ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων»

Η Ανάδειξη του Κυβερνοπολέμου ως τη Σημαντικότερη Ασύμμετρη Απειλή- Μελέτη Περίπτωσης Κυβερνοαπειλής

Μεταπτυχιακή Διπλωματική Εργασία Ειδίκευσης
«Διοικητική της διακινδύνευσης στην παγκόσμια πολιτική»

Δημήτριος Κάππας

Τριμελής επιτροπή:
Αναπληρωτής Καθηγητής Ν. Κουτσούκης
Επίκουρος Καθηγητής Ε. Φακιολάς
Δρ. Π. Χουντάλας (ε)

(ε) – Επιβλέπων

Τελική έκδοση

Κόρινθος,2021

UNIVERSITY OF THE PELOPONNESE
SCHOOL OF SOCIAL & POLITICAL SCIENCES
DEPARTMENT OF POLITICAL SCIENCE &INTERNATIONAL RELATIONS

MASTER'S PROGRAMME IN
"GLOBAL RISKS AND ANALYTICS"

The Emergence of Cyber War as the Most Important Asymmetric Threat-Cyber Threat Case Study

Master's dissertation specializing in
"Risk management in global politics"

Dimitrios Kappas

Committee:
Associate Professor N. Koutsoukis
Assistant Professor E. Fakiolas
Dr. P. Chountalas (s)

(s) – Supervisor

Final version

Corinth, Greece,2021

Φύλλο αξιολόγησης

Η διπλωματική εργασία με τίτλο *«Η ανάδειξη του κυβερνοπολέμου ως τη σημαντικότερη ασύμμετρη απειλή-Μελέτη περίπτωσης κυβερνοαπειλής»* του Δημητρίου Κάππα αξιολογήθηκε από την τριμελή επιτροπή, τόσο ως προς την ποιότητα του κειμένου, όσο και ως προς την ποιότητα της προφορικής παρουσίασης και υπεράσπισης της διπλωματικής εργασίας ενώπιον ακροατηρίου.

Η διαδικασία αξιολόγησης της διπλωματικής εργασίας ολοκληρώθηκε την …/…/… με γενική επίδοση:

☐ Καλώς

☐ Λίαν Καλώς

☐ Άριστα

Τα μέλη της τριμελούς επιτροπής:

1. Αναπληρωτής Καθηγητής Ν. Κουτσούκης

2. Επίκουρος Καθηγητής Ε. Φακιολάς

3. Δρ. Π. Χουντάλας

Abstract

The present master thesis attempts to highlight a new kind of threat that has emerged on the world stage in recent decades, the so-called "asymmetric threats", which are the result of an ever-changing process of changing the modern political scene combined with the dramatic technology evolution and the widespread use of the internet. In particular, the most dangerous threat, that of cyber warfare, is presented, analyzing all the aspects that make it the most important in our society. Also, with the help of modern risk analysis methods, such as the ISO 31000 risk management framework and the STRIDE-LM threat analysis system, the risk matrix and the "Event tree analysis" are extracted, in order to understand how the cyber threat works. Finally, in order to be able to consider the analysis complete, ways of dealing with and mitigating the outcomes of this threat are presented.

Keywords: asymmetric threat, cyber warfare, cyberspace, cybersecurity, risk management

Περίληψη

Η παρούσα διπλωματική εργασία επιχειρεί να αναδείξει ένα νέο είδος απειλών που έκανε την εμφάνισή του στο παγκόσμιο στερέωμα τις τελευταίες δεκαετίες, τις λεγόμενες «ασύμμετρες απειλές», οι οποίες είναι το αποτέλεσμα μιας συνεχούς μεταβαλλόμενης διεργασίας αλλαγής του σύγχρονου πολιτικού σκηνικού σε συνδυασμό με την δραματική εξέλιξη της τεχνολογίας και την ευρεία χρήση του διαδικτύου. Ειδικότερα, γίνεται παρουσίαση της πλέον επικίνδυνης απειλής, αυτής του κυβερνοπολέμου, αναλύοντας όλες τις πτυχές που την αναδεικνύουν ως τη σημαντικότερη της κοινωνίας μας. Επίσης, με τη βοήθεια σύγχρονων μεθόδων ανάλυσης ρίσκου, όπως το πλαίσιο διαχείρισης κινδύνου ISO 31000 και το σύστημα ανάλυσης απειλών STRIDE-LM εξάγονται η μήτρα κινδύνου και η «Δενδρική ανάλυση» των γεγονότων, ώστε να κατανοήσουμε τον τρόπο δράσης της κυβερνοαπειλής. Τέλος, για να μπορέσουμε να θεωρήσουμε την ανάλυση ολοκληρωμένη, παρουσιάζονται τρόποι αντιμετώπισης και μετριασμού των εκβάσεων της απειλής αυτής.

Λέξεις κλειδιά: ασύμμετρη απειλή, κυβερνοπόλεμος, κυβερνοχώρος, κυβερνοασφάλεια, διαχείριση ρίσκου

Πρόλογος

Η παρούσα διπλωματική εργασία είναι το αποτέλεσμα μιας συνεχούς προσωπικής αναζήτησης διεύρυνσης και αναβάθμισης της οπτικής των σύγχρονων πολιτικών εξελίξεων, μια διαδικασία που δυστυχώς θα έπρεπε να ξεκινήσω νωρίτερα. Το μεταπτυχιακό αυτό πρόγραμμα μου έδωσε τις βάσεις για την περεταίρω εξέλιξή μου ως αξιωματικός των ΕΔ, ενώ ταυτόχρονα μου άλλαξε τον τρόπο με τον οποίο κατανοώ το σύνολο των διεργασιών που συνθέτουν την κοινωνία μας και τις νέες προκλήσεις πουν παρουσιάζονται. Παράλληλα, με την εισαγωγή στον κόσμο της διαχείρισης ρίσκου, μπόρεσα να διαμορφώσω μια ολοκληρωμένη εικόνα για τον τρόπο με τον οποίο μπορούν να αντιμετωπιστούν οι προκλήσεις αυτές.

Όλα αυτά δε θα τα είχα καταφέρει χωρίς τη βοήθεια όλων των καθηγητών του προγράμματος αυτού και ιδιαίτερα χωρίς τις πολύτιμες συμβουλές του επιβλέποντα καθηγητή μου Δρ. Παναγιώτη Χουντάλα.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένειά μου, για τις πολύτιμες ώρες που τους στέρησα προσπαθώντας να επιτύχω έναν προσωπικό στόχο και ιδιαίτερα τη σύζυγό μου που βρίσκεται πάντα δίπλα μου και με στηρίζει αλτρουιστικά σε ό,τι κι αν αποφασίσω.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Εικόνων

1. Εισαγωγή

«. . . Αν ο εχθρός είναι υπέρτερος σε ισχύ, απόφυγέ τον. Αν οι δυνάμεις του είναι ενωμένες, διαχώρισέ τις. Να του επιτεθείς εκεί που είναι ανέτοιμος. Εμφανίσου εκεί που είσαι λιγότερο αναμενόμενος. . . ».

Sun – Tzu, "Η Τέχνη Του Πολέμου"

Τις τελευταίες δεκαετίες του αιώνα μας παρατηρείται μια ξέφρενη πορεία της παγκοσμιοποίησης, παράλληλα με μια αλματώδη τεχνολογική επανάσταση, φαινόμενα που αυξάνουν κατακόρυφα το αίσθημα της αβεβαιότητας και της ανασφάλειας και οδηγούν την ανθρωπότητα σε μία κατάσταση όπου καλλιεργείται ο φόβος και ευδοκιμεί το χάος. Οι συνεχόμενες παγκόσμιες ανακατατάξεις, οι κοινωνικές, πολιτικές και οικονομικές διαφορές, η έλλειψη της παιδείας σε πολλά κράτη ανά την υφήλιο, η λειτουργία τρομοκρατικών ομάδων, η έκρηξη της βίας, η έξαρση του θρησκευτικού φανατισμού, διαμόρφωσαν μία νέα κατάσταση όπου οι παραδοσιακές αξίες διαταράχθηκαν, ενώ ταυτόχρονα επιχειρείται μία αλλαγή του «status quo» σε όλα τα επίπεδα.

Μέσα σε αυτόν τον κυκεώνα των συνεχών αλλαγών καλλιεργήθηκε και ευδοκίμησε μία νέα μορφή απειλής, η λεγόμενη «ασύμμετρη απειλή», που έβαλε τις βάσεις για την ανατροπή της διεθνούς ασφάλειας και σταθερότητας στο παγκόσμιο περιβάλλον. Πλέον, όλοι καλούνται να συμφιλιωθούν με τη νέα αυτή απειλή και να καταβάλλουν τεράστια προσπάθεια για την καλύτερη δυνατή αντιμετώπισή της.

Ο όρος «ασύμμετρη απειλή», έκανε την εμφάνισή του στο καθημερινό μας λεξιλόγιο μετά το χτύπημα της 11ης Σεπτεμβρίου,2001 στους δίδυμους πύργους της Νέας Υόρκης. Ενώ ο ορισμός για το τί είναι «ασύμμετρη απειλή» ακόμα και σήμερα δεν έχει επακριβώς αποδοθεί σαν έννοια, θα μπορούσαμε να ισχυριστούμε ότι υπάρχει από την εμφάνιση του ανθρώπου και εκφράζει την προσπάθεια ενός αδύναμου να επιβληθεί σ΄ έναν ισχυρότερο. Περισσότερα στοιχεία περί των ασύμμετρων απειλών κρίθηκε σκόπιμο να παρουσιαστούν σε ξεχωριστό παράρτημα (Παράρτημα Α), ώστε να κατανοηθεί η σημασία τους, τα χαρακτηριστικά τους και οι επιπτώσεις τους.

Στο παραπάνω πλαίσιο η παρούσα διπλωματική εργασία πραγματεύεται την ανάλυση μιας εκ των πλέον διαδεδομένων ασύμμετρων απειλών, των λεγόμενων κυβερνοαπειλών. Ο κυβερνοπόλεμος έχει αναδειχθεί ως μια απειλή του σύγχρονου κόσμου που απασχολεί ιδιαίτερα μεγάλο αριθμό κυβερνητικών και μη οργανισμών και δαπανούνται τεράστια χρηματικά ποσά για την προστασία των ψηφιακών συστημάτων κρίσιμων υποδομών και μεγάλων επιχειρήσεων, σύμφωνα με την AGCS, η οποία κατατάσσει τις κυβερνοαπειλές στην τρίτη θέση του παγκόσμιου χάρτη και μόλις δεύτερη για τη χώρα μας. Επιπλέον, με πρόσφατη έρευνα για την μετά Covid-19 εποχή της αμερικανικής McKinsey & Company, τονίστηκε η επιτάχυνση της ψηφιοποίησης εταιρειών και υπηρεσιών παγκοσμίως κατά τρία με τέσσερα χρόνια, ενώ η σημαντικότητα των ψηφιακών προϊόντων κατά επτά. Επιπλέον, σύμφωνα με την πρόσφατη έκθεση του WEF (The World Economic Forum), οι κυβερνοαπειλές κατατάσσονται μέσα στις δέκα πιο επικίνδυνες παγκοσμίως για τα επόμενα πέντε έτη. Πίνακες των παραπάνω στοιχείων παρουσιάζονται στο Παράρτημα Β. (Alianz 2021, McKinsey & Company 2021, McLennan and Group 2021)

Η βιβλιογραφία που χρησιμοποιήθηκε για τη συλλογή στοιχείων είναι κατά κύριο λόγο ξενόγλωσση, αλλά αξιοποιήθηκε και ελληνική. Το κύριο μέρος της εργασίας οργανώθηκε στα εξής κεφάλαια:

- Στο *δεύτερο κεφάλαιο* γίνεται αρχικά ανάλυση του κυβερνοχώρου σε θεωρητική βάση, των χαρακτηριστικών του και πώς μπορεί να αποτελέσει ένα σύγχρονο πεδίο επιθετικών και αμυντικών ενεργειών, με σκοπό να κατανοήσει ο αναγνώστης τη σημαντικότητα αυτού του νέου τρόπου διεξαγωγής επιχειρήσεων πολεμικού χαρακτήρα. Επίσης,

γίνεται αναφορά στον τρόπο με τον οποίο έχουν οργανώσει το ΝΑΤΟ, η ΕΕ και οι ΗΠΑ την κυβερνοασφάλεια, με σκοπό την αποτελεσματικότερη αντιμετώπιση των κυβερνοαπειλών.

- Στο *τρίτο κεφάλαιο* παρουσιάζεται η μελέτη περίπτωσης ανάλυσης ρίσκου κυβερνοεπίθεσης μέσω του πλαισίου διαχείρισης κινδύνου ISO 31000 και το σύστημα ανάλυσης απειλών STRIDE-LM. Παράλληλα, με τη βοήθεια της «Μήτρας κινδύνου» και τη «Δενδρική ανάλυση κινδύνων» γίνεται αναγνώριση των σημαντικότερων απειλών και ανάλυση των πιθανών εκβάσεων της πλέον σοβαρότερης απειλής. Τέλος, παρουσιάζονται τρόποι μετριασμού της απειλής αυτής.
- Στο *τέταρτο κεφάλαιο* ολοκληρώνεται η εργασία με την παρουσίαση συμπερασμάτων και προτάσεων δημιουργίας ενός πλαισίου ολοκληρωμένης προσέγγισης της αντιμετώπισης του κυβερνοπολέμου.

2. Κυβερνοπόλεμος

Η χρήση ηλεκτρονικών υπολογιστών και συστημάτων επικοινωνίας έχουν διεισδύσει πλέον σε τεράστιο βαθμό στη ζωή μας, και έτσι όλο και αυξάνεται ο βαθμός εξάρτησής μας από τις τεχνολογίες αυτές. Οι τεχνολογίες αυτές χρησιμοποιούνται σήμερα σε πάρα πολλούς τομείς πέραν των επικοινωνιών, για την παραγωγή και μεταφορά ενέργειας, την διαχείριση των συστημάτων ύδρευσης/αποχέτευσης, τις χρηματοπιστωτικές υπηρεσίες, οι ένοπλες δυνάμεις, οι δυνάμεις ασφαλείας, τα κυβερνητικά τμήματα και υπηρεσίες, υγεία, κλπ. Αν και τα οφέλη που έχουν προκύψει από τις τεχνολογίες πληροφορίας και επικοινωνιών είναι τεράστια, οι τεχνολογίες των νέων δικτύων έχουν φέρει μαζί τους και πληθώρα θεμάτων ασφάλειας που αξιοποιούνται από κακόβουλα στοιχεία τα οποία στοχεύουν στην εκμετάλλευση ευάλωτων σημείων σε στοιχεία των υποδομών και των δικτύων, όπως υπολογιστές, διακομιστές, μεταγωγείς, κλπ.

Τα τελευταία χρόνια έχουν εμφανιστεί πολλαπλές απειλές στα δίκτυα επικοινωνίας, ειδικά με την μεγάλη αύξηση της χρήσης του διαδικτύου από τους πολίτες. Οι τεχνολογίες πληροφορίας και επικοινωνιών έχουν χρησιμοποιηθεί κακόβουλα, για την κλοπή χρημάτων από τραπεζικούς λογαριασμούς, την πρόσβαση σε εμπιστευτικές πληροφορίες, την πρόκληση ζημιών σε σημαντικές ιστοσελίδες (με συνεπαγόμενη άρνηση πρόσβασης στο κοινό), κλπ. Παραδείγματα πληροφοριών που έχουν κλαπεί από εταιρείες αναφέρονται σε εμπιστευτικά συμβόλαια, σχέδια προϊόντων, στοιχεία πιστωτικών καρτών, αριθμούς λογαριασμών και άλλα προσωπικά στοιχεία. Τέτοια περιστατικά μπορεί να προκαλέσουν τις πλέον σοβαρές ζημιές σε ένα οργανισμό, αφού πέραν των άμεσων ζημιών πλήττεται και το καλό όνομα του οργανισμού καθώς και η εμπιστοσύνη των πελατών του. Αντίθετα μειώνεται σημαντικά η πιθανότητα τέτοιων περιστατικών εφόσον λαμβάνονται τα κατάλληλα μέτρα από ένα οργανισμό ή εταιρεία.

2.1 Κυβερνοχώρος

Ο κυβερνοχώρος (cyberspace) αποτελείται από το σύνολο των παγκόσμιων δικτύων υπολογιστών (συμπεριλαμβανομένου του Διαδικτύου) και των περιφερειακών μηχανημάτων και εξοπλισμού, όπως οι servers, οι routers, τα

modems, οι εκτυπωτές, οι ενσύρματες και οι ασύρματες γραμμές, τα οποία είναι συνδεδεμένα μεταξύ τους, προκειμένου να είναι δυνατή η επεξεργασία, αποθήκευση και ροή των δεδομένων και πληροφοριών. Εκτός από το διαδίκτυο, ο κυβερνοχώρος περιλαμβάνει και το σύνολο των εσωτερικών δικτύων, τα οποία είναι εγκατεστημένα και λειτουργούν στο διεθνή δημόσιο και ιδιωτικό τομέα, στους διεθνείς οργανισμούς, στις ένοπλες δυνάμεις (εσωτερικά δίκτυα ελέγχου και διοίκησης, δίκτυα οπλικών συστημάτων), αλλά και το σύνολο των μεμονωμένων ηλεκτρονικών υπολογιστών και συσκευών που δεν είναι συνδεδεμένοι σε κανένα δίκτυο.(U.S. DEPARTMENT OF HOMELAND SECURITY 2018, Refsdal et al. 2015)

2.1.1 Χαρακτηριστικά Κυβερνοχώρου

Ο κυβερνοχώρος στηρίζεται και εξαρτάται άμεσα από την τεχνολογική ανάπτυξη. Τα όρια του δεν υφίστανται και μεταβάλλονται, ενώ είναι εύκολα προσβάσιμος με χαμηλό κόστος σε οποιονδήποτε διαθέτει την απαραίτητη τεχνολογία και υποδομή (π.χ. έναν Η/Υ, μία διαδικτυακή σύνδεση (Internet) ή έναν Η/Υ διασυνδεδεμένο στο δίκτυο Η/Υ μιας επιχείρησης). (Geers, 2011)

Τα κύρια χαρακτηριστικά, που προσδιορίζουν τον κυβερνοχώρο περιγράφονται παρακάτω:

1. Το μέγεθος

Ο κυβερνοχώρος δεν έχει γεωγραφικά ή φυσικά σύνορα. Υπάρχει και διαδραματίζει σημαντικό ρόλο σε όλους τους τομείς παρέχοντάς τους μια τεχνολογική υποδομή. Οποιαδήποτε σημαντική δραστηριότητα σε οποιοδήποτε τομέα της ζωής βασίζεται σήμερα στην υποδομή του κυβερνοχώρου.(Geers, 2011)

2. Η ανωνυμία

Η δυνατότητα ανώνυμης εκτέλεσης οποιασδήποτε δραστηριότητας στον κυβερνοχώρο σε οποιαδήποτε διάσταση δεν ενέχει κάποιο κίνδυνο για τους δράστες. Αυτό δημιουργεί νομικά προβλήματα, καθώς η λειτουργία δεν μπορεί να αποδοθεί σε ένα συγκεκριμένο άτομο, οργάνωση ή κράτος. Αυτό το μοναδικό χαρακτηριστικό έχει τις μεγαλύτερες επιρροές και παίζει αποφασιστικό ρόλο στην πραγματοποίηση απειλών στον κυβερνοχώρο.(Geers, 2011)

3. Η ασυμμετρία

Το χαρακτηριστικό της ασυμμετρίας αναφέρεται στους διαφορετικούς δρώντες που δραστηριοποιούνται στον κυβερνοχώρο. Πιο συγκεκριμένα, στον κυβερνοχώρο δραστηριοποιούνται έθνη, κράτη ακόμα και μεμονωμένοι πολίτες (hackers), οι οποίοι όμως έχουν τις ίδιες αναλογίες εντός του κυβερνοχώρου. Επιπλέον, η ασυμμετρία εμφανίζεται και στη σχέση κόστους σε συνάρτηση με το ρίσκο και το επιδιωκόμενο κέρδος που θα αποκομίσει κάποιος μέσα από τον κυβερνοχώρο.(Geers, 2011)

4. Η μεταβλητότητα

Το χαρακτηριστικό της μεταβλητότητας αναφέρεται στο ότι ο κυβερνοχώρος και ο τρόπος λειτουργίας του στηρίζεται στο λογισμικό (software) και το υλικό (hardware), τα οποία δεν λειτουργούν πάντα στο 100% των κατασκευαστικών τους δυνατοτήτων, με αποτέλεσμα η πρόβλεψη να μην είναι πάντα δυνατή και δεύτερον το αποτέλεσμα της ίδιας ενέργειας να είναι διαφορετικό κάθε φορά.(Geers, 2011)

5. Η διπλή χρήση των «κυβερνοεργαλείων»

Με τον όρο «κυβερνοεργαλεία» ορίζονται τα εργαλεία εκείνα τα οποία χρησιμοποιούνται στον κυβερνοχώρο. Τα εργαλεία αυτά δημιουργήθηκαν ως εργαλεία ελέγχου τρωτότητας ενός δικτύου, αλλά έχουν και τη δυνατότητα διπλής χρήσης (dual-use), όταν, για παράδειγμα, γίνονται τα μέσα για κακόβουλες ενέργειες στον κυβερνοχώρο.(Geers, 2011)

2.1.2 Αδυναμίες Κυβερνοχώρου

Ένας από τους βασικούς λόγους εμφάνισης προβλημάτων ασφάλειας στο Internet είναι η βασική αρχιτεκτονική των πρωτοκόλλων TCP/IP και UDP που χρησιμοποιούνται σε αυτό. Κανένα από αυτά δεν σχεδιάστηκε αρχικά με σκοπό να παράσχει αληθινά ασφαλή επικοινωνιακά μονοπάτια. Έτσι όταν στέλνει κανείς στοιχεία χρησιμοποιώντας το πρωτόκολλο TCP/IP, δεν μπορεί να γνωρίζει ποιους ακριβώς επικοινωνιακούς «διαύλους» θα ακολουθήσουν αυτά για να φτάσουν στον προορισμό τους. Αν κάποιος hacker καταφέρει να εγκαταστήσει σε κάποιον από τους «διαύλους» αυτούς ένα πρόγραμμα, γνωστό σαν «sniffer», τότε θα μπορέσει να υποκλέψει όλα τα διαβιβαζόμενα με τον τρόπο αυτό στοιχεία. Ένας ακόμη λόγος για τον οποίο οι hackers έχουν σοβαρές πιθανότητες να επιτύχουν τον στόχο τους είναι αυτή η ίδια η

διαμόρφωση ενός συστήματος, η οποία κάθε άλλο παρά προϋποθέτει την προληπτική λήψη κάποιων μέτρων ασφαλείας και μάλιστα εκείνων με τα οποία θα ελέγχεται η είσοδος κάποιου από το Internet. Σε γενικές γραμμές θα μπορούσαμε να εντοπίσουμε τις αδυναμίες των διαφόρων συστημάτων στα εξής :

1. στην ανυπαρξία μέτρων ασφαλείας (π.χ. ύπαρξη firewalls),
2. στην ατελή διαμόρφωση και διαχείρισή τους,
3. σε βασικά προβλήματα ασφάλειας σε σχέση με τα πρωτόκολλα επικοινωνίας (IP, TCP, UDP) που χρησιμοποιούν,
4. σε προβλήματα ασφαλείας σε σχέση με τις υπηρεσίες του Internet που χρησιμοποιούν
5. στο μη ικανοποιητικό service που τους παρέχεται.

2.1.3 Ο Κυβερνοχώρος ως άσκηση δύναμης

Στον κυβερνοχώρο υπάρχουν αμέτρητες πληροφορίες σχετικά με τη δημιουργία, τον έλεγχο και την επικοινωνία συστημάτων με βάση τους ηλεκτρονικούς υπολογιστές, όπως υποδομές, δίκτυα, λογισμικά και ανθρώπινο δυναμικό. Εάν οι πληροφορίες αυτές χρησιμοποιηθούν για να επιτελεσθεί ένας συγκεκριμένος σκοπός ή αποτέλεσμα, τότε καταλαβαίνουμε τη δύναμη του κυβερνοχώρου. Γενικότερα, η δύναμη αυτή μας δίνει τη δυνατότητα να δημιουργούμε πλεονεκτήματα υπέρ μας και να επηρεάζουμε καταστάσεις ή γεγονότα εντός ή και εκτός του κυβερνοχώρου. Επειδή όμως ο κυβερνοχώρος είναι κατασκευασμένος από τον άνθρωπο, έτσι είναι ευμετάβλητος και επιρρεπής σε μεγάλες τεχνολογικές αλλαγές. (Lin and Zegart 2017, Nye 2010)

Παράλληλα, επειδή η είσοδος στον κυβερνοχώρο είναι πολύ εύκολη, μικρά κράτη και μη κυβερνητικοί δρώντες μπορούν να παίξουν σημαντικό ρόλο, με μικρή κατανάλωση χρηματικών ποσών. Έτσι, εν αντιθέσει με τις στρατιωτικές επιχειρήσεις σε θάλασσα, αέρα και διάστημα, ο κυβερνοχώρος μοιράζεται κάποια κοινά χαρακτηριστικά με τις χερσαίες επιχειρήσεις. Αυτά είναι ο αριθμός των συμμετεχόντων, η εύκολη πρόσβαση και η δυνατότητα της απόκρυψης. Επίσης, στον κυβερνοχώρο δεν μπορούμε να κάνουμε λόγο για κυριαρχία κάποιου, όπως στη θάλασσα ή στον αέρα. Το εναντίον, κράτη ή επιχειρήσεις με πολύπλοκα διαδικτυακά συστήματα φαίνεται να έχουν και περισσότερα τρωτά σημεία που μπορούν εύκολα πλέον να εκμεταλλευτούν μη κυβερνητικοί δρώντες προς όφελός τους. (Lin and Zegart, 2017)

Έτσι λοιπόν, αναλόγως της επιρροής που θέλουν οι δρώντες αυτοί να έχουν, εκμεταλλεύονται τον κυβερνοχώρο και εφαρμόζουν soft ή hard power. Μιλώντας για εφαρμογή soft power εννοούμε τη χρήση πληροφοριών για διαμόρφωση μιας ατζέντας, να πείσουμε κάποιον να κάνει κάτι, να διαμορφώσουμε ή να επηρεάσουμε την κοινή γνώμη. Για παράδειγμα, η Κινεζική κυβέρνηση πολλές φορές χρησιμοποίησε το διαδίκτυο για να κινητοποιήσει κινέζους φοιτητές να διαδηλώσουν εναντίον της Ιαπωνίας, όταν κάποιοι κυβερνητικοί εκπρόσωποι της δεύτερης διατηρούσαν μια στάση προσβλητική ως προς την πρώτη. Επίσης, η Al Qaeda χρησιμοποίησε ευρέως το διαδίκτυο για στρατολόγηση ανθρώπων υπέρ του σκοπού της. Αντίθετα, μιλώντας για hard power εννοούμε τις ενέργειες αυτές που έχουν σοβαρό αντίκτυπο σε επιχειρήσεις ή κρατικές δομές. Για παράδειγμα, κυβερνητικοί ή μη δρώντες μπορούν να οργανώσουν μια συστημική άρνηση υπηρεσιών χρησιμοποιώντας διάφορα εργαλεία του κυβερνοχώρου, με αποτέλεσμα τη μη σωστή λειτουργία των υπολογιστών και των συστημάτων μιας εταιρείας ή ακόμη και μιας ολόκληρης χώρας με καταστροφικές επιπτώσεις, οικονομικές και όχι μόνο. Χαρακτηριστικότερο παράδειγμα είναι η χρήση του ιού «Stuxnet» που κατασκεύασαν οι ΗΠΑ (CIA) και το Ισραήλ (Mossad) το 2008 με σκοπό να πλήξουν τις εγκαταστάσεις εμπλουτισμού ουρανίου στο Natanz του Ιράν.(Lin and Zegart 2017, Nye, 2010, “Ο ιός Stuxnet και το πυρηνικό πρόγραμμα του Ιράν” 2018)

2.1.4 Συγκρούσεις στον Κυβερνοχώρο

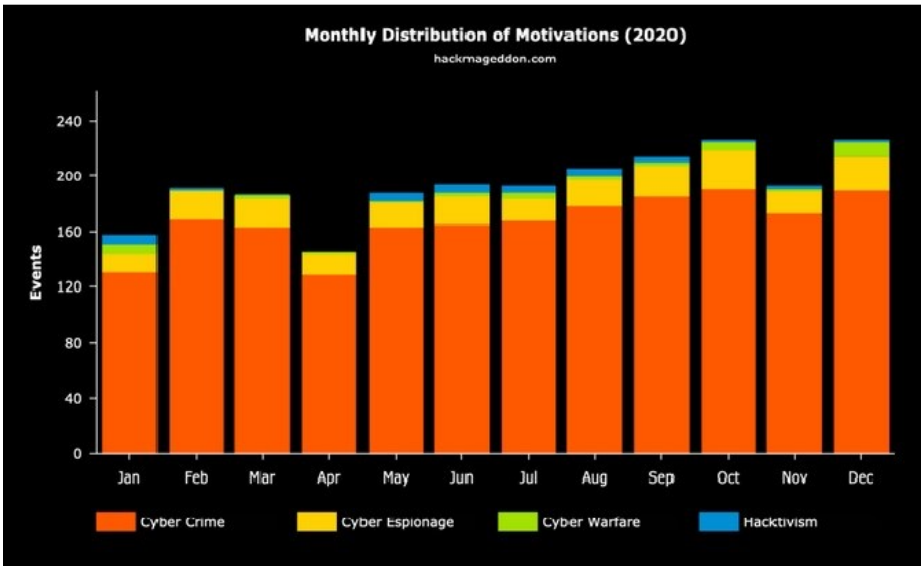
Όταν μιλάμε για Κυβερνοσύγκρουση (Cyber Conflict) αναφερόμαστε στην αντιπαράθεση μεταξύ δύο ή περισσοτέρων πλευρών, με παράλληλη άσκηση κυβερνοεπίθεσης (Cyber attack) από τη μια τουλάχιστον προς τις άλλες. Όταν μιλάμε για κυβερνοεπίθεση εννοούμε κάθε σκόπιμη προσπάθεια που γίνεται από μια πλευρά για την επίτευξη διαταραχής (Disruption), διαφθοράς (Corruption) ή κορεσμού (με αποτέλεσμα το Denial of Service) στα συστήματα Η/Υ της άλλης πλευράς.(Libicki, 2009)

2.1.5 Κατηγορίες Κυβερνοσυγκρούσεων

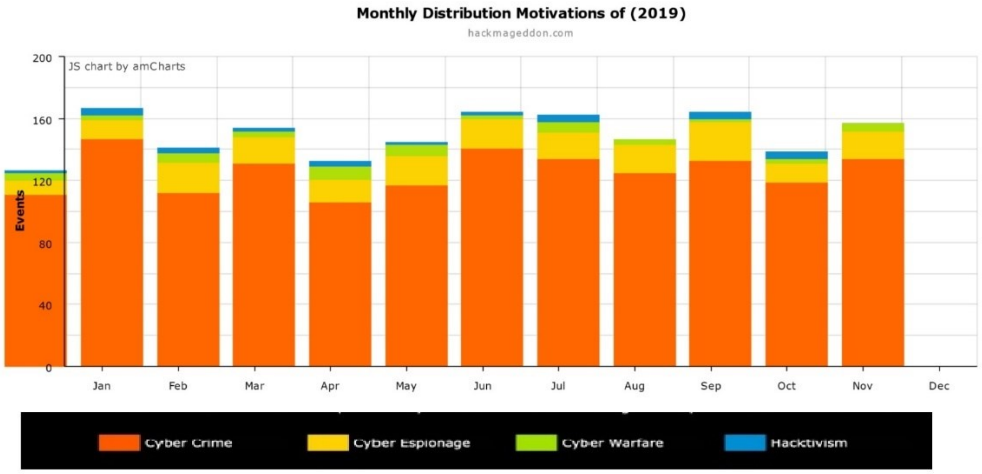
Οι κατηγορίες των Κυβερνοσυγκρούσεων χωρίζονται, με βάση τους δρώντες, στο τι αποσκοπούν και στα μέσα που χρησιμοποιούν, στον βανδαλισμό στον κυβερνοχώρο, στο κυβερνοέγκλημα, στην κυβερνοκατασκοπεία, στην κυβερνοτρομοκρατία και στον κυβερνοπόλεμο.

1. Βανδαλισμός στο κυβερνοχώρο (Cyber Vandalism-Hactivism): περιλαμβάνει το σύνολο των ενεργειών που προέρχονται από ένα άτομο ή και ομάδα ατόμων χωρίς εμφανή πολιτικό, εγκληματικό ή ιδεολογικό κίνητρο ή σκοπό. Συνήθως οι ενέργειες αυτές γίνονται για να αναδειχθούν οι ικανότητες των ατόμων αυτών. (Ziolkowski, 2013)
2. Κυβερνοέγκλημα (Cyber Crime): εννοούμε τις ενέργειες που γίνονται με τη χρήση Η/Υ εναντίων ατόμων, οργανισμών ή επιχειρήσεων ιδιωτικού ή δημόσιου ενδιαφέροντος με σκοπό τα οικονομικά κυρίως οφέλη. Επίσης, πράξεις που παραβιάζουν την προσωπική ζωή κάποιου, όπως επιθέσεις για παραβίαση προσωπικών δεδομένων ή αντιγραφής-κλοπής της ταυτότητας κάποιου με σκοπό τον εκβιασμό. (Ziolkowski, 2013)
3. Κυβερνοκατασκοπεία (Cyber Espionage): περιλαμβάνει τις ενέργειες όπου κυβερνήσεις ή εγκληματικά δίκτυα υποκλέπτουν πληροφορίες σχετικές με κυβερνήσεις, εθνική άμυνα, οργανισμούς ή επιχειρήσεις έτερων κρατών χρησιμοποιώντας κακόβουλα ψηφιακά μέσα και με απώτερο στόχο την εξασφάλιση της ανωτερότητάς τους έναντι αυτών. (Ziolkowski, 2013)
4. Κυβερνοτρομοκρατία (Cyber Terrorism): περιλαμβάνει το σύνολο των πράξεων μη κρατικών δρώντων που αποσκοπούν στην αύξηση των επιπέδων διαταραχής και αμφιβολίας στη λειτουργία ενός έθνους. Γενικά, οι ενέργειες αυτές έχουν σαν στόχο να καλλιεργήσουν το αίσθημα του φόβου μεταξύ των πολιτών μιας χώρας, ένα αίσθημα που προκαλείται από τη μη σωστή λειτουργία των ψηφιακών υπηρεσιών και των δικτύων της χώρας ή από τις τυχόν επιθέσεις σε καίριας σημασίας υποδομές (τραπεζικές, ενεργειακές, υγείας, τροφίμων). Αυτή η κατάσταση μπορεί να οδηγήσει μια χώρα σε αποσταθεροποίηση, σε οικονομική καταστροφή, σε ταραχές και βία. (Ziolkowski, 2013)
5. Κυβερνοπόλεμος: Η διεθνής βιβλιογραφία διαθέτει πλήθος όρων με τους οποίους γίνεται η περιγραφή, αναλύονται οι δυνατότητες και η επίδραση του Κυβερνοπολέμου στις επιχειρήσεις. Έτσι, παρουσιάζεται ως «Κυβερνοπόλεμος» (Cyberwarfare),

«Πληροφοριακός ή Πληροφορικός Πόλεμος» (Information Warfare ή Infowar), «Πόλεμος Δικτύων» (Netwar), ενώ παράλληλα εμπλέκεται με άλλες δραστηριότητες, που περιγράφονται από συναφείς όρους, όπως «Πληροφοριακές Επιχειρήσεις», «Δικτυοκεντρικό Πόλεμο», «Πόλεμο Διοικήσεως και Ελέγχου», «Πόλεμο των ΜΜΕ» κλπ. (Libicki 2009, Ziolkowski 2013)



Εικόνα 1: Περιστατικά κυβερνοεπιθέσεων με βάση την κατηγορία τους το 2020 (Πηγή: "Cyber Attacks Statistics," 2021)



Εικόνα 2: Περιστατικά κυβερνοεπιθέσεων με βάση την κατηγορία τους το 2019 (Πηγή: "Cyber Attacks Statistics," 2021)

Εξετάζοντας τις περιπτώσεις κυβερνοπολέμου, διαπιστώνουμε ότι συχνά αυτές οργανώνονται και υλοποιούνται από κράτη, τα οποία, με ελάχιστο κόστος,

έχουν τη δύναμη να προσβάλλουν ηγετικά κράτη και να ασκήσουν από την πλευρά τους πίεση και πολιτική, όπως για παράδειγμα η Κίνα και η Ρωσία εναντίον των ΗΠΑ. Έτσι, ο κυβερνοπόλεμος αποτελεί μια σειρά δικτυακών συγκρούσεων με σκοπό την εξουθένωση του αντιπάλου, χωρίς επιπτώσεις σε ανθρώπινα θύματα που θα επέφερε ο κανονικός πόλεμος. Η διεξαγωγή του έχει μάλιστα κλιμακούμενη ένταση, σκληρή και ήπια. (Nye 2010, Ranger 2018)

2.2 Διάκριση κυβερνοπολέμου

Ο Κυβερνοπόλεμος διενεργείται με επιχειρήσεις δυο κατηγοριών, επιθετικές και αμυντικές, τα κύρια χαρακτηριστικά των οποίων αναλύονται παρακάτω.

α) Επιθετικές Επιχειρήσεις Κυβερνοπολέμου

Στις εν λόγω επιχειρήσεις επιδιώκεται η καταστροφή του αντίπαλου πληροφοριακού συστήματος και η εκμηδένιση της θέλησης του για τη διενέργεια οποιασδήποτε μορφής κυβερνοπολέμου, εναντίον των φίλιων συστημάτων και δυνάμεων. Η επίθεση διακρίνεται στα στάδια της στοχοποίησης, όπου γίνεται αναζήτηση, εντοπισμός, προσδιορισμός και ανάλυση των στόχων και εν συνεχεία της προσβολής τους, με παραποίηση - διαγραφή δεδομένων και κυριαρχία επί του αντιπάλου στο πληροφοριακό σύστημα (Ελληνική Δημοκρατία, 2020)

Οι επιθετικές επιχειρήσεις Κυβερνοχώρου περιλαμβάνουν μία σειρά από δραστηριότητες – φάσεις. Αρχικά, η φάση προετοιμασίας περιλαμβάνει όλες τις δραστηριότητες που αφορούν την απόκρυψη της επίθεσης (κάλυψη ιχνών - παραπλάνηση) ή την ανάπτυξη κυβερνοόπλων και συγκεκριμένα:

1. Ανάπτυξη κυβερνοόπλων (λογισμικού υλοποίησης κυβερνοεπιθέσεων).
2. Ανάπτυξη τεχνικών επίθεσης.
3. Ανάπτυξη λογισμικών εκμετάλλευσης αδυναμιών λογισμικού, υλικού.
4. Στοχοποίηση
5. Απόκτηση πρόσβασης σε ενδιαμέσους κόμβους- υπολογιστές επίθεσης, με σκοπό την παραπλάνηση του αντιπάλου σχετικά με την προέλευση της επίθεσης.

Στη συνέχεια, η φάση της αναγνώρισης περιλαμβάνει όλες τις δραστηριότητες που σαν σκοπό έχουν την συγκέντρωση των πληροφοριών που αφορούν τον στόχο. Ο στόχος μπορεί να είναι πρόσωπο, εφαρμογή, υπολογιστής, δίκτυο

υπολογιστών, κρίσιμη υποδομή. Στη φάση αυτή αποφασίζεται η μεθοδολογία επίθεσης. Τέλος, η φάση της επίθεσης, απόκτησης πρόσβασης, όπου μετά τη συγκέντρωση των πληροφοριών και κάνοντας χρήση τεχνικών κάλυψης και επίθεσης πραγματοποιείται η επίθεση.

Τις επιθέσεις τις διακρίνουμε σε:

1. Επιθέσεις δικτύων υπολογιστών που περιλαμβάνει εκτός από τους Η/Υ και οποιαδήποτε άλλη ηλεκτρονική συσκευή που συνδέεται στο δίκτυο και διαθέτει επεξεργαστή.
2. Επιθέσεις προσωπικού υπολογιστή.
3. Επιθέσεις εφαρμογών (εφαρμογών ιστοσελίδων, εφαρμογών ελέγχου κλπ).

Ακολουθεί η φάση κάλυψης ιχνών. Μετά την απόκτηση πρόσβασης, ακολουθεί ο καθαρισμός ιχνών, με σκοπό την αποφυγή εντοπισμού της πρόσβασης και της επίθεσης. Εν συνεχεία, η φάση διατήρησης πρόσβασης και ελέγχου, όπου μετά τον καθαρισμό ιχνών πραγματοποιείται η εγκατάσταση λογισμικού διατήρησης πρόσβασης και ελέγχου του στόχου. Η φάση εκμετάλλευσης, όπου συγκεντρώνονται οι τεχνικές πληροφορίες για την επέκταση της επίθεσης και συλλέγονται πληροφορίες γενικού ή ειδικού ενδιαφέροντος και τέλος η φάση προσβολής, όπου σε αυτή τη φάση προστίθεται η δυνατότητα καταστροφής του στόχου. Με τον όρο καταστροφή νοείται κυρίως η καταστροφή ή παραποίηση δεδομένων, η πρόκληση ζημιών ή καταστροφή υπολογιστικών συστημάτων (Η/Υ) και η πρόκληση ζημιών ή καταστροφών σε κρίσιμες υποδομές.(ΓΕΕΘΑ, 2013)

β) Αμυντικές Επιχειρήσεις Κυβερνοπολέμου ή Κυβερνοάμυνα (Cyberdefence)

Σε αυτή τη περίπτωση, επιδιώκεται η προστασία των φίλιων πληροφοριακών συστημάτων με μέτρα που λαμβάνονται για την προστασία του υλικού, λογισμικού και των πληροφοριών, από εχθρική προσέγγιση και αναρμόδια άτομα, που ενδεχομένως θα επιφέρει επισφαλείς επεμβάσεις στο υλικό και λογισμικό ή και απώλεια των πληροφοριών, καθώς επίσης προσβολή του φίλιου πληροφοριακού συστήματος με ιούς.(Ελληνική Δημοκρατία, 2020)

Σκοπός της κυβερνοάμυνας είναι η πρόληψη, ο εντοπισμός, η αξιολόγηση, η αντιμετώπιση και η αποκατάσταση από κυβερνοεπιθέσεις. Η κυβερνοάμυνα απαιτεί μία σειρά από μηχανισμούς, διαδικασίες και συνεχώς αναπτυσσόμενες και δοκιμασμένες δυνατότητες, με σκοπό να προετοιμαστούμε για την πρόληψη, τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση, την αποκατάσταση και την εξαγωγή συμπερασμάτων στην περίπτωση

κυβερνοεπιθέσεων, που έχουν σαν στόχο να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα του κυβερνοχώρου. (ΓΕΕΘΑ, 2013)

Οι στόχοι των επιχειρήσεων κυβερνοάμυνας είναι αρχικά η εκστρατεία ενημέρωσης των χρηστών πληροφοριακών συστημάτων, με σκοπό να αυξηθεί η κατανόηση των κινδύνων και η έκταση των προκλήσεων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, τόσο σε επίπεδο ΕΔ όσο και σε Εθνικό επίπεδο. Επίσης, η έγκαιρη πρόβλεψη, αξιολόγηση και ανάλυση των απειλών κυβερνοχώρου, προκειμένου να λαμβάνονται οι σωστές αποφάσεις από την ηγεσία. Επιπλέον, η πρόληψη, ο εντοπισμός, η αντιμετώπιση και η αποκατάσταση των κυβερνοεπιθέσεων, καθώς και η διατήρηση και αύξηση της τεχνολογικής ανεξαρτησίας της χώρας, μέσω της ενίσχυσης και της ανάπτυξης των εθνικών επιστημονικών ικανοτήτων μας. Ένας ακόμη στόχος είναι η προστασία των πληροφοριακών συστημάτων των ΕΔ και συμβολή στην ασφάλεια των υπολοίπων εθνικών πληροφοριακών συστημάτων και κρίσιμων υποδομών, με σκοπό την εξασφάλιση ισχυρής εθνικής ανθεκτικότητας στις κυβερνοεπιθέσεις.(ΓΕΕΘΑ, 2013)

Η κυβερνοάμυνα χωρίζεται σε τρία επίπεδα: το στρατηγικό, το επιχειρησιακό και το τακτικό. Στο στρατηγικό επίπεδο, υψηλή προτεραιότητα έχει η οργάνωση και ο συντονισμός της Κυβερνοάμυνας με την εφαρμογή της ενιαίας πολιτικής κυβερνοάμυνας. Η συνεχής και σε 24ωρη βάση εγρήγορση, για τον άμεσο εντοπισμό επιχειρήσεων εν εξελίξει Κυβερνοεπιθέσεων, πρέπει είναι το πρωταρχικό μέλημα στη δυνατότητα αντίδρασης της χώρας. Είναι απαραίτητος ο συντονισμός των εμπλεκόμενων φορέων μέσω της «Διακλαδικής Αρχής Κυβερνοάμυνας», της οποίας αποστολή είναι η έγκαιρη προειδοποίηση για επικείμενες ή εκδηλωθείσες Κυβερνοεπιθέσεις, και ο σωστός σχεδιασμός όλων αυτών των απαραίτητων ενεργειών για την καταπολέμησή τους. Στο επιχειρησιακό επίπεδο, η αποτελεσματική άμυνα απαιτεί την ύπαρξη ενός «Σχεδίου Κυβερνοάμυνας» το οποίο θα αναθεωρείται τακτικά σύμφωνα με τις τεχνολογικές εξελίξεις. Η συνεχής επαγρύπνηση και η αποτελεσματική αντιμετώπιση των κυβερνοπεριστατικών θα πρέπει να δοκιμάζονται μέσα από τη διεξαγωγή κατάλληλα σχεδιασμένων ασκήσεων Κυβερνοάμυνας σε εθνικό επίπεδο, με συμμετοχή και του ιδιωτικού τομέα. Τέλος, στο τακτικό επίπεδο αρχικά είναι απαραίτητη η κατασκευή ενός ελεγχόμενου δικτυακού χώρου (domain), ώστε να υλοποιήσουμε κεντρικά την τεχνική εφαρμογή της πολιτικής ασφαλείας. Ως τεχνική εφαρμογή νοείται το σύνολο των κανόνων - μέτρων ασφαλείας, που επιβάλλονται μέσω λογισμικού στους χρήστες των υπολογιστών. Το επόμενο βήμα είναι ο τεχνικός έλεγχος εφαρμογής της πολιτικής ασφαλείας. Ο τεχνικός έλεγχος θα πρέπει να γίνεται στο σύνολο του δικτύου μέσω ενός κέντρου επιτήρησης. Είναι σημαντικό το υλικό και το

λογισμικό να συμβαδίζουν με τις τεχνολογικές εξελίξεις, δηλαδή να ανανεώνονται τακτικά. Εξίσου σημαντική είναι η ύπαρξη τεχνικών βημάτων - σχεδίων αντιμετώπισης συγκεκριμένων κυβερνοεπιθέσεων. Για να μετριαστεί η τρωτότητα του Κυβερνοχώρου, είναι απαραίτητη η λήψη των παρακάτω μέτρων:

1. Κατά τη σχεδίαση των δικτύων πρέπει να λαμβάνονται υπόψη τα θέματα στιβαρότητας και επιβιωσιμότητας (με βάση τις αρχές της πολλαπλότητας των μέσων και της ύπαρξης εφεδρικών συστημάτων).
2. Εκπόνηση εναλλακτικών σχεδίων τα οποία θα βασίζονται λιγότερο στην τεχνολογία των υπολογιστών.
3. Η διασύνδεση των κρίσιμων συστημάτων με άλλα συστήματα και το διαδίκτυο είναι απαραίτητο να εξετάζεται λεπτομερώς, διασφαλίζοντας μια ισορροπία μεταξύ αποτελεσματικότητας και εξυπηρέτησης του κοινού από τη μια και της ασφάλειας από την άλλη. Ο διαχωρισμός (εσωτερικό δίκτυο), ως αρχή της οργάνωσης των συστημάτων, παρέχει μια βάση για την προστασία τους από Κυβερνοεπιθέσεις.
4. Η φυσική ασφάλεια και η εκπαίδευση του προσωπικού μπορούν να ελαχιστοποιήσουν την εσωτερική απειλή, όπως επίσης και την απειλή της Κυβερνοκατασκοπίας.
5. Μείωση των σημείων διασύνδεσης της χώρας με το διαδίκτυο και έλεγχος αυτών.
6. Έλεγχος των αλυσίδων προμήθειας υλικού και ανταλλακτικών, οι οποίες αποτελούν κλασικούς διαύλους μόλυνσης των συστημάτων επικοινωνιών, πληροφορικής και κρίσιμων υποδομών, μέσω της εμφύτευσης κακόβουλων προγραμμάτων.
7. Δεδομένου ότι είναι σχεδόν αδύνατη η απόλυτη προστασία από Κυβερνοεπιθέσεις, είναι επίσης απαραίτητη η ανάπτυξη δυνατοτήτων περιορισμού των επιπτώσεων και αποκατάστασης των προσβληθέντων συστημάτων. (ΓΕΕΘΑ, 2013)

2.3 Στόχοι επιχειρήσεων κυβερνοπολέμου

Οι βασικοί στόχοι του κυβερνοπολέμου εντοπίζονται σε δύο πεδία. Το πρώτο είναι ο χώρος των ΕΔ και το δεύτερο οι κρίσιμες υποδομές μιας χώρας, ακόμη και αυτές που δεν αποτελούν κρατική ιδιοκτησία. Αρχικά, στόχος είναι η αποδυνάμωση του συνόλου ή μέρους των ΕΔ και το επιτυχές πλήγμα των συστημάτων C2 (Command and Control). Στο δεύτερο πεδίο στόχος είναι οι

κρίσιμες υποδομές (critical infrastructure) κάθε κράτους, η προσβολή των οποίων (φυσική ή ηλεκτρονική) μπορεί να παραλύσει τον κρατικό μηχανισμό και την κοινωνία. Οι υποδομές αυτές συνήθως είναι:

1. Υποδομές Εθνικής Άμυνας και Ασφάλειας
2. Οικονομικές-Τραπεζικές υποδομές
3. Υποδομές Πληροφορικής και Δικτύων Επικοινωνιών δημόσιων και ιδιωτικών φορέων
4. Υποδομές Συστημάτων Κοινής Ωφελείας
    - Υποδομές συστήματος παραγωγής και διάθεσης ηλεκτρικής ισχύος
    - Υποδομές Ύδρευσης και Υδάτινων πόρων
    - Υποδομές Συστήματος παραγωγής, αποθήκευσης και διανομής
5. Υποδομές Συγκοινωνιών
6. Υποδομές Παροχής Υπηρεσιών Υγείας
7. Υποδομές Εξυπηρέτησης πολιτών
8. Υποδομές Διακυβέρνηση
9. Υποδομές για Υπηρεσίες έκτακτης ανάγκης
10. Υποδομές Τροφίμων και Γεωργίας

Οι επιχειρήσεις Κυβερνοπολέμου που πλήττουν μια ή περισσότερες από τις παραπάνω υποδομές έχουν σοβαρότατες επιπτώσεις που μπορεί να διαρκέσουν έως και χρόνια. Στόχος εκτός από αυτές είναι και το ανθρώπινο δυναμικό μιας χώρας (τρομοκρατία, απώλεια της εμπιστοσύνης στον κρατικό μηχανισμό, μειωμένη ικανότητα λήψης αποφάσεων). Τα ψηφιακά συστήματα των οργανισμών «κοινής ωφελείας», όπως η παραγωγή και διανομή ηλεκτρικού ρεύματος, συλλογή και διανομή πόσιμου νερού, συλλογή των λυμάτων, αγωγοί πετρελαίου και φυσικού αερίου, ενσύρματα και ασύρματα δίκτυα επικοινωνιών, δορυφορικά συστήματα, έλεγχος εναέριας κυκλοφορίας, διαχείριση κυκλοφορίας οχημάτων, πυρηνικά εργοστάσια, τραπεζικά και χρηματιστηριακά δίκτυα, αναφέρονται διεθνώς ως SCADA (Supervisory Control And Data Acquisition systems). Δεν είναι όμως κάθε υποδομή εκμεταλλεύσιμη ούτε δύναται να υποβαθμιστεί με τον ίδιο τρόπο. Η προσβολή της εξαρτάται άμεσα από τα διαθέσιμα μέσα και την καταλληλότητά τους.(Carayannis et al. 2014, Libicki 2009)

2.4 Δρώντες κυβερνοεπιθέσεων

Στον Κυβερνοχώρο, οι δρώντες κατηγοριοποιούνται κυρίως βάσει του σκοπού που θέλουν να επιτύχουν. Έτσι, χωρίζονται σε:

1. Μεμονωμένους Χάκερς (Script Kiddies), οι οποίοι συνήθως είναι άτομα νεαρής ηλικίας, με μικρές σχετικά ικανότητες να πραγματοποιήσουν πολύπλοκες επιθέσεις. Το κίνητρό τους είναι η καταξίωσή τους ανάμεσα σε μια ομάδα αντίστοιχων ατόμων και δεν θεωρούνται ιδιαίτερα επικίνδυνοι
2. Μεμονωμένους Χάκερς (Black Hat Hackers), οι οποίοι είναι άτομα με μεγαλύτερη εμπειρία και ικανότητες. Οι πλέον καταξιωμένοι είναι αυτοί που οργανώνουν παγκοσμίως την κυβερνοασφάλεια. Το κίνητρό τους είναι το προσωπικό όφελος, κυρίως οικονομικό.
3. Ακτιβιστές Χάκερς (Hacktivist Hackers), οι οποίοι είναι άτομα ή μικρές ομάδες ατόμων με ικανότητες στις κυβερνοεπιθέσεις που μπορεί να ποικίλουν. Οι καλά οργανωμένες ομάδες μπορούν να σχεδιάσουν και να εκτελέσουν σοβαρές κυβερνοεπιθέσεις. Τα κίνητρά τους μπορεί να είναι πολιτικά, ιδεολογικά, θρησκευτικά και σπανίως οικονομικά.
4. Τρομοκρατικές οργανώσεις (Cyber terrorists), δηλαδή ομάδες ατόμων με μεγαλύτερη εμπειρία, περισσότερες δυνατότητες και με πρόσβαση σε σημαντικούς πόρους, ικανοί να σχεδιάσουν, να προετοιμάσουν και να εκτελέσουν αποτελεσματικά μια επίθεση στον Κυβερνοχώρο. Πολλές φορές, μάλιστα, υποστηρίζονται, οικονομικά και πολιτικά, από κυβερνήσεις. Κίνητρά τους είναι ισχυρά πολιτικά, ιδεολογικά ή θρησκευτικά, με σκοπό την αποδιοργάνωση και τον εκφοβισμό μιας κοινωνίας.
5. Χώρες (States), όπου μέσω κρατικών φορέων αξιοποιούν ομάδες ατόμων με πολύ μεγάλη εμπειρία και ικανότητες, ώστε να σχεδιάζουν, να προετοιμάζουν και να εκτελούν μεγάλης ή και μικρής κλίμακας κυβερνοεπιθέσεις χρησιμοποιώντας εξελιγμένα συστήματα. Κίνητρο των επιθέσεων αυτών είναι η στοχοποίηση μιας άλλης χώρας για την επίτευξη ενός συγκριμένου πολιτικού, επιχειρησιακού ή στρατηγικού στόχου.
6. Οργανωμένοι μη κρατικοί δρώντες (Organized Non-State Actors), οι οποίοι είναι οι πλέον υπεύθυνοι για την πλειοψηφία των κυβερνοεπιθέσεων κατασκοπείας, είτε για δικούς τους σκοπούς, είτε για την υποστήριξη κυβερνητικών προσπαθειών. Οι δρώντες αυτοί είναι οι πιο ικανοί στον πεδίο του Κυβερνοχώρου, είναι αυτοί που ουσιαστικά χτίζουν την υποδομή των κυβερνοεπιθέσεων (κυβερνοόπλα) και

δέχονται τεράστια ποσά κερδών. Τρανό παράδειγμα είναι το πρώην Ρωσικό δίκτυο RBN, το οποίο ήταν υπεύθυνη το 2007 για το 60% των κυβερνοεπιθέσεων παγκοσμίως.

7. Μη οργανωμένοι μη κρατικοί δρώντες (Non-Organized Non-State Actors), δηλαδή μικρές ομάδες ή μεμονωμένα άτομα μη μικρή ή καθόλου οργάνωση υπολειπόμενοι σε δυνατότητες εκτέλεσης κυβερνοεπιθέσεων. Η ζημιά που μπορούν να προκαλέσουν είναι περιορισμένη, συνολικά όμως αντιπροσωπεύει ένα σημαντικό ποσοστό του παγκόσμιου εγκλήματος στον κυβερνοχώρο. Δεν διαθέτουν σημαντικούς πόρους, μπορούν όμως να είναι ευέλικτοι και με σημαντικές τεχνικές γνώσεις. (Carayannis et al. 2014, Refsdal et al. 2015, Ziolkowski, 2013)

2.5 Όπλα κυβερνοεπιθέσεων

Τα συστήματα που χρησιμοποιούν όλοι οι παραπάνω δρώντες για να επιτύχουν το σκοπό τους είναι συνεχώς εξελισσόμενα και με την αδιάκοπη τεχνολογική πρόοδο θα εμφανίζονται διαρκώς νέα συστήματα, τα οποία θα απαιτούν και νέους τρόπους αντιμετώπισης. Το σημαντικό είναι πως τεράστια οικονομικά ποσά θα δαπανούνται συνεχώς για την ανάπτυξη των συστημάτων αυτών και άλλα τόσα για την αντιμετώπισή τους. Τα κυβερνοόπλα (Cyber Weapons) είναι τα μέσα που χρησιμοποιούν οι δρώντες των κυβερνοεπιθέσεων, με κακόβουλο ή μη τρόπο, ώστε να διεισδύσουν σε ένα αντίπαλο σύστημα και να προκαλέσουν ζημιά ή να το προστατέψουν. Για το λόγο αυτό τα χωρίζουμε σε επιθετικά, αμυντικά και διπλής χρήσης.

α) Τα επιθετικά (Offensive) μέσα χρησιμοποιούνται με κακόβουλο χαρακτήρα και τα σημαντικότερα από αυτά είναι:

1. Ιός (Virus), το οποίο είναι ένα λογισμικό που προσβάλει απευθείας αρχεία και συστήματα. Το αποτέλεσμα είναι η διαγραφή αρχείων από τον Η/Υ που έχει μολυνθεί χωρίς τη δυνατότητα επαναφοράς τους, η μετατροπή των αρχείων σε διαφορετικά και μη εκτελέσιμα από το χρήστη, ακόμη και η απόκτηση ελέγχου ολόκληρου του Η/Υ.
2. Σκουλήκι (Worm), το οποίο είναι ένα λογισμικό που διαδίδεται ευκολότερα από τον ιό, χρησιμοποιεί το διαδίκτυο για να μεταδίδεται και προσβάλει κυρίως εξυπηρετητές, ηλεκτρονικά ταχυδρομεία και μέσα κοινωνικής δικτύωσης. Για το λόγο αυτό ο κάθε άνθρωπος είναι πιθανό θύμα. Είναι ένα λογισμικό που αντιγράφει τον εαυτό του ασταμάτητα και λόγω του ότι

χρησιμοποιεί ευρέως διαδεδομένα διαδικτυακά μέσα επικοινωνίας η εξάπλωσή του μπορεί να είναι ραγδαία.

3. Phishing Scam, όπου καλείται ο τρόπος κατά τον οποίο οι δρώντες αποσκοπούν στην απόκτηση ευαίσθητων πληροφοριών και προσωπικών δεδομένων από το θύμα, όπως ονόματα χρηστών, προσωπικοί κώδικες, τραπεζικοί λογαριασμοί κ.α.
4. Δούρειος Ίππος (Trojan horse), το οποίο είναι ένα μεταμφιεσμένο λογισμικό με κακόβουλο σκοπό, αλλά με αθώα εμφάνιση. Μπορεί, δηλαδή, να είναι ένα λογισμικό με κοινό όνομα που ξεγελάει το χρήστη με σκοπό να προκαλέσει διαταραχή και σύγχυση του στοχοποιημένου συστήματος.
5. Απαγόρευση παροχής υπηρεσιών (Denial of Service Attack), όπου πλήττεται μια παρεχόμενη υπηρεσία ώστε να καταστεί ανίκανη να ανταποκριθεί στις εισερχόμενες απαιτήσεις των χρηστών. Ουσιαστικά πρόκειται για μια μαζική εκδήλωση επισκέψεων σε δίκτυα ή διακομιστές ατόμων ή οργανισμών, με σκοπό την υποβάθμιση ή διακοπή της λειτουργίας τους.
6. Logic Bomb, ένα λογισμικό που εγκαθίσταται σε ένα Η/Υ, αδρανοποιείται και υπό συγκεκριμένες προϋποθέσεις ενεργοποιείται, με αποτέλεσμα την καταστροφή αρχείων του ή και ολόκληρου του συστήματος.
7. Malware (Malicious Software), το οποίο είναι οποιοδήποτε λογισμικό έχει κατασκευαστεί με σκοπό να δράσει κακόβουλα και να βλάψει Η/Υ, δίκτυα ή servers.
8. Botnet, το οποίο είναι μια ομάδα συστημάτων που χρησιμοποιούν κακόβουλα λογισμικά υπό μια κεντρική διαχείριση και χωρίς να γίνονται αντιληπτά αναλαμβάνουν τον έλεγχο των προσβληθέντων συστημάτων. Το αποτέλεσμα είναι η ικανότητα του δρώντα να ασκεί κεντρικό έλεγχο των συστημάτων αυτών και κατ΄επέκταση να αποκτά πρόσβαση και σε πολλά περισσότερα συστήματα.

β) Τα αμυντικά (Defensive) μέσα χρησιμοποιούνται για την προστασία των συστημάτων από τα κακόβουλα λογισμικά. Τα σημαντικότερα από αυτά είναι:

1. Κρυπτογράφηση (Encryption), όπου πληροφορίες και αρχεία κρυπτογραφούνται και απαιτείται ειδικό «κλειδί» για να διαβαστούν. Με τον τρόπο αυτό, ακόμη και να υποκλαπούν, αυτός που θα τα έχει στην κατοχή του δε θα μπορεί να τα χρησιμοποιήσει.
2. Τοίχος προστασίας (Firewall), το οποίο είναι ένα λογισμικό προστασίας που παρακολουθεί τα εισερχόμενα και εξερχόμενα δεδομένα από ένα σύστημα και εμποδίζει τη ροή αυτή σε ένα μη έμπιστο σύστημα.

γ) Τα μέσα διπλής Χρήσης (Dual Use) χρησιμοποιούνται για τον έλεγχο σωστής λειτουργίας των υπαρχόντων συστημάτων και τα σημαντικότερα από αυτά είναι:

1. Τα Port Vulnerability Scanners, τα οποία είναι λογισμικά που επιτρέπουν τον έλεγχο της κατάστασης του συστήματος και την αναζήτηση των τρωτών σημείων, λειτουργία που συμβάλει στη πρόληψη από τυχόν κακόβουλα λογισμικά.
2. Τα Network Monitoring, τα οποίο είναι αντίστοιχα λογισμικά για τον έλεγχο των δικτύων και τον εντοπισμό τρωτών σημείων. (Carayannis et al. 2014, Elisan and Hypponen, 2013, Thomas and Stoddard 2012)

2.6 Κυβερνοασφάλεια

Η κυβερνοασφάλεια, όπως καθορίζεται και από την ίδια τη λέξη, αφορά την ασφάλεια του κυβερνοχώρου. Οι περισσότεροι οργανισμοί όμως ανησυχούν για την ασφάλεια των συστημάτων τους και των δικτύων τους έναντι των απειλών του κυβερνοχώρου. Έτσι λοιπόν, κυβερνοασφάλεια είναι η προστασία των συστημάτων του κυβερνοχώρου έναντι των απειλών του. Είναι μια στρατηγική πράξεων αποτροπής και πράξεων πρόληψης. Είναι απαραίτητο να την ανάγουμε στο στρατηγικό και επιχειρησιακό πλαίσιο και κατ' επέκταση σε όλα τα κοινωνικό-πολιτικά επίπεδα, οικονομικά, μηχανολογικά, νομικά και θεωρητικά. Είναι επίσης, απαραίτητο να είναι μια στρατηγική ολιστικά και πολιτικά προσανατολισμένη στις επιχειρήσεις, μια στρατηγική σύγχρονη και καινοτόμα. Στον τομέα της άμυνας, η κυβερνοασφάλεια είναι μια κούρσα τεχνολογικής ανάπτυξης και εξοπλισμών. (Efthymiopoulos 2019, Refsdal et al. 2015)

Μια σωστή στρατηγική ξεκινά αρχικά από την απλοποίηση. Πλέον, οι Η/Υ ξεπερνούν σε δυνατότητες τον ανθρώπινο νου, ο οποίος εξελίσσεται πολύ πιο αργά απ΄ότι αυτοί. Παρόλα αυτά, απαιτείται ο ανθρώπινος παράγοντας για καταλάβουμε πως κάτι ύποπτο υπάρχει σε ένα σύστημα και ειδικότερα άτομα πολύ καλά εκπαιδευμένα και εξειδικευμένα. Η απλοποίηση των ρυθμίσεων των Η/Υ ή του δικτύου μιας εταιρείας ή ενός οργανισμού θα βοηθήσει τον διαχειριστή του συστήματος να εντοπίσει γρηγορότερα την απειλή. Εάν η απειλή ή το σύστημα είναι πολύπλοκο τότε θα πρέπει να κατανεμηθούν εργασίες σε περισσότερα άτομα, ώστε η αντιμετώπιση και ο μετριασμός των αποτελεσμάτων να γίνει γρηγορότερα και αποτελεσματικότερα. Επίσης, σε

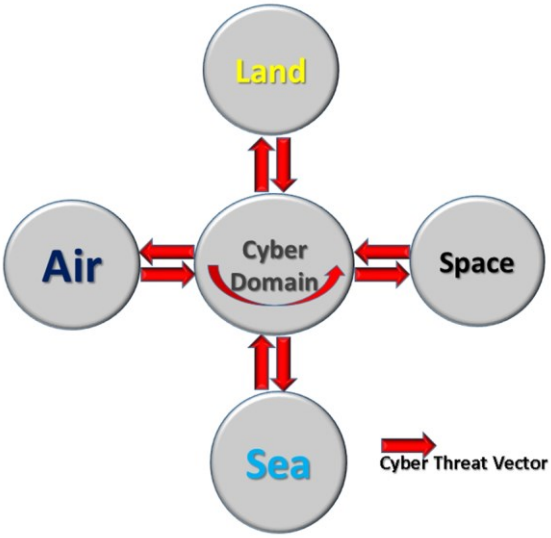
καταστάσεις ανάγκης, όπου η απειλή είναι μεγαλύτερης κλίμακας και διακυβεύονται κρίσιμες υποδομές ή λειτουργίες, τότε πρέπει να γίνεται διαχείριση αρχικά στα πιο χαμηλά επίπεδα με σκοπό την τυχόν απενεργοποίηση του πυρήνα του συστήματος που έχει απειληθεί, διατηρώντας ταυτόχρονα την ικανότητα να απευθυνθούμε στα υψηλότερα επίπεδα διαχείρισης, όπως μια ανώτατη εθνική αρχή αντιμετώπισης των κυβερνοαπειλών.(Henriksen 2019, Libicki 2009)

Οι απειλές του κυβερνοχώρου, όπως αναφέρθηκε και παραπάνω, μπορεί να είναι κακόβουλες ή μη. Αυτό που μας ενδιαφέρει στην στρατηγική της κυβερνοασφάλειας δεν είναι το τι θέλουμε να προστατέψουμε, αλλά από τι θέλουμε να το προστατέψουμε. Ποιος είναι δηλαδή ο σκοπός του επιτιθέμενου. Επιπλέον, σε δεύτερο χρόνο, στόχος μας είναι να καθορίσουμε τις απειλές ώστε να επιτύχουμε την ανθεκτικότητα στον κυβερνοχώρο. Με στόχο αυτό, σε εθνικό επίπεδο, όλοι οι δημόσιοι και ιδιωτικοί φορείς πρέπει να συνεργάζονται στενά και αποτελεσματικά, ώστε να αναπτύσσουν δυνατότητες αντιμετώπισης των κυβερνοαπειλών. Τα Υπουργεία Εθνικής Άμυνας, Εσωτερικών, Προστασίας του Πολίτη και Δικαιοσύνης σε συνεργασία με τα σώματα ασφαλείας και τις υπηρεσίες πληροφοριών, τα πανεπιστήμια και τυχόν κέντρα ερευνών στον τομέα της ασφάλειας, είναι απαραίτητο να συνεργαστούν για τη διαμόρφωση μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας. Επίσης, πρέπει να επιδιώκεται η συνεργασία με άλλες χώρες, ώστε να μοιράζονται νέες στρατηγικές αντιμετώπισης και νέες τεχνολογίες. Επιπλέον, ο ιδιωτικός τομέας μέσω των νέων επιχειρήσεων και της βιομηχανίας πρέπει να παίξει ενεργό ρόλο, μιας και οι σύγχρονες και πρωτοποριακές τεχνικές που χρησιμοποιούνται πολλές φορές αργούν να γίνουν ευρέως γνωστές. Οι κατασκευάστριες εταιρείες είναι αυτές που προμηθεύουν τα υλικά και τα συστήματα σε παγκόσμιο επίπεδο το πεδίο του κυβερνοχώρου. Άρα, αυτές οι ίδιες θέτουν τα κριτήρια λειτουργίας τους, διαμορφώνουν τα πρωτόκολλα, κατά συνέπεια λοιπόν, αυτές μπορούν να μειώσουν και τις επιπτώσεις των κυβερνοαπειλών και του κυβερνοπολέμου. (European Parliament 2017, Henriksen 2019)

Στο πλαίσιο αυτό πολλές χώρες και διεθνής οργανισμοί, μετά τη διαπίστωση πως ο κυβερνοπόλεμος είναι η πλέον σύγχρονη μορφή πολέμου και οι επιπτώσεις του μπορεί να είναι σοβαρότατες, προχώρησαν στη δημιουργία στρατηγικής της κυβερνοασφάλειας. Χώρες όπως οι ΗΠΑ, η Αγγλία, η Γαλλία, η Κίνα, η Ιαπωνία και διεθνής οργανισμοί όπως το ΝΑΤΟ, η ΕΕ, ο ΟΗΕ, ο Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (OSCE), ο Διεθνής Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD), η Αφρικανική Ένωση, η Ένωση Εθνών Νοτιοανατολικής Ασίας (ASEAN) και πολλοί άλλοι έχουν αναπτύξει πολιτικές και στρατηγικές αντιμετώπισης κυβερνοαπειλών.

2.6.1 Η Κυβερνοασφάλεια στο ΝΑΤΟ

Το ΝΑΤΟ ήταν από τους πρώτους διεθνείς οργανισμούς που συνέταξαν μια ολοκληρωμένη πολιτική κυβερνοασφάλειας. Συνειδητοποιώντας πως στον κυβερνοχώρο υπάρχει πλέον ελεύθερη ροή πληροφοριών και η ανάγκη για τη σωστή λειτουργία των δικτύων ώστε να παρέχεται η απρόσκοπτη εκμετάλλευση όλων των κοινωνικών και στρατιωτικών υπηρεσιών είναι κρίσιμη, κρίθηκε σκόπιμη η δημιουργία μιας κοινής πολιτικής κυβερνοασφάλειας μεταξύ των χωρών μελών του ΝΑΤΟ. Η αρχή έγινε με το συνέδριο της Ουαλίας το 2014 και η συνέχεια δόθηκε με τα συνέδρια της Βαρσοβίας και των Βρυξελών το 2016, όπου τα κράτη μέλη συναίνεσαν στην πλήρη εφαρμογή του Διεθνούς Δικαίου στον κυβερνοχώρο και στην αναγνώριση κυβερνοαπειλών συγκεκριμένης βαρύτητας ως επιθέσεις ισάξιες ενόπλων επιθέσεων. Επίσης, αναγνωρίσθηκε ο κυβερνοχώρος ως ένα επιχειρησιακό πεδίο ανάλογο των πεδίων της ξηράς, της θάλασσας και του αέρα. (“Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA),” 2019)



Εικόνα 3: Η σχέση του κυβερνοχώρου με τα άλλα επιχειρησιακά πεδία (πηγή: Cybersecurity in the EU Common Security and Defense Policy)

Αρχικά έπρεπε να δοθεί ιδιαίτερη σημασία στη σωστή σχεδίαση των επιχειρήσεων του κυβερνοχώρου, ο οποίος κρίθηκε απαραίτητο να χωριστεί σε υποτομείς, ώστε οι επιχειρήσεις να μην επηρεάζουν τον κυβερνοχώρο

συνολικά. Επίσης, οι επιχειρήσεις του ΝΑΤΟ είναι υποχρεωτικό να συμβαδίζουν σύμφωνα με το διεθνές δίκαιο, το δίκαιο των ενόπλων συγκρούσεων και το δίκαιο των ανθρωπίνων δικαιωμάτων. Για το λόγο αυτό τέθηκαν εξαρχής αρκετοί περιορισμοί. Το νομικό πλαίσιο των επιχειρήσεων καθορίζεται κάθε φορά από το Βορειοατλαντικό Συμβούλιο (North Atlantic Council,NAC), την εθνική αρχή, τις τυχόν επιπτώσεις των επιχειρήσεων, από το αν διενεργούνται παράλληλα με ένοπλες επιχειρήσεις και από το αν οι επιχειρήσεις αυτές είναι επιθετικές ή αμυντικές.(NATO STANDARDIZATION OFFICE (NSO), 2020)

Ξεκινώντας λοιπόν, γίνεται μια εμπεριστατωμένη ανάλυση από ειδικευμένο προσωπικό της λειτουργικής κατάστασης του κυβερνοχώρου και των πιθανών επιπτώσεων των επιχειρήσεων. Στο σημείο αυτό ο διοικητής των επιχειρήσεων αποφασίζει εάν θα κάνει χρήση του SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies), που ουσιαστικά είναι η έγκριση δικαιοδοσίας χρήσης επιθετικών εργαλείων για την αντιμετώπιση των κυβερνοαπειλών. Στη συνέχεια γίνεται η αναγνώριση των εχθρικών δρώντων, των δυνατοτήτων τους και των απειλών. Εξετάζονται τυχόν εμπλοκές με συμφωνίες ή συμβάσεις μεταξύ κρατών, πολιτικά ή νομικά θέματα, η δυνατότητα συνεργασίας και εμπλοκής στρατιωτικών μέσων και τέλος γίνεται μια αρχική ανάλυση ρίσκου για πιθανές επιπτώσεις σε φίλια τμήματα του κυβερνοχώρου.

Από την παραπάνω αρχική ανάλυση εξάγονται κάποια αποτελέσματα που χρησιμοποιούνται από την ομάδα σχεδίασης για τον καθορισμό του σχεδίου ενεργείας. Έτσι, προτείνεται ο τρόπος διεξαγωγής των επιχειρήσεων ανάλογα με το επιθυμητό αποτέλεσμα, συντονίζονται οι επιχειρήσεις με το επιθυμητό αποτέλεσμα, πιστοποιούνται οι στόχοι, αναγνωρίζονται σημεία κλειδιά για τη λήψη περεταίρω αποφάσεων και τελικά αποφασίζεται ο ενδεδειγμένος τρόπος διεξαγωγής των ενεργειών από το διοικητή. (NATO STANDARDIZATION OFFICE (NSO), 2020)

Φθάνοντας στη φάση της εκτέλεσης, έχει προηγηθεί η εξάσκηση των επιχειρήσεων σε εκπαιδευτικό περιβάλλον και ο σωστός συντονισμός όλων των μέσων και τομέων που θα επιβοηθήσουν την όλη επιχείρηση, ώστε να διασφαλιστεί η επιτυχία της. Κατόπιν, δίνεται η εντολή για την έναρξη των επιχειρήσεων όπου ο διοικητής βρίσκεται σε συνεχή επαφή με το συντονιστικό προσωπικό, ώστε εάν προκύψουν τυχόν προβλήματα να αντιμετωπιστούν άμεσα. Τέλος, με το πέρας των ενεργειών, πραγματοποιείται η εκτίμηση και αξιολόγηση των αποτελεσμάτων ώστε να ξεκινήσει νέος σχεδιασμός σε περίπτωση αποτυχίας ή μη ικανοποιητικού αποτελέσματος. (NATO STANDARDIZATION OFFICE (NSO), 2020)

2.6.2 Η Κυβερνοασφάλεια στην ΕΕ

Η ΕΕ, όπως και το ΝΑΤΟ, δίνει μεγάλη σημασία τα τελευταία χρόνια στην κυβερνοασφάλεια. Υποστηρίζεται πως θα πρέπει να γίνεται συνεχής προσπάθεια για την ενίσχυση των δυνατοτήτων τόσο του δημόσιου όσο και του ιδιωτικού τομέα στην αντιμετώπιση των κυβερνοαπειλών. Περισσότερα κεφάλαια θα πρέπει να αποδεσμεύονται και να αξιοποιούνται για τον εκσυγχρονισμό και τη βελτίωση των διαδικασιών και των υποστηρικτικών μέσων που χρησιμοποιούνται στον κυβερνοχώρο. Έτσι, το 2004 δημιουργήθηκε ο Οργανισμός Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), ο οποίος μάλιστα εδρεύει στο Ηράκλειο της Κρήτης, και έχει σκοπό αρχικά τη δημιουργία της σωστής αντίληψης από τους πολίτες για την ασφαλή χρήση των δικτύων και τη σωστή διακίνηση των πληροφοριών. Ο ρόλος του είναι καθαρά συμβουλευτικός, με σκοπό να παρέχει σε όλα τα κράτη μέλη την κατάλληλη γνώση που έχει αποκτηθεί μέσα από τη συγκέντρωση δεδομένων, ώστε να σχεδιάζονται και να λειτουργούν σωστά τα δίκτυα του κυβερνοχώρου. (ENISA, 2020)

Παρόλο που έχουν γίνει πολλές προσπάθειες σε εθελοντικό επίπεδο, υπάρχουν πάρα πολλά κενά σε όλες τις χώρες της ΕΕ, όσων αφορά στις δυνατότητες, τα μέσα και το συντονισμό στην καταπολέμηση των κυβερνοαπειλών. Τα κενά αυτά ήρθε να καλύψει η στρατηγική κυβερνοασφάλειας της ΕΕ που συντάχθηκε στις Βρυξέλες το 2013 και η οποία συνοδεύεται από νομοθετική πρόταση ώστε να καθοριστούν αρχικά τα ελάχιστα προαπαιτούμενα, σε εθνικό επίπεδο, για τη σωστή δημιουργία ενός πλαισίου κυβερνοασφάλειας. Έτσι, κάθε κράτος μέλος της ΕΕ υποχρεούται να δημιουργήσει μια ομάδα αντιμετώπισης περιστατικών ασφαλείας (CERT), η οποία θα συλλέγει πληροφορίες και περιστατικά, τα καταγράφει, τα ταξινομεί και γενικά είναι υπεύθυνη για τα πληροφοριακά συστήματα των οργανισμών της χώρας, δημόσιων ή ιδιωτικών. Παράλληλα, η ομάδα αυτή είναι υπεύθυνη για το σωστό συντονισμό των μέσων και των υπηρεσιών που χρησιμοποιούνται για το μετριασμό των επιπτώσεων των κυβερνοαπειλών, καθώς και για τη σωστή συνεργασία μεταξύ αυτών. Τέλος, η ομάδα αυτή θα πρέπει να βοηθήσει όλους τους ιδιωτικούς φορείς να κατασκευάσουν και αυτοί δικές τους ομάδες αντιμετώπισης περιστατικών ασφαλείας, μιας και η πλειοψηφία των δικτύων και των πληροφοριακών συστημάτων είναι ιδιωτική. (Carayannis et al. 2014, EUROPEAN COMMISSION 2013)

Στην ΕΕ η κύρια αρχή εξουσίας κυβερνοασφάλειας είναι η Ευρωπαϊκή Επιτροπή. Αυτή είναι υπεύθυνη για τη σωστή συνεργασία με τις εθνικές αρχές ώστε να αναγνωρίζονται τα τρωτά σημεία των δικτυακών υποδομών. Επίσης, μπορεί να ζητήσει τη συμβολή του ENISA να βοηθήσει τα κράτη μέλη στη δημιουργία και την κατασκευή ασφαλούς περιβάλλοντος κυβερνοχώρου, προσφέροντας τις κατάλληλες γνώσεις και παράλληλα, για την αξιολόγηση των μέτρων και των διαδικασιών, δύναται η εκτέλεση ασκήσεων κυβερνοεπιθέσεων για την βέλτιστη επιχειρησιακή ετοιμότητα των κρατών αυτών. Στο πλαίσιο αυτό, η Ευρωπαϊκή Επιτροπή σε συνεργασία με τον ENISA οργάνωσε το 2014 διαγωνισμό μεταξύ των πανεπιστημίων, όπου φοιτητές είχαν την ευκαιρία να προτείνουν λύσεις αύξησης του επιπέδου της κυβερνοασφάλειας. Παράλληλα, από το 2013 και μετά, ορίζεται ετησίως ο μήνας κυβερνοασφάλειας, όπου σκοπεύει στην ευαισθητοποίηση των πολιτών επί αυτών των θεμάτων. Το ίδιο έτος ιδρύθηκε και το Ευρωπαϊκό Κέντρο για Κυβερνοεγκλήματα (European Cybercrime Centre-EC3) σε συνεργασία με τη EUROPOL, με σκοπό την επιβολή κυρώσεων σε όσους διαπράττουν παράνομες πράξεις στον κυβερνοχώρο και την προστασία έτσι των πολιτών, των επιχειρήσεων και των κυβερνήσεων της ΕΕ. Μέσω του κέντρου αυτού παρέχονται πληροφορίες, υποστηρίζονται έρευνες, παρέχονται υψηλού επιπέδου εγκληματολογικά στοιχεία, δημιουργούνται κανάλια επικοινωνίας και διαμοιρασμού πληροφοριών μεταξύ των εμπλεκόμενων φορέων και αρχών ενός έθνους ή μεταξύ του ιδιωτικού τομέα και άλλων δρώντων. Με αυτόν τον τρόπο, το EC3 καταφέρνει την αναγνώριση, καταπολέμηση και αφανισμό των δικτύων κυβερνοεγκλήματος, ιδιαίτερα αυτών που σχετίζονται με κακοποίηση ανηλίκων, οικονομικές απάτες και διείσδυση σε απόρρητα δίκτυα και υπηρεσίες. (EUROPEAN COMMISSION 2013, European Parliament 2017)

2.6.3 Η κυβερνοασφάλεια στις ΗΠΑ

Αντίστοιχα οι ΗΠΑ, μέσω του Υπουργείου Εσωτερικής Ασφάλειας (Department of Homeland Security, DHS), εξέδωσε το 2018 τη στρατηγική περί κυβερνοασφάλειας, με σκοπό να καθοριστεί το πλαίσιο ενεργειών και ευθυνών του έναντι στο συνεχώς εξελισσόμενο τομέα του κυβερνοχώρου. Οι στόχοι της στρατηγικής αυτής είναι η αναγνώριση του ρίσκου, η μείωση των τρωτών σημείων, η μείωση των απειλών, ο μετριασμός των συνεπειών και η δημιουργία συστημάτων διαχείρισης των κινδύνων. Όλοι οι παραπάνω στόχοι θα επιτευχθούν βάσει κάποιων κατευθυντήριων αρχών, όπως η προτεραιοποίηση του ρίσκου, η σχέση κόστους με το αποτέλεσμα, η καινοτομία, η ευελιξία, η

συνεργασία, η προσέγγιση από παγκόσμια οπτική καθώς και βάσει των εθνικών αξιών. (U.S. DEPARTMENT OF HOMELAND SECURITY, 2018)

Όσων αφορά την αναγνώριση του ρίσκου, δίνεται βάση στην κατανόηση του κυβερνοχώρου και του τρόπου λειτουργίας του, ώστε ανάλογη να είναι η στάση, η αντιμετώπιση και η διαχείριση των κινδύνων. Πρέπει να καλλιεργηθεί το πνεύμα συνεργασίας μεταξύ όλων των δρώντων, κυβερνητικών και μη, δημοσίου και ιδιωτικού ενδιαφέροντος, ώστε να γίνει κατανοητή από όλους η κοινή στρατηγική αντιμετώπισης. Με τον τρόπο αυτό θα υπάρξει έγκαιρη αναγνώριση των κινδύνων και των απειλών που μπορεί να επηρεάσουν την εθνική ασφάλεια, την οικονομική ασφάλεια και την ασφάλεια της δημόσιας υγείας. Παράλληλα, θα υπάρχει έγκαιρος εντοπισμός των κενών ασφαλείας στη διαχείριση των κινδύνων αυτών και καλύτερος σχεδιασμός των μελλοντικών συστημάτων ώστε να καλύπτονται τα κενά αυτά.

Στην περίπτωση της μείωσης των τρωτών σημείων, πρέπει να επικεντρωθούν οι προσπάθειες στην προστασία των συστημάτων της ομοσπονδιακής κυβέρνησης και να εξασφαλιστεί το σωστό επίπεδο κυβερνοασφάλειας της κάθε υπηρεσίας. Ταυτόχρονα, κάθε εταιρεία ή οργανισμός ιδιωτικού ενδιαφέροντος είναι υποχρεωμένοι να δημιουργούν τα δικά τους συστήματα διαχείρισης των απειλών του κυβερνοχώρου, τα οποία με τη συμβολή του Υπουργείου Εσωτερικής Ασφάλειας θα εμπλουτίζονται με σύγχρονα μέσα, διαδικασίες και υπηρεσίες ώστε να επιτυγχάνεται μια ολιστική προσέγγιση της κυβερνοασφάλειας. Το μεγάλο πρόβλημα των ΗΠΑ είναι η διασπορά των πληροφοριακών συστημάτων της, τα οποία λειτουργούνται κατά βάση από διαχειριστές με μη επαρκές επίπεδο ασφάλειας. Για το λόγο αυτό η προσέγγιση πρέπει να είναι πολυεπίπεδη, οι πρακτικές και τα εργαλεία που εφαρμόζονται να είναι αποτελεσματικότερα, ώστε τελικά να διασφαλιστούν τα πληροφοριακά συστήματα της ομοσπονδιακής κυβέρνησης. (U.S. DEPARTMENT OF HOMELAND SECURITY, 2018)

Όσων αφορά τη μείωση των κινδύνων, ο καλύτερος τρόπος είναι η επιβολή κυρώσεων σε όσους χρησιμοποιούν τον κυβερνοχώρο για παράνομες δραστηριότητες, όπως η κακοποίηση ανηλίκων, οι οικονομικές απάτες και το ξέπλυμα μαύρου χρήματος, η κλοπή πνευματικής ιδιοκτησίας, η παράνομη πώληση προϊόντων κ.α. Για το λόγο αυτό όλοι οι ερευνητές εγκλημάτων πρέπει να έχουν γνώσεις ηλεκτρονικού εγκλήματος, ψηφιακών ερευνών, διάρθρωσης και λειτουργίας του κυβερνοχώρου. Παράλληλα, όλες οι ομάδες αντιμετώπισης εγκλημάτων, ομοσπονδιακές, πολιτειακές ή τοπικές πρέπει να είναι ικανές να εντοπίζουν παράνομες δραστηριότητες στον κυβερνοχώρο και ταυτόχρονα να έχουν τη δικαιοδοσία να επιβάλλουν τις αντίστοιχες κυρώσεις σε συνεργασία με το Υπουργείο Δικαιοσύνης. Υπέρ αυτού πρέπει να συμβάλει το Υπουργείο με τη συνεχόμενη παροχή εξειδικευμένης και υψηλής ποιότητας εκπαίδευση σε

προσωπικό όλων των επιπέδων επιβολής του νόμου. Επίσης, η συνεργασία με τα πανεπιστήμια θα πρέπει να παίξει σημαντικό ρόλο, ώστε νέες τεχνικές αντιμετώπισης να βρουν εφαρμογή.

Σημαντικός επίσης στόχος είναι ο μετριασμός των συνεπειών. Αρχικά, είναι απαραίτητο να καλλιεργηθεί η κουλτούρα της παρατήρησης, της καταγραφής και της αναφοράς περιστατικών κυβερνοαπειλών και τα περιστατικά αυτά να κοινοποιούνται ώστε να γίνονται ευρέως γνωστά. Με τον τρόπο αυτό θα υπάρχει έγκαιρη ενημέρωση και ο πιθανός κίνδυνος να μην επεκταθεί. Παράλληλα, η σωστή εκπαίδευση όλου του προσωπικού που εμπλέκεται με τον κυβερνοχώρο και ειδικότερα με το κυβερνοέγκλημα, καθώς επίσης και οι ασκήσεις προσομοίωσης απειλών σε τακτά χρονικά διαστήματα, θα δώσει τα εφόδια στους εμπλεκόμενους να επιτύχουν το μετριασμό των συνεπειών.

Τέλος, καίριας σημασίας είναι και η δημιουργία συστημάτων διαχείρισης των κινδύνων σε παγκόσμιο επίπεδο. Προσπάθειες και νέες τεχνολογικές καινοτομίες παγκοσμίου επιπέδου πρέπει να υποστηρίζονται και να υποβοηθούνται με οποιοδήποτε τρόπο, με σκοπό τη δημιουργία νέων και βελτιωμένων συστημάτων ασφαλείας. Επιπλέον, είναι απαραίτητη η εκμετάλλευση της υπάρχουσας τεχνογνωσίας ώστε να καθοριστούν πρότυπα και πρωτόκολλα διαχείρισης των κινδύνων, μιας που ο κυβερνοχώρος είναι συνεχώς εξελισσόμενος και πολυεπίπεδος. (U.S. DEPARTMENT OF HOMELAND SECURITY, 2018)

3. Ανάλυση ρίσκου κυβερνοεπίθεσης

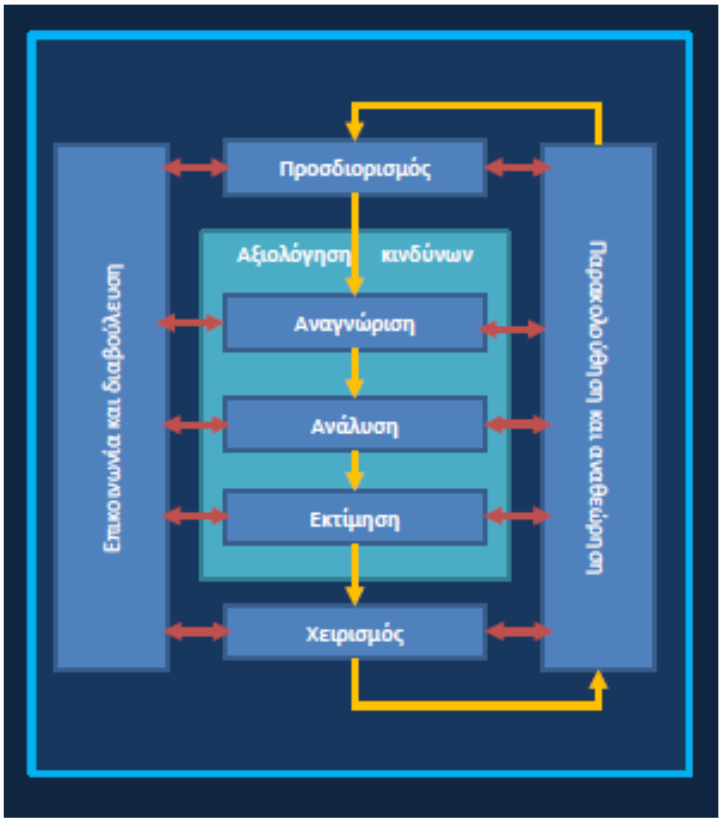
3.1 Η προσέγγιση της απειλής

Το κρίσιμο χαρακτηριστικό του κυβερνοχώρου, όπως αναλύθηκε παραπάνω, είναι το μέγεθός του, καθώς δεν έχει γεωγραφικά ή φυσικά σύνορα. Επιπλέον, οι διαστάσεις του διαρκώς αυξάνονται, λόγω της εξελισσόμενης τάσης στον τομέα της ψηφιακής τεχνολογίας και των δικτύων Η/Υ, καθιστώντας την οριοθέτησή του πρακτικά αδύνατη. Αυτό σημαίνει ότι μια πιθανή απειλή μπορεί να κάνει την εμφάνισή της προερχόμενη από οποιοδήποτε σημείο του πλανήτη και με την ικανότητα να αλλάζει συνεχώς τη θέση της. Και επειδή οι απειλές μπορεί να είναι κακόβουλες ή μη, ανάλυση ρίσκου γίνεται κατά κύριο λόγο σε απειλές της πρώτης κατηγορίας. Εάν καταστραφεί ένας Η/Υ, για παράδειγμα, από μια υπερφόρτωση του δικτύου ρεύματος, δεν θεωρείται κυβερνοαπειλή. Ως εκ τούτου, μια ανάλυση ρίσκου δεν έχει βάση. Εάν όμως την υπερφόρτωση του δικτύου την έχει προκαλέσει κάποιος κακόβουλα και απομακρυσμένα, χρησιμοποιώντας τις δυνατότητες του κυβερνοχώρου, τότε μπορούμε να μιλήσουμε για ανάλυση και διαχείριση ρίσκου. Το ίδιο γίνεται και στην περίπτωση που το άτομο αυτό προκάλεσε την υπερφόρτωση και την καταστροφή του Η/Υ άθελά του, χρησιμοποιώντας πάλι τον κυβερνοχώρο. Τότε και σε αυτή την περίπτωση μπορούμε να κάνουμε ανάλυση και διαχείριση ρίσκου. (Refsdal et al., 2015)

Το πλαίσιο διαχείρισης κινδύνου που θα χρησιμοποιήσουμε πραγματοποιεί ένα κύκλο ενεργειών που δεν σταματάει ποτέ. Το πλαίσιο αυτό είναι το ISO 31000, το οποίο είναι σύστημα διαχείρισης κινδύνου που παρέχει τις αρχές και τις κατευθυντήριες αρχές για την όσο το δυνατό αποτελεσματικότερη διαχείριση ενός κινδύνου και βρίσκει εφαρμογή σε κάθε είδους υπηρεσία ή οργανισμό. Βασικό ρόλο στον κύκλο αυτό παίζει η επικοινωνία μεταξύ εσωτερικών και εξωτερικών ενδιαφερομένων, καθώς και η παρακολούθηση των διαδικασιών παρατήρησης των αποκλίσεων από την επιθυμητή ή υποχρεωτική κατάσταση.

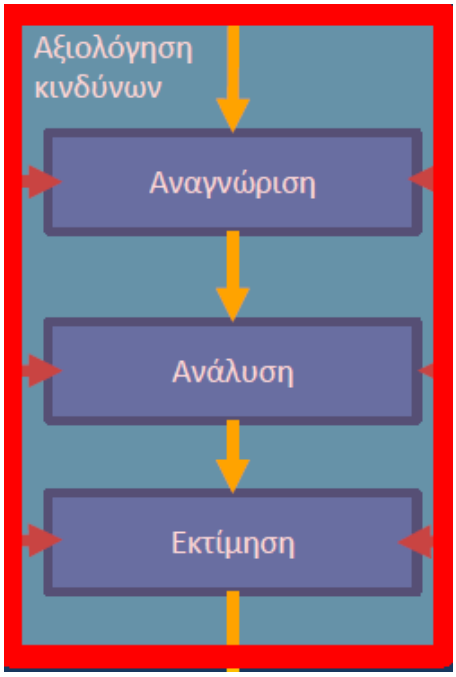
Επίσης, ο προσδιορισμός αφορά την αλληλεπίδραση των κινδύνων με τους στόχους και τους σκοπούς του οργανισμού, αναφορικά με το εσωτερικό και το εξωτερικό περιβάλλον του και με τη διαδικασία διαχείρισης του κινδύνου. Η αξιολόγηση, που περιλαμβάνει την αναγνώριση, την ανάλυση και την εκτίμηση του κινδύνου, έχει σαν σκοπό την παροχή τεκμηριωμένης πληροφόρησης και ανάλυσης για την λήψη αποφάσεων αναφορικά με τον χειρισμό των κινδύνων. Τέλος, ο χειρισμός είναι το σύνολο των αποφάσεων για τον έλεγχο του κινδύνου και η εξέταση του εάν ο υπολειμματικός κίνδυνος (residual risk) είναι ανεκτός.(Χουντάλας, 2020)

.



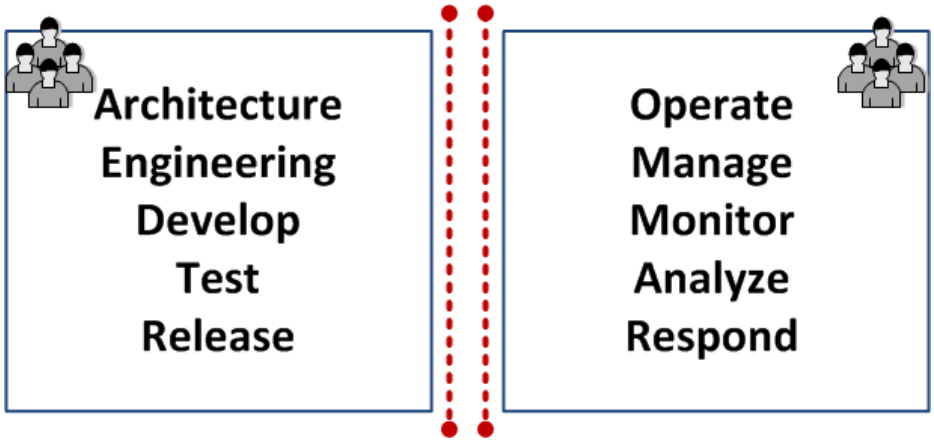
Εικόνα 4: Διαδικασία διαχείρισης κινδύνων κατά ISO 31000 (Πηγή: iso.org, 2018)

Βασικό στοιχείο για να πραγματοποιήσουμε μια ποιοτική ανάλυση (qualitive analysis) είναι ο πυρήνας του παραπάνω πλαισίου, η αξιολόγηση της απειλής. Αυτή θα είναι η βάση μας για ένα σωστά δομημένο σύστημα, δίκτυο, εταιρεία ή οργανισμό.



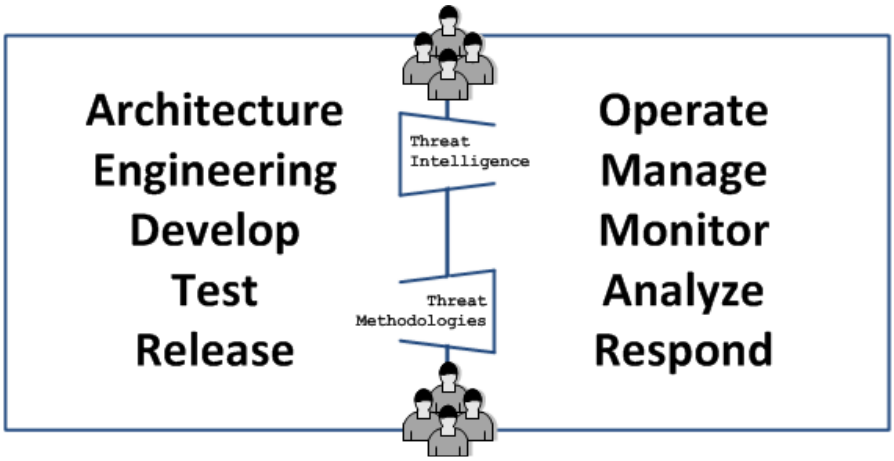
Εικόνα 5: Η διαδικασία αξιολόγησης του κινδύνου (Πηγή: iso.org, 2018)

Είναι βασικό λοιπόν να γνωρίζουμε την απειλή, από τι θέλουμε να προστατευτούμε δηλαδή, και λιγότερο το μέσο που θέλουμε να προστατέψουμε. Η προσέγγιση αυτή θα επιτρέψει σε όλους τους φορείς, δημόσιους ή ιδιωτικούς, να διαθέσουν τους απαραίτητους πόρους, ώστε να αναπτύξουν συστήματα για την αποτελεσματικότερη προστασία τους. Για να είναι αποτελεσματική αυτή η προσέγγιση, όμως, θα πρέπει να υπάρξει συνεργασία μεταξύ αυτών που σχεδιάζουν ένα σύστημα και αυτών που το χρησιμοποιούν. Όπως φαίνεται και στην παρακάτω εικόνα, υπάρχει ένα τείχος μεταξύ των αρχιτεκτόνων των συστημάτων, οι οποίοι είναι υπεύθυνοι για την κατασκευή-ανάπτυξη-έλεγχο των συστημάτων, και των χρηστών, οι οποίοι λειτουργούν-παρακολουθούν-αναλύουν-αξιολογούν το σύστημα. (Beuchelt et al., 2015)



Εικόνα 6: Διαχωρισμός δομής κυβερνοχώρου (Πηγή: Muckin and Fitch, 2019)

Για να υπάρξει μια πιο ολοκληρωμένη προσέγγιση πρέπει γκρεμιστεί το τοίχος αυτό και να συνεργαστούν αρμονικά οι δύο πλευρές. Το ιδεατό θα ήταν να γίνει αυτό εντός κάθε οργανισμού, υποστηριζόμενο σε όλα τα επίπεδα διαχείρισής του, ώστε να υπάρχει άμεση και αποτελεσματικότερη αντιμετώπιση των προβλημάτων και των απειλών. (Muckin and Fitch, 2019)



Εικόνα 7: Ολοκληρωμένη προσέγγιση της απειλής (Πηγή: Muckin and Fitch, 2019)

Οι στόχοι αυτής της προσέγγισης είναι να γίνει αρχικά λεπτομερής εντοπισμός και καταγραφή των στοιχείων εκείνων που έχουν σημαντική αξία για τον επιτιθέμενο, στη συνέχεια πώς μπορούν να απειληθούν και έπειτα ποια θα είναι η τυχόν διαδικασία που μπορεί να ακολουθηθεί. Στη συνέχεια πρέπει να εντοπιστούν τα τρωτά σημεία του συστήματος μέσω ενδελεχούς ανάλυσης και με τη σωστή συνεργασία των σχεδιαστών και των χρηστών αυτού. Άρα, η πρώτη φάση είναι αυτή της ανακάλυψης-αναγνώρισης και η δεύτερη της ανάλυσης-εφαρμογής. (Beuchelt et al., 2015)

Εικόνα 8: Οι δυο φάσεις της ανάλυσης (Πηγή: Muckin and Fitch 2019)

Στο στάδιο της ανακάλυψης συμπεριλαμβάνονται:

1. η αναγνώριση και καταγραφή των στοιχείων αξίας, δηλαδή τα στοιχεία εκείνα που είναι κρίσιμα για τη λειτουργία του οργανισμού ή της επιχείρησης ή τα στοιχεία εκείνα που είναι κρίσιμα για την ασφάλεια αυτού μέσω έγκυρων πληροφοριών που αφορούν τους επιτιθέμενους
2. ο προσδιορισμός του συστήματος στο οποίο βρίσκονται τα στοιχεία αυτά, ώστε να προσδιοριστεί ο τρόπος με τον οποίο θα μπορέσει να αποκτήσει πρόσβαση ο επιτιθέμενος
3. η αναλυτική περιγραφή του συστήματος αυτού για να καθορισθούν όλα τα υποστοιχεία από τα οποία αποτελείται (συσκευές, λογισμικά, πρωτόκολλα, λειτουργίες)
4. η αναγνώριση των διαφορετικών διαδρομών επίθεσης, όπου μελετώντας τα τρωτά σημεία μπορεί να καθοριστεί ο τρόπος ενεργείας της επίθεσης και των διαφορετικών οδών που μπορεί να χρησιμοποιήσει
5. η αναγνώριση των πιθανών δρώντων, όπου γίνεται μια λίστα των ποιων και γιατί θέλουν να βλάψουν το σύστημα, ποια είναι τα κίνητρά τους, οι ικανότητές τους, οι διαθέσιμοι πόροι τους και οι αντικειμενικοί σκοποί τους.

Στο στάδιο της εφαρμογής συμπεριλαμβάνονται:

1. η ανάλυση, όπου με τη βοήθεια όλων των στοιχείων που συγκεντρώθηκαν από το πρώτο στάδιο γίνεται μια λεπτομερής ανάλυση

των αιτιών της επίθεσης, των αποτελεσμάτων που θα έχουν, καθώς και τη δυσμενέστερη έκβαση
2. η εκτίμηση, όπου γίνεται προτεραιοποίηση των εκβάσεων
3. τα μέτρα, όπου αποφασίζονται ποια θα είναι αυτά, ώστε να αντιμετωπισθεί η απειλή και να μετριασθεί ο αντίκτυπός της. Στη φάση αυτή γίνεται και η αξιολόγηση των μέτρων αυτών ως προς την αποτελεσματικότητά τους με σκοπό τη βελτίωσή τους. Με τον τρόπο αυτό, πιθανά τρωτά σημεία και κενά ασφαλείας δύναται να ανακαλυφθούν και να καλυφθούν. (Muckin and Fitch, 2019)

3.2 Εργαλεία ανάλυσης των απειλών

Περνώντας από το στάδιο όπου γίνεται η προσέγγιση των απειλών πρέπει να βρούμε τα εργαλεία εκείνα που θα μας βοηθήσουν να τις αναλύσουμε. Κάποια κοινά εργαλεία που χρησιμοποιούνται για το σκοπό αυτό είναι τα λεγόμενα «πινακοειδή», όπως η μήτρα κινδύνων και η ανάλυση/μελέτη των αστοχιών, καθώς και τα «δενδροειδή», όπως τα δέντρα σφαλμάτων, τα δέντρα γεγονότων, η μέθοδος Bowtie, τα δέντρα επιθέσεων/άμυνας και τα δέντρα αποφάσεων. Μια άλλη μέθοδος που αναπτύχθηκε από τη Microsoft και είναι αρκετά διαδεδομένη είναι η μέθοδος STRIDE-LM.(Χουντάλας, 2020)

STRIDE-LM	Threat	Property	Definition
S	Spoofing	Authentication	Impersonating someone or something
T	Tampering	Integrity / Access Controls	Modifying data or code
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles
D	Denial of Service	Availability	Deny or degrade service
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization
LM	Lateral Movement	Segmentation / Least Privilege	Expand influence post-compromise; often dependent on Elevation of Privilege

Εικόνα 9: Η μέθοδος STRIDE-LM (Πηγή: CSA 2020)

Όπως φαίνεται και από την παραπάνω εικόνα, το STRIDE-LM είναι το αρκτικόλεξο των κατηγοριών απειλής: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege, Lateral Movement.

1. Spoofing (Πλαστοπροσωπία): όταν προσποιούμαστε ότι είμαστε κάποιος ή κάτι άλλο και διακυβεύεται η αυθεντικότητα. Τέτοιες απειλές μπορεί να προέρχονται από άτομα που πλαστογραφούν κάποιον νόμιμο χρήστη για πρόσβαση σε κάποιο μέσο ή δίκτυο ή δημιουργούν ένα ψεύτικο λογαριασμό, αρχείο ή διαδικασία. Αυτές οι περιπτώσεις μπορούν να μειωθούν δημιουργώντας ισχυρούς μηχανισμούς ελέγχου ταυτότητας.
2. Tampering (Αλλοίωση στοιχείων): όταν παραποιούμε στοιχεία χωρίς να είμαστε εξουσιοδοτημένοι, με αποτέλεσμα να χάνεται η ακεραιότητα. Τέτοια αλλοίωση μπορεί να γίνει σε αρχεία, σε δίσκους αποθήκευσης αρχείων, ακόμη και στη λειτουργία κάποιου δικτύου. Μια καλή κρυπτογράφηση και ένας σωστός έλεγχος πρόσβασης μπορεί να βελτιώσουν την απειλή αυτή.
3. Repudiation (Αποποίηση ευθύνης): όταν κάποιος ισχυρίζεται ότι δεν έχει κάνει αυτό για το οποίο κατηγορείται. Συνήθως παρατηρείται από εξουσιοδοτημένους ή μη χρήστες χωρίς την ικανότητα απόδειξης της απάτης από την αντίθετη πλευρά. Μετριασμός αυτή της πιθανότητας γίνεται με την ύπαρξη συστημάτων συνεχούς καταγραφής και με τις ψηφιακές υπογραφές.

4. Information disclosure (Διαρροή ή παραβίαση απορρήτου): όταν αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα απόρρητες ή ευαίσθητες πληροφορίες που προέρχονται από αρχεία, μέσα αποθήκευσης δεδομένων ή δίκτυα. Η ισχυρή κρυπτογράφηση μπορεί να βοηθήσει ξανά στην αποφυγή αυτής της απειλής.
5. Denial of service (Αδυναμία πρόσβασης/παροχής): όπου μια υπηρεσία υποβαθμίζεται μέσω της αυξημένης ζήτησης από ψεύτικους χρήστες, ή απενεργοποιείται, με αποτέλεσμα οι χρήστες να μην έχουν τη δυνατότητα πρόσβασης και χρήσης. Στην περίπτωση αυτή διακυβεύεται η διαθεσιμότητα της υπηρεσίας. Ο σωστός έλεγχος της κίνησης της υπηρεσίας και οι μηχανισμοί υπέρβασης χρηστών βοηθούν να εξαλειφθεί το πρόβλημα αυτό.
6. Elevation of privilege (Πρόσβαση χωρίς διαβάθμιση): όταν κάποιος εκτελεί ενέργειες πέραν της εξουσιοδότησής του. Μετριασμός πραγματοποιείται με την ύπαρξη ελέγχου εξουσιοδότησης και οι λογαριασμοί ελάχιστης εξουσιοδότησης, ώστε κάποιοι να μπορούν να εκτελούν βασικές διεργασίες.
7. Lateral movement (Πλευρική κίνηση): όπου πραγματοποιείται συνεχής αναπήδηση σε όλο το εύρος του δικτύου με τελικό στόχο το στοιχείο αξίας αυτού. Μια τέτοια επίθεση είναι πιο πολύπλοκη και προϋποθέτει άριστες τεχνικές γνώσεις και τις πλέον σύγχρονες τεχνολογίες. Για να εμποδιστεί κάτι τέτοιο πρέπει να γίνει σωστός καταμερισμός του δικτύου ή της υπηρεσίας και για την πρόσβαση από το ένα κομμάτι στο άλλο να υπάρχουν ισχυρά τείχη προστασίας (firewalls). (CSA 2020, Χουντάλας 2020)

3.3 Κίνδυνοι κυβερνοασφάλειας προς ανάλυση

Οι κίνδυνοι που μπορεί να εμφανιστούν στο περιβάλλον του κυβερνοχώρου με βάση τις παραπάνω απειλές είναι αναρίθμητοι. Για να κατανοηθεί ο τρόπος διαχείρισης των απειλών αυτών επιλέξαμε δυο κινδύνους από κάθε κατηγορία και τους κωδικοποιήσαμε ανάλογα με την κατηγορία που ανήκουν, όπως φαίνεται στον πίνακα 1. Επίσης, στον πίνακα 2 αναλύεται η βαθμονόμηση ανάλογα με την πιθανότητα εκδήλωσης των απειλών αυτών και τον αντίκτυπό τους. Όπως παρατηρούμε, η βαθμονόμηση της πιθανότητας εκδήλωσης της απειλής έχει τιμές από (1) έως (5), όπου τιμή (1) παίρνουν οι απειλές με υψηλή πιθανότητα εκδήλωσης και (5) οι απειλές με αμελητέα πιθανότητα εκδήλωσης. Αντίστοιχα, τιμή (1) παίρνουν οι απειλές με ελάχιστο αντίκτυπο και τιμή (5) αυτές που κρίνονται ως καταστροφικές.

Πίνακας 1: Καταγραφή απειλών

	ΚΩΔΙΚΟΣ	**ΑΠΕΙΛΗ**
Spoofing	S1	Πρόσβαση με κλεμμένα διαπιστευτήρια
	S2	Ανάγνωση αρχείων μέσω προγράμματος καταγραφής (log)
Tampering	T1	Αλλοίωση αρχείων
	T2	Ανακατεύθυνση ροής δεδομένων
Repudiation	R1	Αλλοίωση αρχείων καταγραφής
	R2	Ανάγνωση στοιχείων ασφαλείας από το σύστημα καταγραφής
	I1	Πρόσβαση σε λίστες ονομάτων

Information disclosure	I2	Ανακάλυψη κλειδιού κρυπτογράφησης
Denial of service	D1	Υποβάθμιση λειτουργίας του δικτύου
	D2	Μη δυνατότητα σύνδεσης στο δίκτυο
Elevation of privilege	E1	Ανάκτηση συνδυασμών ονομάτων χρήστη-κωδικού
	E2	Εμφύτευση εντολής για δημιουργία κώδικα εντολών
Lateral movement	L1	Πρόσβαση στο δίκτυο από πολλές πηγές ταυτόχρονα
	L2	Εμφύτευση κακόβουλου λογισμικού σε όλο το δίκτυο και υποκλοπή πληθώρας αρχείων

Πίνακας 2: Ερμηνεία βαθμού κλίμακας

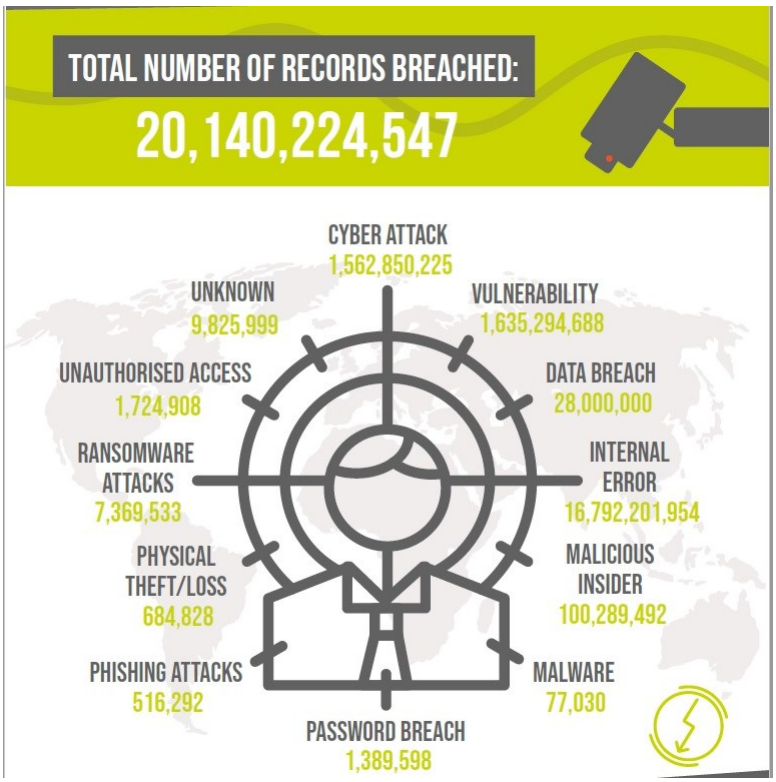
ΒΑΘΜΟΣ ΚΛΙΜΑΚΑΣ	ΠΙΘΑΝΟΤΗΤΑ ΕΚΔΗΛΩΣΗΣ	ΑΝΤΙΚΤΥΠΟΣ
1	ΥΨΗΛΗ	ΕΛΑΧΙΣΤΟΣ
2	ΣΗΜΑΝΤΙΚΗ	ΧΑΜΗΛΟΣ
3	ΜΕΤΡΙΑ	ΣΟΒΑΡΟΣ
4	ΧΑΜΗΛΗ	ΠΟΛΥ ΣΟΒΑΡΟΣ
5	ΑΜΕΛΗΤΕΑ	ΚΑΤΑΣΤΡΟΦΙΚΟΣ

3.4 Διαχείριση κινδύνων κυβερνοασφάλειας

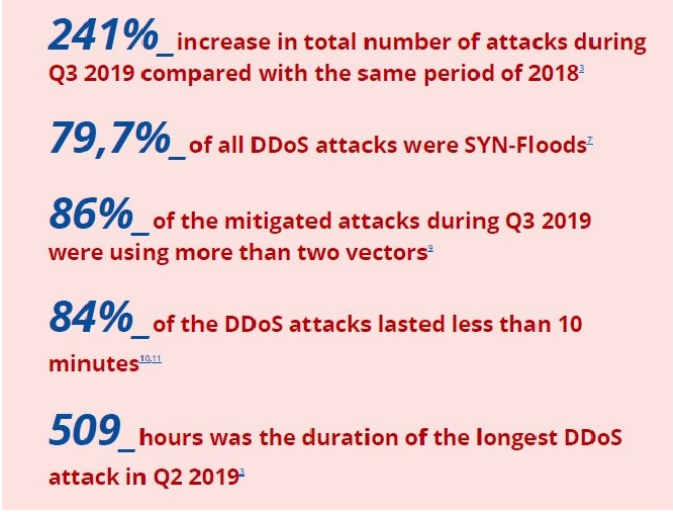
Περνώντας από το στάδιο της ανακάλυψης των απειλών (Discovery phase) στο στάδιο της εφαρμογής (Implementation phase), τα οποία αναλύθηκαν στην παράγραφο 3.1 και με βάση τους παραπάνω πίνακες, δημιουργούμε τον πίνακα 3, όπου παρουσιάζεται η ενδεικτική μήτρα των κινδύνων που επιλέξαμε να αναλύσουμε. Η ένταξη των απειλών στα συγκεκριμένα πεδία πιθανότητας εκδήλωσης και αντίκτυπου έγινε με γνώμονα τα ποσοστά των κυβερνοεπιθέσεων που έχουν αναφερθεί και αναλυθεί σε πληθώρα πηγών στο διαδίκτυο, μερικές από τις οποίες φαίνονται και στις εικόνες 11 έως 14. Σημαντικότερη πηγή από αυτές κρίνεται η τελευταία, η οποία είναι του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια (ENISA). Συγκεκριμένα παρατηρούμε πως τα τελευταία έτη (2019-2020) η αύξηση των κυβερνοεπιθέσεων έχει πάρει δραματικές διαστάσεις με αύξηση κατά 241% και αξιοσημείωτη αύξηση έχει παρατηρηθεί στις κακόβουλες εισβολές (malicious breaches), οι οποίες πραγματοποιούνται με κλεμμένα διαπιστευτήρια. (ENISA 2020, Shevchenko et al., 2021)

Πίνακας 3: Μήτρα κινδύνων (Risk Matrix)

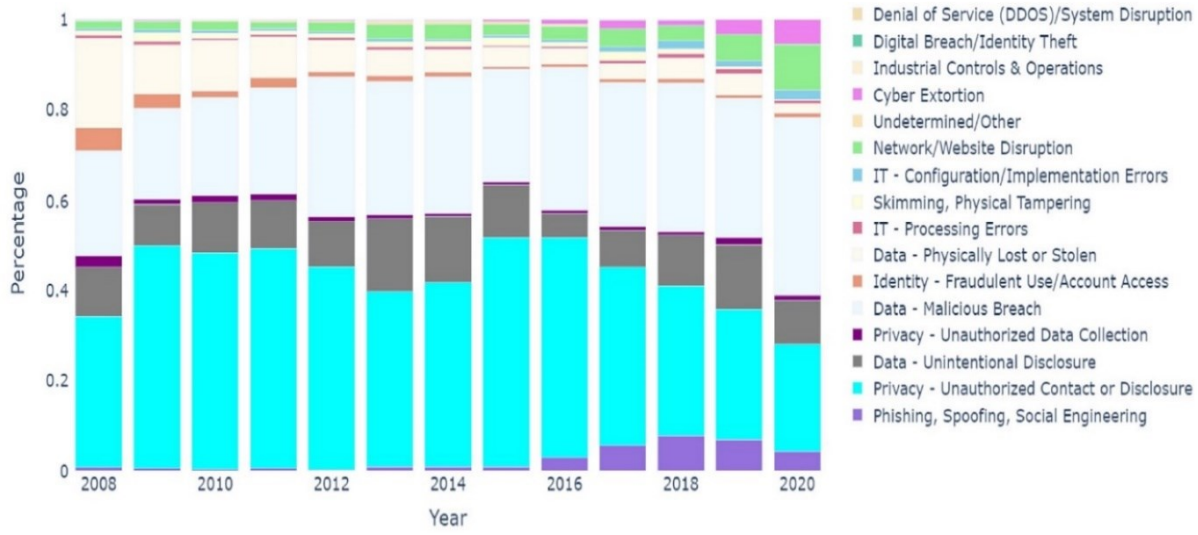
ΠΙΘΑΝΟΤΗΤΑ ΕΚΔΗΛΩΣΗΣ	ΑΝΤΙΚΤΥΠΟΣ					
	1	2	3	4	5
5			D2		
4			R2 T1	S1/R1 D1	
3			E1	I1	S2/T2 L1
2					I2 L2
1					E2



Εικόνα 10: Περιστατικά κυβερνοεπιθέσεων το 2020 (Πηγή: "IT Governance")



Εικόνα 11: Ποσοστά επιθέσεων μορφής DoS το 2019 (Πηγή:"ENISA Threat Landscape 2020 - Distributed denial of service," 2021)



Εικόνα 12: Ποσοστά κυβερνοεπιθέσεων βάσει τύπου, ετών 2008-2020 (Πηγή:Shevchenko et al. 2021)

Εικόνα 13: Οι κυριότερες κυβερνοαπειλές του 2020 (Πηγή: "ENISA Threat Landscape 2020".)

Αξιοποιώντας τα στοιχεία του πίνακα 3 δημιουργούμε τον πίνακα 4, όπου απεικονίζεται η συνολική μήτρα κινδύνων. Έτσι, για κάθε απειλή, πολλαπλασιάζουμε την πιθανότητα εκδήλωσης επί τον αντίκτυπο και ως αποτέλεσμα έχουμε το συντελεστή σημαντικότητας της κάθε απειλής. Παρατηρούμε λοιπόν, πως το μεγαλύτερο συντελεστή σημαντικότητας έχουν οι απειλές **S1,R1,D1** με συντελεστή 16.

Πίνακας 4: Μήτρα κινδύνων-Σημαντικότητα

ΚΩΔΙΚΟΣ	ΑΠΕΙΛΗ	ΠΙΘΑΝΟΤΗΤΑ ΕΚΔΗΛΩΣΗΣ	ΑΝΤΙΚΤΥΠΟΣ	ΣΗΜΑΝΤΙΚΟΤΗΤΑ
S1	Πρόσβαση με κλεμμένα διαπιστευτήρια	4	4	16
S2	Ανάγνωση αρχείων μέσω προγράμματος καταγραφής (log)	3	5	15
T1	Αλλοίωση αρχείων	4	3	12
T2	Ανακατεύθυνση ροής δεδομένων	3	5	15
R1	Αλλοίωση αρχείων καταγραφής	4	4	16
R2	Ανάγνωση στοιχείων ασφαλείας από το σύστημα καταγραφής	4	3	12
I1	Πρόσβαση σε λίστες ονομάτων	3	4	12
I2	Ανακάλυψη κλειδιού κρυπτογράφησης	2	5	10
D1	Υποβάθμιση λειτουργίας του δικτύου	4	4	16
D2	Μη δυνατότητα σύνδεσης στο δίκτυο	5	3	15
E1	Ανάκτηση συνδυασμών ονομάτων χρήστη-κωδικού	3	3	9
E2	Εμφύτευση εντολής για δημιουργία κώδικα εντολών	1	5	5
L1	Πρόσβαση στο δίκτυο από πολλές πηγές ταυτόχρονα	3	5	15
L2	Εμφύτευση κακόβουλου λογισμικού σε όλο το δίκτυο και υποκλοπή πληθώρας αρχείων	2	5	10

Αναλόγως του συντελεστή σημαντικότητας μπορούμε να δημιουργήσουμε τον πίνακα 5, όπου με τιμές μεγαλύτερες του (15) πρέπει να αντιμετωπίσουμε άμεσα την απειλή για μετριασμό των εκβάσεων, απειλές με τιμή (10) έως (15) είτε τις αντιμετωπίζουμε άμεσα είτε αναβάλουμε τις ενέργειές μας για να παρατηρήσουμε την εξέλιξή τους ή να συλλέξουμε περισσότερες πληροφορίες, απειλές με τιμή (5) έως (10) αποφασίζουμε είτε να αναβάλουμε τις ενέργειές μας είτε τις αποδεχόμαστε και, τέλος, απειλές με τιμή κάτω του (5) τις αποδεχόμαστε επειδή οι εκβάσεις τους δεν είναι σημαντικές. Σημαντικό είναι να παρατηρήσουμε πως αν και οι απειλές με τιμή (16) είναι πολύ κοντά στις αντίστοιχες με τιμή (15), οι πρώτες θεωρούνται πιο σημαντικές και κρίνεται σκόπιμη η άμεση αντιμετώπισή τους, κυρίως για το λόγο ότι οι δεύτερες απαιτούν πολύ καλή τεχνική γνώση και συστήματα τελευταίας τεχνολογίας. Έτσι εμφανίζονται πολύ σπάνια και τις περισσότερες φορές δεν καταγράφονται.

Πίνακας 5: Στρατηγική αντιμετώπισης απειλών

ΣΗΜΑΝΤΙΚΟΤΗΤΑ	ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ
>15	ΑΜΕΣΗ ΑΝΤΙΜΕΤΩΠΙΣΗ
10-15	ΑΝΤΙΜΕΤΩΠΙΣΗ Ή ΑΝΑΒΟΛΗ
5-9	ΑΝΑΒΟΛΗ Ή ΑΠΟΔΟΧΗ
<5	ΑΠΟΔΟΧΗ

Στην περίπτωση που η απειλή έχει τιμή >15, οπότε και απαιτείται μια στρατηγική για την άμεση αντιμετώπισή της, πρέπει αρχικά να ειδοποιήσουμε τον άμεσα ενδιαφερόμενο για τους κινδύνους της απειλής, το πλαίσιο της στρατηγικής αντιμετώπισης και για την ύπαρξη τυχόν υπολειμματικών κινδύνων (residual risks). Στη συνέχεια, η στρατηγική που θα αποφασιστεί θα πρέπει να βασιστεί στα παρακάτω ερωτήματα:

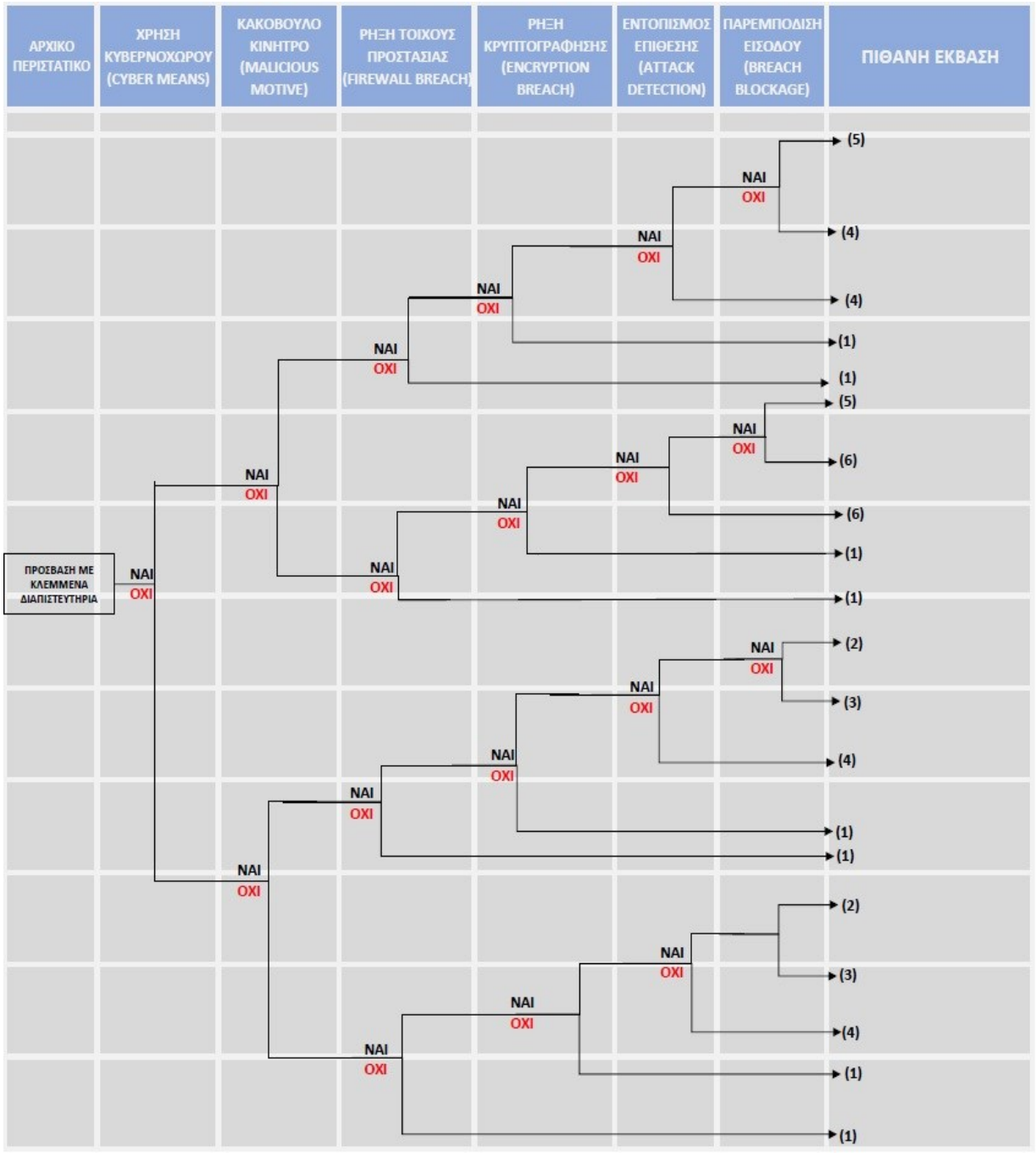
- Πώς θα μπορούσαμε να αποκρύψουμε την αδυναμία του συστήματος ώστε να μην αποκαλυφθεί από τον δρώντα;
- Πώς θα μπορούσαμε να εμποδίσουμε τον δρώντα από το να χρησιμοποιήσει τα συγκεκριμένα μέσα για την εκδήλωση της επίθεσης;

- Πώς θα μπορούσαμε να αποφύγουμε το κίνητρό του;
- Πώς θα μετριάσουμε τις εκβάσεις της επίθεσης;
- Θα μπορούσαμε με κάποιο τρόπο να μειώσουμε την πιθανότητα εκδήλωσης;
- Πάρθηκαν προληπτικά μέτρα;
- Τα μέτρα που θα ληφθούν ικανοποιούν τη στρατηγική της ασφάλειας;

Ουσιαστικά, τα ερωτήματα αυτά απαντώνται εκτελώντας τον κύκλο διαχείρισης κινδύνου κατά ISO 31000 που αναφέρθηκε παραπάνω (Εικόνα 5).

Με σκοπό να γίνει καλύτερα κατανοητός ο τρόπος διαχείρισης ενός κινδύνου, επιλέγουμε έναν από αυτούς που χρήζουν άμεσης αντιμετώπισης και εφαρμόζουμε την τεχνική της «Δενδρικής Ανάλυσης Κινδύνου» (Event Tree Analysis). Η συγκεκριμένη ανάλυση είναι έξι σταδίων, όπου γίνεται η εκτίμηση και η προτεραιοποίηση των εκβάσεων του κινδύνου. Ο κίνδυνος που έχει επιλεχθεί είναι η «Πρόσβαση με κλεμμένα διαπιστευτήρια», ένας κίνδυνος που τα τελευταία έτη παρουσιάζει αυξημένη καταγραφή, όπως αναλύθηκε παραπάνω, και ταυτόχρονα οι συνέπειες είναι πολύ σοβαρές. Η απειλή αυτή μπορεί να εμφανιστεί σε οποιοδήποτε οργανισμό, δημόσιο ή ιδιωτικό, κυβερνητικό ή μη, σε οποιαδήποτε κρίσιμη υποδομή του κράτους ή σε οποιαδήποτε επιχείρηση φυσική ή ψηφιακή. Στο συγκεκριμένο παράδειγμα υποθέτουμε πως ο κίνδυνος εμφανίζεται σε οργανισμό ιδιωτικού ενδιαφέροντος, ο οποίος δραστηριοποιείται σε παγκόσμιο επίπεδο, η λίστα πελατών του συμπεριλαμβάνει, μεταξύ άλλων, καταξιωμένους ιδιώτες και εταιρείες με υψηλό επενδυτικό ποσοστό και αντίστοιχα έσοδα.

Πίνακας 6: Event Tree Analysis



Κάποιες από τις πολλές πιθανές εκβάσεις του συγκεκριμένου κινδύνου παρουσιάζονται στον πίνακα 7. Από τους πίνακες 6 και 7 παρατηρούμε πως ο δρών μπορεί είτε να εισχωρήσει ευρισκόμενος εντός του οργανισμού, να εργάζεται δηλαδή σε αυτόν, είτε να εκδηλώσει την επίθεσή του μέσω εργαλείων του κυβερνοχώρου (1ο στάδιο: Χρήση Κυβερνοχώρου). Επίσης, το κίνητρό του μπορεί να είναι κακόβουλο, δηλαδή να θέλει να υποκλέψει αρχεία που περιέχουν ευαίσθητες πληροφορίες της εταιρείας, ή να κατάφερε την είσοδο

στο δίκτυο έχοντας τις κατάλληλες γνώσεις, με σκοπό την προειδοποίηση για ύπαρξη τρωτών σημείων ή και τον εκβιασμό (2ο στάδιο: Κακόβουλο κίνητρο). Στη συνέχεια, ανάλογα με τις δεξιότητές του και τα μέσα που χρησιμοποιεί, μπορεί να καταφέρει να προσπελάσει τους αμυντικούς μηχανισμούς του συστήματος (3ο στάδιο: firewall breach, 4ο στάδιο: encryption breach) ή όχι. Αυτοί οι αμυντικοί μηχανισμοί σε συνεργασία και με άλλες λειτουργίες, θα καταστήσουν την απειλή ανιχνεύσιμη ή μη, με σκοπό την έγκαιρη παρεμπόδιση του δρώντα και τη διάσωση των ευαίσθητων πληροφοριών (5ο στάδιο: attack detection, 6ο στάδιο: breach blockage). Εάν αυτό τελικά επιτευχθεί, τότε είναι πιθανός ο εντοπισμός του δρώντα, κάτι το οποίο θα είναι πιο εύκολο εάν αυτός εργάζεται εντός της εταιρείας. Έτσι, η δίωξή του και απομάκρυνσή του για το έγκλημά του γίνεται ακόμη πιθανότερη.

Πίνακας 7: Πιθανές εκβάσεις κινδύνου

Α/Α	**ΕΚΒΑΣΕΙΣ**
(1)	Μη δυνατότητα εισόδου στα στοχοποιημένα αρχεία
(2)	Μη δυνατότητα εισόδου στα στοχοποιημένα αρχεία και πιθανή δίωξη του δρώντα
(3)	Πρόσβαση στα αρχεία και υποκλοπή. Πιθανή δίωξη του δρώντα
(4)	Πρόσβαση στα στοχοποιημένα αρχεία και υποκλοπή
(5)	Μη επιτυχής πρόσβαση και προσπάθεια εντοπισμού του δρώντα
(6)	Πρόσβαση στα αρχεία, μη υποκλοπή και προειδοποίηση/εκβιασμός από τον δρώντα

Η παραπάνω «Δενδρική Ανάλυση» μπορεί να γίνει για όλους τους πιθανούς κινδύνους ξεχωριστά και είναι απαραίτητο στοιχείο του κύκλου διαχείρισης ρίσκου. Με τον τρόπο αυτό γίνεται ευκολότερος ο εντοπισμός των απειλών και η οργάνωση του τρόπου και της στρατηγικής αντιμετώπισής τους. Επίσης, η ανάλυση αυτή μας βοηθά στο να ανακαλύψουμε τα πιθανά τρωτά σημεία του συστήματος πριν τα ανακαλύψει κάποιος άλλος. Έτσι ενεργούμε προληπτικά (proactively) και όχι ενεργητικά (actively).

3.5 Μετριασμός απειλών

Το επόμενο στάδιο της διαχείρισης των κινδύνων είναι ο μετριασμός τους (threat mitigation). Με τη μέθοδο STRIDE-LM καταφέραμε να οργανώσουμε τις απειλές. Η μέθοδος αυτή θα μας βοηθήσει να οργανώσουμε και τις μεθόδους αντιμετώπισής τους.

1. Spoofing mitigation

Μια μέθοδος που μπορεί να χρησιμοποιηθεί για τον περιορισμό του spoofing είναι το επαρκές και αποτελεσματικό φιλτράρισμα των εισερχομένων πληροφοριών και η αυθεντικοποίηση των χρηστών. Ιδιαίτερη προσοχή πρέπει να δοθεί όμως στη διαφορά της αυθεντικοποίησης με την έγκριση πρόσβασης (authentication vs authorization). Κι αυτό διότι ένας απομακρυσμένος χρήστης που γνωρίζουμε (κατέχει διαπιστευτήρια) μπορεί να θελήσει να αποκτήσει πρόσβαση, χωρίς να γνωρίζουμε ότι είναι ο πραγματικός χρήστης (κλεμμένα διαπιστευτήρια). Για το λόγο αυτό θα πρέπει να υπάρχουν παραπάνω από ένας τρόπος αυθεντικοποίησης. Μερικοί σύγχρονοι μέθοδοι είναι τα IPSec, DNSSEC, Kerberos, PKI systems, ψηφιακές υπογραφές, κρυπτογράφηση κ.α.

2. Tampering mitigation

Ο περιορισμός αντίστοιχα του tampering μπορεί να γίνει με διάφορες μεθόδους, όπως οι μηχανισμοί έγκρισης πρόσβασης (permission mechanisms) και οι κρυπτογραφικές συναρτήσεις κατατεμαχισμού (hashes). Ο τρόπος που λειτουργούν οι πρώτοι είναι γνωστοί και παρόμοιοι με τις μεθόδους του spoofing mitigation. Τα hashes είναι μηχανισμοί που τεμαχίζουν μια πληροφορία, της δημιουργούν συγκεκριμένο μέγεθος, το οποίο μένει σταθερό. Οπότε, εάν κάποιος αλλάξει οποιοδήποτε input, αποκτά και διαφορετικό output. Επίσης, εάν υπάρχει ένας κεντρικός έλεγχος που ελέγχει όλες τις προσβάσεις, τότε είναι και πιο δύσκολο να μην παρατηρηθεί μια μη εξουσιοδοτημένη πρόσβαση.

3. Repudiation mitigation

Για να ελεγχθεί το repudiation αρκεί το σύστημά μας να έχει ισχυρή κρυπτογράφηση, να χρησιμοποιείται η ψηφιακή υπογραφή και μηχανισμοί καταγραφής (logs). Με τη βοήθεια αυτών γίνεται καταγραφή της οποιασδήποτε

κίνησης εντός συστήματος, με αποτέλεσμα όποιος αρνηθεί κάποια ενέργεια αυτή να είναι καταγεγραμμένη.

4. Information disclosure mitigation

Η κρυπτογράφηση και η σωστή κεντρική διαχείριση των κλειδιών είναι οι πιο αποτελεσματικοί μέθοδοι για τον περιορισμό της διαρροής ή παραβίασης ευαίσθητων πληροφοριών.

5. Denial of service mitigation

Από τη στιγμή που κάποιος θέλει να επιτύχει αδυναμία ή περιορισμό πρόσβασης σε μια υπηρεσία χρησιμοποιεί μεθόδους κορεσμού της μνήμης του συστήματος, ο ενδεδειγμένος τρόπος αντιμετώπισης είναι η ύπαρξη μηχανισμών περιορισμού των χρηστών και η ύπαρξη πλεονάζουσας δυνατότητας επεξεργασίας δεδομένων.

6. Elevation of privilege mitigation

Ο μόνος τρόπος για να μειωθεί η πρόσβαση χωρίς την κατάλληλη διαβάθμιση είναι τα πολλαπλά στρώματα αυθεντικοποίησης. Το σύστημά μας πρέπει να είναι σχεδιασμένο με τη «μέθοδο του κρεμμυδιού», δηλαδή να αποτελείται από πολλά και διαφορετικά επίπεδα πρόσβασης, ανάλογα με τη σημαντικότητα των ενεργειών και πληροφοριών. Με τον τρόπο αυτό, κάποιος που επιθυμεί πρόσβαση στον «πυρήνα» του συστήματος, στις πιο ευαίσθητες πληροφορίες δηλαδή, πρέπει να κατέχει πολλά και διαφορετικά διαπιστευτήρια.

7. Lateral movement mitigation

Ο περιορισμός των απειλών που χρησιμοποιούν τη μέθοδο αυτή είναι πολύ δύσκολος, λόγω του ότι γίνεται με τα πλέον σύγχρονα μέσα κυβερνοεπίθεσης και από άτομα ή ομάδες που κατέχουν μεγάλη τεχνογνωσία. Έτσι, οι επιθέσεις αυτές είναι πιο σπάνιες και δύσκολα ανιχνεύσιμες. Η μόνη επιλογή του οργανισμού ή της επιχείρησης που θέλει να προστατευθεί είναι η χρήση των πιο εξελιγμένων συστημάτων τεχνολογικά, ο συνδυασμός όλων των παραπάνω μεθόδων και ο σχεδιασμός ενός συστήματος άμυνας και διαχείρισης κινδύνων από άτομα αντίστοιχης τεχνογνωσίας. Επίσης, το σύστημα αυτό θα πρέπει να ελέγχετε τακτικά για τρωτά σημεία και να εξελίσσεται συνεχώς. (Shostack 2014, Sood and Sharma 2021)

4. Συμπεράσματα-Προτάσεις

Η παρούσα διπλωματική εργασία προσπάθησε να αναδείξει μια νέα μορφή απειλών, οι οποίες έκαναν την εμφάνισή τους στο σύγχρονο κόσμο, κυρίως τις τελευταίες δύο δεκαετίες, τις λεγόμενες «ασύμμετρες απειλές». Παράλληλα, στο δεύτερο κεφάλαιο τονίστηκε η σημαντικότητα της κυριότερης από αυτές, του κυβερνοπολέμου. Μέσω της περιπτωσιολογικής μελέτης που αναλύθηκε στο επόμενο κεφάλαιο έγινε προσπάθεια ολοκληρωμένης αντιμετώπισης μιας τέτοιας απειλής, σύμφωνα με τα σύγχρονα μέσα διαχείρισης κινδύνων.

Ο κυβερνοπόλεμος λειτουργεί σήμερα ως το πλέον σύγχρονο μέσο άσκησης επιρροής ασύμμετρου χαρακτήρα, που στρέφεται κατά της εθνικής ασφάλειας και ευημερίας των κρατών. Οι κρίσιμες υποδομές αυτών είναι εκτεθειμένες σε τέτοιες απειλές, λόγω της τεράστιας εξάπλωσης χρήσης του διαδικτύου και του κυβερνοχώρου στην εποχή μας. Καθημερινά καταγράφονται αναρίθμητα περιστατικά κυβερνοεπιθέσεων μικρής κλίμακας που δημοσιοποιούνται στο διαδίκτυο και πολλά μεγαλύτερης, τα περισσότερα εκ των οποίων δε γίνονται γνωστά. Το σύνολο αυτών καταδεικνύει τη σημαντικότητα της προστασίας των κρίσιμων υποδομών ενός κράτους. Η ηλεκτρονική ασφάλεια των υποδομών αυτών θα πρέπει να είναι σχεδιασμένη με τέτοιο τρόπο ώστε να εντοπίζεται στο δυνατόν μικρότερο χρονικό διάστημα η κυβερνοαπειλή και να αντιμετωπίζεται αποτελεσματικά εξίσου γρήγορα. Τα μέτρα ασφαλείας που πρέπει να ληφθούν, δηλαδή, πρωταρχικό στόχο να έχουν την αύξηση της ετοιμότητας και την ενίσχυση των δυνατοτήτων πρόληψης, στον εντοπισμό και την άμεση αντίδραση στις ενδεχόμενες απειλές και στο μετριασμό των επιπτώσεων. (Politou et al., 2018)

Για να επιτευχθεί όμως αυτό κρίνεται απαραίτητο τα μέτρα ασφαλείας που λαμβάνονται να τηρούν ορισμένες προϋποθέσεις. Πρώτα απ’ όλα, οι

πληροφορίες που μπορεί να έχει πρόσβαση κάποιος θα πρέπει να είναι κατάλληλα διαβαθμισμένες, όπως επίσης αντίστοιχα και η πρόσβαση σε αυτές. Αυτό επιτυγχάνεται με τη χρήση των κατάλληλων διαπιστευτηρίων, τα οποία θα πρέπει να είναι διαφορετικά για τον καθένα, να ελέγχονται και να αλλάζουν σε τακτά χρονικά διαστήματα. Επιπλέον, το σύνολο των δεδομένων και πληροφοριών ενός συστήματος πρέπει να προστατεύεται με τα κατάλληλα ηλεκτρονικά μέσα, ανάλογα πάλι με τη διαβάθμισή τους. Έτσι λοιπόν, μέσα και εφαρμογές τελευταίας τεχνολογίας θα πρέπει να χρησιμοποιούνται για την προστασία ευαίσθητων πληροφοριών καθώς και για την ασφαλή λειτουργία όλου του συστήματος. Κι αυτό διότι πέραν της πρόσβασης σε δεδομένα, ένα σύστημα είναι απαραίτητο να μπορεί να εκτελεί απρόσκοπτα όλες τις ενέργειες για τις οποίες είναι σχεδιασμένο. Όταν λοιπόν, τηρούνται όλα τα ανωτέρω, ένα σύστημα μπορεί να χαρακτηριστεί αξιόπιστο, λειτουργικό και αποδοτικό και να δημιουργεί στους χρήστες ένα αίσθημα εμπιστοσύνης. (Politou et al., 2018)

Επίσης, είναι απαραίτητο να γίνει κατανοητό πως η συνεργασία μεταξύ κυβερνητικών ή μη φορέων με αντίστοιχους ιδιωτικούς είναι επιτακτική, ώστε να υπάρξει ένας πιο ολοκληρωμένος σχεδιασμός του συστήματος προστασίας από κυβερνοεπιθέσεις και αποτελεσματικότερος τρόπος αντιμετώπισης αυτών. Συγκεκριμένα, κρίνεται σκόπιμη η σύσταση μιας ομάδας, αποτελούμενης από άτομα με υψηλές και εξειδικευμένες γνώσεις στα πληροφοριακά συστήματα και τα συστήματα ασφαλείας και ταυτόχρονα εξοπλισμένης με τα πλέον σύγχρονα τεχνολογικά μέσα. Επιπλέον, είναι σημαντικό τα άτομα της ομάδας αυτής να προέρχονται τόσο από δημόσιους φορείς όσο και από ιδιωτικούς, με σκοπό να αποφεύγεται η σύγκρουση συμφερόντων, αλλά, ταυτόχρονα, να καλλιεργείται ένα κλίμα αμοιβαίας εμπιστοσύνης και αντιμετώπισης των απειλών με στόχο την εθνική ακεραιότητα και συμφέρων. Εκτός των εξειδικευμένων γνώσεων, στην ομάδα αυτή θα πρέπει να παρέχεται μια κατάλληλη νομική εξουσία, ώστε να μπορεί να εκτελεί ανεμπόδιστα όλες τις ενέργειες που κρίνονται απαραίτητες για την καλύτερη ασφάλεια του συστήματος με ταυτόχρονη ικανότητα για επιβολή κυρώσεων σε όσους προσπαθούν να το απειλήσουν.

Κάτι αντίστοιχο πρέπει να γίνει και στους οργανισμούς ιδιωτικού ενδιαφέροντος. Ο ιδιωτικός τομέας μιας χώρας είναι εξίσου σημαντικός, επειδή αυτός είναι ο κύριος πάροχος του διαδικτύου και των δικτύων επικοινωνίας. Επίσης, μεγάλο μέρος του εξοπλισμού και των τεχνικών μέσων που χρησιμοποιούνται για τις λειτουργίες αυτές είναι ιδιοκτησία μεγάλων εταιρειών και τα κεφάλαια που δαπανώνται για τον εκσυγχρονισμό τους προέρχονται από τις εταιρείες αυτές. Άρα, στον ιδιωτικό τομέα υπάρχουν άτομα με μεγάλη εξειδίκευση και πολλές τεχνικές γνώσεις που μπορούν να σχεδιάσουν ολοκληρωμένα και σύγχρονα συστήματα προστασίας από κυβερνοαπειλές υπέρ της προστασίας των κρίσιμων υποδομών του κράτους. Για να

προσδιοριστούν οι υποδομές αυτές θα πρέπει να γίνει μια ολιστική έρευνα και να καθοριστούν κάποια κριτήρια. Στον καθορισμό των κριτηρίων, πέραν από τα εθνικά δεδομένα, λαμβάνονται υπόψη και οι σχετικές εργασίες του ΝΑΤΟ, της Ευρωπαϊκής Επιτροπής και του ENISA, όπως αναφέρθηκε και στο δεύτερο κεφάλαιο, με κατάλληλη προσαρμογή στα δεδομένα του κάθε κράτους.

Συγκεκριμένα για τη χώρα μας, με σκοπό την επίτευξη ενός ικανοποιητικού επιπέδου ασφάλειας των κρίσιμων υποδομών, θα πρέπει να καθοριστεί ένα σύγχρονο Εθνικό Πλαίσιο Κυβερνοασφάλειας. Η πρώτη και πολύ σημαντική προσπάθεια έχει γίνει πριν αρκετά χρόνια και αποτέλεσμα αυτής ήταν η έκδοση του Διακλαδικού Δόγματος Επιχειρήσεων Κυβερνοχώρου από το ΓΕΕΘΑ το 2013. Σκοπός του δόγματος είναι η κάλυψη όλων των πτυχών των δραστηριοτήτων στον κυβερνοχώρο σε διακλαδικό επίπεδο και να καθοριστούν οι αρχές, οι κανόνες και οι διαδικασίες που διέπουν τις επιχειρήσεις κυβερνοχώρου των ΕΔ. Αυτές αποτελούν τη βάση για τη σωστή σχεδίαση των επιχειρήσεων αυτών, τη συντονισμένη διεξαγωγή και την υποστήριξή τους. Επιπλέον, σκοπός του δόγματος είναι η αποσαφήνιση των ευθυνών και αρμοδιοτήτων όλων των εμπλεκόμενων με τις επιχειρήσεις κυβερνοχώρου, ώστε να λειτουργούν αποτελεσματικότερα. (ΓΕΕΘΑ, 2013)

Για τη σωστή εφαρμογή του δόγματος αυτού έχει συσταθεί στο ΓΕΕΘΑ η Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ), η οποία έχει ως αποστολή τη σχεδίαση, το συντονισμό και τη διεξαγωγή των επιχειρήσεων στον κυβερνοχώρο. Επίσης, είναι υπεύθυνη για την αντιμετώπιση περιστατικών σε καθημερινή βάση για την προστασία των πληροφοριακών δικτύων και υποδομών των ΕΔ, αλλά και μεταξύ υπηρεσιών του ευρύτερου δημόσιου και ιδιωτικού τομέα και διεθνών οργανισμών, όπου αυτές αλληλοεπιδρούν με τις αντίστοιχες υποδομές των ΕΔ. Τέλος, οργανώνει κατάλληλες εκπαιδεύσεις του προσωπικού για την αύξηση των γνώσεων και της επιχειρησιακής ετοιμότητας. (ΓΕΕΘΑ, 2013)

Πέραν όμως των ΕΔ ένα σύγχρονο Εθνικό Πλαίσιο Κυβερνοασφάλειας θα πρέπει να σχεδιασθεί με βάση διεθνή πρότυπα ασφάλειας και να περιλαμβάνει:

1. Διοίκηση και Διαχείριση Κινδύνων (Risk Management)
2. Εκτίμηση της ευπάθειας των συστημάτων πληροφορικής (Vulnerability Assessment)
3. Τακτικές δοκιμές διείσδυσης (Penetration Testing)
4. Διαχείριση χώρων, εξοπλισμού και λογισμικού
5. Κατάλληλη εξουσιοδότηση και διαπίστευση προσωπικού
6. Φυσική ασφάλεια και ασφάλεια περιβάλλοντος χώρου (Environmental Management)
7. Αξιοποίηση των CERT (Computer Emergency Response Team) για αντιμετώπιση περιστατικών

8. Συνεχής παρακολούθηση ηλεκτρονικών επικοινωνιών για κακόβουλες επιθέσεις για εντοπισμό περιστατικών που βρίσκονται υπό εξέλιξη (Continuous Monitoring).

Επιπλέον, για να υπάρξει μια σωστή συνεργασία μεταξύ δημόσιων και ιδιωτικών φορέων απαραίτητο είναι να υπάρχουν και μηχανισμοί που να εξετάζουν σε τακτική βάση τη σωστή λειτουργία και την ετοιμότητα του συστήματος αντιμετώπισης των κυβερνοαπειλών. Τέτοιοι μηχανισμοί είναι η εκτέλεση ρεαλιστικών ασκήσεων για την αντιμετώπιση κυβερνοαπειλών, σύμφωνα με τα πρότυπα αντίστοιχων ασκήσεων που πραγματοποιούνται σε ευρωπαϊκό και νατοϊκό επίπεδο, διαδικασία η οποία θα συμβάλει στη μεγιστοποίηση του βαθμού ετοιμότητας της χώρας μας ώστε να ανταπεξέλθει σε περιστατικά ασφάλειας δικτύων και πληροφοριών. Οι ασκήσεις που έχουν διεξαχθεί μέχρι τώρα στα νατοϊκά πλαίσια έχουν δείξει πως υπάρχει σοβαρή έλλειψη συντονισμού των απαραίτητων ενεργειών για την αντιμετώπιση μιας κυβερνοαπειλής μεταξύ όλων των εμπλεκόμενων φορέων και ατόμων και όχι τόσο στην ύπαρξη των κατάλληλων μέσων. Κι αυτό διότι δεν υπάρχει ένας κεντρικός φορέας συντονισμού και εκτέλεσης των προβλεπόμενων ενεργειών.

Εκτός των ασκήσεων, η ανάλογη εκπαίδευση των ατόμων που θα επανδρώσουν την ομάδα συντονισμού και αντιμετώπισης των κυβερνοαπειλών είναι απαραίτητη. Η ανάπτυξη των σχετικών ικανοτήτων είναι μείζονος σημασίας και ο στόχος είναι η δημιουργία ενός συνόλου ανθρώπινου δυναμικού, τόσο εντός όσο και εκτός του δημοσίου τομέα, που θα έχει την απαραίτητη τεχνική γνώση και εμπειρία για να ανταπεξέλθει στις σύγχρονες απαιτήσεις. Συμπερασματικά λοιπόν, ένα κράτος θα πρέπει να οργανώσει την εκπαίδευση του προσωπικού τηρώντας ορισμένες προϋποθέσεις, όπως:

1. Να υπάρχει συμμετοχή των ατόμων αυτών σε εκπαιδευτικά προγράμματα ή σεμινάρια που διοργανώνουν φορείς στο εξωτερικό
2. Τα προγράμματα αυτά να υπάρχει σχεδιασμός να εκτελεστούν στη συνέχεια και από εθνικούς φορείς εκπαίδευσης, με σκοπό την ενίσχυση και διεύρυνση των κατάλληλων ανθρωπίνων πόρων
3. Ως αποτέλεσμα των ανωτέρω θα είναι η δημιουργία μιας «ανθρώπινης δεξαμενής» εξοπλισμένης με άρτιες και εξειδικευμένες γνώσεις
4. Η εξειδικευμένη αυτή εκπαίδευση να προσδίδει στα άτομα αυτά αντίστοιχες πιστοποιήσεις με σκοπό την ύπαρξη κινήτρου
5. Ένταξη μαθημάτων και σεμιναρίων επιμόρφωσης περί θεμάτων ασφάλειας πληροφοριακών συστημάτων σε σχολές ανώτερης και ανώτατης εκπαίδευσης στον Ελλαδικό χώρο και ανάληψη από αυτές ερευνητικών προγραμμάτων εξέλιξης νέων μεθόδων κυβερνοάμυνας

Από τα παραπάνω συμπεραίνουμε πως η δημιουργία μιας ομάδας αποτελούμενης από άτομα εξοπλισμένα με τις κατάλληλες γνώσεις σε συνδυασμό με την εμπειρία από τη συμμετοχή τους σε διεθνή σεμινάρια και ασκήσεις, παρέχοντάς τους παράλληλα τα κατάλληλα τεχνολογικά μέσα, είναι το κλειδί της επιτυχίας για την ανάπτυξη της κυβερνοασφάλειας στη χώρα μας.

Κατάλογος Πηγών

Air Force Doctrine Document. Irregular Warfare. USAF, 2013.

Alianz. “Allianz Risk Barometer.” AGCS Global, 2021, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

Andress, Jason, and Steve Winterfeld. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Second edition, Elsevier, 2014.

Arnaboldi, Luca, et al. “Modelling Load-Changing Attacks in Cyber-Physical Systems.” Elsevier/Electronic Notes in Theoretical Computer Science, vol. 353, Nov. 2020, pp. 39–60. DOI.org (Crossref), https://doi.org/10.1016/j.entcs.2020.09.018.

Beuchelt, Gerald, et al. “Cyber Security: A Peer-Reviewed Journal Volume 1,No. 3.” Excelsior College, vol. 1, no. 3, 2015, p. 68, https://www.excelsior.edu/page/national-cybersecurity-institute/.

Billo, Charles, and Welton Chang. November 2004 Revised December 2004. INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE, 2004. Zotero, https://www.researchgate.net/publication/230687826_CYBER_WARFARE_AN_ANALYSIS_OF_THE_MEANS_AND_MOTIVATIONS_OF_SELECTED_NATION_STATES.

Brenner, Susan W. Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford University Press, 2009. Library of Congress ISBN, https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780195385014.001.0001/acprof-9780195385014.

Caralli, Richard A., et al. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process: Defense Technical Information Center, 1 May 2007. DOI.org (Crossref), https://doi.org/10.21236/ADA470450.

Carayannis, Elias G., et al., editors. Cyber-Development, Cyber-Democracy and Cyber-Defense. Springer New York, 2014. DOI.org (Crossref), https://doi.org/10.1007/978-1-4939-1028-1.

Castells, Manuel. Communication Power. Oxford University Press, 2009. Library of Congress ISBN,

https://journals.sagepub.com/doi/abs/10.1177/0163443710379951?journalCode=mcsa.

CSA. GUIDE TO CYBER THREAT MODELLING-Cyber Security Agency of Singapore (CSA). 2020.

Cukier, Kenneth Neil, et al. “Ensuring (and Insuring?) Critical Information Infrastructure Protection.” Harvard University/John F. Kennedy School of Government, 2005. DOI.org (Crossref), https://doi.org/10.2139/ssrn.832628.

“Cyber Attacks Statistics.” HACKMAGEDDON, 2021, https://www.hackmageddon.com/2021/07/22/q2-2021-cyber-attack-statistics/.

Distributed Denial of Service/ENISA Threat Landscape. ENISA, 2020.

Dr Clayton Richard and Professor Ross Anderson. “RISk AND UNCERTAINTY.” University of Cambridge, no. 19, 2012, p. 32, www.cam.ac.uk/research Issue 19.

Efthymiopoulos, Marios Panagiotis. “A Cyber-Security Framework for Development, Defense and Innovation at NATO.” Journal of Innovation and Entrepreneurship, vol. 8, no. 1, Dec. 2019, p. 12. DOI.org (Crossref), https://doi.org/10.1186/s13731-019-0105-z.

Elisan, Christopher C., and Mikko Hypponen. Malware, Rootkits & Botnets: A Beginner’s Guide. McGraw-Hill, 2013. Open WorldCat, http://www.books24x7.com/marc.asp?bookid=50494.

ENISA. EU ENISA. 2020, https://www.enisa.europa.eu/about-enisa/about/el.

ENISA Threat Landscape 2020 - Distributed Denial of Service. 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

ENISA Threat Landscape 2020 - Top 15 Threats. 2021, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats.

Ertan, A., et al. Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDCOE. Zotero, https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/.

EUROPEAN COMMISSION. Cybersecurity Strategy of the European Union. EUROPEAN COMMISSION, 2013.

European Parliament. Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU. European Parliament Publications Office, 2017. DOI.org (CSL JSON), https://data.europa.eu/doi/10.2861/853031.

Geers, Kenneth. NATO Cooperative Cyber Defence Centre of Excellence. Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, 2011. Open WorldCat, https://www.pdfdrive.com/strategic-cyber-security-an-evaluation-of-nation-state-cyber-attack-mitigation-strategies-e20625645.html.

Glaser, Charles L. “Deterrence of Cyber Attacks and U.S. National Security.” The George Washington University, vol. Report GW-CSPRI-2011-5, 2011, p. 8, https://www.semanticscholar.org/paper/Deterrence-of-Cyber-Attacks-and-U.S.-National-Glaser/0546af254548b6636724fb0d2f60122c45fe055f.

Halpin, Edward F., editor. Cyberwar, Netwar and the Revolution in Military Affairs. Palgrave Macmillan, 2006. Library of Congress ISBN, https://link.springer.com/book/10.1057/9780230625839.

Henriksen, Anders. “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace.” Oxford University, vol. 5, no. 1, Jan. 2019. DOI.org (Crossref), https://doi.org/10.1093/cybsec/tyy009.

Islam, Mohammad Rafsun, and K. M. Aktheruzzaman. “An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions.” Journal of Computer and Communications, vol. 08, no. 04, 2020, pp. 11–25. DOI.org (Crossref), https://doi.org/10.4236/jcc.2020.84002.

IT Governance Free Downloadable Infographics. 2021, https://itgovernance.co.uk/infographics/list-of-data-breaches-in-2020.

Kitzen, Martijn. “Operations in Irregular Warfare.” Handbook of Military Sciences, edited by Anders McD Sookermany, Springer International Publishing, 2020, pp. 1–21. DOI.org (Crossref), https://doi.org/10.1007/978-3-030-02866-4_81-1.

Libicki, Martin C. Cyberdeterrence and Cyberwar. RAND, 2009. Library of Congress ISBN, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiw69GHuvPxAhXmgP0HHcfxDvsQFjABegQIBBAD&url=https%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Fmonographs%2F2009%2FRAND_MG877.pdf&usg=AOvVaw3vSa4GId9RRkCb-KinS8jI.

Lin, Herbert, and Amy Zegart. “Introduction to the Special Issue on Strategic Dimensions of Offensive Cyber Operations.” Oxford University, Mar. 2017. DOI.org (Crossref), https://doi.org/10.1093/cybsec/tyx002.

Long, Janice R. “WHY IRREGULARS WIN: ASYMMETRY OF MOTIVATIONS AND THE OUTCOMES OF IRREGULAR WARFARE.” NAVAL POSTGRADUATE SCHOOL, 2016, p. 213. Zotero, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi3g6e-uvPxAhWYhv0HHdvzA6oQFjABegQIAxAD&url=https%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D812538&usg=AOvVaw2gqA6ZsgYJaugPGtQk-PYi.

McKinsey & Company. COVID-19 Digital Transformation & Technology. 2021, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

McLennan, Marsh, and SK Group. The Global Risks Report 2021 16th Edition. 2021, p. 97. , https://www.weforum.org/reports/the-global-risks-report-2021.

Metz, Steven, et al. Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts: Defense Technical Information Center, 1 Jan. 2001. DOI.org (Crossref), https://doi.org/10.21236/ADA392257.

Mikael, Minberger S., and Svendsen O. Geir. “Irregular Warfare as a National Military Strategy Approach for Small States.” NAVAL POSTGRADUATE SCHOOL, 2013, p. 154. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjQ9obuuvPxAhVbgP0HHSWyCjgQFjADegQIFRAD&url=https%3A%2F%2Fwww.semanticscholar.org%2Fpaper%2FIrregular-Warfare-as-a-National-Military-Strategy-Minberger-Svendsen%2F8c7000b8f23381270a757e1d635c6c5f6a93d12a&usg=AOvVaw2D4VxHSHOzdFzEB0HVrNJw.

Miles,Brundage, et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. University of Oxford/University of Cambridge/Centre for the Study of Existential Risk, 2018, p. 101.

Muckin, Michael, and Scott C. Fitch. “A Threat-Driven Approach to Cyber Security.” Lockheed Martin Corporation, 2019, p. 45.

NATO Cooperative Cyber Defence Centre of Excellence and ALEXANDER KLIMBURG. NATO Cooperative Cyber Defence Centre of Excellence. NATO CCD COE Publication, 2012.

NATO STANDARDIZATION OFFICE (NSO). “AJP-3.20.” NATO STANDARDIZATION OFFICE (NSO), 2020, p. 53.

Nye, Joseph. Cyber Power. Harvard College, 2010, https://www.belfercenter.org/publication/cyber-power.

Politou, Eugenia, et al. “Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions.” Oxford University, vol. 4, no. 1, Jan. 2018. DOI.org (Crossref), https://doi.org/10.1093/cybsec/tyy001.

Professor Jon Crowcroft and Dr Richard Mortier. “Horizons.” Univercity of Cambridge, no. 27, p. 36, www.cam.ac.uk/research.

Ranger, Steve. “What Is Cyberwar? Everything You Need to Know about the Frightening Future of Digital Conflict.” ZDNet, 2018, https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/.

Rashid, Professor Awais, et al. “The Future of the UK’s Cyber Security Research Position in the World.” University of Bristol, 2020, p. 13. University of Bristol, http://www.bris.ac.uk/engineering/news/2020/the-future-of-the-uks-cyber-security-research-position-in-the-world.html.

Refsdal, Atle, et al. Cyber-Risk Management. Springer International Publishing, 2015. DOI.org (Crossref), https://doi.org/10.1007/978-3-319-23570-7.

Russell, Alison. Cyber Blockades. The Fletcher School of Law and Diplomacy, 2012, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjLnKKxu_PxAhUhg_0HHX-WARUQFjAAegQIAxAD&url=https%3A%2F%2Fdl.tufts.edu%2Fconcern%2Fpdfs%2Fpv63gb62x&usg=AOvVaw0jaRPkDkL1ntyy39YO6dJk.

Shevchenko, Pavel V., et al. “Quantification of Cyber Risk – Risk Categories and Business Sectors.” SSRN Electronic Journal, 2021. DOI.org (Crossref), https://doi.org/10.2139/ssrn.3858608.

Shostack, Adam. Threat Modeling: Designing for Security. John Wiley & Sons, Inc, 2014.

Sigfusson, Thor, and Simon Harris. “Cyberspace: A Paradigm Shift for International Entrepreneurs’ Relationships?” International Business, edited by Simon Harris et al., The University of Edinburgh, 2012, pp. 170–87. DOI.org (Crossref), https://doi.org/10.1057/9781137007742_11.

Singhal, Anoop, and Ximming Ou. “Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs.” National Institute of Standards and Technology, 2011, p. 24.

Smith, Rupert. The Utility of Force: The Art of War in the Modern World. Knopf, 2007. Open WorldCat, http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=718535.

Sood, Isha, and Varsha Sharma. “Computational Intelligent Techniques To Detect DDOS Attacks : A Survey.” Journal of Cyber Security, vol. 3, no. 2, 2021, pp. 89–106. DOI.org (Crossref), https://doi.org/10.32604/jcs.2021.018623.

“Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA).” Cyber Defense Magazine, 11 Nov. 2019, https://www.cyberdefensemagazine.com/sovereign-cyber/.

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. National Academies Press, 2009, p. 12651. DOI.org (Crossref), https://doi.org/10.17226/12651.

Thomas, Thomas M., and Donald Stoddard. Network Security First-Step. Cisco Press, 2012.

U.S. DEPARTMENT OF HOMELAND SECURITY. DHS-Cybersecurity-Strategy. 2018, https://www.dhs.gov/publication/dhs-cybersecurity-strategy.

Vatis, Michael. “Cyber Attacks: Protecting America’s Security Against Digital Threats.” John F. Kennedy School of Government, Harvard University, 2002, p. 38.

Winterfeld, Steve, and Jason Andress. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress/Elsevier, 2013. Library of Congress ISBN, https://www.researchgate.net/publication/230687826_CYBER_WARFARE_AN_ANALYSIS_OF_THE_MEANS_AND_MOTIVATIONS_OF_SELECTED_NATION_STATES.

Wulf Reiners and Ebru Turhan, editors. EU-Turkey Relations: Theories, Institutions, and Policies. Springer International Publishing, 2021. DOI.org (Crossref), https://doi.org/10.1007/978-3-030-70890-0.

Zhang, Minxing, et al. “Membership Inference Attacks Against Recommender Systems.” Cornell University, Sept. 2021. arXiv.org, http://arxiv.org/abs/2109.08045.

ΓΕΕΘΑ. Διακλαδικό Δόγμα Επιχειρήσεων Κυβερνοχώρου ΔΕ 3.9. Τυπογραφείο Ελληνικού Στρατού, 2013.

---. Στρατιωτικό Στρατηγικό Δόγμα. Τυπογραφείο Ελληνικού Στρατού, 2013.

Ελληνική Δημοκρατία. Εθνική Στρατηγική Κυβερνοασφάλειας. 2020, https://mindigital.gr/ εθνικη-στρατηγικη-κυβερνοασφαλεια.

Ντόκος, Θάνος. Ασύμμετρες Απειλές Και Διεθνής Ασφάλεια.

“Ο ιός Stuxnet και το πυρηνικό πρόγραμμα του Ιράν.” ΚΕΔΙΣΑ - KEDISA, 9 June 2018, https://kedisa.gr/ ο-ιός-stuxnet-και-το-πυρηνικό-πρόγραμμα-του-ιράν/

Χουντάλας, Παναγιώτης. Τεχνικές Αξιολόγησης Κινδύνων/Σημειώσεις Μαθήματος. ΠΕΔΙΣ.

Παράρτημα Α

1.Γενικά περί ασύμμετρων απειλών

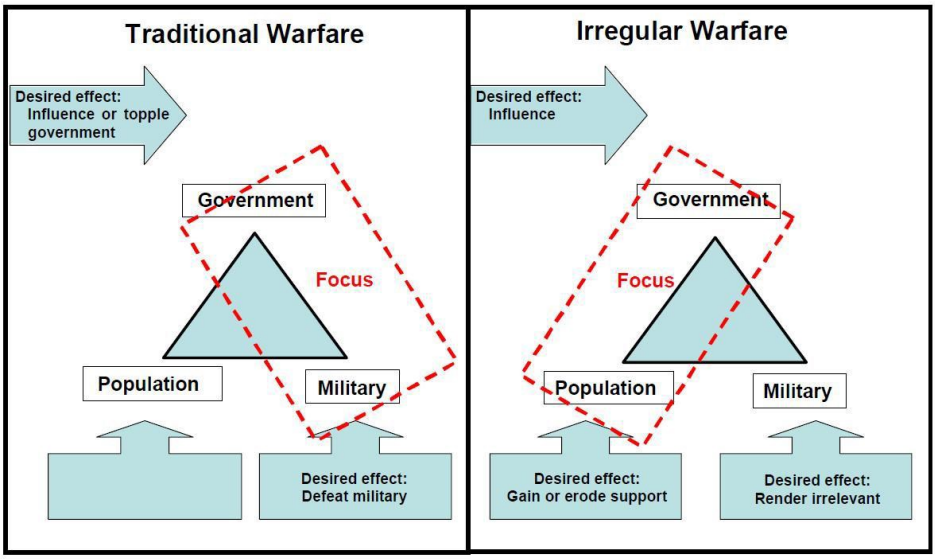
Η τακτική των ασύμμετρων απειλών, βασίζεται στη χρήση μέσων εύκολα ευρισκόμενων και μικρού κόστους. Το αποτέλεσμα όμως της δράσης τους, προκαλεί δυσανάλογα μεγάλο κόστος, σε ζωές και υποδομές, αλλά αυτό που στην ουσία επιδιώκεται είναι η πρόκληση τρόμου και ψυχολογικής βίας, παράγοντες καταλυτικοί για την πρόκληση μεγάλου κοινωνικού κόστους. Οι συγκεκριμένες μέθοδοι, κινούνται κατά κανόνα εκτός νομικών και ηθικών πλαισίων και έχουν έντονο το χαρακτήρα του απρόβλεπτου.

Ο όρος «ασύμμετρος» είναι γενικά το αντίθετο του «συμμετρικός», δηλαδή κάτι που δεν έχει συμμετρία και κατ' επέκταση δεν είναι αρμονικό ή είναι δυσανάλογο. Ο όρος «απειλή», υποδηλώνει πράξεις, χειρονομίες ή λόγια που αποσκοπούν στον εκφοβισμό κάποιου, ενώ σε μια άλλη προσέγγιση ο όρος «απειλή», αναφέρεται σε κάτι κακό ή ανεπιθύμητο που βάζει σε κίνδυνο κάποιον. Συνδυάζοντας τους δύο παραπάνω όρους, θα μπορούσαμε να ορίσουμε ετυμολογικά την «ασύμμετρη απειλή» ως προσπάθεια δημιουργίας μιας επικίνδυνης κατάστασης για κάποιους, με δημιουργία κλίματος εκφοβισμού, κάνοντας χρήση μέσων και διαδικασιών που είναι δυσανάλογα και μη αρμονικά με τις κοινές πρακτικές, είναι δηλαδή αντισυμβατικές. Όταν αναφερόμαστε στον πόλεμο και στις συγκρούσεις, τον χρησιμοποιούμε για να περιγράψουμε οποιαδήποτε σύγκρουση που δεν περιλαμβάνει παρόμοια οργανωμένα αντίπαλα στρατεύματα και τα οποία επιζητούν την επικράτηση έναντι του άλλου στο πεδίο της μάχης με σκοπό την ισχυροποίηση ή την επικράτηση των συμφερόντων των κρατών τους. (Kitzen, 2020)

Η ασυμμετρία, από την στρατηγική σκοπιά, ενεργεί, οργανώνει και σκέφτεται διαφορετικά από τους αντιπάλους για να μεγιστοποιήσει τα δικά της πλεονεκτήματα, να εκμεταλλευτεί τις αντίπαλες αδυναμίες, να επιτύχει την πρωτοβουλία ή να κερδίσει μεγαλύτερη ελευθερία δράσης. Μπορεί να είναι πολιτικό-στρατηγική, στρατιωτικό-στρατηγική, επιχειρησιακή ή συνδυασμός των ανωτέρω. Μπορεί να περιλαμβάνει διαφορετικές μεθόδους, τεχνολογίες, αξίες, οργανώσεις, προοπτικές χρόνου ή συνδυασμό αυτών. Μπορεί να είναι

βραχυπρόθεσμη ή μακροπρόθεσμη . Μπορεί να είναι διακριτή ή επιδιωκόμενη σε συνδυασμό με συμμετρικές προσεγγίσεις. Μπορεί να έχει ψυχολογικές και φυσικές διαστάσεις.(Metz et al., 2001)

Ο «ασύμμετρος πόλεμος», όπως και ο πόλεμος με την παραδοσιακή του έννοια, αποσκοπούν την επίλυση της σύγκρουσης μέσω της επιτακτικής αλλαγής της αντίπαλης συμπεριφοράς. Παρόλα αυτά, διαφέρουν σημαντικά στην στρατηγική και την εκτέλεσή τους. Ο πόλεμος, με την παραδοσιακή του έννοια, επικεντρώνεται στην αντίπαλη δυνατότητα αντοχής στη μάχη. Αντίθετα, ο «ασύμμετρος πόλεμος» επικεντρώνεται σε πληθυσμιακό-κεντρικές προσεγγίσεις που επηρεάζουν τους δρώντες, τις συμπεριφορές, τις σχέσεις και τη σταθερότητα στην περιοχή ενδιαφέροντος. Πολίτες στις πόλεις, στους δρόμους και στα σπίτια τους μπορούν να αποτελέσουν μέρος του σύγχρονου πεδίου μάχης. Για το λόγο αυτό ο «ασύμμετρος πόλεμος» χρήζει διαφορετικής προσέγγισης στρατηγικής σκέψης και κατανόησης των απειλών. (Air Force Doctrine Document, 2013)



Εικόνα 14: Αντιπαράθεση παραδοσιακού και ασύμμετρου πολέμου (Πηγή: http://irregularwarrior.com/defining-irregular-warfare)

Καταλήγοντας, μπορούμε να πούμε πως ο ασύμμετρος πόλεμος μπορεί να οριστεί ως ένας βίαιος αγώνας που περιλαμβάνει μη κρατικούς φορείς, συμπεριλαμβανομένων των βίαιων ένοπλων ομάδων που ενεργούν ως κρατικοί αντιπρόσωποι, και κράτη με σκοπό την καθιέρωση εξουσίας, ελέγχου και νομιμότητας στον σχετιζόμενο πληθυσμό. Λόγω της στρατιωτικής ασυμμετρίας και της πολιτικής φύσης του αγώνα, η χρήση βίας λαμβάνει ως επί

το πλείστων μη συμβατικές ή ανορθόδοξες μορφές και είναι συνήθως σε συνδυασμό με άλλες δραστηριότητες. Ως εκ τούτου, ο ασύμμετρος πόλεμος ευνοεί μια έμμεση προσέγγιση που δεν επικεντρώνεται στη στρατιωτική ήττα, αλλά στη νίκη του σχετιζόμενου πληθυσμού.(Smith, 2007)

2.Ιστορικό

Οι πρώτες ασύμμετρες απειλές εμφανίστηκαν την περίοδο μετά το 1991, εποχή δηλαδή μετά τον πόλεμο του Κόλπου. Η πιο ακραία όμως μορφή ασύμμετρης μεθόδου ήταν το τρομοκρατικό χτύπημα της 11 Σεπτεμβρίου 2001 στους δίδυμους πύργους, ένα χτύπημα στην καρδιά μίας μεγάλης δύναμης, και το οποίο έμελλε να αλλάξει ριζικά τον τρόπο σκέψης της ανθρωπότητας. Το αίσθημα ασφάλειας κλονίστηκε σε τεράστιο βαθμό, αφού μία τεράστια δύναμη βρέθηκε αντιμέτωπη με έναν ανύπαρκτο μέχρι τότε εχθρό. Η ισχύς και τα οπλικά συστήματα δεν αρκούσαν για να τους θωρακίσει από την ασύμμετρη απειλή, ενώ οι συνέπειες ήταν τεράστιες και ανυπολόγιστες. Η διεθνής ασφάλεια κλονίστηκε και οι άνθρωποι από τότε και στο εξής ζουν σε ένα περιβάλλον αβεβαιότητας και φόβου. (Mikael and Geir, 2013)

3.Μορφές ασύμμετρων απειλών

Η κατηγοριοποίηση των απειλών ως ασύμμετρες είναι γενική και δεν μπορεί να ορισθεί με αυστηρά κριτήρια. Αυτές δύνανται να διαφοροποιούνται, να εξελίσσονται ακόμα να μην υφίστανται στην παρούσα χρονική περίοδο, αφού όπως εξηγήσαμε κύριο χαρακτηριστικό τους είναι η προσπάθεια υιοθέτησης μη προβλέψιμης δράσης. Οι βασικότερες μορφές ασύμμετρης απειλής σύμφωνα με το ΓΕΕΘΑ είναι:

α. Η διεθνής τρομοκρατία
β. Τα όπλα μαζικής καταστροφής
γ. Η παράνομη δράση ένοπλων ομάδων
δ. Η παράτυπη μετανάστευση
ε. Το διεθνές οργανωμένο έγκλημα
στ. Η διακίνηση ναρκωτικών
ζ. Ο εθνικοθρησκευτικός φανατισμός
η. Ο κυβερνοπόλεμος

4.Αίτια ασύμμετρων απειλών

Οι ασύμμετρες απειλές αποτελούν ένα πολύπλοκο ζήτημα. Η ολιστική προσέγγιση του θέματος απαιτεί αρχικά να προσδιοριστούν και να αναλυθούν

σε βάθος όλοι οι κύριοι παράγοντες αλλά και οι αιτίες που καλλιεργούν αυτού του είδους τη νέα απειλή που μαστίζει την ανθρωπότητα. Σαν κύριες αιτίες εντοπίζονται οι πολιτικές, οικονομικές, κοινωνικές διαφορές μεταξύ ανεπτυγμένων χωρών και ο θρησκευτικός και εθνικιστικός φονταμενταλισμός. Οι συνεχείς αλλαγές στο διεθνές σύστημα, οι αλλαγές των συνόρων μετά και τη διάλυση της Σοβιετικής Ένωσης και η συνεχής αμφισβήτηση για τις ηγεμονίες των αραβικών πετρελαιοπαραγωγών χωρών, θέτουν τους όρους και τις προϋποθέσεις για να ευδοκιμήσουν οι ασύμμετρες απειλές. Η άνιση κατανομή πλούτου και γενικά των αγαθών, οδηγεί σε οικονομική εξάρτηση των μη ανεπτυγμένων χωρών από τα ανεπτυγμένα κράτη με πολλά δυσάρεστα συνεπακόλουθα, με σημαντικότερο την αύξηση της παράνομης μετανάστευσης, η οποία με τη σειρά της συμβάλει στη δημιουργία των προϋποθέσεων για ασύμμετρες απειλές.

Παράλληλα, οι πολίτες αρκετών χωρών με χαμηλό βιοτικό και μορφωτικό επίπεδο τείνουν να αποτελούν εύκολα θύματα επιτηδείων που θέλουν να ικανοποιήσουν τα συμφέροντα τους και εν τέλει να στρατεύονται από φανατικούς Φονταμενταλιστές για την εκτέλεση τρομοκρατικών ενεργειών. Αυτοί εκμεταλλεύονται τις συνθήκες εξαθλίωσης των πολιτών αυτών και δημιουργούν τις προϋποθέσεις για την εκδήλωση αισθημάτων φθόνου και εκδίκησης προς ανθρώπους, οι οποίοι ευημερούν και απολαμβάνουν μία ήσυχη και ξέγνοιαστη ζωή. Καλλιεργείται με τον τρόπο αυτό ο θρησκευτικός και εθνικιστικός φανατισμός, εκδηλώνουν πράξεις εγκληματικότητας και τρομοκρατίας, μη αναλογιζόμενοι το κόστος και τις επιπτώσεις.(Long, 2016)

5.Χαρακτηριστικά των ασύμμετρων απειλών

Τα αποτελέσματα και οι συνέπειες των ασύμμετρων απειλών διαφέρουν ανάλογα με τους σκοπούς για τους οποίους εκτελούνται και έχουν επίδραση τόσο σε τακτικό όσο και σε στρατηγικό επίπεδο, ενώ χαρακτηρίζονται από πέντε πολύ βασικά στοιχεία:

1. Από τον αιφνιδιασμό, το αναπάντεχο δηλαδή τους μη προειδοποίησης σε ενδεχόμενη τρομοκρατικό χτύπημα με άμεσο στόχο την δυσκολία του εντοπισμού και τους αντιμετώπισης τους
2. Τον ακραίο φανατισμό και της τακτικής της αυτοθυσίας
3. Την άφθονη χρηματοδότηση για την επίτευξη των στόχων
4. Την άρτια οργάνωση
5. Την παγκόσμια εξάπλωση των οργανώσεων με τη βοήθεια τους προηγμένης τεχνολογίας και των ψηφιακών δικτύων

Τέλος, οι ασύμμετρες απειλές αψηφούν βασικούς νόμους που ακολουθούν οι κλασικοί πόλεμοι, τους η κατάργηση τους έννοιας τους αποτροπής, η σχεδίαση τους τακτικής και ακριβώς αυτό είναι που τους καθιστά τόσο επικίνδυνη απειλή για τη διεθνή ασφάλεια.(Kitzen, 2020)

6.Επιπτώσεις

Οι επιπτώσεις από την εμφάνιση των ασύμμετρων απειλών ποικίλουν αναλόγως του στόχου που θέλουν να πετύχουν. Κοινή συνισταμένη αποτελεί το γεγονός ότι η εμφάνισή τους έτριξε τα θεμέλια της διεθνούς ασφάλειας, καθ' όσον οι υπάρχοντες μηχανισμοί κρίνονται ακατάλληλοι σε πολλές των περιπτώσεων να προστατέψουν τη σταθερότητα και να αποτρέψουν την εμφάνιση τέτοιων μορφών εκδηλώσεων σε απειλή.

Πλέον οι άνθρωποι βιώνουν σε πολλές περιπτώσεις ωμή βία, γεγονός που κλονίζει το ηθικό τους και αυξάνει κατακόρυφα την αβεβαιότητα. Σε όλα αυτά έρχεται να προστεθεί το γεγονός ότι αυξάνεται η ξενοφοβία και οι φυλετικές διακρίσεις, με αποτέλεσμα να δημιουργούνται κοινωνικές αναταραχές, φοβίες και να εκδηλώνονται ακραίες συμπεριφορές. Στο πλαίσιο της αντιμετώπισης των ασύμμετρων απειλών περιορίστηκε η προσωπική ελευθερία των πολιτών, αφού θεσμοθετήθηκαν νόμοι που ελέγχουν τις κινήσεις και τα προσωπικά δεδομένα από όλες τις καθημερινές τους δραστηριότητες.(Metz et al., 2001)

Επίσης σημαντική επίπτωση αποτελεί το γεγονός ότι σε πολλές των περιπτώσεων για την αντιμετώπιση αυτής της απρόκλητης νέας απειλής υιοθετούνται αυστηρά μέτρα, που προβλέπουν ανάληψη ακόμη και πολεμικών επιχειρήσεων μεταξύ των κρατών. Τέλος, υφίσταται σπατάλη αμυντικών κεφαλαίων, τόσο από την αυξημένη χρηματοδότηση για την εξεύρεση αποτελεσματικών μέτρων αντιμετώπισης των ασύμμετρων απειλών, όσο και για την έρευνα της ανάπτυξης προηγμένης τεχνολογίας κατά της τρομοκρατίας.(Long, 2016)

7.Πιθανοί στόχοι

Οι πιθανοί στόχοι των ασύμμετρων απειλών ποικίλουν. Ωστόσο επιλέγονται στόχοι που παραδοσιακά έχουν μικρή ή καθόλου προστασία, χωρίς αυτό να αποτελεί κανόνα επιλογή της επίθεσης. Η επιλογή του στόχου εξαρτάται από το μεγαλύτερο ψυχολογικό αντίκτυπο που θα επιφέρει, σε συνδυασμό με τους ελάχιστους μειωμένους κινδύνους αποτυχίας. Περιλαμβάνουν ένα ευρύ φάσμα της πολιτικής, κοινωνικής και οικονομικής ζωής και δεν είναι εύκολο εξ αρχής

να προσδιοριστούν με ακρίβεια, προκειμένου να ληφθούν τα απαραίτητα μέτρα, αφού είναι δύσκολο να αποκαλυφθούν ποιοι είναι αυτοί που τους επιλέγουν και ποιες είναι οι προθέσεις τους.

Ο πρωταρχικός στρατηγικός στόχος των ασύμμετρων απειλών είναι η άσκηση ψυχολογικής βίας και όχι επίτευξης στρατιωτικών στόχων, καθώς αποσκοπούν να εκφοβίσουν τον αντίπαλο ψυχολογικά με την άμεση ή έμμεση προσβολή του επιδιωκόμενου στόχου και μέσω αυτής της οδού οι εκφραστές τους να πετύχουν τους πολιτικούς στόχους. Επιπλέον, στρατηγικό στόχο αποτελεί και η προσπάθεια που γίνεται ώστε με τις ασύμμετρες απειλές να παραπλανήσουν τους ανθρώπους, να κατευθύνουν τον τρόπο σκέψης τους προωθώντας τις ενέργειές τους ως νόμιμες. Επιδιώκουν έτσι να πετύχουν υποστηρικτές που θα συμβάλλουν οικονομικά στον αγώνα τους, υλοτεχνική υποστήριξη, πρόσβαση σε προηγμένη τεχνολογία, ασφαλές καταφύγιο και το κυριότερο την δυνατότητα να στρατολογούν νέους μαχητές για την υλοποίηση των σχεδίων τους.

Σε πολλές των περιπτώσεων οι ασύμμετρες απειλές κατευθύνονται προς τον πληθυσμό και σε κρίσιμες υποδομές. Αυτό όμως που κινδυνεύει περισσότερο είναι η ασφάλεια των στρατιωτικών εγκαταστάσεων και συγκεκριμένα τα κέντρα ελέγχου και διοίκησης, εγκαταστάσεις υποστήριξης, αποθήκες με κρίσιμο και επικίνδυνο υλικό. Οι απειλές όμως απευθύνονται και στις κρατικές λειτουργίες, σε κρίσιμες κρατικές υποδομές, όπως είναι τα διάφορα υπουργεία, τα νοσοκομεία και τα όποια εφ’ όσον πληγούν θα φέρουν τεράστιες κοινωνικές επιπτώσεις. Επιπλέον, κύριο στόχο αποτελούν τα δίκτυα πληροφοριών, οι κόμβοι πληροφορικής, τα μέσα κοινωνικής δικτύωσης και τα εργοστάσια παραγωγής ηλεκτρικής ενέργειας.

Παράρτημα Β

Στο παρών παράρτημα παρουσιάζονται πίνακες και εικόνες από πρόσφατες μελέτες και αναφορές έγκυρων διεθνών οργανισμών για την ανάδειξη των επικινδυνότερων απειλών παγκοσμίως.

Πίνακας 8: Οι δέκα σημαντικότερες απειλές για τη χώρα μας (Πηγή: Alianz, 2021)

TOP 10 RISKS IN GREECE

Source: Allianz Global Corporate & Specialty.

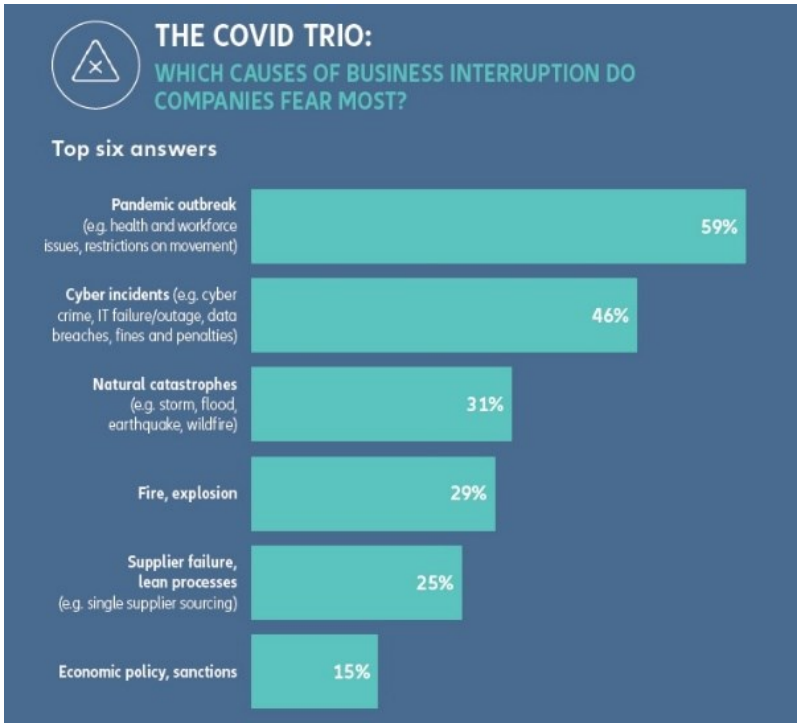
Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 28

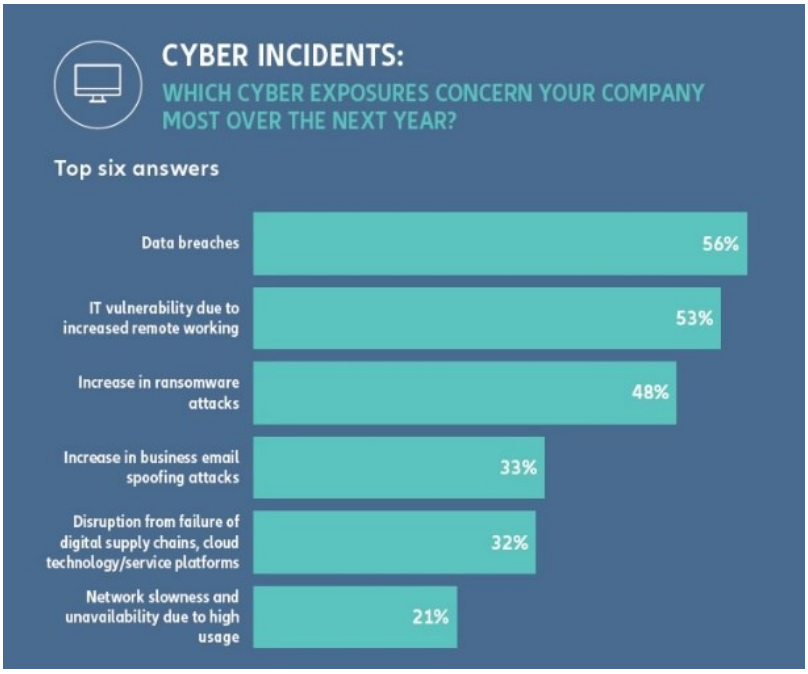
Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2020 rank	Trend
1	**Pandemic outbreak (e.g. health and workforce issues, restrictions on movement)**	**54%**	**NEW**	▲
2	Business interruption (incl. supply chain disruption)	**36%**	7 (21%)	▲
2	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	**36%**	2 (37%)	=
4	Natural catastrophes (e.g. storm, flood, earthquake, wildfire)	**29%**	4 (32%)	=
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**21%**	2 (37%)	▼
5	Climate change/increasing volatility of weather	**21%**	6 (26%)	▲
5	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	**21%**	4 (32%)	▼
8	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**18%**	1 (53%)	▼
9	Political risks and violence (e.g. political instability, war, terrorism, civil commotion, riots and looting)	**14%**	8 (16%)	▼
10	Environmental risks (e.g. pollution)	**11%**	**NEW**	▲

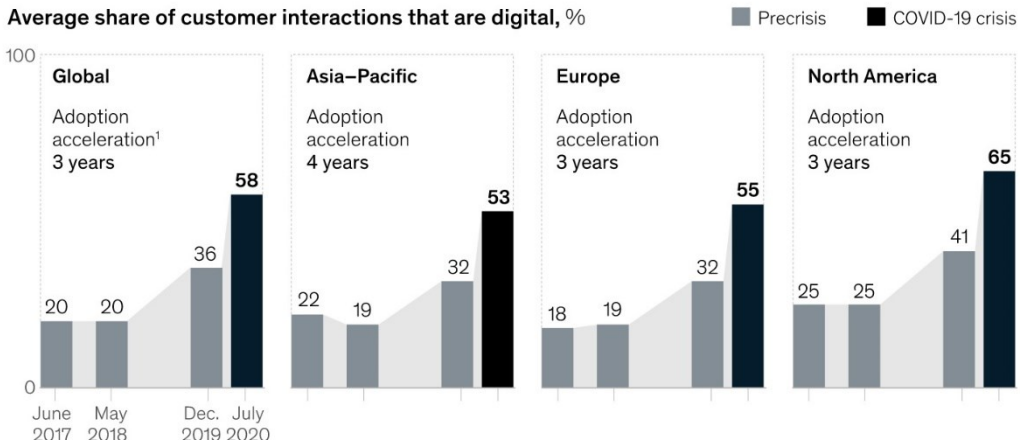
Πίνακας 9: Οι κυβερνοαπειλές ως νούμερο δύο κίνδυνος για τις επιχειρήσεις (Πηγή: Alianz, 2021)



Πίνακας 10: Τα πιο επικίνδυνα είδη κυβερνοαπειλών (Πηγή: Alianz, 2021)



Πίνακας 11 :Η παγκόσμια αύξηση της ψηφιοποίησης στη μετά Covid-19 εποχή (Πηγή: McKinsey & Company, 2021)



Πίνακας 12: Οι σημαντικότερες παγκόσμιες απειλές σε βάθος δεκαετίας (Πηγή: McLennan and Group, 2021)