Η πρόβλεψη αυτή ενισχύει την προστασία των προσώπων που ενδέχεται να επηρεαστούν από την παραβίαση. Μάλιστα, σύμφωνα με τις κατευθυντήριες οδηγίες του European

[26]« Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί…..να του ζητήσει να το πράξει..» European Union, 2016. *General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. Article 34(4). [online] *Official Journal of the European Union*, L119, pp.1–88.

Data Protection Board, ένας υπεύθυνος επεξεργασίας θεωρείται ότι έχει λάβει γνώση ενός περιστατικού παραβίασης δεδομένων όταν μπορεί, με μεγάλη βεβαιότητα, να διαπιστώσει ότι έλαβε χώρα περιστατικό ασφάλειας που είχε ως αποτέλεσμα τη διαρροή ή παραβίαση των προσωπικών δεδομένων (EDPB, 2023).

Η οδηγία NIS2 θεσπίζει σαφείς και αυστηρές υποχρεώσεις κοινοποίησης, όπως προείπαμε, περιστατικών ασφάλειας για τους ουσιώδεις και σημαντικούς φορείς, με στόχο την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών και υπηρεσιών. Συγκεκριμένα, απαιτείται αρχική ειδοποίηση εντός 24 ωρών από τη στιγμή που ο φορέας αντιληφθεί το περιστατικό, ενδιάμεση αναφορά με αναλυτικότερα στοιχεία εντός 72 ωρών, καθώς και τελική έκθεση εντός ενός μηνός, η οποία περιγράφει τα αίτια, τις επιπτώσεις και τα διορθωτικά μέτρα. Οι κοινοποιήσεις αυτές αποστέλλονται στις αρμόδιες εθνικές αρχές ή στα CSIRT, ενώ, όπου κρίνεται αναγκαίο, οι φορείς υποχρεούνται να ενημερώνουν και τους χρήστες των υπηρεσιών τους. Το πλαίσιο αυτό υπογραμμίζει τη σημασία της έγκαιρης πληροφόρησης και της συνεργασίας με τις εποπτικές αρχές, προκειμένου να ενισχυθεί η πρόληψη, ο μετριασμός και η συνολική κυβερνοανθεκτικότητα στην Ευρωπαϊκή Ένωση.

Η υποχρέωση κοινοποίησης παραβίασης αποτελεί κρίσιμο εργαλείο για την ενίσχυση της εμπιστοσύνης των πολιτών και τη διατήρηση ενός υψηλού επιπέδου κυβερνοασφάλειας. Η δημοσιοποίηση περιστατικών, σε συνδυασμό με τον κίνδυνο επιβολής προστίμων και τη ζημία στη φήμη, λειτουργεί ως κίνητρο για τους οργανισμούς να επενδύουν περισσότερο στην ασφάλεια (Zuiderveen Borgesius et al., 2023). Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) έχει ενισχύσει σημαντικά αυτή την τάση στην Ευρώπη, καθώς οι αυστηρές κυρώσεις οδηγούν σε αυξημένη συμμόρφωση. Παράλληλα, η οδηγία NIS2 ενισχύει περαιτέρω το κανονιστικό πλαίσιο, καθιερώνοντας αυστηρά χρονοδιαγράμματα κοινοποίησης περιστατικών ασφάλειας σε κρίσιμους και σημαντικούς φορείς. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) έχει ενισχύσει σημαντικά αυτή την τάση στην Ευρώπη, καθώς οι αυστηρές κυρώσεις οδηγούν σε αυξημένη συμμόρφωση. Παράλληλα, η οδηγία NIS2 ενισχύει περαιτέρω το κανονιστικό πλαίσιο, καθιερώνοντας αυστηρά χρονοδιαγράμματα κοινοποίησης περιστατικών

ασφάλειας σε κρίσιμους και σημαντικούς φορείς. Έτσι, τόσο ο GDPR όσο και η NIS2 συμβάλλουν στην καλλιέργεια μιας κουλτούρας διαφάνειας και υπευθυνότητας, προάγοντας την κυβερνοανθεκτικότητα σε ευρωπαϊκό επίπεδο.

4.5.2. ΚΥΡΩΣΕΙΣ

Στο πλαίσιο του ΓΚΠΔ, το ύψος των προστίμων καθορίζεται από παράγοντες όπως η βαρύτητα και η διάρκεια της παράβασης, ο βαθμός υπαιτιότητας, οι ενέργειες μετριασμού των συνεπειών, το επίπεδο ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασίας καθώς και τα τεχνικά ή οργανωτικά μέτρα τα οποία είχαν ληφθεί (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, 2023). Επιπλέον, λαμβάνονται υπόψη τυχόν προηγούμενες παραβιάσεις, ο βαθμός συνεργασίας με την εποπτική αρχή, η συμμόρφωση με τα μέτρα που αυτή ορίζει, οι κατηγορίες των δεδομένων που επηρεάστηκαν, ο τρόπος γνωστοποίησης της παράβασης καθώς και λοιποί επιβαρυντικοί ή ελαφρυντικοί παράγοντες, όπως το οικονομικό όφελος που αποκόμισε η επιχείρηση. Σύμφωνα με το άρθρο 83 του Κανονισμού, τα διοικητικά πρόστιμα διακρίνονται σε δύο κατηγορίες: α. έως 20 εκατομμύρια ευρώ ή το 4% του ετήσιου παγκόσμιου κύκλου εργασιών για σοβαρές παραβάσεις που πλήττουν τα δικαιώματα και τις θεμελιώδεις αρχές επεξεργασίας, και β. έως 10 εκατομμύρια ευρώ ή 2% του ετήσιου κύκλου εργασιών για παραβάσεις υποχρεώσεων που συνδέονται με τον υπεύθυνο ή τον εκτελούντα την επεξεργασία, καθώς και με φορείς πιστοποίησης και παρακολούθησης.

Αντίστοιχη λογική υιοθετεί και η NIS2, με τη διαφορά ότι τα προβλεπόμενα ανώτατα πρόστιμα διαφοροποιούνται ανάλογα με την κατηγορία του φορέα, όπως έχει ήδη ειπωθεί. Παρά την ύπαρξη ξεχωριστών μηχανισμών κυρώσεων, είναι σημαντικό να τονιστεί πως η εφαρμογή των διατάξεων της NIS2 δεν αναιρεί τις υποχρεώσεις συμμόρφωσης με τον ΓΚΠΔ. Συνεπώς, οι αρμόδιες αρχές μπορούν να επιβάλλουν κυρώσεις τόσο το πλαίσιο της προστασίας δεδομένων όσο και της κυβερνοασφάλειας. Ωστόσο, όταν ένα περιστατικό υπάγεται ταυτοχρόνως και στα δύο κανονιστικά πλαίσια, εφαρμόζεται η αρχή ne bis in idem, γεγονός που σημαίνει ότι το ίδιο αδίκημα δεν μπορεί να τιμωρηθεί δύο φορές.[27]

[27] European Parliament and Council. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

4.5.3. Συμπεράσματα

Συνολικά, ο Κανονισμός Προστασίας Δεδομένων και η Οδηγία NIS2, παρότι θεσπίστηκαν με διαφορετικό πρωταρχικό αντικείμενο, συγκλίνουν ως προς τον ευρύτερο στόχο τους, ο οποίος είναι η ενίσχυση της ψηφιακής ανθεκτικότητας των οργανισμών και των λοιπών φορέων και η προστασία από σύγχρονες ψηφιακές απειλές. Προς την επίτευξη του σκοπού αυτού, καθιερώνουν την αρχή της συνεργασίας των αρμόδιων αρχών σε εθνικό και διακρατικό επίπεδο. Η τήρηση των διατάξεων αμφοτέρων δημιουργεί ένα συνεκτικό πλαίσιο το οποίο συμβάλλει τόσο στην ασφάλεια των δεδομένων όσο και στη συνολική κυβερνοασφάλεια.

Ωστόσο, μία βασική διαφορά δεν μπορεί να παραβλεφθεί. Ο Κανονισμός ρυθμίζει αποκλειστικά ζητήματα τα οποία άπτονται της προστασίας των προσωπικών δεδομένων ενώ, η NIS2 επεκτείνεται ευρύτερα, σε θέματα ασφάλειας συστημάτων πληροφορικής και επικοινωνιών, ανεξάρτητα από το αν εμπλέκονται προσωπικά δεδομένα (Zuiderveen Borgesius et al., 2023). Το στοιχείο αυτό αναδεικνύει τον συμπληρωματικό χαρακτήρα των δύο ρυθμίσεων και καθιστά σαφές ότι η αποτελεσματική εφαρμογή τους απαιτεί μία ολιστική προσέγγιση, η οποία συνδυάζει την προστασία της ιδιωτικότητας με την οργανωτική θωράκιση των ψηφιακών υποδομών.

4.6. Κανονισμός {ΕΕ} 2022/2554 για την Ψηφιακή και Λειτουργική Ανθεκτικότητα-Digital Operational Resilience Act (DORA).

Τον Σεπτέμβριο του 2020, η Ευρωπαϊκή Επιτροπή εξέδωσε μία πρόταση Κανονισμού, η οποία αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα στον χρηματοπιστωτικό τομέα. Στόχος του Κανονισμού αυτού αποτελεί η εγκαθίδρυση ενός ολοκληρωμένου πλαισίου κυβερνοασφάλειας στον χρηματοοικονομικό κλάδο της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένων των «παραδοσιακών» και ψηφιακών τραπεζών, των ιδρυμάτων ηλεκτρονικού χρήματος και πληρωμών, των ασφαλιστικών εταιρειών, των διαχειριστών περιουσιακών στοιχείων, των

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May, pp. 1–88, σκέλος 149 του προοιμίου (recital 149).

πιστωτικών ιδρυμάτων, και των εταιρειών ιδιωτικών κεφαλαίων. Ο DORA τέθηκε σε ισχύ στις 17 Ιανουαρίου του 2025 .

Με την υιοθέτηση του DORA, τα χρηματοπιστωτικά ιδρύματα υποχρεούνται, πλέον, στην εφαρμογή αυστηρών απαιτήσεων οι οποίες καλύπτουν την πρόληψη, την ανίχνευση, την απομόνωση, την ανάκαμψη και την αποκατάσταση από περιστατικά τα οποία σχετίζονται με τις τεχνολογίες πληροφορικής και επικοινωνιών. Ο Κανονισμός καθιερώνει σαφείς κανόνες, οι οποίοι αφορούν τη διαχείριση των τεχνολογιών πληροφορικής και επικοινωνιών και τους κινδύνους που αυτοί εγκυμονούν, την αναφορά σοβαρών περιστατικών, τη δοκιμαστική αξιολόγηση της λειτουργικής ανθεκτικότητας καθώς και , την εποπτεία των κινδύνων που προέρχονται από τρίτους παρόχους τέτοιων υπηρεσιών (European Supervisory Authorities, 2025).

4.6.1. Βασικοί άξονες και σκοποί.

Σύμφωνα με το Άρθρο 1 του Κανονισμού (Ευρωπαϊκή Επιτροπή, 2022), ο DORA θέτει ομοιόμορφες απαιτήσεις για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων τα οποία υποστηρίζουν τις επιχειρησιακές διαδικασίες των χρηματοπιστωτικών φορέων, εστιάζοντας σε επιμέρους τομείς. Ένας από τους βασικότερους άξονες του Κανονισμού αποτελεί η υιοθέτηση ενιαίων και δεσμευτικών απαιτήσεων, στο πλαίσιο διασφάλισης της ψηφιακής λειτουργικής ανθεκτικότητας των χρηματοπιστωτικών φορέων της Ευρωπαϊκής Ένωσης (Άρθρο 6). Πιο συγκεκριμένα, ο Κανονισμός προβλέπει ότι οι φορείς του χρηματοοικονομικού τομέα οφείλουν να αναπτύξουν και να εφαρμόζουν ένα συνεκτικό πλαίσιο διαχείρισης κινδύνων οι οποίο σχετίζονται με τις τεχνολογίες πληροφορικής και επικοινωνιών. Το πλαίσιο αυτό δεν περιορίζεται σε εσωτερικές διαδικασίες, αλλά, επεκτείνεται σε κάθε κρίσιμο στοιχείο του ψηφιακού τους οικοσυστήματος, ενισχύοντας την πρόληψη, ανίχνευση και απόκριση απέναντι σε τεχνικές βλάβες ή κακόβουλες ενέργειες (European Supervisory Authorities, 2025). Ιδιαίτερη βαρύτητα ενέχει η υποχρέωση έγκαιρης και τυποποιημένης αναφοράς σημαντικών περιστατικών, στο πλαίσιο των τεχνολογιών πληροφορικής και επικοινωνιών, στις αρμόδιες εποπτικές αρχές, καθώς και, προαιρετικώς, η αναφορά

περιστατικών σχετιζόμενων με τη λειτουργία ή την ασφάλεια των συστημάτων πληρωμών (Άρθρο 19), διασφαλίζοντας την ακεραιότητα των συναλλαγών, σε ένα περιβάλλον αυξημένης ψηφιακής διασύνδεσης.

Προκειμένου να διασφαλιστεί η επάρκεια και η ανθεκτικότητα των συστημάτων σε συνθήκες πίεσης και επίθεσης, ο DORA καθιερώνει μηχανισμούς τακτικής δοκιμαστικής αξιολόγησης της ψηφιακής λειτουργικής ανθεκτικότητας των οργανισμών (Κεφάλαιο IV Κανονισμού). Οι δοκιμές αυτές, οι οποίες περιλαμβάνουν από τεχνικούς ελέγχους μέχρι προσομοιώσεις κρίσεων, αποτελούν βασικό εργαλείο για την βελτίωση της ετοιμότητας και της απόκρισης. Ταυτόχρονα, ενισχύεται η οργανωμένη ανταλλαγή πληροφοριών και πληροφοριακής νοημοσύνης σχετικά με τις κυβερνοαπειλές, ευπάθειες και τεχνικές επιθέσεων, μεταξύ χρηματοπιστωτικών οργανισμών και αρμοδίων αρχών. Η προσέγγιση αυτή ευνοεί την καλλιέργεια μιας κουλτούρας συνεργασίας και συλλογικής άμυνας, εντός του οικοσυστήματος. Επιπλέον, στο πλαίσιο του εν λόγω Κανονισμού προβλέπονται και ρυθμίσεις σχετικά με τις συμβατικές σχέσεις μεταξύ των χρηματοπιστωτικών φορέων και των τρίτων παρόχων υπηρεσιών πληροφορικής και επικοινωνιών (Άρθρο 28,29,30) καθώς και τη δημιουργία και λειτουργία ενός συστήματος εποπτείας, για τους κρίσιμους τρίτους παρόχους, όπως είναι η Amazon Web Services, η Google Cloud Platform και η Microsoft Azure,οι οποίοι παρέχουν υπηρεσίες στους χρηματοπιστωτικούς οργανισμούς.(Κεφάλαιο II).

Τέλος, ο DORA προβλέπει τη συστηματική διαχείριση των κινδύνων, οι οποίοι απορρέουν από τρίτους παρόχους υπηρεσιών πληροφορικής και επικοινωνιών, καθορίζοντας συγκεκριμένες απαιτήσεις για τις συμβατικές σχέσεις και την παρακολούθηση των υπηρεσιών που προσφέρουν. Σκοπός είναι η αποτροπή της εξάρτησης από μη διαχειρίσιμες ή επισφαλείς τεχνολογικές υποδομές και η εξασφάλιση της επιχειρησιακής συνέχειας.

4.6.2. ΚΥΡΩΣΕΙΣ

Σε περίπτωση μη συμμόρφωσης με τον Κανονισμό, προβλέπονται χρηματικές κυρώσεις, οι οποίες επιβάλλονται μετά από έλεγχο των αρμόδιων εποπτικών αρχών. Οι κυρώσεις μπορεί να φτάσουν και στο 2% του ετήσιου προϋπολογισμού

στις χρηματοπιστωτικές επιχειρήσεις ενώ μπορεί να επιβληθούν κυρώσεις και σε μεμονωμένα στελέχη τα οποία μπορούν να φτάσουν και το ποσό του ενός εκατομμυρίου. Επιπρόσθετα, για παρόχους τεχνολογικών υπηρεσιών, οι κυρώσεις μπορεί να αγγίζουν το 1% των μέσων ημερήσιων εσόδων του προηγούμενου οικονομικού έτους ενώ για κρίσιμους τρίτους παρόχους υπηρεσιών πληροφορικής και επικοινωνιών πρόστιμα έως πέντε εκατομμύρια ευρώ και για μεμονωμένα στελέχη πρόστιμα έως μισό εκατομμύριο ευρώ (European Supervisory Authorities, 2025). Τέλος, ορίζεται και οι επιβολή καθημερινών κυρώσεων για περίοδο 6 μηνών, μέχρι την επίτευξη της συμμόρφωσης της επιχείρησης ή του οργανισμού.

4.6.3. Συμπέρασμα

Συνολικά, ο DORA μετατοπίζει το επίκεντρο της λειτουργικής ανθεκτικότητας από τη μονοδιάστατη διαχείριση οικονομικών κινδύνων στη δημιουργία ενός ολοκληρωμένου, προληπτικού και ελεγχόμενου περιβάλλοντος αντιμετώπισης των κινδύνων οι οποίο σχετίζονται με τις τεχνολογίες πληροφορικής και τεχνολογιών, αναγνωρίζοντας ότι η ψηφιακή ανθεκτικότητα αποτελεί θεμελιώδη προϋπόθεση στην προσπάθεια διασφάλισης της εμπιστοσύνης ενώ, αναμένεται να μεταβάλλει ουσιωδώς το ισχύον ρυθμιστικό καθεστώς το οποίο διέπει την εξωτερική ανάθεση τεχνολογικών υπηρεσιών από χρηματοπιστωτικά ιδρύματα, αντικαθιστώντας τις εθνικές προσεγγίσεις και οδηγίες με ενιαίες ευρωπαϊκές διατάξεις (European Supervisory Authorities, 2025). Σε ένα γενικό πλαίσιο, ο Κανονισμός αναμένεται να επηρεάσει σημαντικά τα χρηματοπιστωτικά ιδρύματα στην Ευρωπαϊκή Ένωση. Οι αλλαγές που θα επιφέρει αφορούν την αύξηση του κόστους συμμόρφωσης καθώς, τα ιδρύματα και οι επιχειρήσεις θα πρέπει να επενδύσουν σε νέες διαδικασίες, συστήματα και πόρους, καθώς και την εντατικοποίηση της εποπτείας από τις αρμόδιες αρχές, με συχνότερους και αυστηρότερους ελέγχους. Επιπλέον, θα πρέπει να προσαρμόσουν τις επιχειρησιακές πρακτικές τους, ενισχύοντας την κυβερνοασφάλεια. Ιδιαίτερη έμφαση δίνεται στη διαδικασία διαχείρισης των κινδύνων, μέσω της θέσπισης ισχυρών πλαισίων και διαδικασιών (European Supervisory Authorities, 2025). Έτσι, μόλις ο Κανονισμός εδραιωθεί στον χρηματοπιστωτικό τομέα, οι φορείς θα πρέπει να επιδεικνύουν κατάλληλο επίπεδο εποπτείας και διαχείρισης, όσον αφορά την επιχειρησιακή ανθεκτικότητα.

4.7. Κανονισμός για την Κυβερνοανθεκτικότητα (Cyber Resilience Act)

Οι νέες τεχνολογίες έχουν επιφέρει και νέες τεχνολογικές προκλήσεις και ρίσκα. Όλο και περισσότεροι χρήστες έχουν πέσει θύματα προβλημάτων ασφαλείας σε καθημερινές ψηφιακές συσκευές όπως είναι τα ρούτερ wifi και οι ρομποτικές σκούπες καθαρισμού. Έτσι, στην Ομιλία για την Κατάσταση της Ένωσης το 2021, η Πρόεδρος της Ευρωπαϊκής Επιτροπής Ούρσουλα φον ντερ Λάιεν ανακοίνωσε έναν νέο «Κανονισμό για την Κυβερνοανθεκτικότητα» (Cyber Resilience Act-CRA), ο οποίος ενσωματώνει υποχρεωτικές απαιτήσεις για τους κατασκευαστές προϊόντων με ψηφιακά στοιχεία (Chiara, 2022). Η εν λόγω πρωτοβουλία θεμελιώνεται στη Στρατηγική Κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία (European Commission, 2020), στα Συμπεράσματα του Συμβουλίου της 2ας Δεκεμβρίου του 2020 και στο Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 10ης Ιουνίου του 2021.

Εν συνεχεία, στις 15 Σεπτεμβρίου του 2022, η Ευρωπαϊκή Επιτροπή κατέθεσε πρόταση κανονισμού, οι οποία θέτει οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία, τροποποιώντας τον Κανονισμό (ΕΕ) 2019/1020 (European Commission, 2020). Η νομική της βάση εντοπίζεται στα Άρθρο 114 ΣΛΕΕ, το οποίο παρέχει η δυνατότητα υιοθέτησης μέτρων τα οποία εξασφαλίζουν την εδραίωση και την ομαλή λειτουργία της εσωτερικής αγοράς.

4.7.1. Στόχοι

Η ενσωμάτωση των κανόνων της Πράξη Κυβερνοανθεκτικότητας στο εθνικό δικαιικό σύστημα κάθε κράτους-μέλους στοχεύει στη θέσπιση ενιαίων και δεσμευτικών απαιτήσεων κυβερνοασφάλειας για όλα τα προϊόντα τα οποία φέρουν ψηφιακά στοιχεία και των οποίων η χρήση, είτε προβλέπεται άμεσα είτε έμμεσα, συνδέεται με τη μετάδοση δεδομένων μέσω συσκευών ή δικτύων (Council of the European Union, 2025). Το ρυθμιστικό αυτό πλαίσιο εισάγει τις αρχές της κυβερνοασφάλειας κατά τον σχεδιασμό (security by design) και εξ ορισμού (security by default), ενσωματώνοντας, παράλληλα και την αρχή της διαρκούς φροντίδας (duty of care) για την κυβερνοασφάλεια, καθόλη τη διάρκεια της ζωής του προϊόντος (Chiara, 2022). Η εν λόγω νομοθετική πρωτοβουλία αποτελεί μέρος της ευρύτερης στρατηγικής της ΕΕ για την ενίσχυση της ψηφιακής ανθεκτικότητας και

αποσκοπεί στην αντιμετώπιση των υπαρκτών ρυθμιστικών κενών τα οποία σχετίζονται με την ασφάλεια των προϊόντων τεχνολογίας πληροφορικής.

Η πρόταση αναθέτηκε, αρχικώς, στην Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας (ITRE) γεγονός το οποίο καταδεικνύει την σύνδεση της κυβερνοασφάλειας με την βιομηχανική ανάπτυξη και την τεχνολογική καινοτομία. Σύμφωνα με τα άρθρα 2 και 3 της πρότασης του Κανονισμού, ως «προϊόντα με ψηφιακά στοιχεία» ορίζονται όλα τα προϊόντα λογισμικού ή υλικού, συμπεριλαμβανομένων εκείνων που διατίθενται ξεχωριστά στην αγορά. Ο Κανονισμός έχει οριζόντια εφαρμογή, καλύπτοντας ευρύ φάσμα προϊόντων, από συσκευές συνδεδεμένες στο Διαδίκτυο έως λειτουργικά συστήματα, μη ενσωματωμένο λογισμικό και, σε ορισμένες περιπτώσεις, συστήματα τεχνητής νοημοσύνης (AI) που χαρακτηρίζονται υψηλού κινδύνου.

Ο Κανονισμός διακρίνει δύο βασικές κατηγορίες ψηφιακών προϊόντων, βάση του επιπέδου κινδύνου τους. Έτσι, στην πρώτη κατηγορία εντάσσονται τα μη κρίσιμα προϊόντα χαμηλής επικινδυνότητας, όπως οικιακοί ψηφιακοί βοηθοί ή διασυνδεδεμένα παιχνίδια, και στη δεύτερη κατηγορία κρισιμα προϊόντα, τα οποία υποδιαιρούνται σε δύο υποκατηγορίες: κλάση Ι (χαμηλού κινδύνου) όπως οι δρομολογητές και κλάση ΙΙ (υψηλού κινδύνου), όπως λειτουργικά συστήματα εξυπηρετητών, επιτραπέζιοι υπολογιστές και έξυπνα κινητά τηλέφωνα (Άρθρο 7) (European Commission, 2025). Ανάλογα με την κατηγορία στην οποία υπάγεται κάθε προϊόν, διαφοροποιούνται και οι υποχρεώσεις συμμόρφωσης. Για τα μη κρίσιμα προϊόντα αρκεί μια αυτοαξιολόγηση κυβερνοασφάλειας από τον κατασκευαστή, ενώ για τα κρίσιμα προϊόντα απαιτείται διαδικασία συμμόρφωσης από τρίτο ανεξάρτητο φορέα, τον ENISA (Άρθρο 16).

Η νομοθετική αυτή πρωτοβουλία έχει ευρύτερη στόχευση, καθώς η συμμόρφωση με τις απαιτήσεις του Κανονισμού καθίσταται απαραίτητη προϋπόθεση για την πρόσβαση ενός προϊόντος στην εσωτερική αγορά της ΕΕ. Κατά συνέπεια, ακόμα και προϊόντα από τρίτες χώρες, υποχρεούνται να τηρούν τις διατάξεις του. Η διάσταση αυτή καθιστά τον Κανονισμό πιθανό σημείο αναφοράς, σε διεθνές επίπεδο, αντίστοιχο με τον ρόλο που διαδραμάτισε ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων στο πεδίο της ιδιωτικότητας. Σημαντικό

στοιχείο του κανονιστικού πλαισίου αποτελεί η σαφής κατανομή υποχρεώσεων κατά μήκος της εφοδιαστικής αλυσίδας. Οι κατασκευαστές φέρουν την κύρια ευθύνη συμμόρφωσης των προϊόντων με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας πριν από τη διάθεσή του στην αγορά και οφείλουν να τηρούν σχετική τεχνική τεκμηρίωση καθώς και να αναφέρουν περιστατικά παραβίασης ασφάλειας. Οι εισαγωγείς, από την πλευρά τους, υποχρεούνται να διασφαλίζουν ότι τα προϊόντα πληρούν τα πρότυπα ασφαλείας και φέρουν τη σήμανση CE (Ευρωπαϊκή Επιτροπή, 2022) (Άρθρο 19). Τέλος, οι διανομείς καλούνται να επιβεβαιώνουν την ύπαρξη της σήμανσης CE και να διασφαλίζουν, στο πλαίσιο της ευθύνης επιμέλειας (duty of care), ότι οι κατασκευαστές και οι εισαγωγείς έχουν συμμορφωθεί πλήρως με τις απαιτήσεις του Κανονισμού (Άρθρο 10).

4.7.2.Συμπέρασμα

Στις 10 Οκτωβρίου του 2024, το Συμβούλιο ενέκρινε τον νέο αυτόν Κανονισμό με σκοπό να διασφαλιστεί ότι τα ψηφιακά προϊόντα να είναι ασφαλή, πριν διατεθούν στην αγορά. Κατ'αυτόν τον τρόπο, διασφαλίζεται η κυβερνοασφάλεια σε όλο το φάσμα της ψηφιακής αλληλεπίδρασης και τα προϊόντα καθίστανται ασφαλή καθόλη τη διάρκεια της ζωής τους (European Commission, 2025). Ο Κανονισμός τέθηκε σε ισχύ στις 10 Δεκεμβρίου του 2024 και οι κύριες υποχρεώσεις τις οποίες εισήγαγε θα εφαρμοστούν από τις 11 Δεκεμβρίου του 2027 (European Commission, 2025).

Η υιοθέτηση του CRA αναμένεται να εναρμονίσει το ρυθμιστικό πλαίσιο της Ευρωπαϊκής Ένωσης, να μειώσει τη νομική αβεβαιότητα και να προάγει την ασφάλεια στον ψηφιακό εφοδιαστικό κύκλο, διασφαλίζοντας ένα ασφαλές περιβάλλον τόσο για τις επιχειρήσεις όσο και για τους ίδιους του καταναλωτές. Η εφαρμογή του θα επιφέρει σημαντική βελτίωση όσον αφορά την κυβερνοανθεκτικότητα, μειώνοντας τον κύκλο διαδοχικών επιθέσεων, μέσω των διασυνδεδεμένων συστημάτων και του οριζόντιου ελέγχου, σε κάθε στάδιο.

5. ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ

ΕΝΣΩΜΑΤΩΣΗ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ.

5.1. Ενσωμάτωση Κανονισμών και Οδηγιών.

Η μεταφορά στο εθνικό δίκαιο αποτελεί τη διαδικασία ενσωμάτωσης των οδηγιών της Ευρωπαϊκής Ένωσης στα εθνικά νομικά συστήματα των κρατών-μελών. Οι Κανονισμοί, όπως ο ΓΚΠΔ, έχουν άμεση εφαρμογή στα κράτη μέλη. Αντιθέτως, για την ενσωμάτωση των Οδηγιών, τα κράτη-μέλη οφείλουν να θεσπίζουν τα απαιτούμενα εκτελεστικά μέτρα, εντός της προθεσμίας την οποία ορίζει η κάθε Οδηγία, και να ενημερώνουν την Ευρωπαϊκή Επιτροπή, η οποία ελέγχει τη συμμόρφωση και μπορεί να προσφύγει στο Δικαστήριο της Ευρωπαϊκής Ένωσης σε περίπτωση παράβασης. Αν το Δικαστήριο διαπιστώσει ότι το κράτος-μέλος δεν έχει συμμορφωθεί, δύναται να επιβάλλει χρηματική ποινή, σύμφωνα με τα όσα ορίζονται στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης.

5.2. Νόμος 5160/2024: Ενσωμάτωση της Οδηγίας NIS2 στην ελληνική νομοθεσία.

Η ενσωμάτωση της NIS2 στην εθνική νομοθεσία των κρατών μελών όφειλε να ολοκληρωθεί, χωρίς αδικαιολόγητη καθυστέρηση έως τις 17 Οκτωβρίου του 2024. Η Ελλάδα ανταποκρίθηκε στην υποχρέωσή αυτή, μεταφέροντας την Οδηγία σε εθνικό δίκαιο με τη δημοσίευση του Νόμου 5160/2024, στις 27 Νοεμβρίου του 2024 (Pella, 2025). Πριν από την ψήφιση του νόμου πραγματοποιήθηκε δημόσια διαβούλευση διάρκειας δύο εβδομάδων, κατά την οποία φορείς, επιχειρήσεις και πολίτες είχαν την ευκαιρία να συμμετάσχουν ενεργά. Η διαδικασία αυτή αποτελεί σημαντικό βήμα διαλόγου και ενίσχυσης της διαφάνειας, διασφαλίζοντας ότι το τελικό θεσμικό πλαίσιο ανταποκρίνεται στις ανάγκες και τις ιδιαιτερότητες του ελληνικού περιβάλλοντος.

Η εθνική νομοθεσία που προέκυψε αντανακλά τα βασικά χαρακτηριστικά και τις απαιτήσεις της Οδηγίας NIS2, περιλαμβάνοντας το πεδίο εφαρμογής, την κατηγοριοποίηση των βασικών και σημαντικών οντοτήτων, τους τομείς και

υποτομείς που υπάγονται σε αυστηρούς κανόνες, τις χρηματικές κυρώσεις καθώς και τον καθορισμό των ρόλων της Εθνικής Συντονιστικής Κεντρικής, των ομάδων CSIRTs και των αρμοδίων αρχών εποπτείας. Επιπλέον, το νομοθετικό πλαίσιο προβλέπει μέτρα διαχείρισης κινδύνων, υποχρεώσεις αναφοράς περιστατικών, μητρώο οντοτήτων και άλλες σημαντικές ρυθμίσεις για τη διασφάλιση της συμμόρφωσης και της αποτελεσματικής εφαρμογής της κυβερνοασφάλειας.

Ιδιαίτερη σημασία στην ελληνική ενσωμάτωση έχει η εισαγωγή του ρόλου του Υπευθύνου Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών, ο οποίος λειτουργεί ως κεντρικό πρόσωπο, υπεύθυνο για την υλοποίηση των μέτρων κυβερνοασφάλειας σε κάθε οντότητα (EY Ελλάδος, 2025). Αναλαμβάνει την εκπαίδευση και ευαισθητοποίηση του προσωπικού, την ενημέρωση της διοίκησης και τη διασφάλιση της συμμόρφωσης με το νομοθετικό πλαίσιο, χωρίς να επηρεάζονται οι αρμοδιότητες των ήδη υφιστάμενων ανεξάρτητων αρχών, όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.

Επιπρόσθετα, η ελληνική νομοθεσία αναθέτει σημαντικό ρόλο στο Υπουργείο Ψηφιακής Διακυβέρνησης για την υποστήριξη της υλοποίησης της Οδηγίας, ενώ η Εθνική Αρχή Κυβερνοασφάλειας αναλαμβάνει την ανάπτυξη εκπαιδευτικών προγραμμάτων, πιστοποιήσεων και λοιπών πρωτοβουλιών με σκοπό την κάλυψη των αυξανόμενων αναγκών σε ειδικούς και υπηρεσίες, στον τομέα της κυβερνοασφάλειας Σύμφωνα με τη Pella (2025). Η εφαρμογή της NIS2 αναμένεται να ενισχύσει σημαντικά τη δομή και τη λειτουργία των συστημάτων ασφάλειας, προωθώντας τη βιώσιμη ανάπτυξη και την ψηφιακή ανθεκτικότητα στην Ελλάδα.

5.2.1. Διαδικασία Ελέγχου Υπαγωγής στην Οδηγία NIS2 από την Εθνική Αρχή Κυβερνοασφάλειας.

Ο έλεγχος υπαγωγής που έχει σχεδιάσει η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με το Υπουργείο Ψηφιακής Διακυβέρνησης, αποτελεί μία δομημένη διαδικασία, μέσω της οποίας οι οργανισμοί και οι επιχειρήσεις μπορούν να αξιολογήσουν αν εμπίπτουν στις Διατάξεις του Νόμου 5160/2024 (Lawspot.gr, 2025). Η διαδικασία αυτή υλοποιείται ως διαδικτυακό εργαλείο στην επίσημη ιστοσελίδα

της Εθνικής Αρχής Κυβερνοασφάλειας, ώστε κάθε ενδιαφερόμενος φορέας να μπορεί να απαντήσει σε μία σειρά ερωτήσεων και να λάβει άμεσα αποτελέσματα, τα οποία θα δείχνουν αν υπάγεται στο πεδίο εφαρμογής της νομοθεσίας, σε ποια δικαιοδοσία και σε ποια κατηγορία μεγέθους και είδους οντότητας ανήκει.

Ο έλεγχος υλοποιείται σε τρεις διαδοχικές φάσεις. Σε πρώτο στάδιο, ο οργανισμός καλείται να απαντήσει σε τρεις βασικές ερωτήσεις οι οποίες αφορούν τον αριθμό των εργαζομένων, το ύψος του ετήσιου κύκλου εργασιών, το συνολικό ύψος του ετήσιου ισολογισμού. Για κάθε ερώτηση παρέχονται προκαθορισμένες επιλογές, και η επιλογή γίνεται με βάση τα πραγματικά στοιχεία του φορέα. Η συνδυαστική αξιολόγηση αυτών των απαντήσεων καθορίζει αν η οντότητα χαρακτηρίζεται ως μικρή, μεσαία ή μεγάλη. Η κατηγοριοποίηση δε βασίζεται μόνο στον αριθμό των εργαζομένων, αλλά, λαμβάνει υπόψη και οικονομικούς δείκτες. Για παράδειγμα, αν μία επιχείρηση διαθέτει 50 έως 249 εργαζομένους και κύκλο εργασιών 10 έως 50 εκατομμύρια ευρώ, κατατάσσεται στις μεσαίες επιχειρήσεις. Ακόμη και αν ο κύκλος εργασιών είναι μικρότερος των 10 εκατομμυρίων, η κατάταξη ως «μεσαία» διατηρείται, εφόσον ο αριθμός των εργαζομένων εμπίπτει στο συγκεκριμένο εύρος. Αν ωστόσο ο κύκλος εργασιών υπερβαίνει τα 50 εκατομμύρια ευρώ και ο ισολογισμός τα 43 εκατομμύρια ευρώ, η επιχείρηση χαρακτηρίζεται ως «μεγάλη», ακόμη και αν ο αριθμός των εργαζομένων είναι μικρότερος. Αυτό το βήμα είναι κρίσιμο, καθώς το μέγεθος της οντότητας επηρεάζει τον τρόπο εφαρμογής των υποχρεώσεων που προβλέπει η NIS2.

Σε δεύτερη φάση, το εργαλείο εξετάζει σε ποιο κράτος μέλος της ΕΕ υπάγεται η επιχείρηση ή ο φορέας. Η υπαγωγή καθορίζεται βάση του τόπου όπου λαμβάνονται οι καθοριστικές αποφάσεις για την κυβερνοασφάλεια του οργανισμού. Τα πιθανά αποτελέσματα είναι η υπαγωγή στην Ελλάδα, η υπαγωγή σε άλλο κράτος-μέλος της ΕΕ και η μη υπαγωγή στην εν λόγω νομοθεσία. Το αποτέλεσμα αυτού του βήματος εξαρτάται σε μεγάλο βαθμό από τις απαντήσεις που δόθηκαν στο πρώτο βήμα, αλλά και από το πού βρίσκεται το κέντρο λήψης αποφάσεων για θέματα ασφαλείας.

Το τρίτο και τελευταίο στάδιο αφορά την ταυτοποίηση του τομέα και υποτομέα στον οποίο δραστηριοποιείται η οντότητα (επιχείρηση, οργανισμός). Η διαδικασία

περιλαμβάνει τρεις διαδοχικές ερωτήσεις. Η πρώτη ερώτηση αφορά την επιλογή πρωτεύοντος τομέα.Ο οργανισμός επιλέγει έναν από τους τομείς που περιλαμβάνονται στη NIS2, όπως είναι για παράδειγμα η ενέργεια, οι μεταφορές, οι ψηφιακές υποδομές κλπ. Εάν ο τομέας δεν περιλαμβάνεται στη λίστα, ο οργανισμός δηλώνει ότι δραστηριοποιείται εκτός αυτών των πεδίων. Για κάθε τομέα υπάρχει μία λίστα υποτομέων. Για παράδειγμα, στον τομέα της ενέργειας υπάρχει ο υποτομέας «Πετρέλαιο». Σε ορισμένες περιπτώσεις, ζητούνται επιπρόσθετες λεπτομέρειες, όπως αν η οντότητα είναι «διαχειριστής αγωγών πετρελαίου», «διαχειριστής παραγωγής πετρελαίου» ή «κεντρικός φορέας διατήρησης αποθεμάτων». Παρά την επιπλέον εξειδίκευση, η βασική κατηγοριοποίηση ως «σημαντική» ή «ουσιώδης» οντότητα παραμένει ίδια, καθώς αυτό καθορίζεται εξ αρχής από τον συνδυασμό τομέα και υποτομέα.

Κατ'αυτόν τον τρόπο, ο έλεγχος υπαγωγής λειτουργεί ως πρακτικός οδηγός, παρέχοντας σαφείς και αυτοματοποιημένες απαντήσεις στους οργανισμούς και τις επιχειρήσεις. Μέσα από τα τρία στάδια, οι επιχειρήσεις και οι λοιποί φορείς μπορούν να διαπιστώσουν αν υπόκεινται στις απαιτήσεις της NIS2 και να προχωρήσουν εγκαίρως στη λήψη απαραίτητων μέτρων κυβερνοασφάλειας.

5.2.2. Ο ρόλος και οι αρμοδιότητες της Εθνικής Αρχής Κυβερνοασφάλειας.

Η Εθνική Αρχή Κυβερνοασφάλειας έχει αναλάβει τον θεσμικό ρόλο της ενιαίας αρμόδιας αρχής για την εφαρμογή της Οδηγίας (ΕΕ) NIS2 στην Ελλάδα, ενώ παράλληλα, εκτελεί και τα καθήκοντα του Εθνικού CSIRT (Computer Security Incident Response Team). Ο ορισμός της ως αρμόδιας αρχής γνωστοποιήθηκε επίσημα στην Ευρωπαϊκή Επιτροπή εντός της προβλεπόμενης προθεσμίας των τριών μηνών από την έναρξη ισχύος της σχετικής νομοθεσίας. Η ίδρυση και λειτουργία της Αρχής δεν αναιρεί ούτε περιορίζει την αρμοδιότητα των υπόλοιπων εθνικών φορέων στον τομέα της κυβερνοασφάλειας. Αντίθετα, ενισχύει τη συνεργασία και τον συντονισμό τους, με στόχο τη συνολική θωράκιση της χώρας έναντι κυβερνοαπειλών (Pella, 2025).

Σύμφωνα με τις προβλέψεις της Οδηγίας, η Αρχή ασκεί κανονιστικές, συντονιστικές, συμβουλευτικές, ελεγκτικές και κυρωτικές αρμοδιότητες. Οι δράσεις της καλύπτουν όλες τις οντότητες που υπάγονται στο πεδίο εφαρμογής της

Οδηγίας και περιλαμβάνουν τον καθορισμό και τη διαχείριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Η Εθνική Στρατηγική Κυβερνοασφάλειας αφορά τη διαμόρφωση στρατηγικών στόχων και προτεραιοτήτων για την κυβερνοασφάλεια, τον προσδιορισμό των απαιτούμενων πόρων και μέτρων πολιτικής, καθώς και των ρυθμιστικών παρεμβάσεων καθώς και τη θέσπιση πλαισίου διακυβέρνησης που καθορίζει ρόλους, αρμοδιότητες και διαδικασίες συνεργασίας μεταξύ όλων των εμπλεκόμενων φορέων, σε εθνικό επίπεδο (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020). Επιπρόσθετα, αφορά τη δημιουργία μηχανισμών εκτίμησης κινδύνων, σχεδίων ετοιμότητας, απόκρισης και αποκατάστασης μετά από περιστατικά παραβίασης δεδομένων ή πληροφοριών, την κατάρτιση λίστας εμπλεκόμενων αρχών και φορέων και την ανάπτυξη πολιτικών ενισχυμένου συντονισμού καθώς και την προώθηση δράσεων ευαισθητοποίησης και εκπαίδευσης τόσο σε επαγγελματίες όσο και στο ευρύ κοινό (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020). Οι δράσεις περιλαμβάνουν επίσης την συμμετοχή σε διεθνείς δομές και πρότυπα μέσω της εκπροσώπησης της Ελλάδας στο EU-CyCLONE (Ευρωπαϊκό Δίκαιο οργανώσεων διασύνδεσης) και, μέσω της συμβολής στη διαμόρφωση διεθνών και εθνικών προτύπων, για την ασφάλεια των πληροφοριών.

Η Εθνική Αρχή Κυβερνοασφάλειας λειτουργεί και ως κεντρικός μηχανισμός αναφοράς περιστατικών κυβερνοασφάλειας. Οι οντότητες που επηρεάζονται μπορούν να υποβάλλουν αναφορές είτε μέσω ειδικής διαδικτυακής φόρμας είτε μέσω ηλεκτρονικού ταχυδρομείου. Σε περιπτώσεις που ένα περιστατικό λαμβάνει νομικές διαστάσεις, η Αρχή καθοδηγεί την οντότητα για την ορθή αναφορά του στις αρμόδιες εισαγγελικές ή αστυνομικές αρχές. Παράλληλα, μπορεί να διαβιβάσει στοιχεία σε άλλες εξειδικευμένες αρχές, για την καλύτερη αντιμετώπιση του περιστατικού, χωρίς όμως να παρεμβαίνει στον τρόπο λειτουργίας τους ή να επηρεάζει ρόλους, όπως ο Υπεύθυνος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

5.3. Συμπεράσματα

Βάσει των, μέχρι πρότινος, εξελίξεων, η ενσωμάτωση της Οδηγίας NIS2 στην Ελλάδα συνιστά ένα καθοριστικό βήμα για την αναβάθμιση της εθνικής κυβερνοασφάλειας και την εναρμόνιση με τα αυστηρότερα ευρωπαϊκά πρότυπα. Με την ανάληψη ρόλου από την Εθνική Αρχή Κυβερνοασφάλειας ως κεντρικού συντονιστή, διασφαλίζεται η ύπαρξη ενός ενιαίου μηχανισμού εποπτείας, ανταπόκρισης σε περιστατικά και διαχείρισης κρίσεων. Επιπρόσθετα, η συγκεντρωτική εποπτεία ενισχύει την παρακολούθηση και αξιολόγηση των κινδύνων, την ανάπτυξη συνεκτικών πολιτικών ασφαλείας και τη λήψη έγκαιρων μέτρων πρόληψης και αντιμετώπισης απειλών, ενισχύοντας την ανθεκτικότητα του ψηφιακού οικοσυστήματος της χώρας.

6. ΚΕΦΑΛΑΙΟ ΕΚΤΟ

ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΛΥΣΗ ΜΕ ΔΙΕΘΝΕΙΣ ΡΥΘΜΙΣΤΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ.

6.1. *Κυβερνοασφάλεια στις ΗΠΑ (CISA).*

Κάθε κράτος αναπτύσσεις και εφαρμόζει εθνικές στρατηγικές κυβερνοασφάλειας, οι οποίες, συνήθως, περιλαμβάνουν μηχανισμούς για τον εντοπισμό, το πλάνο δράσης και την ανάλυση και καταπολέμηση των κυβερνοεπιθέσεων. Στις Η.Π.Α., η Cybersecurity and Infrastructure Security Agency (CISA) (Lawspot.gr, 2024) η οποία είναι μία υπηρεσία του Υπουργείου Εσωτερικής Ασφάλειας των ΗΠΑ, ιδρυθείσα το 2018, έχει ως σκοπό την ενίσχυση της κυβερνοασφάλειας και τη προστασίας των κρίσιμων υποδομών της χώρας. Η υπηρεσία φροντίζει για την αποτροπή και ανίχνευση κυβερνοεπιθέσεων όπως επιθέσεις ransomware και, παρέχει συμβουλευτική καθοδήγηση και υποστήριξη σε κυβερνητικούς-δημόσιους και ιδιωτικούς φορείς, για την προστασία των δεδομένων και των υποδομών τους. Συνεργάζεται, επιπλέον, με διεθνείς οργανισμούς στο πλαίσιο ανάπτυξης κοινών στρατηγικών για την ενίσχυση της κυβερνοασφάλειας. Ο οργανισμός είναι υπεύθυνος για την ανάπτυξη στρατηγικών και πολιτικών που ενισχύουν την κυβερνοασφάλεια, ενώ παρέχει εργαλεία και υπηρεσίες για την παρακολούθηση και τη διαχείριση των κυβερνο κινδύνων.

Το Πρόγραμμα Continuous Diagnostics and Mitigation (CDM) (Lawspot.gr, 2024) της CISA βοηθά τις ομοσπονδιακές υπηρεσίες να παρακολουθούν και να προστατεύουν τα συστήματά τους σε πραγματικό χρόνο. Η CISA, επιπλέον, αναπτύσσει και πρωθεί τεχνολογίες για την αξιολόγηση των κινδύνων και την προστασία των κρίσιμων υποδομών, όπως οι τομείς της ενέργειας, των τηλεπικοινωνιών και των χρηματοπιστωτικών υπηρεσιών.

Η CISA διαδραματίζει κεντρικό ρόλο στην ενίσχυση της κυβερνοασφάλειας των Η.Π.Α., συντονίζοντας εθνικές και διεθνείς προσπάθειες και παρέχοντας καθοδήγηση και πόρους για την προστασία των υποδομών κρίσιμης σημασίας. Μέσω αυτής της δράσης, συμβάλλει στη δημιουργία ενός ασφαλέστερου κυβερνοχώρου, προστατεύοντας την εθνική ασφάλεια και την οικονομία των Η.Π.Α.

6.2. Πολιτικές κυβερνοασφάλειας στην Ασία: Κίνα-Ιαπωνία.

Η Ασία αποτελεί έναν πολύ δυναμικά αναπτυσσόμενο χώρο, όσον αφορά τον τομέα της κυβερνοασφάλειας, με την Κίνα και την Ιαπωνία να έχουν υιοθετήσει διαφορετικές στρατηγικές, γεγονός το οποίο αναδεικνύει και τα ιδιαίτερα πολιτικά, οικονομικά και κοινωνικά τους χαρακτηριστικά.

6.2.1. ΚΙΝΑ

Η Κίνα ακολουθεί ένα σύστημα κυβερνοασφάλειας το οποίο προσφέρει ολοένα και μεγαλύτερη έμφαση στην κρατική κυριαρχία στον κυβερνοχώρο και στα δεδομένα, το οποίο ενσωματώνεται στην ευρύτερη στρατηγική της για «κυριαρχία στον κυβερνοχώρο». Παράλληλα, υιοθετεί πληθώρα κανονισμών και πολιτικών, ενώ προωθεί την ανάπτυξη εθνικών προτύπων για την κυβερνοασφάλεια και την προστασία των δεδομένων. Τα δικαιώματα ιδιωτικότητας και οι αρχές ασφαλείας έχουν θεμελιωθεί στο Σύνταγμα της Λαϊκής Δημοκρατίας της Κίνας, στον Αστικό Κώδικα και στον Νόμο για την Εθνική Ασφάλεια και στηρίζεται σε τρεις βασικούς πυλώνες: Τον Νόμο για την Κυβερνοασφάλεια (CSL), τον Νόμο για την Ασφάλεια Δεδομένων (DSL) και τον Νόμο για την Προστασία των Προσωπικών Δεδομένων (PIPL). Το 2017 τέθηκε σε ισχύ ο «Cybersecurity Law of the People's Republic of China»(DigiChina, 2018). Το νομοθετικό αυτό κείμενο εισήγαγε αυστηρές απαιτήσεις, οι οποίες αφορούσαν τον τρόπο αποθήκευσης των δεδομένων εντός της κινεζικής επικράτειας, τον έλεγχο των κρίσιμων υποδομών του τομέα της πληροφορικής και της ασφάλειας συστημάτων και την απαίτηση για ενισχυμένο κρατικό έλεγχο τόσο στην πρόσβαση όσο και τη διαχείριση των δεδομένων. Η προσέγγιση της Κινεζικής Δημοκρατίας, βέβαια ενισχύει την εθνική ασφάλεια, αλλά, ταυτόχρονα εγείρει ζητήματα τα οποία σχετίζονται με την ελευθερία πληροφόρησης και τα ανθρώπινα δικαιώματα.

Παράλληλα, η κυβέρνηση της Κινεζικής Δημοκρατίας προέβη στην ίδρυση ρυθμιστικών αρχών κυβερνοασφάλειας, με κυριότερη τη «Cyberspace Administration of China» (CAC) (DigiChina, 2018). Η ρυθμιστική αυτή αρχή διαδραματίζει κεντρικό ρόλο στην εποπτεία του διαδικτύου και τη διαμόρφωση πολιτικών ασφαλείας. Προσφάτως, μάλιστα δημοσίευσε αποτελέσματα ελέγχου κυβερνοασφάλειας, ο οποίος είχε διεξαχθεί στην εταιρεία Didi, επιβάλλοντας πρόστιμο 1,2 δισ. Δολαρίων. Ο έλεγχος

διεξήχθη πριν τεθούν σε ισχύ οι αναθεωρημένες διατάξεις για τον έλεγχο της κυβερνοασφάλειας. Με την αναθεώρηση επιτεύχθηκε διεύρυνση του πεδίου εφαρμογής και στους φορείς εκμετάλλευσης διαδικτυακών πλατφορμών, οι οποίοι επιδιώκουν την καταχώρηση σε χρηματιστήρια του εξωτερικού. Οι φορείς αυτοί επεξεργάζονται δεδομένα περισσότερων του ενός εκατομμυρίου χρηστών. Ο έλεγχος επεκτείνεται επίσης σε φορείς προμήθειας δικτυακών προϊόντων.

Η σύγχρονη κινέζικη νομική τάξη στον τομέα της κυβερνοασφάλειας και της προστασίας των προσωπικών δεδομένων προβλέπει αυστηρές κυρώσεις, σε περίπτωση παραβιάσεων. Οι νομοθεσίες, όπως ο Νόμος για την Προστασία των Προσωπικών Δεδομένων (PIPL), θεσπίζουν βαρύτατες διοικητικές, ποινικές και αστικές κυρώσεις, συμπεριλαμβανομένης τόσο της κατάσχεσης παράνομων εσόδων όσο και την επιβολή σημαντικών χρηματικών προστίμων, τα οποία μπορούν να φτάσουν και το 5% του ετήσιου κύκλου εργασιών μιας επιχείρησης. Εξίσου σοβαρές είναι οι κυρώσεις που προβλέπονται για τα άτομα τα οποία έχουν άμεση ευθύνη, τα οποία μπορεί να αντιμετωπίσουν προσωπικά πρόστιμα. Το πρόσφατο παράδειγμα του προστίμου, το οποίο επιβλήθηκε στην εταιρεία DiDi αναδεικνύει την αυξημένη αυστηρότητα στην εφαρμογή των διατάξεων αυτών (DigiChina, 2018).

Επιπλέον, έχουν προταθεί περαιτέρω τροποποιήσεις στο Νόμο για την Κυβερνοασφάλεια (CSL), οι οποίες προβλέπουν ακόμη βαρύτερες ποινές, γεγονός το οποίο καταδεικνύει την πρόθεση των κινεζικών αρχών να ενισχύσουν την εποπτεία και την επιβολή του νόμου. Οι εισαγγελικές και δικαστικές αρχές δείχνουν αυξανόμενο ενδιαφέρον για την προστασία των προσωπικών δεδομένων και την καταπολέμηση των εγκλημάτων, τα οποία σχετίζονται με την επεξεργασία δεδομένων, τόσο στο πλαίσιο αστικών όσο και ποινικών υποθέσεων. Η δυναμική αυτή επιβεβαιώνει τη στροφή της Κίνας προς ένα αυστηρότερο ρυθμιστικό πλαίσιο, στον τομέα της ψηφιακής διακυβέρνησης.

6.2.2. ΙΑΠΩΝΙΑ

Η δράση της Ιαπωνίας, στον χώρο της Κυβερνοασφάλειας, ως κρίσιμου τομέα, έχει εξελιχθεί σημαντικά από το 2000. Τη χρονιά αυτή, η ιαπωνική κυβέρνηση υιοθέτησε το πρώτο Σχέδιο Δράσης για την καθιέρωση Προστασίας των Πληροφοριακών Συστημάτων. Έκτοτε, το κράτος έχει προβεί στην υιοθέτηση μιας σειράς πρωτοβουλιών

ενίσχυσης της άμυνας στον κυβερνοχώρο, όπως το Ειδικό Σχέδιο Δράσης κατά της Κυβερνοτρομοκρατίας και την Ειδική Στρατηγική για την Ασφάλεια Πληροφοριών, με έμφαση στην πρόληψη των κυβερνοεγκλημάτων και την θωράκιση των υποδομών(Basu, 2024). Το 2014 το νομικό πλαίσιο ενισχύθηκε περαιτέρω, με την ψήφιση του Βασικού Νόμου για την Κυβερνοασφάλεια, το οποίο οδήγησε στη σύσταση της Στρατηγικής Έδρας για την Κυβερνοασφάλεια και του Συμβουλίου Κυβερνοασφάλειας. Το 2015, η νέα Στρατηγική Κυβερνοασφάλειας σηματοδότησε την ανάδειξη της κυβερνοασφάλειας ως αυτόνομου τομέα, καθοριστικού για την τεχνολογική πρόοδο και τις εξωτερικές και αμυντικές πολιτικές της χώρας (Basu, 2024).

Η στρατηγική την οποία ακολουθεί το κράτος δίνει έμφαση στην έρευνα και την ανάπτυξη, για την πρόληψη και αντιμετώπιση της αυξανόμενης πολυπλοκότητας των κυβερνοαπειλών, προωθώντας, παράλληλα, τη συνεργασία με διάφορους τομείς της οικονομίας για την ενίσχυση της τεχνολογίας ασφαλείας σε δίκτυα, υλικό και λογισμικό, ιδίως λόγω της εξάπλωσης του Διαδικτύου των Πραγμάτων (IoT).Η Ιαπωνία δίνει έμφαση στην ανάπτυξη αυτόνομων δυνατοτήτων στον κυβερνοχώρο, ενισχύοντας τη διεθνή συνεργασία και προάγοντας τη διεπιστημονική έρευνα σε νομικό, πολιτικό και τεχνολογικό επίπεδο. Ο συντονιστικός ρόλος του Συμβουλίου Επιστήμης, Τεχνολογίας και Καινοτομίας έχει αποδειχθεί κομβικός στην ενίσχυση της συνεργασίας μεταξύ βιομηχανίας, ακαδημαϊκής κοινότητας και δημόσιου τομέα.

Για την επίτευξη των στόχων της, η Ιαπωνία αύξησε διαρκώς τον αμυντικό της προϋπολογισμό, με το 2020 να επενδύει σημαντικά ποσά στην ανάπτυξη τεχνητής νοημοσύνης για την ανίχνευση κυβερνοαπειλών και στην ενίσχυση της Ομάδας Κυβερνοάμυνας. Παράλληλα, προχώρησε σε αναβάθμιση των δυνατοτήτων ηλεκτρονικού πολέμου, αναγνωρίζοντας τη στρατηγική σημασία του ηλεκτρομαγνητικού πεδίου.

Παρά τις σημαντικές επιδόσεις, όπως η 12η θέση στην Παγκόσμια Κατάταξη Κυβερνοασφάλειας του 2017, διαπιστώνονται ακόμη περιθώρια βελτίωσης στην κυβερνοάμυνα. Σημαντικό ορόσημο αποτέλεσε η έγκριση, το 2022, της νέας Εθνικής Στρατηγικής Ασφαλείας και του Προγράμματος Ενίσχυσης Άμυνας, που προβλέπουν την αύξηση των αμυντικών δαπανών, την ενίσχυση των δυνατοτήτων στον κυβερνοχώρο και την υιοθέτηση ενεργητικών μέτρων άμυνας (Basu, 2024).

Επιπλέον, η Ιαπωνία αξιοποιεί την τεχνητή νοημοσύνη για την ενίσχυση της ανάλυσης πληροφοριών και την εκπαίδευση κυβερνοδυναμικού, με το Εθνικό Κέντρο Ετοιμότητας και Στρατηγικής για την Κυβερνοασφάλεια να αναλαμβάνει κεντρικό ρόλο στον συντονισμό των δράσεων με τις Δυνάμεις Αυτοάμυνας και την αστυνομία.

Στο διεθνές πεδίο, η Ιαπωνία προωθεί ένα δίκτυο κυβερνοάμυνας στην περιφέρεια Ινδο-Ειρηνικού, επενδύοντας σε συνεργασίες με χώρες της Νότιας και Νοτιοανατολικής Ασίας και ενισχύοντας τις σχέσεις της με Quad, ASEAN και NATO. Αυτές οι πρωτοβουλίες αποτυπώνουν τη στρατηγική της επιδίωξη να αναδειχθεί σε κορυφαία δύναμη στον τομέα της κυβερνοασφάλειας (Basu, 2024).

7. ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ-ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ

7.1. ΖΗΤΗΜΑΤΑ ΚΑΙ ΔΥΣΧΕΡΕΙΕΣ ΣΤΗΝ ΕΝΑΡΜΟΝΙΣΗ ΜΕ ΤΟ ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

7.1.1. Προκλήσεις ως προς την εφαρμογή των Οδηγιών και των Κανονισμών.

Η συμμόρφωση με διεθνείς και εθνικές οδηγίες και Κανονισμούς, όπως οι Οδηγίες NIS2, για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων, και η απαιτήσεις του DORA για την ανθεκτικότητα των ψηφιακών υποδομών, καθιστούν αναγκαία τη δημιουργία ενός ολοκληρωμένου συστήματος ασφαλείας. Οι οργανισμοί καλούνται να αναπτύξουν και να υλοποιήσουν στρατηγικές που να διασφαλίζουν την προστασία των δεδομένων και την ανθεκτικότητα των συστημάτων τους απέναντι σε κυβερνοεπιθέσεις και άλλες απειλές. Η συμμόρφωση με αυτούς τους κανονισμούς και η εφαρμογή των πολιτικών ασφαλείας αναδεικνύει τη σημασία της διαφάνειας, της συνεχούς παρακολούθησης και της αναγκαίας εκπαίδευσης του προσωπικού, καθώς και της υιοθέτησης τεχνολογικών λύσεων οι οποίες ανταποκρίνονται στις σύγχρονες απαιτήσεις ασφαλείας(Martino and Gamal, 2023). Η υιοθέτηση των Κανονισμών στο πλαίσιο της Κυβερνοασφάλειας και της Κυβερνοανθεκτικότητας συχνά, συνοδεύεται από ποικίλες προκλήσεις, τόσο σε πολιτικό όσο και σε τεχνικό επίπεδο. Κρίσιμο ζήτημα αποτελεί η εγκαθίδρυση ενός κοινού πλαισίου δραστηριοποίησης και νομοθεσίας στα κράτη-μέλη, τα οποία παρουσιάζουν διαφορές στην κουλτούρα και τον τρόπο ενσωμάτωσης της εκάστοτε ευρωπαϊκής νομοθεσίας (Martino and Gamal, 2023). Έτσι, θα πρέπει να βρεθεί η σωστή ισορροπία ανάμεσα στην ομαλή και πανευρωπαϊκή ενσωμάτωση των κανονισμών αυτών και στην διατήρηση των ιδιαίτερων χαρακτηριστικών κάθε κράτους-μέλους. Μία ακόμη πρόκληση παρατηρείται ως προς την επικοινωνία μεταξύ κρατών-μελών, οργανισμών και μεταξύ τους, σε περιπτώσεις κυβερνο-απειλών και λοιπών ζητημάτων. Ειδικότερα, λοιπόν, ενώ έχουν γίνει σημαντικά βήματα για την καταπολέμηση του κυβερνοεγκλήματος και την προστασία κρίσιμων υποδομών, υπάρχει ακόμη ανάγκη για μεγαλύτερη ανταλλαγή πληροφοριών

τόσο μεταξύ των κρατών-μελών όσο μεταξύ φορέων του ιδιωτικού και του δημόσιου τομέα. Το πρόβλημα αυτό έγκειται στην απροθυμία για κοινοποίηση των περιστατικών κυβερνοασφάλειας, φαινόμενο το οποίο παρατηρείται σε πανευρωπαϊκό επίπεδο και θα πρέπει να ξεπεραστεί ώστε να ξεπεραστούν και τα προβλήματα επικοινωνίας και ενημέρωσης για ζητήματα κυβερνοασφάλειας, γεγονός το οποίο οδήγησε και στην ψήφιση της Οδηγίας NIS2 (Martino and Gamal, 2023).

7.1.2. Τεχνολογικές προκλήσεις.

Η αλματώδης πρόοδος της τεχνολογίας, με την ανάπτυξη της τεχνητής νοημοσύνης, τα συστήματα cloud και το Internet of things, οδηγεί στην εμφάνιση πληθώρας νέων κυβερνοαπειλών. Οι επιχειρήσεις και οι οργανισμοί καλούνται να αντιμετωπίσουν απειλές οι οποίες εξελίσσονται σε τέτοιο ρυθμό, ώστε τα παραδοσιακά μέτρα ασφαλείας καθίστανται σταδιακά ανεπαρκή. Έτσι, παρόλο που οι νέες τεχνολογίες παρέχουν ευκαιρίες για ενίσχυση του τομέα ασφάλειας, οι διαρκώς μεταβαλλόμενες και εξελισσόμενες απειλές απαιτούν συνεχιζόμενη προσαρμογή και προνοητικότητα από τους οργανισμούς και τα κράτη-μέλη.

Το Internet of Things, με τη δυνατότητα σύνδεσης εκατομμυρίων συσκευών στο διαδίκτυο, έχει φέρει επανάσταση στο χώρο της τεχνολογίας. Ωστόσο, αυτή η εκρηκτική αύξηση των συνδεδεμένων συσκευών δημιουργεί σημαντικές προκλήσεις κυβερνοασφάλειας. Οι συσκευές IoT, πολλές από τις οποίες δεν διαθέτουν την απαιτούμενη ασφάλεια ή τη δυνατότητα ενημέρωσης των πολιτικών ασφαλείας, καθιστούν τα δίκτυα πιο ευάλωτα σε κυβερνοεπιθέσεις. Επιθέσεις όπως οι DDoS (Distributed Denial of Service) μπορούν να αξιοποιήσουν τα αδύνατα σημεία των συσκευών IoT, επηρεάζοντας κρίσιμες υποδομές. Επομένως, η Κυβερνοασφάλεια θα πρέπει να εστιάζει στην ασφάλεια των ως άνω συσκευών, η οποία επιτυγχάνεται και με την ενσωμάτωσή τους σε ασφαλή δίκτυα, προσφέροντας μέτρα προστασίας όπως είναι η κρυπτογράφηση, η ταυτοποίηση και οι ενημερώσεις ασφαλείας (Martino and Gamal, 2023).

Η μετάβαση σε cloud computing έχει προσφέρει πολλαπλά οφέλη όπως η κλιμάκωση της υποδομής και ευκολία πρόσβασης. Βέβαια, η λύση αυτή της αποθήκευση δεδομένων και υπηρεσιών μέσω τρίτων παρόχων εντείνει τα ζητήματα περί κυβερνοασφάλειας καθώς η ασφάλεια εξαρτάται πλέον από το επίπεδο

προστασίας και μέτρων τα οποία έχουν λάβει οι πάροχοι αυτοί. Η χρήση του cloud δημιουργεί πιθανούς κινδύνους , όπως η διαρροή δεδομένων ή η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα. Η προστασία της κυβερνοασφάλειας σε cloud περιβάλλοντα απαιτεί κρυπτογράφηση δεδομένων, ισχυρή αυθεντικοποίηση χρηστών και τακτική παρακολούθηση συστημάτων (Martino and Gamal, 2023).

Παράλληλα, η τεχνητή νοημοσύνη και η μηχανική μάθηση έχουν αναδειχθεί σε κύρια εργαλεία για την πρόληψη και την ανίχνευση κυβερνοαπειλών συμβάλλοντας ουσιαστικά στην ενίσχυση της κυβερνοασφάλειας. Παρά τα οφέλη τους, οι τεχνολογίες αυτές ενέχουν, ταυτοχρόνως, σημαντικούς κινδύνους καθώς αποτελούν και οι ίδιες δυνητικούς στόχους κακόβουλης εκμετάλλευσης. Συγκεκριμένα, οι κυβερνοεγκληματίες δύναται να αξιοποιήσουν την τεχνητή νοημοσύνη για την ανάπτυξη αυτοματοποιημένων και ιδιαίτερα εξελιγμένων μηχανισμών, γεγονός το οποίο αυξάνει και την πολυπλοκότητα των απειλών (Brundage et al., 2018). Δεδομένου ότι τα ευφυή συστήματα μπορούν να αξιοποιηθούν για ποικίλους σκοπούς, είναι πιθανό ότι στο μέλλον θα αναπτυχθούν ή θα παραβιαστούν συστήματα υψηλών δυνατοτήτων, τα οποία θα επιτρέπουν την εισαγωγή νέων, ενδεχομένως επικίνδυνων στόχων. Κατά συνέπεια, τα συστήματα που σχεδιάζονται για την ενίσχυση της ασφάλειας ενδέχεται, παράλληλα, να δημιουργήσουν και νέες ευπάθειες, υπονομεύοντας έτσι την κυβερνοασφάλεια. Έτσι, κρίνεται απαραίτητη η έγκαιρη λήψη μέτρων πρόληψης και προετοιμασίας, προτού οι δυνατότητες κακόβουλης αξιοποίησης δεδομένων καταστούν τεχνικά εφικτές. Στο πλαίσιο αυτό, ερευνητές και υπεύθυνοι χάραξης πολιτικής οφείλουν να αντλήσουν εμπειρία από άλλους τομείς, με μακρά παράδοση στη διαχείριση κινδύνων, ώστε να διαμορφώσουν αποτελεσματικά εργαλεία και κανονιστικά πλαίσια για την ασφαλή εφαρμογή της τεχνητής νοημοσύνης (Brundage et al., 2018).

7.1.3. Επιπτώσεις στις επιχειρήσεις.

Οι επιδράσεις της πολιτικής κυβερνοασφάλειας στις επιχειρήσεις και τους πολίτες κρίνονται καθοριστικές για την ενίσχυση της εμπιστοσύνης και της σταθερότητας στον ψηφιακό κόσμο. Η εφαρμογή αυτών των πολιτικών έχει ευρείες συνέπειες, τόσο για την στρατηγική των οργανισμών όσο και για την καθημερινότητα των πολιτών. Η συμμόρφωση των οργανισμών με τα πρότυπα και τις Οδηγίες στο πλαίσιο της

Κυβερνοασφάλειας, όπως είναι η συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR) καθώς και με τον Κανονισμό για την Ανθεκτικότητα των ψηφιακών Υποδομών (DORA), επιβάλλει την υιοθέτηση αυστηρών πολιτικών ασφαλείας και την ενσωμάτωση προηγμένων τεχνολογικών λύσεων. Αν και η συμμόρφωση αυτή συνεπάγεται σημαντικό οικονομικό κόστος, κυρίως λόγω των αναγκαίων επενδύσεων στην τεχνολογία και την εκπαίδευση του προσωπικού, εντούτοις, συμβάλλει στη μείωση του κινδύνου κυβερνοεπιθέσεων, αποτρέπει την απώλεια δεδομένων καθώς και την παράνομη πρόσβαση σε αυτά. Παράλληλα, η επιτυχής εφαρμογή των κανονιστικών πλαισίων ενισχύει την εμπιστοσύνη των καταναλωτών και, συνεπώς, τη φήμη της επιχείρησης στην αγορά, δημιουργώντας ανταγωνιστικό πλεονέκτημα έναντι των άλλων επιχειρήσεων (ENISA, 2024).

Η αυξημένη συμμόρφωση με κανονισμούς και πολιτικές κυβερνοασφάλειας συνεπάγεται σημαντικές, άμεσες και έμμεσες οικονομικές επιπτώσεις, οι οποίες διαμορφώνουν την επιχειρηματική στρατηγική και ανταγωνιστικότητα, σε ευρωπαϊκό και διεθνές επίπεδο. Ειδικότερα, οι επιχειρήσεις καλούνται να επενδύσουν σε νέες τεχνολογικές λύσεις, στην αναβάθμιση συστημάτων πληροφορικής, στην πρόσληψη εξειδικευμένου προσωπικού, σε προγράμματα εκπαίδευσης και κατάρτισης, καθώς και στη διενέργεια εσωτερικών και εξωτερικών ελέγχων για τη συμμόρφωση με τις ισχύουσες Οδηγίες και τους Κανονισμούς. Αυτές οι επενδύσεις αποτελούν προϋπόθεση για την κυβερνοανθεκτικότητα των οργανισμών.

Η διαχείριση περιστατικών παραβίασης δεδομένων συνεπάγεται και σημαντικές δαπάνες ως προς τη διαδικασία διαχείρισης περιστατικών, τις νομικές συνέπειες και την απώλεια της εμπιστοσύνης των πελατών. Επιπλέον, όπως έχει προαναφερθεί, οι επιχειρήσεις και οι λοιποί φορείς εκτίθενται σε διαρκείς ελέγχους οι οποίοι μπορεί να επιφέρουν και την επιβολή μεγάλων προστίμων, προκαλώντας σημαντική οικονομική ζημία. Παράλληλα, ο ENISA, στην ετήσια έκθεσή του (ENISA, 2024), τονίζει ότι οι κυβερνοπιθέσεις γίνονται ολοένα και πιο εξελιγμένες και στοχευμένες, με αποτέλεσμα το κόστος αποκατάστασης να αυξάνει σημαντικά, ειδικά για τις μικρομεσαίες επιχειρήσεις οι οποίες,συχνά, στερούνται επαρκών πόρων για ασφάλεια.

Σε παγκόσμια κλίμακα, το συνολικό κόστος του κυβερνοεγκλήματος ανήλθε σε περίπου 8 τρισεκατομμύρια δολάρια το 2023, ενώ εκτιμάται ότι, μέσα στο 2025, θα

φτάσει τα 10,5 τρισεκατομμύρια δολάρια Cybersecurity Ventures (2023) *Cybercrime to cost the world $8 trillion annually in 2023*.. Αν το κυβερνοέγκλημα θεωρηθεί ως «οικονομία» θα αποτελούσε την τρίτη μεγαλύτερη στον κόσμο μετά τις Η.Π.Α. και την Κίνα Cybersecurity Ventures (2023) *Cybercrime to cost the world $8 trillion annually in 2023*. Η εκτίμηση αυτή αναδεικνύει το μέγεθος της απειλής και την κρισιμότητά της σε σχέση με άλλες μορφές οργανωμένου εγκλήματος, αλλά και με παγκόσμιες προκλήσεις όπως είναι η κλιματική αλλαγή.

Επομένως, οι οικονομικές επιπτώσεις του κυβερνοεγκλήματος δεν περιορίζονται μόνο σε επίπεδο επιχειρήσεων αλλά, επεκτείνονται και στις εθνικές οικονομίες και κοινωνίες, υπογραμμίζοντας ότι η κυβερνοασφάλεια αποτελεί αναγκαία συνθήκη για την πρόοδο και τη σταθερότητα της ψηφιακής οικονομίας.

7.1.4.Επιπτώσεις στους πολίτες.

Από την πλευρά των πολιτών, η εφαρμογή πολιτικών κυβερνοασφάλειας ενισχύει την προστασία των προσωπικών τους δεδομένων και διασφαλίζει την ιδιωτικότητα τους στον ψηφιακό κόσμο. Η συμμόρφωση των οργανισμών με τα ισχύοντα πρότυπα προστασίας δεδομένων επιτρέπει στους πολίτες να αλληλεπιδρούν με τις ψηφιακές υπηρεσίες με αυξημένη ασφάλεια, μειώνοντας τον κίνδυνο αποστολής των προσωπικών τους δεδομένων σε μη εξουσιοδοτημένα άτομα και φορείς.

Η διασφάλιση της εμπιστοσύνης των πολιτών στην ψηφιακή τεχνολογία αποτελεί αναγκαία προϋπόθεση για την ομαλή λειτουργία της κοινωνίας της πληροφορίας. Βέβαια, ο μεγάλος όγκος πληροφοριών, η τεχνολογική πολυπλοκότητα και η ταχύτητα των εξελίξεων δημιουργούν ένα κενό κατανόησης και αποδοχής (Martino and Gamal, 2023). Σε αυτό το πλαίσιο, η ενημέρωση και η ευαισθητοποίηση των πολιτών σε θέματα κυβερνοασφάλειας αποκτούν στρατηγική σημασία. Πρωτοβουλίες όπως αποτελούν οι εκπαιδευτικές εκστρατείες και τα σεμινάρια, στο πλαίσιο μίας δια βίου μαθήσεως, έχουν ως στόχο να καταστήσουν τους πολίτες όχι μόνο χρήστες της τεχνολογίας αλλά και συνειδητούς και υπεύθυνους ψηφιακούς πολίτες (European Commission, 2018).

7.2. ΕΠΙΛΟΓΟΣ

Η Ένωση, μέσω των θεσμικών της πρωτοβουλιών, ενθαρρύνει δράσεις, οι οποίες στοχεύουν στην καλλιέργεια μία ψηφιακής συνείδησης και γνώσης , στην εκπαίδευση

των πολιτών καθώς και στη διάδοση σαφών οδηγιών για ασφαλέστερη πλοήγηση στο Διαδίκτυο. Ο ENISA επιτελεί, επίσης σημαντικό ρόλο σε αυτό το πεδίο, παράγοντας εκπαιδευτικό υλικό, εργαλεία αυτοαξιολόγησης και καμπάνιες ευαισθητοποίησης (European Commission, 2018). Κατ'αυτόν τον τρόπο, επιτυγχάνεται η καλλιέργεια μιας κουλτούρας ασφάλειας και η ανάγκη για ενεργό συμμετοχή στην δόμηση ενός ανθεκτικού και ασφαλούς κυβερνοχώρου. Η επένδυση στην εκπαίδευση και την ευαισθητοποίηση των χρηστών αποτελεί αναγκαίο συμπλήρωμα κάθε στρατηγικής κυβερνοασφάλειας.

Η ΕΕ, στην προσπάθεια εναρμόνισης των κανονισμών για την κυβερνοασφάλεια, κατόρθωσε να δημιουργήσει ένα, ένα σύστημα δηλαδή το οποίο εστιάζει στη θέσπιση ισχυρών κανονιστικών πλαισίων, όπως είναι η Οδηγία NIS2 και ο GDPR και στην προώθηση της διακρατικής συνεργασίας μεταξύ των κρατών-μελών. Το μοντέλο της ΕΕ δίνει έμφαση στην προστασία των θεμελιωδών δικαιωμάτων των ανθρώπων, όπως είναι το δικαίωμα στην ιδιωτικότητα, στη διαφάνεια και στη δημιουργία διεθνών προτύπων που προάγουν μία ηθική και υπεύθυνη χρήση των τεχνολογιών. Αξιοσημείωτη θεωρείται, επίσης η δημοκρατική και ανθρωποκεντρική διάσταση της ευρωπαϊκής πολιτικής για την κυβερνοασφάλεια. Η Ένωση δίνει ιδιαίτερη έμφαση στην προστασία των θεμελιωδών δικαιωμάτων και την ενίσχυση της διαφάνειας, σε αντίθεση με άλλες, περισσότερο αυταρχικές προσεγγίσεις, όπως εκείνες της Κίνας, στις οποίες ο τομέας της κυβερνοασφάλειας εντάσσεται, κυρίως στο ευρύτερο πλαίσιο της εθνικής ασφάλειας, με θεμελιώδη δικαιώματα όπως η ιδιωτικότητα, να υποχωρούν μπροστά στην ασφάλεια.

Στον αντίποδα, η Ευρωπαϊκή Ένωση αντιμετωπίζει σημαντικές προκλήσεις , όπως είναι η βραδύτητα στην λήψη των αποφάσεων, λόγω των διαφοροποιημένων εθνικών συμφερόντων κάθε κράτους-μέλους, και ο περιορισμένος βαθμός ενοποίησης των επιμέρους εθνικών υποδομών κυβερνοασφάλειας. Επιπλέον, σε σύγκριση με άλλες μεγάλες δυνάμεις, παρουσιάζει σχετικά χαμηλά επίπεδα επενδύσεων σε τομείς όπως η κυβερνοάμυνα, η τεχνητή νοημοσύνη και οι επιθετικές επιχειρησιακές δυνατότητες στον κυβερνοχώρο.

Την ίδια στιγμή, κυβερνήσεις όπως αυτή των Η.Π.Α. και της Κίνας διαθέτουν ανεπτυγμένες στρατιωτικές δυνατότητες στον κυβερνοχώρο και σημαντική

τεχνολογική υπεροχή, αν και υφίστανται, συχνά κριτική για ανεπαρκείς μηχανισμούς λογοδοσίας. Η Κίνα εφαρμόζει ένα κεντρικά ελεγχόμενο μοντέλο, το οποίο εστιάζει στην «κυβερνο κυριαρχία», εξασφαλίζοντας εκτεταμένους κρατικούς πόρους αλλά σε βάρος των ατομικών ελευθεριών και με αυξημένη διεθνή καχυποψία. Τέλος, η Ιαπωνία υιοθετεί μία προσέγγιση η οποία συνδυάζει την ενίσχυση της άμυνας με τη διεθνή συνεργασία, επενδύοντας σε έρευνα και τεχνητή νοημοσύνη, αν και ακόμα διατηρεί περιορισμένη αυτονομία στον τομέα της κυβερνοάμυνας.

Συνοψίζοντας, η Ένωση διαμορφώνει ολοένα και πιο ώριμο και ρυθμιστικά προοδευτικό σύστημα κυβερνοασφάλειας, εστιάζοντας στην δημιουργία ενός εναρμονισμένου και ολιστικού πλαισίου κυβερνοανθεκτικότας, με σεβασμό στην προστασία κρίσιμων θεμελιωδών δικαιωμάτων. Συνολικά, η ΕΕ αναδεικνύεται σε παγκόσμιο πρότυπο θεσμικής και ρυθμιστικής διαχείρισης της κυβερνοασφάλειας, αλλά απαιτείται περαιτέρω ενίσχυση της επιχειρησιακής της ικανότητας και επιτάχυνση των διαδικασιών λήψης αποφάσεων, ώστε να ανταποκριθεί αποτελεσματικοτερα στο ιδιαίτερα ανταγωνιστικό και μεταβαλλόμενο διεθνές τεχνολογικό περιβάλλον.

Η παρούσα διπλωματική εργασία, αποπειράθηκε να προσεγγίσει ένα σύνθετο και πολυδιάστατο ζήτημα, αυτό της κυβερνοασφάλειας, μέσα από ένα ευρωπαϊκό θεσμικό και ρυθμιστικό πρίσμα. Έμφαση δόθηκε στην χρονική πορεία, από τα πρώτα εγχειρήματα για την εδραίωση μίας εναρμονισμένης πολιτικής έως την σύγχρονη συνεκτική πολιτική της ψηφιακής ανθεκτικότητας.Μέσα από τη μελέτη Κανονισμών, όπως ο Cybersecurity Act, οι Οδηγίες NIS και NIS 2 αλλά και πιο σύγχρονων Κανονισμών από ο Dora, αναδείχθηκε η προσπάθεια της Ευρωπαϊκής Ένωσης να εδραιώσει ένα αποτελεσματικό πλαίσιο πρόληψης και αντιμετώπισης των κυβερνοαπειλών, διασφαλίζοντας την ενίσχυση και την προστασία των κρίσιμων υποδομών, με σεβασμό στην ανθρώπινη αξιοπρέπεια και τα θεμελιώδη ανθρώπινα δικαιώματα των πολιτών. Μέσα από την προσπάθεια αυτή έγινε αντιληπτές οι προκλήσεις της σύγχρονης ψηφιακής ζωής και η ανάγκη για μία, δια βίου μάθηση, στην προσπάθεια του κάθε χρήστη για την προστασία της ιδιωτικότητας και των προσωπικών του δεδομένων. Έτσι, η ενίσχυση της κυβερνοανθεκτικότητας δεν αποτελεί απλά έναν όρο τεχνικό αλλά, αντίθετα, έναν βασικό παράγοντα για την προστασία της

δημοκρατικής ζωής και ελευθερίας, σε έναν κόσμο που διαρκώς εξελίσσεται τεχνολογικά.

Ολοκληρώνοντας αυτή τη μελέτη, δεν μπορώ παρά να σκεφτώ πως αυτή είναι μόνο η αρχή στην προσπάθεια για κατανόηση και δόμηση ενός ανθεκτικού κυβερνοχώρου. Σε ένα διαρκώς μεταβαλλόμενο περιβάλλον, θα επικρατεί η ανάγκη για διαρκή ενημέρωση, θεσμοθέτηση και ενδυνάμωση της ευρωπαϊκής στρατηγικής για την κυβερνοασφάλεια. Αυτό που προέχει, στο εξής είναι η διαρκής γνώση, εγρήγορση και προσαρμογή, σε μία αέναη προσπάθεια εξέλιξης, διαφάνειας και δημοκρατικού πνεύματος.

Βιβλιογραφικές Αναφορές-Πηγές:

1. Bay, M. (2016) 'What is cybersecurity? In search of an encompassing definition for the post-Snowden era', French Journal For Media Research, 6. ISSN 2264-4733.

2. Τάσσης, Σ. (2024) 'Το Ευρωπαϊκό πλαίσιο Κυβερνοασφάλειας', ΔιΜΕΕ, 1, σσ. 78–92. ΤΝΠ QUALEX.

3. Moore, T. and Pym, D. (2015) 'Welcome from the Editors-in-Chief', Journal of Cybersecurity, 1(1), pp. 1–2. doi: 10.1093/cybsec/tyv010.

4. Craigen, D., Diakun-Thibault, N. and Purse, R. (2014) 'Defining Cybersecurity', Technology Innovation Management Review.

5. Charles Babbage Institute (2021) Donn B. Parker (1929–2021). College of Science and Engineering. Available at: https://cse.umn.edu/cbi/news/donn-b-parker-1929-2021.

6. ENISA (2015) Definition of Cybersecurity: Gaps and overlaps in standardisation, Version 1.0, December 2015.

7. Valkenburg, B. and Bongiovanni, I. (2024) 'Unravelling the three lines model in cybersecurity: a systematic literature review', *Computers & Security*, 139, p. 103708. Available at: https://doi.org/10.1016/j.cose.2024.103708.

8. Tanczer, L.M., Brass, I. and Carr, M. (2018) 'CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy', *Global Policy*, 9(S3), pp. 60–66. Available at: https://doi.org/10.1111/1758-5899.12625.

9. Andrukiewicz, E. and Krawiec, P. (2025) 'The Proactive Face of Cybersecurity: Certification. Legislation and Market Response from the Perspective of ITSEF', *Journal of Telecommunications and Information Technology*, pp. 6–10. Available at: https://doi.org/10.26636/jtit.2025.FITCE2024.1984.

10. Penedo, D. (2006) 'Technical Infrastructure of a CSIRT', in *International Conference on Internet Surveillance and Protection (ICISP'06). International Conference on Internet Surveillance and Protection (ICISP'06)*, pp. 27–27. Available at: https://doi.org/10.1109/ICISP.2006.32.

11. ISO/IEC (2022) ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection: Information security management systems – Requirements. Geneva: International Organization for Standardization.

12. ENISA (2015) Definition of Cybersecurity: Gaps and overlaps in standardisation, Version 1.0, December 2015. Available at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity-gaps-and-overlaps-in-standardisation.

13. Council of the European Union (2024) 'Cyber-security – How the EU is strengthening its cyber-defences', Council of the European Union, 2 December. Available at: https://www.consilium.europa.eu/en/policies/cyber-security/.

14. *The European Cybersecurity Certification Group | Shaping Europe's digital future* (2025). Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group

15. European Commission (2020) 'Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων', Δελτίο Τύπου, 16 December. Available at: https://ec.europa.eu/commission/presscorner/detail/el/IP_20_2356.

16. Porcedda, M.G. (2021) Hart Studies in Information Law and Regulation: Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis. Oxford: Hart Publishing.

17. Coopenergy Consortium (2015) A Guide to Multi-level Governance for Local and Regional Public Authorities. December 2015. Available at: [πρόσθεσε URL αν υπάρχει] (Accessed: 12 September 2025).

18. European Commission (2017) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence – Building strong cybersecurity for the EU. Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017JC0028.

19. European Union Agency for Cybersecurity (ENISA) (2024) A Trusted and Cyber Secure Europe – ENISA Strategy. Luxembourg: Publications Office of the European Union.

20. The European Cybersecurity Certification Group (2025) Shaping Europe's digital future.

21. CERT-EU (no date) Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/cybersecurity-service-union-institutions-bodies-offices-and-agencies-cert-eu_en. (No publication date available on website).

22. European Cybercrime Centre - EC3 (no date) Europol. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed: 12 September 2025). (No publication date available on website).

23. Vagianos, D. (2024) Digital Media and Society. Chapter 11: Cybercrimes and the Deep/Dark Web. Open Academic Editions.

24. ENISA (2022) 2021 Report on CSIRT-LE Cooperation: A study of the roles and synergies among sixteen selected EU/EEA Member States. Reviewed November 2022. Available at: https://www.enisa.europa.eu/publications/2021-report-on-csirt-le-cooperation.

25. Κατσιαρμάς, Α. (2018) 'Το ηλεκτρονικό έγκλημα με έμφαση στη Σύμβαση της Βουδαπέστης, την Οδηγία 2013/40/Ε.Ε. και τον Νόμο 4411/2016'. Available at: http://dspace.lib.uom.gr/handle/2159/22992.

26. Mohurle, S. and Patil, M. (2017) 'A brief study of Wannacry Threat: Ransomware Attack 2017', International Journal of Advanced Research in Computer Science, 8(5), pp. 1938–1940.

27. Lawspot.gr (2024) 'Κυβερνοασφάλεια: Ευρωπαϊκή Ένωση και Ηνωμένες Πολιτείες Αμερικής ενισχύουν τη μεταξύ τους συνεργασία', Lawspot.gr, 05/02/2024 (updated 09/02/2024). Available at: https://www.lawspot.gr/.

28. EEAS (2023) 'The European Union and NATO intensify cooperation on addressing cyber threats', European External Action Service, 22 September. Available at: https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en.

29. European Commission (2021) Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO-INTERPOL). COM(2021) 177 final, Brussels, 14 April.

30. Council of Europe (2023) Σύμβαση για το έγκλημα στον κυβερνοχώρο, 28 November. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

31. Λ. Μήτρου, Το κανονιστικό πλαίσιο της Κυβερνοασφάλειας σε Σ. Γκρίτζαλη/Σ. Κάτσικα, Κ. Λαμπρινουδάκη (επιμ.), Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, Αθήνα, 2021, σελ. 75-104.

32. Mavridis, I. (2015) 'Internet Privacy & Cybercrime', σε I. Mavridis, Information Security on the Internet. Kallipos, Open Academic Editions.

33. International Organization for Standardization (2023) *ISO/IEC 27032:2023 – Cybersecurity — Guidelines for Internet security*. Geneva: ISO.

34. ISO/IEC, 2022. *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: International Organization for Standardization / International Electrotechnical Commission. ΕΛΟΤ EN ISO/IEC 27001:2023.

35. Wadhwa, A. and Arora, N. (2017) 'A Review on Cyber Crime: Major Threats and Solutions', *International Journal of Advanced Research in Computer Science*, 8(5), p. 2217. Available at: www.ijarcs.info.

36. Kaspersky (no date) *Ransomware WannaCry: All you need to know*. Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

37. Europol (2017) *WannaCry Ransomware*. Available at: https://www.europol.europa.eu/newsroom/news/wannacry-ransomware.

38. European Commission (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001.

39. Tassis, S. (2024) *The European Cybersecurity Framework*.

40. Markopoulou, D., Papakonstantinou, V. and de Hert, P. (2019) 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation', *Computer Law & Security Review*, 35(6), Article 105336.

41. Schmitz-Berndt, S. and Anheier, F. (2020) 'Synergies in cybersecurity incident reporting – The NIS Cooperation Group Publication 04/20 in context'.

42. European Commission (2016) *The Directive on security of network and information systems (NIS Directive): A harmonised approach to cybersecurity*. [online]

Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/nis-directive-harmonised-approach-cybersecurity.

43. European Parliament (2018) *ENISA and a new cybersecurity act: EU Legislation in Progress*. [online] Brussels: European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)620230.

44. Khurshid, A., Alsaaidi, A., Aslam, N. and Raza, S. (2022) 'EU Cybersecurity Act and IoT Certification: Landscape, Perspective, and a Proposed Template Scheme', *IEEE Access*, 10, pp. 12245–12260.

45. European Commission (2020) *Hitting the refresh button on cybersecurity rules: NIS2 – Proposal for a Directive on measures for high common level of cybersecurity across the Union*. COM(2020) 823 final, 16 December. Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823.

46. Vandezande, N. (2023) 'Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor', *Computer Law & Security Review*, 49, Article 105765. Available at: https://doi.org/10.1016/j.clsr.2023.105765.

47. DSA Cyprus (2024) *Συνοπτικός οδηγός αναφορικά με την Οδηγία NIS2*. NIS2 Guide. Λευκωσία: DSA Cyprus. Available at: https://dsa.cy/images/pdf-upload/nis2-guide.pdf.

48. European Union Agency for Cybersecurity (ENISA) (2025) *EUCC Scheme – Guidelines on Vulnerability Management and Disclosure*, version 1.1, January 2025. Approved by the European Cybersecurity Certification Group (ECCG), in support of Commission Implementing Regulation (EU) 2024/482.

49. Zuiderveen Borgesius, F., Asghari, H., Bangma, N. & Hoepman, J.-H., 2023. *The GDPR rules on data breaches: analysing their rationales and effects*.

50. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, 2023. *Κατευθυντήριες γραμμές 9/2022 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του ΓΚΠΔ*. Έκδοση 2.0, 28 Μαρτίου.Διαθέσιμο: https://edpb.europa.eu/system/files/2023-03/edpb_guidelines_202209_personal_data_breach_notification_v2.0_el.pdf.

51. Zuiderveen Borgesius, F., Asghari, H., Bangma, N. & Hoepman, J.-H., 2023. *The GDPR Rules on Data Breaches: Analysing Their Rationales and Effects*.

52. European Data Protection Board (EDPB), 2023. *Guidelines 9/2022 on personal data breach notification under GDPR*. Τελική έκδοση, 4 Απριλίου.

53. European Supervisory Authorities, 2025. DORA Oversight Guide. 15 Ιουλίου. Διαθέσιμο στο: https://www.eiopa.europa.eu/publications/dora-oversight-guide_en.

54. Chiara, P. G., 2022. 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements – An introduction'.

55. European Commission, 2020. Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία. Βρυξέλλες, 16 Δεκεμβρίου.

56. Ευρωπαϊκή Επιτροπή, 2025. *Cyber Resilience Act*. Διαθέσιμο στο: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

57. Συμβούλιο της Ευρωπαϊκής Ένωσης, 2025. *EU cybersecurity: strategy and key policies*. Διαθέσιμο στο: https://www.consilium.europa.eu/el/policies/cybersecurity/.

58. Ευρωπαϊκή Επιτροπή, 2022. *Σήμανση CE — απόκτηση του πιστοποιητικού, απαιτήσεις της ΕΕ*. Διαθέσιμο στο: https://digital-strategy.ec.europa.eu/en/policies/ce-marking.

59. Pella, A., 2025. *Πλαίσιο εφαρμογής της Οδηγίας (ΕΕ) NIS2 2022/2555*. Μεταπτυχιακή διατριβή. Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων.

60. ΕΥ Ελλάδος, 2025. *Ν.5160/2024: Ενσωμάτωση της Οδηγίας NIS2 σχετικά με τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας στην Ένωση*. [online] Διαθέσιμο σε: https://www.ey.com/el_gr/technical/tax/tax-alerts/nomos-5160-2024-enswmatwsi-tis-odigias-nis-2.

61. Lawspot.gr, 2025. *Κυβερνοασφάλεια: Δημοσιεύθηκε ο Ν. 5160/2024 με την ενσωμάτωση της Οδηγίας NIS2*. [online] Διαθέσιμο σε: https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-dimosieythike-o-n-5160-2024-me-tin-ensomatosi-tis-odigias-nis-2.

62. Υπουργείο Ψηφιακής Διακυβέρνησης, 2020. *Εθνική Στρατηγική Κυβερνοασφάλειας 2020–2025*. Εγκρίθηκε από τον Υπουργό Επικρατείας Κυριάκο Πιερρακάκη. Διαθέσιμο σε: https://www.mindigital.gr/wp-content/uploads/2022/11/EL-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf.

63. Martino, L. and Gamal, N. (eds.), 2023. *European Cybersecurity in Context: A Policy-Oriented Comparative Analysis*. Techno-Politics Series: 3. Cham: Springer.

64. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* arXiv preprint arXiv:1802.07228.

65. Buczak, A. L. and Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), pp.1153-1176.

66. ENISA, 2024. *ENISA Threat Landscape 2024 (July 2023–June 2024)*. European Union Agency for Cybersecurity (ENISA), Σεπτέμβριος 2024.

67. Cybersecurity Ventures (2023) *Cybercrime to cost the world $8 trillion annually in 2023*.

68. European Commission, 2018. *Connecting Europe Facility supports expansion of cybersecurity capabilities*. News article, 27 March 2018. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/connecting-europe-facility-supports-expansion-cybersecurity-capabilities.

69. Lawspot.gr, 2024. *Κυβερνοασφάλεια: Ευρωπαϊκή Ένωση και Ηνωμένες Πολιτείες Αμερικής ενισχύουν τη μεταξύ τους συνεργασία*. [online] Διαθέσιμο σε: https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-e-e-kai-ipa-enisxoyn-ti-metaxy-tous-synergasia.

70. *Η Ευρωπαϊκή Ένωση και το ΝΑΤΟ εντείνουν τη συνεργασία για την αντιμετώπιση των κυβερνοαπειλών | Shaping Europe's digital future* (no date). Available at:

https://digital-strategy.ec.europa.eu/el/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats.

71. DigiChina, 2018. *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*. [online] Published 29 June 2018. Available at: https://digichina.stanford.edu/work/translation-cybersecurity-law-peoples-republic-china-effective-june-1-2017/.

72. Basu, P., 2024. *From reactive to proactive: Japan's advances in cybersecurity and cyber defence strategies*. Expert Speak Digital Frontiers, 27 March 2024. [online] Available at: https://www.orfonline.org/expert-speak/from-reactive-to-proactive-japan-s-advances-in-cybersecurity-and-cyber-defence-strategies.

ΝΟΜΟΘΕΣΙΑ:

1. Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), 2019. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32019R0881.

2. European Union (2022) *Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS 2)*. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32022L2555.

3. European Commission (2002) *Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την ιδιωτικότητα και τις ηλεκτρονικές επικοινωνίες)*. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, L 201, σσ. 37–47. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058.

4. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο (2016) *Οδηγία (ΕΕ) 2016/1148 της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας των δικτύων και των συστημάτων πληροφοριών στην Ένωση*. Επίσημη Εφημερίδα της Ευρωπαϊκής

Ένωσης, L 194, σσ. 1–30. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L1148.

5. Ευρωπαϊκή Επιτροπή, 2022. *Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοπιστωτικό τομέα και τροποποίηση των Κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) αριθ. 2016/1011*. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 333, 27.12.2022, σ. 1–79. Διαθέσιμο στο: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

6. Ευρωπαϊκή Επιτροπή, 2022. *Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοπιστωτικό τομέα και τροποποίηση των Κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) αριθ. 2016/1011*. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 333, 27.12.2022, σ. 1–79. Διαθέσιμο στο: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.