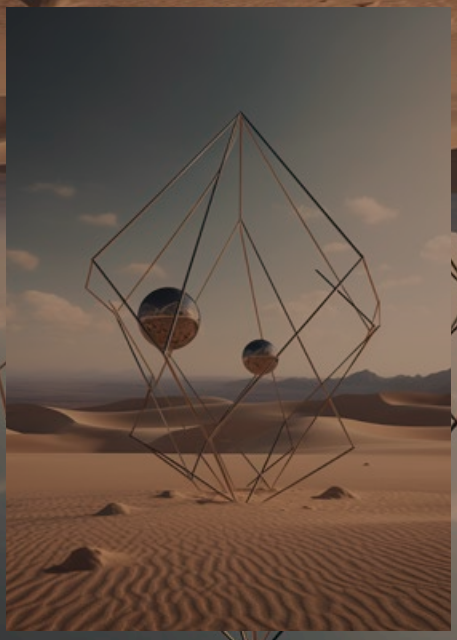
DELPHI ECONOMIC FORUM

CENTER FOR CYBER RESILIENCE

ΣΕ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟ ΕΛΙΑΜΕΠ ELIAMEP



ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑ

ΠΩΣ ΘΩΡΑΚΙΖΟΥΜΕ ΤΟ ΨΗΦΙΑΚΟ ΜΕΛΛΟΝ ΤΗΣ ΧΩΡΑΣ;

POLICY PAPER

ΜΕ ΤΗΝ ΥΠΟΣΤΗΡΙΞΗ ΤΗΣ VODAFONE GREECE vodafone

Το policy paper **«Κυβερνοασφάλεια: Πώς θωρακίζουμε το ψηφιακό μέλλον της χώρας»** συνοψίζει και εξειδικεύει τα συμπεράσματα της συζήτησης στρογγυλής τραπέζης που είχε διοργανώσει τον Μάρτιο του 2024 το **Center for Cyber Resilience (Κέντρο για την Κυβερνο-Ανθεκτικότητα) του Οικονομικού Φόρουμ των Δελφών**, σε συνεργασία με τον **ΕΛΙΑΜΕΠ**, με την υποστήριξη της **Vodafone Ελλάδας** και τη συμμετοχή κορυφαίων κυβερνητικών, πολιτικών, ακαδημαϊκών παραγόντων και εκπροσώπων της αγοράς.

Το παρόν κείμενο παρουσιάζει: μία συνοπτική ιστορική αναδρομή στην εξέλιξη και τη διαμόρφωση της αρχιτεκτονικής κυβερνοασφάλειας σε επίπεδο Ευρωπαϊκής Ένωσης, καθώς και στις αντίστοιχες προσπάθειες διαμόρφωσης ενός πλαισίου πολιτικής στην Ελλάδα· τα ευρήματα μιας έρευνας κοινής γνώμης για την κυβερνοασφάλεια σε Έλληνες πολίτες και επιχειρήσεις που δραστηριοποιούνται στην Ελλάδα, την οποία εκπόνησε η **Metron Analysis**· μία σειρά προτάσεων πολιτικής για την ενίσχυση της κυβερνοασφάλειας στην Ελλάδα.

FORE-WORD

ΤΟΥ ΓΙΑΝΝΗ ΘΩΜΑΤΟΥ
ΑΝΤΙΠΡΟΕΔΡΟΥ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΟΥΜ ΤΩΝ ΔΕΛΦΩΝ

Το Οικονομικό Φόρουμ των Δελφών, επιθυμώντας να συνεχίσει να αποτελεί μία σταθερά εμπλουτισμού του δημοσίου διαλόγου με επιστημονική γνώση και ολοκληρωμένες προτάσεις πολιτικής σε ζητήματα αιχμής, δημιούργησε το 2024 το Κέντρο Κυβερνο-Ανθεκτικότητας (Center for Cyber Resilience).

Τον περασμένο Μάρτιο, το Κέντρο διοργάνωσε, με την υποστήριξη της Vodafone Ελλάδας, μια εξαιρετικά πλούσια σε περιεχόμενο συζήτηση στρογγυλής τραπέζης, με θέμα τους κινδύνους και τις κυβερνο-απειλές που επηρεάζουν την ψηφιακή οικονομία, αλλά και την ίδια μας τη ζωή. Σε συνδυασμό με τις επίκαιρες τοποθετήσεις των αρμόδιων υπουργών, κορυφαίων ακαδημαϊκών και παραγόντων της αγοράς, τη συζήτηση τροφοδότησε και μία έρευνα κοινής γνώμης της Metron Analysis, σε συνεργασία με το ΕΛΙΑΜΕΠ, σχετικά με τη χρήση του διαδικτύου στις επιχειρήσεις και στον δημόσιο τομέα, από την οποία προκύπτει ξεκάθαρα το εξής: όσο περισσότερο το διαδίκτυο γίνεται αναπόσπαστο κομμάτι της ζωής μας, τόσο περισσότερες είναι οι πιθανότητες να έρθουμε αντιμέτωποι με το κυβερνο-έγκλημα και τόσο μεγαλύτερος ο αντίκτυπος αυτού του νέου τύπου εγκλήματος στη ζωή πολιτών και επιχειρήσεων.

Το policy paper που κρατάτε στα χέρια σας αποτελεί μια προσπάθεια εμβάθυνσης στη σημαντική συζήτηση που ξεκίνησε εκείνο το απόγευμα, την 1η Μαρτίου 2024. Με τη βοήθεια του ΕΛΙΑΜΕΠ, και ιδιαίτερα του Δρος Τριαντάφυλλου Καρατράντου και της εξαιρετικής ομάδας του,έχουμε την ευκαιρία να αποκτήσουμε μία σαφή εικόνα για την εξέλιξη του φαινομένου τις τελευταίες δεκαετίες, όσο και για τη θεσμική και νομική απάντηση σε αυτό, που έχει επιχειρήσει να προσφέρει τόσο η Ευρωπαϊκή Ένωση όσο και το ελληνικό κράτος.

Λέμε συχνά πως η τεχνολογία μοιραία βρίσκεται κάποια βήματα μπροστά ακόμα και από τις πλέον αποτελεσματικές κρατικές υπηρεσίες ασφαλείας, και η θεσμική και νομική θωράκιση των δημοκρατιών μας, αποτέλεσμα διαβούλευσης και συμβιβασμών, συνήθως έρχεται κατόπιν εορτής. Για τον λόγο αυτό, το policy paper περιέχει και μία σειρά από συγκεκριμένες προτάσεις πολιτικής, που θα μπορούσαν να αξιοποιηθούν από την πολιτική και επιχειρηματική ηγεσία, την ακαδημαϊκή κοινότητα, αλλά και κάθε ενδιαφερόμενο, ώστε αυτή η «διαφορά φάσης», μεταξύ τεχνολογικού εγκλήματος και νομικού και επιχειρησιακού πλαισίου, να αμβλυνθεί όσο είναι εφικτό.

Είναι αυτού του τύπου η ολοκληρωμένη παρέμβαση στα δημόσια πράγματα που φιλοδοξεί να πετύχει το Οικονομικό Φόρουμ των Δελφών, μέσω της δραστηριότητας των –τριών πλέον– κέντρων πολιτικής που έχει δημιουργήσει τα τελευταία χρόνια: του Κέντρου για το Μέλλον της Εργασίας, του Κέντρου για το Μέλλον της Υγείας, και πλέον του Κέντρου Κυβερνο-Ανθεκτικότητας. Αποτελεί δέσμευσή μας να συνεχίσουμε σε αυτόν τον δρόμο και τα επόμενα χρόνια.

Καλή ανάγνωση

FORE-WORD

ΤΟΥ ΧΑΡΗ ΜΠΡΟΥΜΙΔΗ
ΠΡΟΕΔΡΟΥ ΚΑΙ ΔΙΕΥΘΥΝΟΝΤΟΣ ΣΥΜΒΟΥΛΟΥ ΤΗΣ VODAFONE ΕΛΛΑΔΑΣ

Η κυβερνοασφάλεια αποτελεί έναν από τους πιο κρίσιμους τομείς της σύγχρονης ψηφιακής εποχής, καθώς οι τεχνολογικές εξελίξεις και η αυξανόμενη συνδεσιμότητα δημιουργούν νέες προκλήσεις και κινδύνους. Σε μία εποχή που οι κυβερνοαπειλές γίνονται όλο και πιο περίπλοκες και επικίνδυνες, η Vodafone αναγνωρίζει τη σημασία της προστασίας των δεδομένων και των πληροφοριών τόσο για τις επιχειρήσεις όσο και για τους πολίτες. Η στρατηγική μας, λοιπόν, επικεντρώνεται στην ενίσχυση των αμυντικών μηχανισμών μας, στην προληπτική ανάλυση κινδύνων, στην εκπαιδευτική ενδυνάμωση των χρηστών, αλλά και στην ευρύτερη ευαισθητοποίηση της κοινωνίας στο κορυφαίο ζήτημα της κυβερνοασφάλειας.

Στο πλαίσιο αυτό, και ειδικά στο τελευταίο σημείο, είμαστε εξαιρετικά ικανοποιημένοι για το γεγονός ότι είχαμε την ευκαιρία να συνεργαστούμε εκ νέου με το Center for Cyber Resilience του Οικονομικού Φόρουμ των Δελφών και το ΕΛΙΑΜΕΠ, με αποτέλεσμα το policy paper που διαβάζετε.

Σε αυτή την έκθεση, εξετάζονται οι κυριότερες προκλήσεις που αφορούν τον τομέα της κυβερνοασφάλειας, το πώς φτάσαμε στο υπάρχον θεσμικό πλαίσιο προστασίας τόσο στην Ευρωπαϊκή Ένωση όσο και στην Ελλάδα, ενώ ιδιαίτερη σημασία έχουν τα εξαιρετικά ενδιαφέροντα ευρήματα της έρευνας κοινής γνώμης που εκπόνησε η Metron Analysis ειδικά γι’ αυτό το θέμα, που αναδεικνύουν ανάγλυφα τη σημασία που έχει για τις ελληνικές επιχειρήσεις, αλλά και τους πολίτες. Αξίζει, τέλος, να διαβάσει κανείς με προσοχή τα συμπεράσματα και τις προτεινόμενες πολιτικές για την ενίσχυση της κυβερνοασφάλειας που, αν εισακουστούν, μπορούν να επιτρέψουν στη χώρα μας να συμμετάσχει απρόσκοπτα στην ψηφιακή επανάσταση του μέλλοντος.

ΠΡΟΛ

Η ραγδαία ανάπτυξη της τεχνολογίας, στην εποχή της 4ης Βιομηχανικής Επανάστασης, της τεχνητής νοημοσύνης και του «διαδικτύου των πραγμάτων» (Internet of Things), έχει μεταβάλει «εκ βάθρων» τη λειτουργία των κρατών, τις υποδομές και, κυρίως, την καθημερινότητα των πολιτών. Πράγματι, η ανάπτυξη της τεχνολογίας μπορεί να βελτιώνει την ποιότητα της ζωής μας αλλά, παράλληλα, διευρύνει και την τρωτότητά μας. Αυτός είναι και ο βασικός λόγος που οι νέες τεχνολογίες είναι πλέον στενά συνδεδεμένες με τις πολιτικές ασφάλειας. Η αλματώδης εξέλιξη της τεχνολογίας είναι αυτή που έχει επηρεάσει τόσο την έννοια της ασφάλειας, όσο και τη φύση των απειλών. Από τις κυβερνοαπειλές μέχρι την τρομοκρατία και τις διάφορες μορφές βίας η κακόβουλη χρήση της τεχνολογίας έχει καταστεί εργαλείο των εγκληματιών. Η τεχνολογία είναι, όμως, και το μεγαλύτερο όπλο για τους φορείς επιβολής του νόμου και τα κράτη. Μεταξύ των χρήσεων της νέας τεχνολογίας περιλαμβάνεται και η αξιοποίησή της για τη συλλογή και ανάλυση πληροφοριών. Οι υπηρεσίες πληροφοριών πολλών χωρών έχουν πλέον περάσει στη φάση της 4ης Βιομηχανικής Επανάστασης. Αντίστοιχα τεχνολογικά εξελιγμένες, ωστόσο, είναι και οι απειλές τόσο από κρατικούς, όσο και μη κρατικούς δρώντες. Μετα-δεδομένα, αλγόριθμοι, τεχνητή νοημοσύνη, διαδίκτυο των πάντων είναι συστατικά στοιχεία αυτής της φάσης.

Όπως είναι φυσικό, αυτός ο θαυμαστός καινούριος κόσμος αντιμετωπίζεται από πολλούς με σκεπτικισμό. Κατά κάποιο τρόπο βλέπουμε μία νέα τοποθέτηση του απλουστευτικού, εν πολλοίς, διλήμματος «ασφάλεια ή ελευθερία» στον τομέα των τεχνολογιών. Είναι αναμενόμενο, ειδικότερα αν λάβουμε υπόψη μας πως, από τη μία πλευρά, η τεχνολογία τρέχει γρηγορότερα από τις ρυθμιστικές πρωτοβουλίες των κρατών και, από την άλλη, σε χώρες όπως η Ελλάδα, υπάρχει ένας σημαντικός αριθμός πολιτών που δεν είναι πλήρως εξοικειωμένος με τις δυνατότητες και τη σωστή χρήση των νέων τεχνολογιών. Μέσα σε αυτό το πλαίσιο, οι παρακολουθήσεις και η χρήση κατασκοπευτικών λογισμικών έχουν δημιουργήσει ρωγμές στην εμπιστοσύνη των πολιτών έναντι των κρατών και των θεσμών, αλλά και των ιδιωτικών εταιρειών/παρόχων επικοινωνίας, γεγονός που επεκτείνεται και στις δυνατότητες των νέων τεχνολογιών γενικότερα. Μία ακόμα παράμετρος είναι οι θεωρίες συνωμοσίας και η τεχνο-φοβία, ως μορφή αντισυστημικής αντίδρασης, η οποία, κατά τη διάρκεια της πανδημίας, γνώρισε μεγάλη έξαρση.

Ο Γ Ο Σ

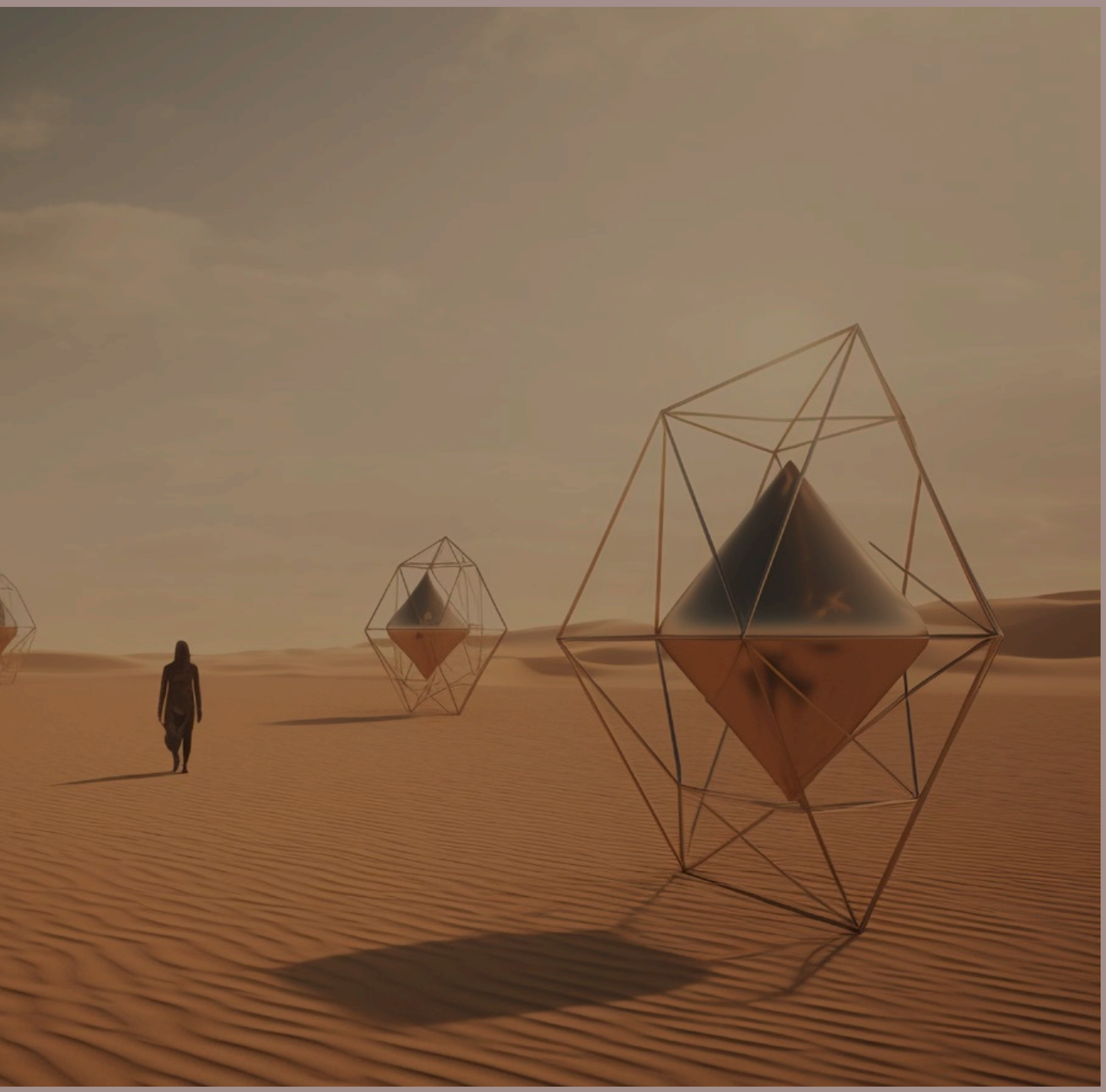
«Όπως είναι φυσικό, αυτός ο θαυμαστός καινούριος κόσμος αντιμετωπίζεται από πολλούς με σκεπτικισμό. Κατά κάποιο τρόπο βλέπουμε μία νέα τοποθέτηση του απλουστευτικού, εν πολλοίς, διλήμματος "ασφάλεια ή ελευθερία" στον τομέα των τεχνολογιών».

Κρίσιμη παράμετρο σε όλη αυτή τη διαδικασία αποτελεί η συνεργασία του δημοσίου και του ιδιωτικού τομέα, όπως και των παρόχων επικοινωνίας και δικτύων. Σε αυτή την κατεύθυνση άλλωστε κινείται και η ΕΕ, με τη δημιουργία του EU Internet Forum, αλλά και με την ενθάρρυνση της ενισχυμένης αλληλεπίδρασης δημοσίου και ιδιωτικού τομέα. Αυτή η συνεργασία μπορεί να πάρει διάφορες μορφές. Έχει ιδιαίτερο ενδιαφέρον η ενεργοποίηση του ιδιωτικού τομέα για την ευαισθητοποίηση και την εκπαίδευση τόσο των πολιτών, όσο και των διαφόρων επαγγελματιών στις νέες τεχνολογίες και στην ορθή αξιοποίηση των δυνατοτήτων τους.

Η χρήση νέων τεχνολογιών, τόσο από τις κρατικές υπηρεσίες όσο και από τον ιδιωτικό τομέα, πρέπει να γίνεται κατόπιν μίας διαδικασίας ορθής αξιοποίησης, που θα προστατεύει τα ανθρώπινα δικαιώματα και τις ελευθερίες. Αυτός είναι και ο λόγος που η ΕΕ δίνει ιδιαίτερη έμφαση στο ζήτημα της προστασίας της ιδιωτικότητας και έχει θεσπίσει ένα αρκετά αυστηρό πλαίσιο προστασίας των προσωπικών δεδομένων, το οποίο αποτελεί και τη βάση για τις πολιτικές προστασίας δεδομένων τόσων των δημοσίων φορέων, όσων και των ιδιωτικών εταιρειών.

Σε αυτό το πλαίσιο κινείται και η συγκεκριμένη μελέτη, αποτέλεσμα της συνεργασίας του Κέντρου για την Κυβερνο-Ανθεκτικότητα του Οικονομικού Φόρουμ των Δελφών με τη Vodafone, το ΕΛΙΑΜΕΠ και τη Metron Analysis, για μια πρώτη, αλλά συστηματική αποτύπωση της κατάστασης, των τάσεων, αλλά και της οπτικής των πολιτών για την κυβερνοασφάλεια στην Ελλάδα. Η μελέτη έχει τέσσερις βασικούς άξονες: α) τις νέες τάσεις για τις νέες τεχνολογίες και την κυβερνοασφάλεια, β) το πλαίσιο και τις πολιτικές της ΕΕ, γ) την αρχιτεκτονική και το πλαίσιο της κυβερνοασφάλειας στην Ελλάδα και δ) την οπτική των πολιτών και των επιχειρήσεων. Η τελευταία ενότητα περιλαμβάνει τα συμπεράσματα και μια σειρά προτάσεων πολιτικής για τον δημόσιο και τον ιδιωτικό τομέα.

Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΟΝ 21ο ΑΙΩΝΑ: ΤΑΣΕΙΣ ΚΑΙ ΑΠΕΙΛΕΣ



Η ΨΗΦΙΑΚΗ ΕΠΑΝΑΣΤΑΣΗ ΣΤΙΣ ΑΡΧΕΣ ΤΟΥ 21ου ΑΙΩΝΑ προσέφερε αμέτρητες δυνατότητες για τη συλλογή, επεξεργασία, διάδοση και ανταλλαγή πληροφοριών, ξεπερνώντας σε σημαντικό βαθμό τους γεωγραφικούς και χρονικούς περιορισμούς. Κομμάτι της ραγδαίας τεχνολογικής ανάπτυξης αποτελούν οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) και ο κυβερνοχώρος. Ο κυβερνοχώρος είναι βασικό συστατικό της σύγχρονης κοινωνίας, της οποίας εντείνει την ψηφιοποίηση. Αποτελεί ένα δυναμικό φαινόμενο, με μεγάλο βαθμό πολυπλοκότητας και με ιδιαίτερα τεχνολογικά και κοινωνικοπολιτικά χαρακτηριστικά[1]. Το συγκεκριμένο πεδίο αποτελεί τον πέμπτο τομέα επιχειρησιακών δράσεων μαζί με την ξηρά, τη θάλασσα, τον εναέριο χώρο και το Διάστημα[2].

Οι χρήστες του κυβερνοχώρου υπολογίζεται ότι είναι πάνω από 5,18 δισ. ανά τον κόσμο, δηλαδή αποτελούν το 64,6% του παγκόσμιου πληθυσμού, με αποτέλεσμα να καθιστούν τη χρήση του τόσο σημαντική στην καθημερινότητά μας, όσο και απαραίτητη για την επίτευξη των συναλλαγών και των ανταλλαγών δεδομένων. Οι χρήστες του κυβερνοχώρου είναι «ενεργοί» για τουλάχιστον 6,5 ώρες σε καθημερινή βάση, και ο αριθμός αυτών που έχουν δημιουργήσει προσωπικό λογαριασμό στα μέσα κοινωνικής δικτύωσης ανέρχεται στα 4,8 δισ. (59% του παγκόσμιου πληθυσμού)[3].

Η δύναμη της κοινωνικής δικτύωσης μεγαλώνει μέρα με την ημέρα. Η αύξηση του αριθμού είναι τεράστια και μέσα σε λίγα χρόνια. Τα μέσα κοινωνικής δικτύωσης αποτελούν αναπόσπαστο μέρος της καθημερινής χρήσης του διαδικτύου. Κατά μέσο όρο, οι χρήστες του διαδικτύου ξοδεύουν 144 λεπτά την ημέρα σε ΜΚΔ και εφαρμογές ανταλλαγής μηνυμάτων. Το πιο διαδεδομένο μέσο κοινωνικής δικτύωσης είναι το Facebook, με 2,958 δισ. ενεργούς χρήστες μηνιαίως. Η εταιρεία κατέχει άλλες τέσσερις μεγάλες πλατφόρμες, όλες με πάνω από 1 δισ. ενεργούς χρήστες κάθε μήνα: WhatsApp (2 δισ.), Messenger (931 εκατ.) και Instagram (2 δισ.). Άλλες σημαντικές πλατφόρμες κοινωνικής δικτύωσης είναι το YouTube με 2,514 δισ. χρήστες, το Twitter με 556 εκατ. χρήστες, το TikTok με 1,05 δισ. χρήστες[4]. Η αναφορά στο μέγεθος και τη χρήση που γίνεται από τους πολίτες είναι πολύ σημαντική, γιατί αντιλαμβανόμαστε την έκταση και τον αντίκτυπο που έχουν.

Η μορφή και η τυπολογία των νέων απειλών στη σύγχρονη κοινωνία έχουν αναδείξει την κρισιμότητα των προκλήσεων από τις αναδυόμενες τεχνολογίες και τον τομέα του κυβερνοχώρου. Η αξιοποίηση του κυβερνοχώρου για την ανάπτυξη κακόβουλων δράσεων εντείνει την ανασφάλεια της κοινωνίας και των πολιτών. Η ανάδυση νέων ασύμμετρων απειλών αποκτά διεθνή χαρακτήρα, καθώς ο κυβερνοχώρος δεν γνωρίζει γεωγραφικά όρια. Τις τελευταίες δύο δεκαετίες ο κυβερνοχώρος και ο τρόπος χρήσης του έχουν αναδειχθεί σε ζητήματα μείζονος πολιτικής, αφού οι δυνατότητες και οι χρήσεις του αποτελούν και πηγή ευπάθειας, ανάδυσης απειλών ασφάλειας και διαταραχής της κοινωνίας[5]. Οι πληροφοριακές και κρίσιμες υποδομές έχουν γίνει όλο και περισσότερο ευάλωτες στις επιθέσεις στον κυβερνοχώρο, λόγω της ραγδαίας ψηφιοποίησης και του κοινωνικού μετασχηματισμού[6].

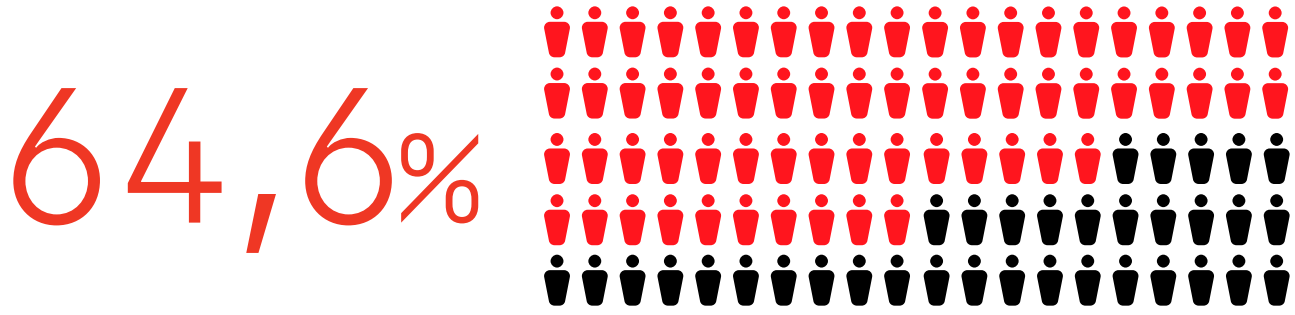
Η ψηφιακή επανάσταση και η ψηφιοποίηση της κοινωνίας προκαλούν τη δημιουργία ενός μεταβαλλόμενου πεδίου ασφάλειας, το οποίο έχει επηρεάσει σχεδόν κάθε κοινωνική, οικονομική και πολιτική πτυχή, καθώς εγείρει σημαντικές προκλήσεις. Το διαρκώς μεταβαλλόμενο πεδίο ασφάλειας καλείται να αντιμετωπίσει άμεσα πέρα από τις παραδοσιακές απειλές και νέες. Οι νέες προκλήσεις που αναδύονται από τον κυβερνοχώρο αφορούν την ανάπτυξη κακόβουλων δραστηριοτήτων. Όροι όπως κυβερνοασφάλεια (cybersecurity), κυβερνοάμυνα (cyberdefence), κυβερνοεπίθεση (cyberattack), κυβερνοτρομοκρατία (cyberterrorism), κυβερνοπόλεμος (cyberwar), κυβερνοκατασκοπεία (cyberespionage), παραπληροφόρηση (disinformation) και κυβερνοέγκλημα (cybercrime) αναλύονται όλο και περισσότερο από τις επιστήμες που ασχολούνται άμεσα με αυτές.

Οι απειλές στον κυβερνοχώρο χαρακτηρίζονται από τη μέθοδο και τα μέσα που χρησιμοποιούν οι δρώντες. Οι κακόβουλες δραστηριότητες διεξάγονται στον κυβερνοχώρο από κρατικούς και μη κρατικούς δρώντες, και χαρακτηρίζονται ανάλογα με τα κίνητρά τους. Οι πιο κοινές κακόβουλες τακτικές που χρησιμοποιούν μέσω του κυβερνοχώρου είναι: η χρήση κακόβουλου λογισμικού (malware), ο βανδαλισμός

ιστοσελίδων (web defacement), η παραβίαση πληροφοριακών συστημάτων με πολιτικούς σκοπούς (hacktivism), η διασπορά ψευδών ειδήσεων (fake news), ο ιός (virus), τα σκουλήκια (worms), οι Δούρειοι Ίπποι (Trojan Horses), η επίθεση άρνησης παροχής υπηρεσιών (Denial of Service Attack – DoS) ή οι κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών (Distributed Denial of Service Attacks – DDoS), η λογική βόμβα (logic bomb), το δίκτυο από bots (botnet), το ηλεκτρονικό ψάρεμα (phishing), η επίθεση man-in-the-middle, και το λυτρισμικό (ransomware). Οι επιτιθέμενοι είναι ικανοί με τις κακόβουλες ενέργειές τους να επηρεάσουν τρία βασικά συστατικά της ασφάλειας: την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των δεδομένων. Πλέον, όποιος επιθυμεί να βλάψει ή να υποσκάψει ένα σύστημα πληροφοριών ή τις υποδομές ενός ολόκληρου κράτους αρκεί να έχει τις απαραίτητες γνώσεις και δεξιότητες και ένα πληκτρολόγιο, μέσω του οποίου θα εξαπολύσει εικονικές επιθέσεις σε οποιαδήποτε γεωγραφική κατεύθυνση και από οποιονδήποτε προορισμό.

Υπάρχουν δύο χαρακτηριστικά παραδείγματα που αναδεικνύουν με τον πλέον χαρακτηριστικό τρόπο τον καταλυτικό ρόλο του διαδικτύου σε ζητήματα ασφάλειας: α) ο ρόλος του δικτύου Telegram στην επικοινωνιακή διαχείριση και την κινητοποίηση του δικτύου υποστήριξης της Ουκρανίας από τον πρόεδρο Ζελένσκι, ένα πραγματικό παράδειγμα αλλαγής στην επικοινωνιακή διαχείριση μιας πολεμικής αντιπαράθεσης, με αντίπαλο μια επικοινωνιακή υπερδύναμη όπως η Ρωσία και β) η απόφαση, μετά την τρομοκρατική επίθεση στο Μάντσεστερ, τον Μάιο του 2017, της τότε πρωθυπουργού της Βρετανίας Τερέζα Μέι, να ζητήσει από τη Facebook να συνεργαστεί στενότερα με τις αρχές, με στόχο την καταπολέμηση της τρομοκρατίας και την πρόληψη της ριζοσπαστικοποίησης. Ειδική αναφορά πρέπει να γίνει στο πώς λειτουργούν τα ΜΚΔ. Η στροφή από τα παραδοσιακά κανάλια επικοινωνίας προς τα μέσα κοινωνικής δικτύωσης δεν βελτίωσε απαραίτητα την ποιότητα του πολιτικού λόγου. Αντίθετα, τα μέσα κοινωνικής δικτύωσης είναι γνωστό ότι λειτουργούν ως echo chamber της πόλωσης και προωθούν τη ρητορική «εμείς εναντίον των άλλων»[7]. Αυτοί οι παράγοντες συσχετίζονται με τον διαδικτυακό εκφοβισμό, την παρενόχληση και, ειδικότερα, τη ρητορική μίσους. Σε ένα ευρύ πλαίσιο, ως ρητορική μίσους χαρακτηρίζεται η υβριστική ή απειλητική ομιλία (ή γραφή) που εκφράζει προκατάληψη εναντίον μιας συγκεκριμένης ομάδας, συχνά στη βάση της εθνότητας ή του σεξουαλικού προσανατολισμού.

Η ρητορική μίσους στα μέσα κοινωνικής δικτύωσης συχνά προέρχεται από μερικώς ή πλήρως ανώνυμα τρολ, και είναι ιδιαίτερα έντονη σε συζητήσεις που προκαλούν μεγάλη συναισθηματική ανταπόκριση, όπως οι πολιτικές αντιπαραθέσεις. Σε ατομικό επίπεδο, η ρητορική μίσους μπορεί να οδηγήσει στη στοχοποίηση ανθρώπων, με τραγική μάλιστα κατάληξη ορισμένες φορές, όπως είδαμε στην περίπτωση του καθηγητή Πατί στη Γαλλία. Σε κοινωνικό επίπεδο, ενθαρρύνει την πολιτική πόλωση, που μπορεί να έχει σοβαρές συνέπειες για την κοινωνική συνοχή και την εμπιστοσύνη στους θεσμούς[8] – χαρακτηριστικά παραδείγματα αποτελούν η αύξηση



Οι χρήστες του κυβερνοχώρου υπολογίζεται ότι είναι πάνω από 5,18 δισ. ανά τον κόσμο, δηλαδή αποτελούν το 64,6% του παγκόσμιου πληθυσμού, με αποτέλεσμα να καθιστούν τη χρήση του τόσο σημαντική στην καθημερινότητά μας, όσο και απαραίτητη για την επίτευξη των συναλλαγών και των ανταλλαγών δεδομένων.

της ριζοσπαστικοποίησης που οδηγεί στον εξτρεμισμό και στην πολιτική βία, και η διάδοση παραπληροφόρησης και θεωριών συνωμοσίας[9].

Ας δούμε όμως δύο παραδείγματα των κινδύνων και των απειλών στα μέσα κοινωνικής δικτύωσης.

Η πανδημία, ιδιαίτερα στο πρώτο της κύμα, προκάλεσε μια πρωτόγνωρη κατάσταση για πολλούς ανθρώπους. Μέσα σε ένα καθεστώς άγχους και πίεσης, αρκετοί άνθρωποι αναζήτησαν εξηγήσεις για την προέλευση, αλλά και την έκταση της κρίσης. Το lockdown, εκ των πραγμάτων, συνέβαλε στην αύξηση της περιήγησης στο διαδίκτυο, κάτι που ενίσχυσε την έκθεση και την ευαλωτότητα στην παραπληροφόρηση και στην εξτρεμιστική προπαγάνδα. Άνθρωποι που ένιωθαν απομονωμένοι, αλλά ακόμα και έφηβοι, που δραστηριοποιούνταν έντονα στο διαδίκτυο και στα μέσα κοινωνικής δικτύωσης, ήταν εκτεθειμένοι στην παραπληροφόρηση και σε διάφορα εξτρεμιστικά αφηγήματα.

Οι εξτρεμιστικές και ακραίες ομάδες εργαλειοποίησαν την πανδημία, για να ενισχύσουν τη δικτύωση, την παρουσία τους, αλλά και τη στρατολόγηση νέων μελών. Επίσης, το ζήτημα της πανδημίας λειτούργησε και ως συνδετικός κρίκος σε παγκόσμιο, αλλά και περιφερειακό επίπεδο γι' αυτές τις ομάδες. Η εξτρεμιστική ρητορική στο διαδίκτυο σχετικά με την κρίση της πανδημίας γνώρισε μεγάλη έξαρση. Τα ακροδεξιά αφηγήματα, που στοχοποιούν και κατηγορούν για τις κρίσεις διάφορες εθνικές, φυλετικές ή θρησκευτικές ομάδες (π.χ. Ασιάτες, εβραίους, μετανάστες, μουσουλμάνους, Δυτικούς, «άπιστους», κ.ά.) έτυχαν μεγαλύτερης απήχησης, μιας και η πανδημία ενίσχυσε τα αισθήματα του φόβου, της απελπισίας και της ανασφάλειας[10].

Οι ακροδεξιές εξτρεμιστικές ομάδες αξιοποίησαν την ευκαιρία για να προσαρμόσουν την προπαγάνδα τους (τον ιό τον έφτιαξαν οι Κινέζοι, οι Ισραηλινοί, οι καπιταλιστικές ελίτ κ.ο.κ.), να κινητοποιήσουν ριζοσπαστικοποιημένους ανθρώπους στην ακροδεξιά σκηνή και να προσεγγίσουν νέες ομάδες αντίδρασης. Η τελευταία διάσταση είναι ιδιαιτέρως σημαντική, καθώς είδαμε πώς η Ακροδεξιά προσέγγισε με ιδιαιτέρως αποτελεσματικό τρόπο συγκεκριμένες κατηγορίες αντιδραστικής ριζοσπαστικοποίησης, όπως οι αντιεμβολιαστές ή οι τεχνοφοβικοί, ομάδες που σε χώρες της ΕΕ ήταν και ιδιαιτέρως βίαιες, προκαλώντας επεισόδια και πραγματοποιώντας επιθέσεις. Επίσης, ακροδεξιές οργανώσεις, σε αρκετές περιπτώσεις, πραγματοποίησαν κυβερνοεπιθέσεις και κυρίως κακόβουλες ενέργειες hacking[11].

6,5
ΩΡΕΣ

Οι χρήστες του κυβερνοχώρου είναι «ενεργοί» για τουλάχιστον 6,5 ώρες σε καθημερινή βάση.

Όπως έχει πολλές φορές αναλυθεί, η Daesh είναι η τρομοκρατική οργάνωση που αναβάθμισε εντυπωσιακά τη χρήση του διαδικτύου και των μέσων κοινωνικής δικτύωσης σε σχέση με αντίστοιχες οργανώσεις, συμβάλλοντας, επί της ουσίας, στη δημιουργία μιας ηλεκτρονικής jihadi σφαίρας[12].Ειδικότερα:

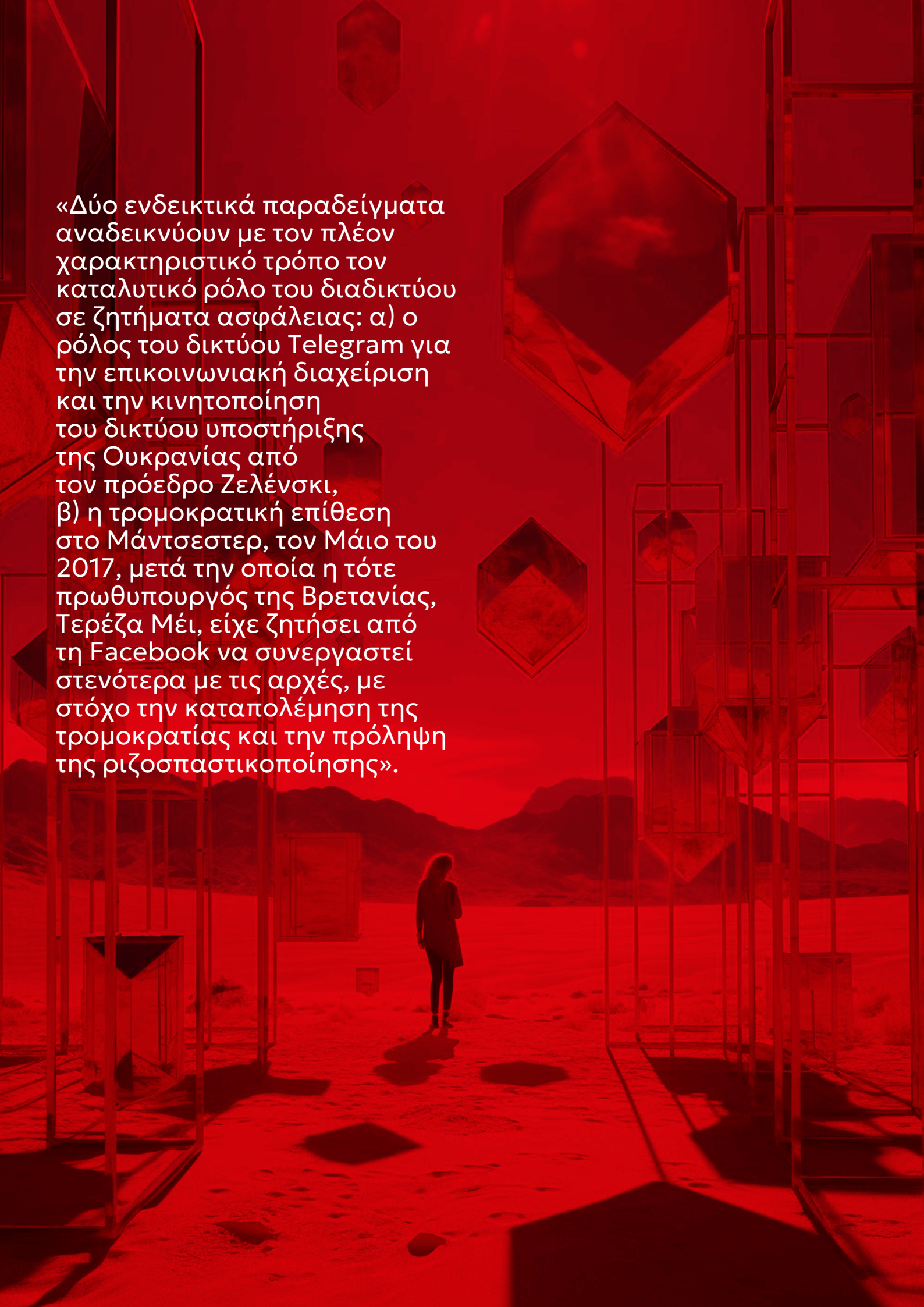
- **Τελειοποίησε την προπαγάνδα, επενδύοντας στο τετράπτυχο: εδαφική υπόσταση, εσχατολογική ρητορική, στοχοποίηση της Ummah (παγκόσμια κοινότητα των πιστών) και δυνατότητα άμεσης δράσης κατά των απίστων.**
- **Αξιοποίησε τα πλέον σύγχρονα μέσα επικοινωνίας για τη ριζοσπαστικοποίηση, τη στρατολόγηση, την υποστήριξη και τη διοργάνωση επιθέσεων.**
- **Οπτικοποίησε με σύγχρονο τρόπο το μήνυμά της, κάνοντάς το εύληπτο και θελκτικό για τους νέους ανθρώπους.**
- **Περιόρισε σημαντικά τον χρόνο ριζοσπαστικοποίησης ενός ανθρώπου, κυρίως λόγω της ευρείας χρήσης του διαδικτύου[13].**

Δημοφιλείς πλατφόρμες μέσων κοινωνικής δικτύωσης, και ειδικότερα το Twitter, αποτέλεσαν τον πυρήνα αυτής της επικοινωνιακής στρατηγικής της Daesh, με στόχο τη διάδοση της προπαγάνδας και τις επιχειρήσεις παραπληροφόρησης. Η τρομοκρατική οργάνωση χρησιμοποίησε αυτά τα μέσα ως πυρήνα ενός ιστού περιεχομένου που διαδίδεται σε πολλά μέρη του ακυβέρνητου διαδικτύου. Αξιοποιεί επίσης με καινοτόμο τρόπο τα τρωτά σημεία των μέσων κοινωνικής δικτύωσης, τα οποία της επιτρέπουν να αποφεύγει τον εντοπισμό αλλά και την αναστολή και διαγραφή των λογαριασμών από κρατικούς και μη κρατικούς φορείς, τόσο από αυτοματοποιημένες όσο και από χειροκίνητες μεθόδους ανίχνευσης[14].

Παράλληλα, η οργάνωση είχε κινητοποιήσει έναν ισχυρό πυρήνα υποστηρικτών, οι οποίοι λειτουργούσαν ως μια αφοσιωμένη ανθρώπινη υποδομή, που της επέτρεψε να έχει ένα σημαντικό αντίκτυπο στο επικοινωνιακό περιβάλλον των μέσων κοινωνικής δικτύωσης. Μέσω της χρήσης μιας δομής δικτύου κέντρου–περιφέρειας και ενός μεγάλου αριθμού δρώντων, η Daesh δημιούργησε μια υποδομή που μπορεί να αντέξει στις προσπάθειες διακοπής της επικοινωνιακής-προπαγανδιστικής της αλυσίδας[15].

Για την Ελλάδα, με όρους εκτίμησης επικινδυνότητας, οι σημαντικότερες απειλές αφορούν τις οικονομικές απάτες, τη σεξουαλική εκμετάλλευση ανηλίκων, τα εξαρτώμενα από το διαδίκτυο εγκλήματα, τη διακίνηση ψευδών ειδήσεων και τις «κυβερνοεπιθέσεις» με τη χρήση κακόβουλου λογισμικού κατά κρίσιμων υποδομών, στρατηγικών δικτύων και κυβερνητικών υπηρεσιών. Πρέπει, επίσης, να επισημανθεί και ο κίνδυνος συνδυαστικής-υβριδικής επίθεσης, που θα εμπεριέχει και τη διάσταση του διαδικτύου. Σημαντικός είναι ακόμα ο κίνδυνος από δραστηριότητες των δικτύων του οργανωμένου εγκλήματος και της τρομοκρατίας στο «σκοτεινό διαδίκτυο» (dark web), όπως το εμπόριο όπλων και ναρκωτικών, η προπαγάνδα, η ριζοσπαστικοποίηση, η στρατολόγηση μαχητών, η χρηματοδότηση τρομοκρατικών επιθέσεων κ.ά. Εξίσου βαρύνουσα είναι η απειλή από κυβερνοεπιθέσεις, όπως αυτή κατά των ΕΛΤΑ, τον Δεκέμβριο του 2022, που είχε κυρίως τη μορφή Ransomware, δηλαδή επίθεσης με κακόβουλο λογισμικό με σκοπό τα λύτρα από τον κάτοχο της συσκευής/του δικτύου/ή της υπηρεσίας[16].

Η μεγαλύτερη ωστόσο συζήτηση στην Ελλάδα για την κυβερνοασφάλεια έγινε με αφορμή τη διήμερη κυβερνοεπίθεση, τύπου κατανεμημένης επίθεσης άρνησης υπηρεσίας (DDoS–Distributed Denial of Service), που δέχτηκε η υποδομή της Τράπεζας Θεμάτων του Ινστιτούτου Εκπαιδευτικής Πολιτικής τον Ιούνιο του 2023. Επί της ουσίας, ο συγκεκριμένος τύπος επίθεσης έχει στόχο την πρόκληση τεχνητής υπερβολικής ζήτησης πρόσβασης σε ένα δίκτυο, με αποτέλεσμα αυτό να καθυστερήσει ή να διακόψει τη λειτουργία του – μοιάζει κάπως σαν εκατοντάδες άνθρωποι να εισβάλουν την ίδια στιγμή σε ένα πολυκατάστημα και να ζητούν να εξυπηρετηθούν, μπλοκάροντας στην πράξη τη διαδικασία εξυπηρέτησης πελατών[17].



«Δύο ενδεικτικά παραδείγματα αναδεικνύουν με τον πλέον χαρακτηριστικό τρόπο τον καταλυτικό ρόλο του διαδικτύου σε ζητήματα ασφάλειας: α) ο ρόλος του δικτύου Telegram για την επικοινωνιακή διαχείριση και την κινητοποίηση του δικτύου υποστήριξης της Ουκρανίας από τον πρόεδρο Ζελένσκι, β) η τρομοκρατική επίθεση στο Μάντσεστερ, τον Μάιο του 2017, μετά την οποία η τότε πρωθυπουργός της Βρετανίας, Τερέζα Μέι, είχε ζητήσει από τη Facebook να συνεργαστεί στενότερα με τις αρχές, με στόχο την καταπολέμηση της τρομοκρατίας και την πρόληψη της ριζοσπαστικοποίησης».

Αυτό κάνει και η επίθεση DDoS σε ψηφιακό δίκτυο που παρέχει υπηρεσία και οι «πελάτες» είναι τα περίφημα bot (ή το δίκτυο botnet), μια σύντμηση από τη λέξη robot, δηλαδή ένα αυτοματοποιημένο πρόγραμμα που πραγματοποιεί προκαθορισμένες ενέργειες και προσποιείται τον χρήστη. Αυτός είναι και ο λόγος που πολύ συχνά συναντάμε καρτέλες που προσπαθούν να διασφαλίσουν πως ο χρήστης δεν είναι robot-bot.

Τόσο η Ελλάδα όσο και όλες οι χώρες παγκοσμίως δέχονται καθημερινά μεγάλο όγκο κυβερνοεπιθέσεων, κυρίως DDoS και Ransomware, που είναι και οι πλέον διαδεδομένες, τη συντριπτική πλειονότητα των οποίων αντιμετωπίζουν, γι' αυτό και δεν αποκτούν δημοσιότητα. Αν δούμε τις εκθέσεις ευρωπαϊκών υπηρεσιών και διεθνών οργανισμών, θα διαπιστώσουμε πως οι κυβερνοεπιθέσεις είναι μια καθημερινή μάχη για όλες τις χώρες.

Οι συγκεκριμένες επιθέσεις δεν πραγματοποιούνται ωστόσο μόνο εναντίον δημοσίων υπηρεσιών, αλλά και κατά εταιρειών, ακόμα και ιδιωτών. Μια επίθεση DDoS μπορεί να στοχεύσει από το online τραπεζικό σύστημα μέχρι μια ηλεκτρονική πλατφόρμα παραγγελίας φαγητού, αλλά και ένα μέσο κοινωνικής δικτύωσης. Ενώ η πιο απλή μορφή επίθεσης Ransomware γίνεται κατά ιδιώτη, όπου με κλείδωμα του υπολογιστή τού ζητούν ένα συγκεκριμένο χρηματικό ποσό ως αντάλλαγμα.

Τα πράγματα γίνονται δυσκολότερα όταν συζητάμε για το ποιος μπορεί να πραγματοποιεί τέτοιες επιθέσεις και γιατί. Πρόκειται για μια πραγματική Λερναία Ύδρα: μεμονωμένοι χάκερ, ομάδες κυβερνοακτιβιστών, κυβερνοεγκληματίες που μισθώνουν τις υπηρεσίες τους, αλλά και παρακρατικές και κρατικές υπηρεσίες συγκεκριμένων κρατών. Ως παράδειγμα, πίσω από μια τέτοια επίθεση μπορούμε να βρούμε από τους Anonymous μέχρι τη Mustang Panda, κινεζική κυβερνοομάδα, ή τους KillNet, που είναι οι πλέον ειδικοί σε επιθέσεις DDoS και λειτουργούν υποστηρικτικά προς τα συμφέροντα της Ρωσίας. Οι κυβερνοεπιθέσεις είναι άλλωστε συστατικό στοιχείο του δόγματος υβριδικού πολέμου και επιχειρήσεων, που αποτελεί τη βασική στρατηγική της Ρωσίας τα τελευταία χρόνια.

Ο ανθρώπινος παράγοντας παραμένει μια κρίσιμη τρωτότητα τόσο για τις επιχειρήσεις όσο και για τα άτομα. Το 82% των παραβιάσεων κατά των επιχειρήσεων αφορούσε τον ανθρώπινο παράγοντα, μέσω ζητημάτων όπως το σφάλμα και η κοινωνική μηχανική (social engineering). Οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) είναι η πιο κοινή μορφή απειλής στον κυβερνοχώρο και οι πιο επιβλαβείς επιθέσεις συχνά εξαρτώνται από την επιτυχία ενός αρχικού κακόβουλου μηνύματος ηλεκτρονικού ταχυδρομείου. Ενθαρρύνοντας τους ανθρώπους να ακολουθήσουν έναν σύνδεσμο προς έναν πλαστό ιστότοπο και να εισαγάγουν διαπιστευτήρια ή να κατεβάσουν κακόβουλο λογισμικό, οι χάκερ εξασφαλίζουν τα απαραίτητα εργαλεία για την κλιμάκωση των επιθέσεων. Ο ανθρώπινος παράγοντας αντιπροσωπεύει σχεδόν το 80% των συνολικών τρωτών σημείων που εκμεταλλεύονται οι επιτιθέμενοι κατά τη χρήση του κυβερνοχώρου.

4,8

δισ.

Υπολογίζεται ότι 4,8 δισ. άνθρωποι (δηλαδή το 59% του παγκόσμιου πληθυσμού) έχουν δημιουργήσει λογαριασμό κοινωνικής δικτύωσης.

Στην εποχή του κυβερνοχώρου, η ανωνυμία ξεθωριάζει, τα προσωπικά δεδομένα είναι ευάλωτα, και η ασφάλεια της ιδιωτικότητάς τους παραμένει αβέβαιη. Οι σύγχρονες δημοκρατίες, στην προσπάθειά τους να ισορροπήσουν μεταξύ της προστασίας των προσωπικών δεδομένων και των ανθρωπίνων δικαιωμάτων, της ιδιωτικότητας και της εθνικής ασφάλειας, αντιμετωπίζουν σειρά προκλήσεων, μεταξύ των οποίων η κακόβουλη χρήση, ειδικά σε περιπτώσεις αυταρχικών καθεστώτων, από τα οποία απουσιάζουν οι ελεγκτικοί μηχανισμοί και οι ανεξάρτητοι θεσμοί και οι σχετικές αρχές. Το έργο της εθνικής ασφάλειας και των υπηρεσιών πληροφοριών εξαρτάται σε μεγάλο βαθμό από την παρακολούθηση των ψηφιακών αποτυπωμάτων της δραστηριότητας των πολιτών στον κυβερνοχώρο. Η πανδημία COVID-19 ήταν μια «ώθηση» για την παγκόσμια ψηφιοποίηση και διασυνδεσιμότητα. Οι εταιρείες και οι δημόσιες αρχές αποτελούν σχεδόν το 95% των χρηστών που εξαρτώνται απόλυτα από τις τεχνολογίες πληροφοριών και επικοινωνιών, και υπολογίζεται ότι κάθε 40 δευτερόλεπτα μια εταιρεία ή ένας δημόσιος φορέας πέφτει θύμα κυβερνοεπίθεσης.

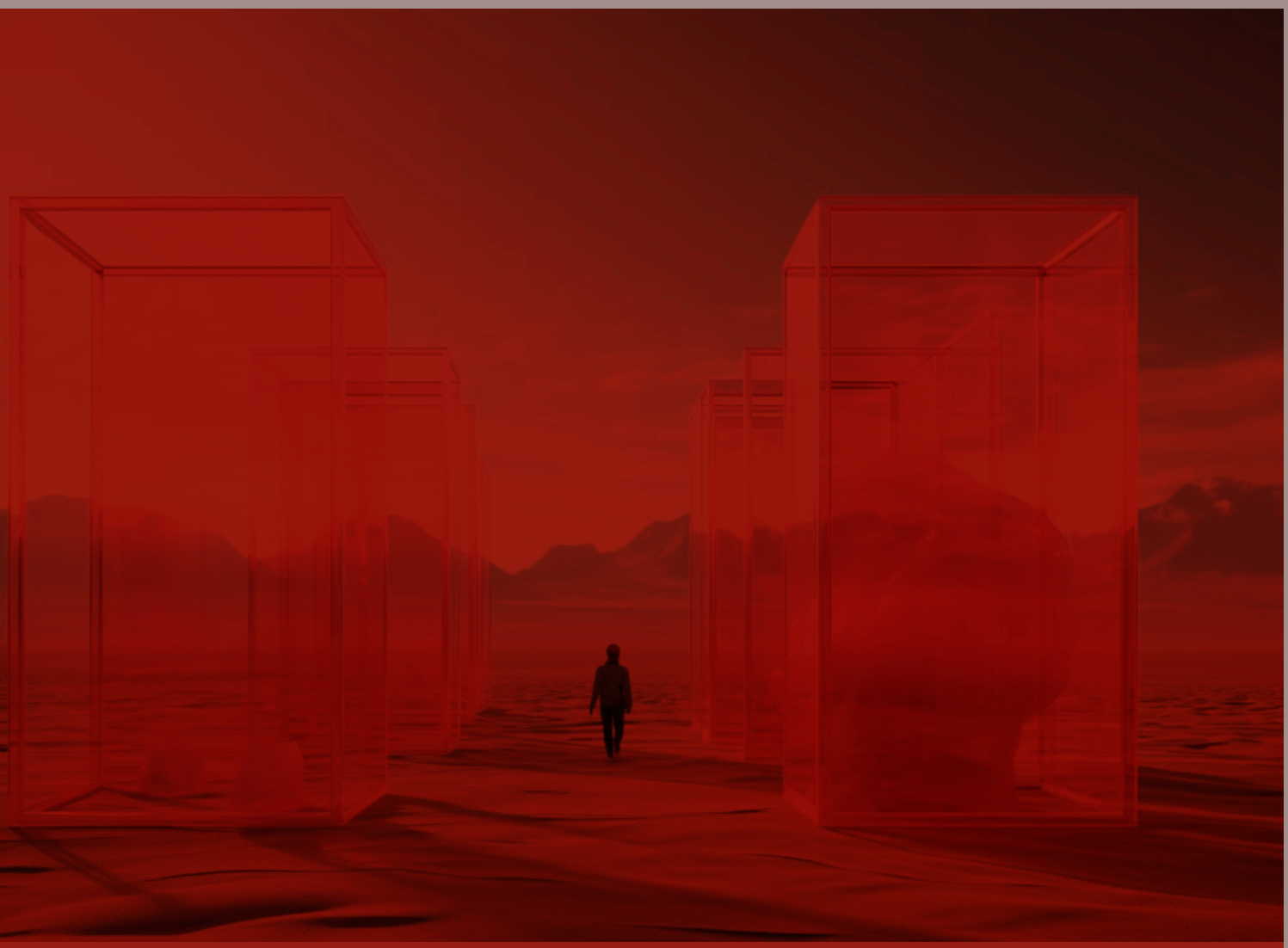
Όπως αναδεικνύεται λοιπόν, η κυβερνοασφάλεια είναι μια ολοένα και πιο ζωτικής σημασίας έννοια στον σημερινό κόσμο, καθώς οι απειλές στον κυβερνοχώρο συνεχίζουν να εξελίσσονται. Η κυβερνοασφάλεια είναι η πρακτική προστασίας των συστημάτων υπολογιστών, των δικτύων και των ευαίσθητων πληροφοριών από κλοπή, ζημιά ή μη εξουσιοδοτημένη πρόσβαση. Περιλαμβάνει έναν συνδυασμό τεχνολογιών, διαδικασιών και βέλτιστων πρακτικών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ψηφιακών στοιχείων.

1. Craigen, D., Diakun-Thibault, N., και Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review: 1*.
2. Το NATO έχει ως επιχειρησιακούς τομείς δράσεις το Διάστημα, την ξηρά, τη θάλασσα, τον εναέριο χώρο και τον κυβερνοχώρο. Αυτό σημαίνει ότι οποιαδήποτε επίθεση σε μέλη του NATO σε έναν από τους πέντε επιχειρησιακούς τομείς θα μπορεί να ενεργοποιήσει το Άρθρο 5 της συλλογικής άμυνας του NATO.
3. Statista Research Department. (22 Μαΐου 2023). *Αριθμός χρηστών διαδικτύου και μέσων κοινωνικής δικτύωσης έως τον Απρίλιο 2023*. https://www.statista.com/statistics/617136/digital-population-worldwide/
4. Statista Research Department. (14 Φεβρουαρίου 2023). *Παγκόσμια κοινωνικά δίκτυα, ταξινομημένα σύμφωνα με τον αριθμό χρηστών το 2023*. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
5. Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press: 3.
6. Libicki, M. (2007). *Conquest in Cyberspace. National Security and Information Warfare*. RAND: 40-41.
7. Chan, M. (2016), «Social network sites and political engagement: Exploring the impact of Facebook connections and uses on political protest and participation», *Mass Communication and Society*, 19(4), σ. 430-451.
8. Applebaum, A. (2019), «Regulate Social Media now. The future of Democracy is at stake», *The Washington Post*, 1 Φεβρουαρίου.
9. Siripurapu, A., Merrow, W. (2021), «Social Media and Online Speech: How should countries regulate tech giants?», Council on Foreign Relations.
10. EU Counter-Terrorism Coordinator, (2020), «Terrorism in times of Corona: The development of the terrorist threat as a result of the Covid-19 crisis», 7838/20, Βρυξέλλες.
11. Bliuc, A. M., Betts, J., Vergani, M., Iqbal, M. & Dunn, K. (2020), «The growing power of online communities of the extreme-right: deriving strength, meaning, and direction from significant sociopolitical events "in real life"», ICCT Policy Brief, Χάγη.
12. Zekulin, M. (2021), «From Inspire to Rumiyah: does instructional content in online jihadist magazines lead to attacks?», *Behavioral Sciences of Terrorism and Political Aggression* 13:2, σ. 115-141.
13. Shaheen, J. (2016), «Network of Terror: How DAESH uses adaptive social networks to spread its message», NATO StratCom.
14. Lakomy, M. (2021), «Mapping the online presence and activities of the Islamic State's unofficial propaganda cell: Ahlut-Tawhid Publications», *Security Journal 34:2*, σ. 358-384.
15. Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A.& Weir, D. (2019), «Disrupting Daesh: Measuring takedown of online terrorist material and its impacts», *Studies in Conflict & Terrorism*, 42:1-2, σ. 141-160.
16. Kara, I., Aydos, M. (2022), «The rise of ransomware: forensic analysis for windows-based ransomware attacks», *Expert Systems with Applications, τόμ. 190,* τχ. C. Ibrar, Y., Ejaz, A., Rehman, H., Abdelmuttlib, A., et al. (2017), «The rise of ransomware and emerging security challenges in the Internet of Things», *Computer Networks*, τόμ. 129, Μέρος 2, σ. 444-458.
17. Singh, R., Ram, M. (2021), *Distributed Denial of Service Attacks: Concepts, Mathematical and Cryptographic Solutions*. Βερολίνο, Βοστόνη: De Gruyter.

ΠΟΛΙΤΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ -ΤΗΣ ΕΕ

Η ΕΕ ξεκίνησε τις δράσεις της στον τομέα της κυβερνοασφάλειας από το 2004, με τη δημιουργία του ENISA, και του πρωταρχικού σχεδίου ευρωπαϊκής οδηγίας για την ασφάλεια των υποδομών που χρονολογείται από το 2008. Ο ENISA, ως οργανισμός της ΕΕ για την κυβερνοασφάλεια, αναφέρεται στην κρισιμότητα που έχει η υιοθέτηση μιας εθνικής στρατηγικής για την κυβερνοασφάλεια, που θα στοχεύει σε μια σειρά από εθνικούς στόχους οι οποίοι πρέπει να επιτευχθούν σε συγκεκριμένο χρονικό πλαίσιο.

Κάθε κράτος-μέλος της ΕΕ ευθύνεται για τη χάραξη μιας εθνικής στρατηγικής για την ασφάλεια των συστημάτων δικτύων και πληροφοριών, ενώ οφείλει να είναι αποτελεσματικό στην προστασία βασικών υπηρεσιών (ζωτικής ή κρίσιμης σημασίας υποδομές, όπως ενέργεια, μεταφορές, τραπεζική/χρηματοπιστωτική αγορά, υγεία, παροχή/διανομή νερού, ψηφιακή υποδομή), αλλά και υπηρεσιών που σχετίζονται με την ηλεκτρονική αγορά, τη μηχανή αναζήτησης και τη νεφοϋπολογιστική (Cloud computing).



ΟΙ ΧΡΟΝΟΛΟΓΙΕΣ-ΟΡΟΣΗΜΑ ΤΩΝ ΕΥΡΩΠΑΪΚΩ

2011

Δημιουργείται η μόνιμη CERT-EU (Computer Emergency Response Team – CERT) και φιλοξενείται διοικητικά από τη Γενική Διεύθυνση Πληροφορικής της Ευρωπαϊκής Επιτροπής.

2013

Υιοθετείται η «Στρατηγική κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης για έναν ανοιχτό, ασφαλή και προστατευμένο κυβερνοχώρο», το πρώτο συνεκτικό κείμενο στρατηγικής της ΕΕ για θέματα ασφάλειας στον κυβερνοχώρο.

Ιδρύεται το Ευρωπαϊκό Κέντρο για Εγκλήματα στον Κυβερνοχώρο (European Cybercrime Centre – EC3) και υπάγεται στην Europol.

2014

Εγκρίνεται από την ΕΥΕΔ (Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης – European External Action Service) το «Πλαίσιο πολιτικής για την κυβερνοάμυνα», στο οποίο αναφέρονται οι βασικοί πυλώνες αντιμετώπισης των κυβερνο-απειλών.

2016

Ψηφίζεται ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulatory – GDPR), που ορίζει τις υποχρεώσεις στις οποίες οφείλουν να προσαρμόζονται οι οργανισμοί και οι εταιρείες κατά την επεξεργασία των προσωπικών δεδομένων των χρηστών σε ευρωπαϊκό, και μη, περιβάλλον.

Εγκρίνεται από το Ευρωπαϊκό Κοινοβούλιο η «Οδηγία για την ασφάλεια των δικτύων και πληροφοριών» (NIS – Directive on Security of Network and Information Systems), ο πρώτος ευρωπαϊκός νόμος για την ασφάλεια στον κυβερνοχώρο. Αποτελεί τον ακρογωνιαίο λίθο για την ενίσχυση και βελτίωση των εθνικών δυνατοτήτων ασφάλειας των κρατών-μελών.

Η ΠΟΛΙΤΙΚΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

2017

Η ΕΕ προχωρά στην αναθεώρηση της στρατηγικής της κυβερνοασφάλειας. Η στρατηγική ονομάστηκε «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής κυβερνοασφάλειας για την ΕΕ» (Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU) και αναφέρεται σε απειλές στον οικονομικό, πολιτικό και στρατιωτικό τομέα.

Η Ευρωπαϊκή Επιτροπή παρουσιάζει το «Blueprint for a Coordinated Response to Large Scale Cybersecurity Incidents and Crises» (Πρόγραμμα δράσης για μια συντονισμένη απόκριση σε μεγάλης κλίμακας περιστατικά και κρίσεις κυβερνοασφάλειας).

2019

Υιοθετείται το European Cybersecurity Act [Regulation (EU) 2019/881], που αφορά την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών. Ο ENISA εξελίσσεται σε κεντρικό, καθοριστικό παράγοντα στο (ψηφιακό) «οικοσύστημα της ασφάλειας».

2022

Τίθεται σε ισχύ η Πράξη για τις Ψηφιακές Υπηρεσίες (Digital Services Act– DSA), που αφορά τις μεγαλύτερες εταιρείες ψηφιακής τεχνολογίας και όλους τους διαδικτυακούς μεσάζοντες που προσφέρουν τις υπηρεσίες τους στην ενιαία αγορά της ΕΕ, ανεξάρτητα από το αν είναι εγκατεστημένοι στην ΕΕ ή εκτός.

Η Ευρωπαϊκή Επιτροπή παρουσιάζει τον Νόμο για την Ανθεκτικότητα στον Κυβερνοχώρο (Cyber Resilience Act –CRA), που έρχεται να συμπληρώσει την Πράξη περί Τεχνητής Νοημοσύνης (AI Act), τον Νόμο της ΕΕ για την Κυβερνοασφάλεια (EU Cybersecurity Act) και την Οδηγία NIS 2.

Η Ευρωπαϊκή Επιτροπή ανακοινώνει το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (European Cyber-defence policy). Η νέα πολιτική απαιτεί επενδύσεις στην άμυνα στον κυβερνοχώρο, για να ενισχύσει τον συντονισμό και τη συνεργασία μεταξύ των στρατιωτικών και πολιτικών κοινοτήτων.

2023 Η Ευρωπαϊκή Ένωση θεωρεί τον κυβερνοχώρο ως πεδίο στρατηγικού ανταγωνισμού, από τον οποίο απορρέουν κίνδυνοι που αφορούν την ασφάλεια και την άμυνα της ΕΕ. Οι κίνδυνοι αυτοί έχουν μια αυξητική τάση, λόγω των διαρκών γεωπολιτικών εντάσεων και της αυξανόμενης εξάρτησης από τις ψηφιακές τεχνολογίες. Η αυξανόμενη τρωτότητα έναντι απειλών και συμβάντων στον κυβερνοχώρο απαιτεί αποτελεσματική ρύθμιση. Ωστόσο, το παρόν πλαίσιο έναντι τέτοιων απειλών μέχρι σήμερα έχει κριθεί ανεπαρκές. Σε απάντηση, στις 18 Απριλίου 2023, η Ευρωπαϊκή Επιτροπή κατέθεσε σχέδιο νόμου με κύριο στόχο την ενίσχυση της εναρμόνισης προκειμένου να μετριαστεί η αυξανόμενη ευπάθεια με τον εντοπισμό, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας εντός της ΕΕ. Ο Νόμος για την Αλληλεγγύη στον Κυβερνοχώρο (Cyber Solidarity Act) είναι μια πρόταση που επιδιώκει να εφαρμόσει μέτρα από τις υπάρχουσες στρατηγικές.

ΤΟ ΕΘΝΙΚΟ ΣΥΣΤΗΜΑ -ΚΥΒΕΡΝΟ ΑΣΦΑΛΕΙΑΣ

Η Ελλάδα λειτουργεί εντός του στρατηγικού και θεσμικού πλαισίου της ΕΕ, που παρουσιάστηκε αναλυτικά. Στο εθνικό σύστημα κυβερνοασφάλειας τον κύριο συντονιστικό ρόλο έχει το Υπουργείο Ψηφιακής Διακυβέρνησης. Στο πλαίσιο αυτό, το 2018, το τότε Υπουργείο Ψηφιακής Πολιτικής, δημοσίευσε την «Εθνική Στρατηγική Κυβερνοασφάλειας», η οποία καθόριζε τον κεντρικό σχεδιασμό του κράτους για την ασφάλεια στον κυβερνοχώρο. Επίσης, από το 2017, η Γενική Διεύθυνση Κυβερνοασφάλειας ορίστηκε ως Εθνική Αρχή Κυβερνοασφάλειας, με αρμοδιότητα την υλοποίηση και επικαιροποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Τον Δεκέμβριο του 2020, η Εθνική Αρχή Κυβερνοασφάλειας εξέδωσε τη νέα «Εθνική Στρατηγική Κυβερνοασφάλειας 2020–2025». Κεντρικός στόχος της εν λόγω στρατηγικής είναι «ένα σύγχρονο και ασφαλές ψηφιακό περιβάλλον πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών, προς όφελος της οικονομικής και κοινωνικής ευημερίας, με την εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων των πολιτών, την ανάπτυξη κουλτούρας ασφαλούς χρήσης των ψηφιακών υπηρεσιών και εφαρμογών, και την επαύξηση της εμπιστοσύνης των πολιτών και επιχειρήσεων στις ψηφιακές τεχνολογίες».

Το εθνικό σύστημα κυβερνοασφάλειας έχει τρεις βασικούς επιχειρησιακούς βραχίονες: α) την Εθνική Υπηρεσία Πληροφοριών– Εθνικό CERT, β) τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και γ) τη Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας – αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT).

Σημαντικές αλλαγές στον τομέα της κυβερνοασφάλειας προέκυψαν και από τον Νόμο 5002/2022 – Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών. Ειδικότερα, συστάθηκε η Επιτροπή Συντονισμού για Θέματα Κυβερνοασφάλειας[18], με αποστολή τον προγραμματισμό, την παρακολούθηση, τον συντονισμό ενεργειών, τις παρεμβάσεις σε ζητήματα που άπτονται της κυβερνοασφάλειας –από το αρχικό στάδιο της πρόληψης μέχρι το στάδιο της αποτελεσματικής αντιμετώπισης περιστατικών κυβερνοεπιθέσεων– και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο. Στις αρμοδιότητες της επιτροπής περιλαμβάνονται μεταξύ άλλων: α) η παροχή κατευθύνσεων σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο, β) ο συντονισμός, η παρακολούθηση και η αξιολόγηση της υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας, γ) η έγκριση του Εθνικού Σχεδίου Έκτακτης Ανάγκης, και δ) η εισήγηση προς το Κυβερνητικό Συμβούλιο Εθνικής Ασφάλειας οποιουδήποτε θέματος άπτεται της κυβερνοασφάλειας. Η δεύτερη σημαντική πρόβλεψη του νόμου είναι το Εθνικό Σχέδιο Αποτίμησης Επικινδυνότητας συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ).

Η πλέον πρόσφατη θεσμική εξέλιξη στον τομέα της κυβερνοασφάλειας είναι η σύσταση, με τον Νόμο 5086/2024, της Εθνικής Αρχής Κυβερνοασφάλειας. Σκοπός της Αρχής είναι η οργάνωση, ο συντονισμός, η εφαρμογή και ο έλεγχος ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, σε επίπεδο πρόληψης, προστασίας, αποτροπής, εντοπισμού, αντιμετώπισης, αποκατάστασης και ανάκαμψης από κυβερνοεπιθέσεις.

18. Η Επιτροπή αποτελεί το συντονιστικό όργανο μεταξύ: α) της Γενικής Διεύθυνσης Κυβερνοασφάλειας της Γενικής Γραμματείας Τηλεπικοινωνιών και Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης, που έχει οριστεί ως Εθνική Αρχή Κυβερνοασφάλειας κατά τον Ν. 4577/2018 (Α' 199), β) της Διεύθυνσης Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας, που έχει οριστεί ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT), γ) της Διεύθυνσης Κυβερνοχώρου της Ε.Υ.Π. ως ομάδας αντιμετώπισης ηλεκτρονικών επιθέσεων (Εθνικό CERT), και δ) της Ελληνικής Αστυνομίας.

Μεταξύ των άλλων αρμοδιοτήτων της, η Εθνική Αρχή Κυβερνοασφάλειας:

1) Χαράσσει την ενιαία πολιτική κυβερνοασφάλειας στο πλαίσιο της Στρατηγικής Εθνικής Ασφάλειας.

2) Διαμορφώνει, συντάσσει και επικαιροποιεί την Εθνική Στρατηγική Κυβερνοασφάλειας, που προβλέπεται στο άρθρο 6 του Ν. 4577/2018 (Α' 199), και συντονίζει, επιβλέπει και αξιολογεί την εφαρμογή της, υποβάλλοντας αναφορές στην Επιτροπή Συντονισμού για Θέματα κυβερνοασφάλειας του άρθρου 22 του Ν. 5002/2022 (Α' 228) και στον υπουργό Ψηφιακής Διακυβέρνησης.

3) Εισηγείται στον υπουργό Ψηφιακής Διακυβέρνησης την πρόταση νομοθετικών μέτρων και την έκδοση κανονιστικών πράξεων που αφορούν τον τομέα της κυβερνοασφάλειας, καθώς και στην Επιτροπή Συντονισμού του άρθρου 23 του Ν. 5002/2022 οποιοδήποτε θέμα άπτεται της κυβερνοασφάλειας και υπόκειται στις αρμοδιότητές της, όπως αυτές προβλέπονται στο άρθρο 22 του Ν. 5002/2022.

4) Αναπτύσσει και προτείνει στα κατά περίπτωση αρμόδια όργανα ολοκληρωμένο πλαίσιο κινήτρων για επενδύσεις στον τομέα της κυβερνοασφάλειας.

5) Προάγει την εκπαίδευση, την ενημέρωση και την ευαισθητοποίηση σε θέματα κυβερνοασφάλειας.

6) Καθορίζει τις προτεραιότητες και ενισχύει την επιστημονική έρευνα και την ανάπτυξη δυνατοτήτων, καινοτόμων υπηρεσιών, λύσεων, εφαρμογών και εξοπλισμού στο πλαίσιο του σκοπού της.

7) Αναπτύσσει συνεργασίες με δημόσιους, ιδιωτικούς, ακαδημαϊκούς και ερευνητικούς φορείς.

8) Διαμορφώνει και παρακολουθεί το πλαίσιο τεχνικών μέτρων και απαιτήσεων ασφάλειας συστημάτων Τεχνολογιών Πληροφορικής και Επικοινωνιών.

9) Λαμβάνει, προπαντός, τεχνικά μέτρα αποτροπής και αντιμετώπισης του κυβερνοεγκλήματος, σε συνεργασία με άλλες αρμόδιες αρχές και υπηρεσίες, και ιδίως με την Ελληνική Αστυνομία.

10) Ασκεί ελεγκτικές αρμοδιότητες, διενεργεί επιθεωρήσεις και επιβάλλει κυρώσεις στο πλαίσιο του ελέγχου συμμόρφωσης προς το νομικό πλαίσιο για την κυβερνοασφάλεια, σύμφωνα με τις διατάξεις του Νόμου 4577/2018 (Α' 199) και του Νόμου 4961/2022 (Α' 146).

11) Διαμορφώνει και υλοποιεί πλαίσιο πιστοποίησης κυβερνοασφάλειας για τα προϊόντα, τις διαδικασίες, τις υπηρεσίες και τους αξιόπιστους παρόχους υπηρεσιών κυβερνοασφάλειας, καθώς και για τη συμμόρφωσή τους προς τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας.

«Η πλέον πρόσφατη θεσμική εξέλιξη στον τομέα της κυβερνοασφάλειας είναι η σύσταση, με τον Νόμο 5086/2024, της Εθνικής Αρχής Κυβερνοασφάλειας. Σκοπός της Αρχής είναι η οργάνωση, ο συντονισμός, η εφαρμογή και ο έλεγχος ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, σε επίπεδο πρόληψης, προστασίας, αποτροπής, εντοπισμού, αντιμετώπισης, αποκατάστασης και ανάκαμψης από κυβερνοεπιθέσεις».

12) Παρακολουθεί το συνολικό επίπεδο ασφάλειας του κυβερνοχώρου στη χώρα και προλαμβάνει, προστατεύει, συντονίζει και συμβάλλει στην αντιμετώπιση απειλών και κυβερνοεπιθέσεων, καθώς και στη διαχείριση περιστατικών ασφάλειας, μεταξύ άλλων, με τη λειτουργία του Ενοποιημένου SOC, του Εθνικού Δικτύου SOC και της Ομάδας Απόκρισης συμβάντων στον κυβερνοχώρο (CSIRT), σε συνεργασία με τις συναρμόδιες για την κυβερνοασφάλεια αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο, για την επίτευξη των εθνικών στόχων, τη διασφάλιση υψηλού επιπέδου ασφάλειας, καθώς και για την προάσπιση των ατομικών δικαιωμάτων στον κυβερνοχώρο.

13) Καταρτίζει το Εθνικό Σχέδιο Έκτακτης Ανάγκης, συμβάλλει στην εκπόνηση του Εθνικού Σχεδίου Αποτίμησης Κινδύνων Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών, και καταρτίζει το Εθνικό Σχέδιο Αντιμετώπισης Περιστατικών και Κρίσεων στον Κυβερνοχώρο, τα οποία υποβάλλει προς έγκριση στην Επιτροπή Συντονισμού για Θέματα Κυβερνοασφάλειας.

14) Αποτελεί το ενιαίο σημείο αναφοράς σχετικά με απειλές και συμβάντα στον κυβερνοχώρο, συλλέγοντας και διαμοιράζοντας πληροφορίες προς άλλους δημόσιους και ιδιωτικούς φορείς, σε συνεργασία με άλλες αρχές, σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, για την ανίχνευση, συγκέντρωση και ανάλυση δεδομένων που σχετίζονται με απειλές και περιστατικά στον κυβερνοχώρο.

15) Παρέχει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες για την αντιμετώπιση κυβερνοαπειλών σε δημόσιους και ιδιωτικούς φορείς, σε συνεργασία με τις κατά περίπτωση αρμόδιες αρχές και την Επιτροπή Συντονισμού για θέματα κυβερνοασφάλειας.

16) Ενημερώνει, χωρίς καθυστέρηση, την Επιτροπή Συντονισμού για Θέματα Κυβερνοασφάλειας σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο.

17) Υποστηρίζει την ανάπτυξη εφαρμογών ηλεκτρονικής διακυβέρνησης από τη σκοπιά της κυβερνοασφάλειας.

18) Εκπροσωπεί τη χώρα για θέματα κυβερνοασφάλειας και συντονίζει τους εκπροσώπους συναρμόδιων φορέων σε όλους τους ευρωπαϊκούς και διεθνείς οργανισμούς, καθώς και στις διεθνείς και διακρατικές σχέσεις.

Η ΓΝΩΜΗ ΤΩΝ ΠΟΛΙΤΩΝ ΚΑΙ ΤΩΝ -ΕΠΙΧΕΙΡΗΣΕΩΝ

Μέσα σε αυτό το πλαίσιο, πώς κινείται η κοινή γνώμη στην Ελλάδα; Με άλλα λόγια τι πιστεύουν οι Έλληνες, αλλά και οι επιχειρήσεις για την ασφάλεια στο διαδίκτυο; Αυτό ήταν το αντικείμενο των δύο ειδικών ερευνών που διεξήγαγε η Metron Analysis, τα βασικά στοιχεία των οποίων παρουσιάζονται σε αυτή την ενότητα.

Η κατανόηση της απειλής από τους πολίτες είναι εξαιρετικά κρίσιμη για τα ζητήματα κυβερνοασφάλειας. Γι' αυτό έχει ενδιαφέρον να αναφερθούμε στο πώς αντιλαμβάνονται οι Έλληνες τις απειλές στο διαδίκτυο. Σύμφωνα με την έρευνα της Metron Analysis, παρότι το 84% δηλώνει πως αντιμετωπίζει κινδύνους στο διαδίκτυο, το 67% είναι αυτό που λαμβάνει μέτρα προστασίας κατά τη διάρκεια της περιήγησής του[19]. Σε αυτά συμπεριλαμβάνονται: α) η επίσκεψη μόνο σε ιστοσελίδες που γνωρίζουν και εμπιστεύονται, β) το μη άνοιγμα μηνυμάτων ηλεκτρονικού ταχυδρομείου από αποστολείς που δεν γνωρίζουν, γ) η αποκλειστική χρήση του προσωπικού υπολογιστή και δ) η εγκατάσταση λογισμικού antivirus.

Προκαλεί προβληματισμό πως το 38% του γενικού πληθυσμού δηλώνει όχι τόσο (25%) και καθόλου (13%) ενημερωμένο για τους κινδύνους ασφάλειας στο διαδίκτυο. Από το 62% που δηλώνει ενημερωμένο, μόνο το 13% είναι πολύ ενημερωμένο, ενώ η πλειοψηφία (49%) δηλώνει αρκετά ενημερωμένη. Οι περιστασιακοί χρήστες και οι μεγαλύτερες ηλικίες είναι λιγότερο ενημερωμένοι για τους κινδύνους, ενώ οι περισσότερο ευαισθητοποιημένοι είναι οι νεότεροι ηλικιακά (83% των Millennials), οι υψηλότερης κοινωνικής τάξης και μορφωτικού επιπέδου (78%) και οι φοιτητές (89%)[20].

Οι Έλληνες αισθάνονται ανασφάλεια και για τα προσωπικά τους δεδομένα στο διαδίκτυο. Σε σύγκριση με πέντε χρόνια πριν, ένας στους δύο (51%) δηλώνει ότι αισθάνεται λιγότερη ασφάλεια ως προς τα προσωπικά του δεδομένα και τις πληροφορίες, το 27% δηλώνουν ότι νιώθουν το ίδιο ασφαλείς, ενώ ένα 17% δηλώνουν ότι νιώθουν μεγαλύτερη ασφάλεια[21]. Πρέπει να τονίσουμε πως δεν πρόκειται για έναν ελληνικό εξαιρετισμό, καθώς αντίστοιχες μετρήσεις σε άλλες χώρες της ΕΕ, αλλά και στις ΗΠΑ, δείχνουν αντίστοιχη τάση. Στις τελευταίες, σύμφωνα με την έρευνα «Americans and Privacy» του 2019 του Pew Research Center, το 70% δήλωνε αυξημένη ανασφάλεια ως προς τα προσωπικά του δεδομένα σε σύγκριση με πέντε χρόνια νωρίτερα[22].

Σύμφωνα με τα ευρήματα της έρευνας για τις επιχειρήσεις, ο κίνδυνος των κυβερνοεπιθέσεων βαίνει κλιμακούμενος, με τις ελληνικές επιχειρήσεις να βρίσκονται συστηματικά αντιμέτωπες με την πρόκληση της κυβερνοασφάλειας. Η συντριπτική πλειονότητα των εταιρειών στην Ελλάδα διαπιστώνει ότι οι κίνδυνοι της ασφάλειας στον κυβερνοχώρο αυξάνονται με την πάροδο του χρόνου, ενώ ένα σημαντικό ποσοστό απαντά ότι έχει πέσει θύμα κυβερνοεπίθεσης ή κυβερνοεγκλήματος. Πιο συγκεκριμένα:

Α Ξ Ι Ζ Ε Ι Ν Α Σ Η Μ Ε Ι Ω Θ

ΟΙ MILLENNIALS ΚΑΙ ΟΙ GEN Z ΕΙΝΑΙ ΟΙ ΦΑΝΑΤΙΚΟΤΕΡΟΙ ΧΡΗΣΤΕΣ ΤΟΥ GOV.GR ΚΑΙ ΤΩΝ ΜΕΣΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ, ΔΕΙΧΝΟΝΤΑΣ ΞΕΚΑΘΑΡΑ ΤΗΝ ΠΡΟΤΙΜΗΣΗ ΤΟΥΣ ΣΕ ΕΝΑ ΠΕΡΙΣΣΟΤΕΡΟ ΨΗΦΙΑΚΟ, ΦΙΛΙΚΟ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟ ΚΡΑΤΟΣ.

Όσο περισσότερο χρησιμοποιούν το διαδίκτυο, τόσο περισσότερο θεωρούν πως αντιμετωπίζουν κινδύνους (84%). Οι μεγαλύτεροι κίνδυνοι είναι οι απάτες, η κατάχρηση προσωπικών δεδομένων, και η σεξουαλική κακοποίηση και εκμετάλλευση ανηλίκων.

ΕΙΝΑΙ ΕΜΦΑΝΕΣ ΠΩΣ ΟΙ ΚΙΝΔΥΝΟΙ ΘΑ ΠΟΛΛΑΠΛΑΣΙΑΣΤΟΥΝ ΕΑΝ ΔΙΕΥΡΥΝΘΕΙ Η ΕΡΕΥΝΑ ΣΤΟ ΠΕΔΙΟ ΤΗΣ ΕΘΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ (ΤΡΟΜΟΚΡΑΤΙΑ, ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ, ΥΒΡΙΔΙΚΕΣ ΑΠΕΙΛΕΣ).

Έχει αυξηθεί σημαντικά το ποσοστό των Ελλήνων που χρησιμοποιεί καθημερινά το διαδίκτυο – στις νεότερες γενιές (Millennials και Gen Z) φτάνει το 100%.

ΤΟ ΔΙΑΔΙΚΤΥΟ, ΑΠΟ ΚΟΙΝΟΥ ΜΕ ΤΗΝ ΤΗΛΕΟΡΑΣΗ, ΕΙΝΑΙ ΤΟ ΒΑΣΙΚΟ ΜΕΣΟ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΨΥΧΑΓΩΓΙΑΣ ΤΩΝ ΕΛΛΗΝΩΝ.

Ο Έλληνας κρατά τον θαυμαστό κόσμο του διαδικτύου κυριολεκτικά στα χέρια του, καθώς τα Smartphones είναι το βασικό μέσο περιήγησης στο ίντερνετ.

ΟΙ ΕΛΛΗΝΕΣ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΤΟ ΔΙΑΔΙΚΤΥΟ ΓΙΑ ΝΑ ΕΠΙΚΟΙΝΩΝΗΣΟΥΝ (ΜΕ ΠΛΑΤΦΟΡΜΕΣ ΚΑΙ SOCIAL MEDIA ΝΑ ΕΧΟΥΝ ΑΝΤΙΚΑΤΑΣΤΗΣΕΙ ΤΗΝ ΠΑΡΑΔΟΣΙΑΚΗ ΤΗΛΕΦΩΝΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ), ΓΙΑ ΝΑ ΑΠΟΚΤΗΣΟΥΝ ΠΡΟΣΒΑΣΗ ΣΕ ΥΠΗΡΕΣΙΕΣ, ΝΑ ΔΙΑΣΚΕΔΑΣΟΥΝ, ΝΑ ΕΚΠΑΙΔΕΥΤΟΥΝ ΚΑΙ ΝΑ ΠΡΑΓΜΑΤΟΠΟΙΗΣΟΥΝ ΑΓΟΡΑΠΩΛΗΣΙΕΣ.

Η κρίση της πανδημίας λειτούργησε ως ευκαιρία στον ψηφιακό κόσμο, με το Gov.gr και την τηλεκπαίδευση να αποτελούν τους βασικούς παράγοντες εντατικοποίησης και ποιοτικοποίησης της χρήσης από τους Έλληνες.

Παρουσιάζει ενδιαφέρον πως, για την πλειοψηφία, οι θεωρίες συνωμοσίας και τα fake news δεν έχουν συνδεθεί με κινδύνους και απειλές ασφάλειας.

ΑΝ ΚΑΙ ΔΗΛΩΝΟΥΝ ΠΩΣ ΚΙΝΔΥΝΕΥΟΥΝ, Ο ΕΝΑΣ ΣΤΟΥΣ ΤΡΕΙΣ ΔΕΝ ΛΑΜΒΑΝΕΙ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ, ΕΝΩ ΜΕΓΑΛΟ ΠΡΟΒΛΗΜΑΤΙΣΜΟ ΠΡΟΚΑΛΕΙ ΤΟ ΓΕΓΟΝΟΣ ΠΩΣ ΤΟ 38% ΔΕΝ ΔΗΛΩΝΕΙ ΤΟΣΟ ΕΝΗΜΕΡΩΜΕΝΟ ΓΙΑ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ.

Το 11% του συνόλου δηλώνει πως έχει πέσει θύμα εγκληματικής δραστηριότητας, κάτι που, ωστόσο, αλλάζει ριζικά στους εντατικούς χρήστες, με το 60% να έχει εντοπίσει κακόβουλο λογισμικό ή παραπλανητικό email.

ΟΛΟΙ ΓΝΩΡΙΖΟΥΝ ΤΗ ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ, ΑΛΛΑ ΜΟΝΟ ΕΝΑΣ ΣΤΟΥΣ ΤΡΕΙΣ ΠΟΥ ΔΗΛΩΝΟΥΝ ΠΩΣ ΕΧΟΥΝ ΠΕΣΕΙ ΘΥΜΑ ΑΠΕΥΘΥΝΟΝΤΑΙ ΣΕ ΑΥΤΗ, ΕΝΩ ΤΟ 25% ΤΩΝ ΘΥΜΑΤΩΝ ΑΠΕΥΘΥΝΟΝΤΑΙ ΣΕ ΣΥΓΓΕΝΕΙΣ ΚΑΙ ΦΙΛΟΥΣ.

Οι Έλληνες αισθάνονται ανασφάλεια για τα προσωπικά τους δεδομένα στο διαδίκτυο. Μεγάλο πρόβλημα αποτελεί η άγνοια για τον GDPR, αλλά και, παράλληλα, δηλώνουν πως θέλουν ένα αυστηρότερο νομοθετικό πλαίσιο!

Η ΑΝΗΣΥΧΙΑ ΓΙΑ ΤΗ ΣΥΛΛΟΓΗ ΚΑΙ ΤΗ ΧΡΗΣΗ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΑΦΟΡΑ ΤΟΣΟ ΤΟΥΣ ΔΗΜΟΣΙΟΥΣ, ΟΣΟ ΚΑΙ ΤΟΥΣ ΙΔΙΩΤΙΚΟΥΣ ΦΟΡΕΙΣ, ΕΝΩ ΙΔΙΑΙΤΕΡΟ ΠΡΟΒΛΗΜΑ ΣΥΝΙΣΤΑ ΚΑΙ Η ΚΑΤΑΝΟΗΣΗ ΤΟΥ ΤΡΟΠΟΥ ΧΡΗΣΗΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ.

Αξίζει αναφοράς η διαφοροποίηση για τα οφέλη της χρήσης προσωπικών δεδομένων από δημόσιους και ιδιωτικούς φορείς, με το Δημόσιο να κερδίζει τους πολίτες στα οφέλη, σε σημαντικό βαθμό λόγω του Gov.gr.

ΜΠΡΟΣΤΑ ΣΤΟ ΑΓΝΩΣΤΟ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΤΩΝ ΚΙΝΔΥΝΩΝ ΤΟΥ, ΟΙ ΕΛΛΗΝΕΣ ΖΗΤΟΥΝ ΠΕΡΙΣΣΟΤΕΡΗ ΑΣΦΑΛΕΙΑ, ΕΝΑΝΤΙ ΤΗΣ ΕΛΕΥΘΕΡΙΑΣ.

ΣΥΜΦΩΝΑ ΜΕ ΤΑ ΕΥΡΗΜΑΤΑ ΤΗΣ ΕΡΕΥΝΑΣ ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ, Ο ΚΙΝΔΥΝΟΣ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΒΑΙΝΕΙ ΚΛΙΜΑΚΟΥΜΕΝΟΣ, ΜΕ ΤΙΣ ΕΛΛΗΝΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΝΑ ΒΡΙΣΚΟΝΤΑΙ ΣΥΣΤΗΜΑΤΙΚΑ ΑΝΤΙΜΕΤΩΠΕΣ ΜΕ ΤΗΝ ΠΡΟΚΛΗΣΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ. Η ΣΥΝΤΡΙΠΤΙΚΗ ΠΛΕΙΟΝΟΤΗΤΑ ΤΩΝ ΕΤΑΙΡΕΙΩΝ ΣΤΗΝ ΕΛΛΑΔΑ ΔΙΑΠΙΣΤΩΝΕΙ ΟΤΙ ΟΙ ΚΙΝΔΥΝΟΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΑΥΞΑΝΟΝΤΑΙ ΜΕ ΤΗΝ ΠΑΡΟΔΟ ΤΟΥ ΧΡΟΝΟΥ, ΕΝΩ ΕΝΑ ΣΗΜΑΝΤΙΚΟ ΠΟΣΟΣΤΟ ΑΠΑΝΤΑ ΟΤΙ ΕΧΕΙ ΠΕΣΕΙ ΘΥΜΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗΣ Ή ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ. ΠΙΟ ΣΥΓΚΕΚΡΙΜΕΝΑ:

- Το **ένα τρίτο των ελληνικών εταιρειών** αναφέρει περιστατικά κυβερνοεπίθεσης ή κυβερνοεγκλήματος που αφορούν, κατά κύριο λόγο, παραπλανητικά emails και δευτερευόντως κακόβουλο λογισμικό ή χακάρισμα κοινωνικών δικτύων και emails, ενώ ελάχιστα σχετίζονται με παραβίαση προσωπικών δεδομένων πελατών.

- Όσον αφορά την επίπτωση των περιστατικών αυτών, **σχεδόν 4 στις 10 επιχειρήσεις** θεωρούν ότι ήταν πολύ/αρκετά σοβαρή. Σε κάθε περίπτωση, η αίσθηση κινδύνου παραμένει, καθώς **2 στις 3 επιχειρήσεις** θεωρούν ότι είναι πολύ/αρκετά πιθανό να επαναληφθεί στο μέλλον κάποιου είδους κυβερνοεπίθεση.

- Το ασφυκτικό περιβάλλον που δημιουργούν για τις ελληνικές επιχειρήσεις οι κίνδυνοι κυβερνοασφάλειας γίνεται εμφανές από πολλά ευρήματα της έρευνας. Για παράδειγμα, **περισσότερες από 1 στις 5 εταιρείες (21%)** έχουν απευθυνθεί στη Δίωξη Ηλεκτρονικού Εγκλήματος για θέματα ασφάλειας στο διαδίκτυο.

- Πάντως, παρά την κλιμάκωση των κινδύνων, οι ελληνικές επιχειρήσεις, και ειδικά οι μεγαλύτερες σε μέγεθος, δηλώνουν σήμερα πιο ασφαλείς και θωρακισμένες συγκριτικά με **πέντε χρόνια νωρίτερα**, με το **41%** να θεωρεί ότι τα προσωπικά δεδομένα είναι πλέον πιο ασφαλή.

- Οι επιχειρήσεις που θεωρούν ότι η χρήση του διαδικτύου εγκυμονεί κινδύνους αντιλαμβάνονται ως μεγαλύτερους εξ αυτών το **κακόβουλο λογισμικό (50%)** και την **εξαπάτηση σε συναλλαγές (50%).** Ακολουθούν το **χακάρισμα μέσω των social media ή του ηλεκτρονικού ταχυδρομείου (48%)** και η **κατάχρηση προσωπικών δεδομένων από τρίτους (25%).**

- Αναφορικά με τα μέτρα πρόληψης, στη μεγάλη τους πλειονότητα **(85%)**, οι επιχειρήσεις δηλώνουν ότι παίρνουν μέτρα διαφύλαξης της ασφάλειας στις ηλεκτρονικές αγορές/συναλλαγές. Η τάση αυτή είναι εντονότερη μεταξύ των μεγαλύτερων επιχειρήσεων **(94%).**

- Ωστόσο, πέρα από τα επιμέρους μέτρα, σημαντικά μικρότερο είναι το ποσοστό των επιχειρήσεων που δηλώνει ότι διαθέτει σχέδιο πρόληψης/αντιμετώπισης κυβερνοεπιθέσεων: **σχεδόν 6 στις 10 εταιρείες στην Ελλάδα (57%)** απαντούν ότι διαθέτουν σχέδιο πρόληψης των περιστατικών κυβερνοασφάλειας, ποσοστό που στις μεγαλύτερες εταιρείες φθάνει το 85%.

- Σε όλες σχεδόν τις περιπτώσεις αναφέρεται η εγκατάσταση λογισμικού προστασίας (ποσοστό μικρότερο στον γενικό πληθυσμό 79%) και ακολούθως άλλα μέτρα, που αφορούν κυρίως την ασφαλή πλοήγηση στο διαδίκτυο. Για ένα ποσοστό **μεγαλύτερο από το 1/3 των περιπτώσεων** η σχετική ευθύνη έχει ανατεθεί σε **εξωτερικό συνεργάτη (38%)**, ενώ για το **30% η ευθύνη αυτή έχει ανατεθεί σε εργαζόμενο της επιχείρησης** (ιδίως σε μεγαλύτερες).

- Πάντως, μόνο το **19%** των εταιρειών του δείγματος της έρευνας έχει αξιοποιήσει, μέχρι σήμερα, **εθνική ή ευρωπαϊκή χρηματοδότηση** για την αναβάθμιση στο πεδίο της κυβερνοασφάλειας.

- Οι επιχειρήσεις αντιλαμβάνονται ως πιο ευάλωτο σημείο της στρατηγικής κυβερνοασφάλειας την **ελλιπή γνώση συναφών κινδύνων**, αλλά και την **έλλειψη εκπαίδευσης/κουλτούρας**. Ειδικά σε ό,τι αφορά την εκπαίδευση, το **37%** των επιχειρήσεων του δείγματος την αντιλαμβάνεται ως ευάλωτο σημείο της στρατηγικής τους.

- Πάντως, αν και η εκπαίδευση θεωρείται κομβικό σημείο, πρακτικά **μόνο 3 στις 10 επιχειρήσεις** παρείχαν τον τελευταίο χρόνο **εκπαίδευση στο προσωπικό** τους σε θέματα ασφάλειας, ενώ η μεγάλη πλειονότητα δεν έχει οργανώσει τον τελευταίο χρόνο κάποια εκπαίδευση του ανθρώπινου δυναμικού σε θέματα κυβερνοασφάλειας.

19. Καρατράντος, Τ. (2023), «Τι πιστεύουν οι Έλληνες για την ασφάλεια στο διαδίκτυο», Policy Brief 181, ΕΛΙΑΜΕΠ.
20. Ό.π.
21. Ό.π.
22. Pew Research Center, (2019), «Americans and Privacy». Έχει ιδιαίτερο ενδιαφέρον και η πρόσφατη έκθεση «How Americans View Data Privacy» (Οκτώβριος 2023), του ίδιου κέντρου, με ειδική αναφορά στην ιδιωτικότητα των δεδομένων.

ΣΥΜΠΕΡΑΣΜΑΤΑ ΠΡΟΤΑΣΕΙΣ -ΠΟΛΙΤΙΚΗΣ

Ο τομέας των αναδυόμενων τεχνολογιών είναι αυτή τη στιγμή το σημαντικότερο ζήτημα, με όρους στρατηγικής πρόκλησης, που αντιμετωπίζουν οι αρμόδιοι για τη χάραξη πολιτικής για την ασφάλεια σε διεθνές αλλά και εθνικό επίπεδο. Στην εποχή της 4ης Βιομηχανικής Επανάστασης, και για ορισμένους στο μεταίχμιο με την 5η, οι αναδυόμενες τεχνολογίες αποτελούν ευκαιρία, αλλά και παράλληλα απειλή. Από τη μία πλευρά προσφέρουν στα κράτη και στις υπηρεσίες ασφάλειας και πληροφοριών σημαντικά εργαλεία και όπλα για να αντιμετωπίσουν το έγκλημα και τις διάφορες απειλές, και από την άλλη πλευρά δημιουργούν κινδύνους –κυρίως λόγω πιθανής κακόβουλης χρήσης–, αλλά και νέες ευαλωτότητες, λόγω και της υψηλής συνδεσιμότητας και εξάρτησής μας από τις τεχνολογικές λύσεις και υπηρεσίες. Εξίσου σημαντικά είναι και τα ζητήματα που αφορούν το ηθικό μέρος της χρήσης και αξιοποίησης των αναδυόμενων τεχνολογιών, αλλά και το νομικό πλαίσιο και τις διαφοροποιήσεις στους περιορισμούς μεταξύ των κρατών και των ιδιωτών. Μια αρκετά δύσκολη εξίσωση με πολλές άγνωστες παραμέτρους.

Όπως είναι αναμενόμενο, η μεγαλύτερη συζήτηση γίνεται για την τεχνητή νοημοσύνη, η οποία υπάρχει ήδη στην καθημερινότητα της ζωής των πολιτών, αλλά και της λειτουργίας των κρατών και των διεθνών οργανισμών. Δεν είναι άλλωστε τυχαίο πως η τεχνητή νοημοσύνη αποτελεί το σημαντικότερο τεχνολογικό εργαλείο που μπορεί να επηρεάσει πολλούς τομείς του σχεδιασμού ασφάλειας, αλλά και των επιχειρήσεων. Η τεχνητή νοημοσύνη αξιοποιείται ήδη για τη μοντελοποίηση απειλών και την πρόγνωση, αλλά και την εκτίμηση της εξέλιξης καταστροφών, την αξιολόγηση επικινδυνότητας, την παρακολούθηση των επιχειρήσεων και την εξέταση διαφορετικών σεναρίων που μπορούν να αξιοποιηθούν, αλλά και για τη λήψη αποφάσεων, τόσο σε στρατηγικό και πολιτικό επίπεδο όσο και σε επιχειρησιακό – ακόμα και σε τακτικό επίπεδο, για παράδειγμα κατά τη διάρκεια μιας δασικής πυρκαγιάς. Αρκετές υπηρεσίες ασφάλειας και πληροφοριών αξιοποιούν εργαλεία τεχνητής νοημοσύνης για την ιδιαιτέρως κρίσιμη ανάλυση Ανοικτών Πηγών, που μπορεί να τους παρέχει σημαντικές πληροφορίες για την αποτροπή μιας τρομοκρατικής επίθεσης.

Υπάρχουν όμως και αρκετοί κίνδυνοι από την πιθανή κακόβουλη χρήση της τεχνητής νοημοσύνης. Έχουν ήδη προκύψει μεγάλες συζητήσεις και ενστάσεις σε ηθικό και νομοθετικό επίπεδο για την πιθανή κατάχρησή της από τα κράτη και τις αρμόδιες υπηρεσίες για τη συλλογή και ανάλυση πληροφοριών. Ωστόσο, η μεγαλύτερη απειλή προέρχεται από την πιθανή κακόβουλη χρήση της για παραπληροφόρηση και προπαγάνδα –στο πλαίσιο υβριδικών επιχειρήσεων–, κυβερνοεπιθέσεις, αλλά και για τρομοκρατικές ενέργειες, ενώ δεν πρέπει να ξεχνάμε πως τρομοκρατικές οργανώσεις, όπως η Daesh, ανέπτυξαν εξελιγμένες δυνατότητες προπαγάνδας και η τεχνητή νοημοσύνη μπορεί να αξιοποιηθεί όχι μόνο σε επιθέσεις, αλλά και για προπαγανδιστικούς σκοπούς, στρατολόγηση και κινητοποίηση ριζοσπαστικοποιημένων ανθρώπων.

Η δεύτερη αναδυόμενη τεχνολογία που ενέχει σημαντικές προκλήσεις και κινδύνους ασφάλειας είναι το Διαδίκτυο των Πραγμάτων (Internet of Things). Οι εταιρείες, αλλά και οι κυβερνήσεις έχουν αυξήσει σημαντικά τα τελευταία χρόνια την αξιοποίηση εφαρμογών IoT για την παροχή υπηρεσιών στους πολίτες και στους πελάτες τους, ενώ την ίδια στιγμή οι κυβερνοαπειλές από διάφορους δρώντες αυξάνονται συνεχώς, που σημαίνει πως μια αρχιτεκτονική IoT, που απαιτεί πολλούς και διαφορετικούς δρώντες τόσο στον σχεδιασμό όσο και στην υλοποίηση διαδικασιών ασφάλειας, εμφανίζει τρωτότητες.

Χαρακτηριστικό ως προς αυτό είναι το παράδειγμα των συσκευών που λειτουργούν σε πλαίσιο IoT και δεν έχουν περάσει από διαδικασία αυθεντικής λειτουργίας, καθώς ακόμα και μια συσκευή που δεν κάνει αποθήκευση σημαντικών δεδομένων, όπως το ψυγείο ή το κλιματιστικό, μπορεί να αποτελέσει τρωτό σημείο για την ασφάλεια ολόκληρου του δικτύου. Αρκετές από αυτές τις συσκευές προσπαθούν να λειτουργήσουν με ελάχιστα ή καθόλου δεδομένα, ώστε να μειωθεί το κόστος και να αυξηθεί η διάρκεια ζωής της μπαταρίας και του χρόνου χρήσης, αυτή όμως η τάση δημιουργεί δυσκολίες σε αναβαθμίσεις και μπορεί να οδηγήσει σε περιορισμένη χρήση δυνατοτήτων προστασίας, όπως τα firewall, και να καταστήσει τη συσκευή –αλλά και κυρίως ολόκληρο το δίκτυο– ευάλωτη σε μια κυβερνοεπίθεση. Υπάρχουν περιπτώσεις που σε ένα δίκτυο συνδέονται και αξιοποιούνται συσκευές που δεν έχουν σχεδιαστεί ειδικά για διαδικασίες διασύνδεσης νέφους (cloud) και είναι πολύ πιθανό να μην είναι συμβατές με τις νέες τεχνολογίες κρυπτογράφησης, με αποτέλεσμα να καθίστανται ιδιαιτέρως τρωτές σε κυβερνοεπιθέσεις νέας γενιάς. Τέλος, σημαντικό πρόβλημα αποτελούν οι διαφοροποιημένες προδιαγραφές ασφάλειας που ακολουθούν οι συσκευές, που μπορούν να αξιοποιηθούν σε μια διαδικασία Διαδικτύου των Πραγμάτων[23].

23. Η μετεξέλιξη του Διαδικτύου των Πραγμάτων είναι το Διαδίκτυο των Πάντων (Internet of Everything).

Η πρόκληση των αναδυόμενων τεχνολογιών είναι προφανές πως θα καταστήσει το περιβάλλον γύρω από την κυβερνοασφάλεια περισσότερο σύνθετο και απαιτητικό. Σε αυτόν καθαυτόν τον τομέα όμως, το σημαντικότερο ίσως ζήτημα είναι οι κυβερνοαπειλές για τις κρίσιμες υποδομές. Είναι χαρακτηριστικό πως, συμπληρωματικά με την Οδηγία NIS 2, η ΕΕ, στα τέλη Δεκεμβρίου 2022, προχώρησε στην πρόταση μίας ακόμη «Οδηγίας για την ανθεκτικότητα των κρίσιμων οντοτήτων» (Critical Entities Resilience), τη γνωστή και ως Οδηγία CER. Η συγκεκριμένη Οδηγία έχει δύο βασικές

«Υπάρχουν αρκετοί κίνδυνοι από την πιθανή κακόβουλη χρήση της τεχνητής νοημοσύνης. Έχουν ήδη προκύψει μεγάλες συζητήσεις και ενστάσεις σε ηθικό και νομοθετικό επίπεδο για την πιθανή κατάχρησή της από τα κράτη και τις αρμόδιες υπηρεσίες για τη συλλογή και ανάλυση πληροφοριών. Ωστόσο, η μεγαλύτερη απειλή προέρχεται από την πιθανή κακόβουλη χρήση της για παραπληροφόρηση και προπαγάνδα στο πλαίσιο υβριδικών επιχειρήσεων, για κυβερνοεπιθέσεις, αλλά και για τρομοκρατικές ενέργειες».

αλλαγές στο σχήμα των κρίσιμων υποδομών. Η πρώτη αφορά τη μετάβαση από τις υποδομές στις οντότητες. Οι ευρωπαϊκές υποδομές, και κυρίως τα δίκτυα, στην εποχή της 4ης Βιομηχανικής Επανάστασης, έχουν γίνει περισσότερο διασυνδεδεμένες και αλληλεξαρτώμενες, γεγονός που τις καθιστά ισχυρότερες και αποτελεσματικότερες, αλλά και πιο ευάλωτες σε περίπτωση κινδύνου. Είναι σημαντικό πως οι υποδομές, εκτός από το φυσικό πεδίο, έχουν πλέον και ένα ξεκάθαρο ψηφιακό, κάτι που οδήγησε την ΕΕ στη μετάβαση στην έννοια «κρίσιμες οντότητες». Το δεύτερο στοιχείο αφορά την έννοια της ανθεκτικότητας (resilience), η οποία προτάσσεται από την παλιότερη έννοια της προστασίας (protection).

Πρέπει να τονιστεί πως η συγκεκριμένη πρωτοβουλία είναι αποτέλεσμα και της εισβολής της Ρωσίας στην Ουκρανία, και της πολεμικής σύγκρουσης που την ακολούθησε και διαρκεί για περισσότερο από δύο χρόνια, η οποία κατέστησε την ασφάλεια των ενεργειακών υποδομών ως βασική προτεραιότητα της ΕΕ, κατάσταση που εντατικοποιήθηκε μετά τη δολιοφθορά στον αγωγό Nord Stream, με αποτέλεσμα η Ένωση να πιέζει τα κράτη-μέλη να «τρέξουν» δοκιμές αντοχής των υποδομών ενέργειας έναντι διαφόρων μορφών απειλών. Η απειλή της Ρωσίας και η επιστροφή των διακρατικών πολέμων στην ευρωπαϊκή ήπειρο κατέστησε σαφές πως η ΕΕ πρέπει να δώσει έμφαση στην ασφάλεια των κρίσιμων οντοτήτων και στην ευρύτερη γειτονιά της, διάσταση που υπάρχει στην Οδηγία CER. Πρέπει να τονιστεί πως η συγκεκριμένη πρωτοβουλία σχετίζεται και με την προσπάθεια της Ένωσης να μετεξελίξει τον μηχανισμό διαχείρισης κρίσεων, δίνοντας έμφαση στις κρίσεις του μέλλοντος που θα συνδυάζουν περισσότερα του ενός στοιχεία, καθώς και στη διάσταση των πολυ-κρίσεων.

«Η πρόκληση των αναδυόμενων τεχνολογιών είναι προφανές πως θα καταστήσει το περιβάλλον γύρω από την κυβερνοασφάλεια περισσότερο σύνθετο και απαιτητικό. Σε αυτόν καθαυτόν τον τομέα όμως, το σημαντικότερο ίσως ζήτημα είναι οι κυβερνοαπειλές για τις κρίσιμες υποδομές. Είναι χαρακτηριστικό πως, συμπληρωματικά με την Οδηγία NIS 2, η ΕΕ, στα τέλη Δεκεμβρίου 2022, προχώρησε στην πρόταση μίας ακόμη «Οδηγίας για την ανθεκτικότητα των κρίσιμων οντοτήτων» (Critical Entities Resilience), τη γνωστή και ως Οδηγία CER».

ΥΠΑΡΧΟΥΝ ΤΡΕΙΣ ΔΟΜΙΚΕΣ ΠΑΘΟΓΕΝΕΙΕΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΛΛΑΔΑ:

Α) Ο κατακερματισμός της πολιτικής εσωτερικής ασφάλειας, μιας και σε αυτή, ως υποσύνολο, εντάσσεται η κυβερνοασφάλεια, μεταξύ διαφορετικών υπουργείων και υπηρεσιών. Μία οριζόντια πολιτική, όπως αυτή της κυβερνοασφάλειας, και κυρίως η διάσταση της προστασίας των κρίσιμων υποδομών, συναντά σημαντικές δυσκολίες σε ένα δαιδαλώδες σύστημα δημόσιας διοίκησης, όπως είναι το ελληνικό. Αξίζει αναφοράς πως μόνο σε επίπεδο βασικών παρόχων ασφάλειας εμπλέκονται τέσσερα διαφορετικά υπουργεία (Προστασίας του Πολίτη, Πολιτικής Προστασίας και Κλιματικής Κρίσης, Ψηφιακής Διακυβέρνησης, Ναυτιλίας και Νησιωτικής Πολιτικής), καθώς και το Υπουργείο Εθνικής Άμυνας και η Ε.Υ.Π.

Β) Η προβληματική συνεργασία μεταξύ δημοσίου και ιδιωτικού τομέα. Τις περισσότερες κρίσιμες υποδομές τις διαχειρίζονται ιδιωτικές εταιρείες, οι οποίες έχουν τον δικό τους σχεδιασμό ασφάλειας. Το πρόβλημα ξεκινά από το γεγονός ότι το δημόσιο δεν έχει ένα ολοκληρωμένο πλαίσιο και συγκεκριμένα standards, τα οποία θα πρέπει να ακολουθεί ο διαχειριστής της υποδομής, είτε είναι δημόσιος είτε ιδιωτικός.

Γ) Απουσία κουλτούρας ασφάλειας από το ανθρώπινο δυναμικό που «τρέχει» στην καθημερινότητα τις κρίσιμες υποδομές. Πρέπει εδώ να προσθέσουμε και δύο δομικά προβλήματα του σχεδιασμού. Το πρώτο είναι η μη αξιοποίηση των μελλοντικών τάσεων – ο σχεδιασμός ασφάλειας δεν μπορεί να ακολουθεί τις απειλές και τους κινδύνους, αλλά να προσπαθεί να τους προβλέψει, ώστε να κινείται εμπροσθοβαρώς (Foresight Led Planning). Το δεύτερο είναι η μη επένδυση στην ανάδειξη των τρωτοτήτων. Επιτυχής σχεδιασμός σημαίνει εντοπισμός τρωτοτήτων και θωράκισή τους.

ΚΑΤΑ ΠΡΟΤΕΡΑΙΟΤΗΤΑ ΟΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ ΑΛΛΑΓΩΝ ΚΑΙ ΜΕΤΑΡΡΥΘΜΙΣΕΩΝ ΑΦΟΡΟΥΝ:

(Α) τη δημιουργία δυνατοτήτων με στόχο την έγκαιρη ανίχνευση, πρόληψη και ταχεία αντίδραση στις απειλές, αλλά και στις προκύπτουσες κρίσεις ασφάλειας, μέσω ολοκληρωμένης και συντονισμένης προσέγγισης, τόσο συνολικά όσο και με τομεακές πρωτοβουλίες (π.χ. χρηματοπιστωτικές, ενεργειακές, απονομής δικαιοσύνης, επιβολής του νόμου, υγείας, μεταφορών) και με βάση τα διαθέσιμα εργαλεία.

(Β) Την αλλαγή του υφιστάμενου νομοθετικού πλαισίου για την προστασία και την ενίσχυση της «ανθεκτικότητας» των κρίσιμων υποδομών προκειμένου: να συμβαδίζει με τους εξελισσόμενους κινδύνους· να αντιμετωπίζει την αυξημένη διασύνδεση και αλληλεξάρτηση των διαφόρων τομέων κοινωνικής δραστηριότητας· να αποκτήσει την ικανότητα έγκαιρης προετοιμασίας για την αντιμετώπιση ανεπιθύμητων συμβάντων και επαρκούς σχεδιασμού για την αντίδρασή του σε αυτά·, και κυρίως να ενισχύσει την ικανότητά του να απορροφά, να ανακάμπτει και να προσαρμόζεται με τη μεγαλύτερη δυνατή αποτελεσματικότητα. Ειδικότερα, η διασφάλιση της

αδιάλειπτης λειτουργίας του διαδικτύου συνεπάγεται την προσαρμογή της υφιστάμενης νομοθεσίας προκειμένου να εξασφαλιστεί ένα υψηλό επίπεδο ασφάλειας των συστημάτων δικτύων και πληροφοριών, περισσότερες επενδύσεις σε έρευνα και καινοτομία, και μέριμνα για ανάπτυξη ή/και ενίσχυση των βασικών υποδομών και πόρων του διαδικτύου.

(Γ) Την ανάπτυξη συνεργειών μεταξύ των φορέων του δημοσίου και ιδιωτικού τομέα σε κοινή κατεύθυνση όσον αφορά την ανταλλαγή πληροφοριών σχετικά με την ασφάλεια και εντατικότερη συνεργασία με άλλα κράτη, καθώς και με τα θεσμικά όργανα και τους οργανισμούς της ΕΕ, ώστε να οικοδομηθεί η κατανόηση και η ανταλλαγή που είναι αναγκαίες για την επίτευξη κοινών στόχων. Ειδικότερα για την κυβερνοασφάλεια, η συνεργασία με τον ιδιωτικό τομέα και η δημιουργία «κομβικών χώρων γνώσης» (knowledge hubs) είναι καθοριστικής σημασίας, δεδομένου ότι ο κλάδος κατέχει σημαντικό μέρος της ψηφιακής και μη ψηφιακής υποδομής, που είναι κεντρικής σημασίας για την αποτελεσματική καταπολέμηση του εγκλήματος και της τρομοκρατίας.

(Δ) Την προσαρμογή των επαγγελματιών στους τομείς της επιβολής του νόμου και απονομής της δικαιοσύνης στις σύγχρονες μεθόδους επιβολής του νόμου και στη νέα και καινοτόμο τεχνολογία. Οι τεχνολογικές εξελίξεις και οι αναδυόμενες απειλές απαιτούν από τις αρχές επιβολής του νόμου την πρόσβαση σε νέα εργαλεία, την απόκτηση νέων δεξιοτήτων και την ανάπτυξη εναλλακτικών τεχνικών έρευνας. Η τεχνητή νοημοσύνη θα μπορούσε να λειτουργήσει ως ένα ισχυρό εργαλείο για την καταπολέμηση του εγκλήματος, δημιουργώντας τεράστιες ερευνητικές ικανότητες μέσω της ανάλυσης μεγάλου όγκου δεδομένων και της ταυτοποίησης «μοτίβων». Μπορεί, επίσης, να συμβάλει στον εντοπισμό στο διαδίκτυο υλικού τρομοκρατικού περιεχομένου ή ύποπτων συναλλαγών στις πωλήσεις επικίνδυνων προϊόντων ή/και να παρέχει βοήθεια σε πολίτες σε καταστάσεις έκτακτης ανάγκης. Για την αξιοποίηση αυτού του δυναμικού, απαιτείται η σύνδεση της έρευνας, της καινοτομίας και των χρηστών της τεχνητής νοημοσύνης, και η ενεργός συμμετοχή του ιδιωτικού τομέα και των πανεπιστημίων.

(Ε) Την «ευαισθητοποίηση» της ελληνικής κοινωνίας σε θέματα ασφάλειας και την απόκτηση των δεξιοτήτων για τη βελτίωση της ετοιμότητάς της στην αντιμετώπιση πιθανών απειλών. Ακόμα και βασικές γνώσεις σχετικά με τις απειλές κατά της ασφάλειας και τον τρόπο αντιμετώπισής τους μπορούν να συνεισφέρουν ουσιαστικά στην «ανθεκτικότητα» της κοινωνίας.

ΟΙ ΒΑΣΙΚΟΙ ΠΥΛΩΝΕΣ ΑΛΛΑΓΩΝ

ΠΡΟΒΛΕΨΗ
Έγκαιρη αναγνώριση

Η πρόβλεψη και η έγκαιρη αναγνώριση των απειλών είναι ικανή να οδηγήσει στον σχεδιασμό μακροπρόθεσμης στρατηγικής κυβερνοασφάλειας και στην αποτελεσματική διαχείριση κρίσεων.
Σε αυτή την κατεύθυνση είναι σημαντική η συνεργασία με την επιστημονική και ερευνητική κοινότητα, ώστε οι φορείς του Δημοσίου να μπορούν να αξιοποιήσουν τη νέα γνώση που αφορά τις προκλήσεις και την πιθανή εξέλιξη των απειλών και κινδύνων. Επίσης, απαιτείται η αξιοποίηση μεθοδολογιών «μέλλοντος» (Foresight) και η χρήση νέων τεχνολογιών-αλγοριθμικών μοντέλων και εφαρμογών τεχνητής νοημοσύνης, οι οποίες θα περιγράφουν πιθανά σενάρια αλλαγών στο εσωτερικό και στο εξωτερικό περιβάλλον ασφάλειας, καθώς και την εξέλιξη των κινδύνων και των απειλών. Απαραίτητη είναι, επίσης, η εντατικοποίηση της χρήσης της έρευνας και της καινοτομίας από τους τελικούς χρήστες.

ΠΡΟΛΗΨΗ
Ανθεκτικότητα

Η ανάπτυξη συστημάτων «έγκαιρης προειδοποίησης» (early warning systems) για την έγκαιρη αντίδραση σε περιπτώσεις επιθέσεων είναι κρίσιμη. Η «ανθεκτικότητα» (resilience) αφορά στη δυνατότητα των κοινωνιών να διαχειριστούν τις επιπτώσεις μίας κρίσης, καταστροφής ή επίθεσης με στόχο τον περιορισμό των απωλειών και την αποφυγή περαιτέρω κλιμάκωσης, όπως έγινε για παράδειγμα το 2007 στην Εσθονία.

ΠΡΟΣΤΑΣΙΑ
Αντιμετώπιση

Ο δημόσιος τομέας και οι κρίσιμες υποδομές βρίσκονται στο επίκεντρο των δράσεων προστασίας από τις απειλές κυερνοασφάλειας. Ένα ολοκληρωμένο πλαίσιο προστασίας, που θα περιλαμβάνει ειδικά σχέδια ασφάλειας και την αξιοποίηση της τεχνολογίας, η συνεργασία του δημοσίου με τον ιδιωτικό τομέα, η ενίσχυση των δυνατοτήτων ανταπόκρισης των σωμάτων ασφάλειας και η έγκαιρη ανταλλαγή πληροφοριών σε εθνικό και σε διεθνές επίπεδο, συνιστούν απαραίτητα και κρίσιμα στοιχεία για την αποτελεσματική αντιμετώπιση των απειλών και προκλήσεων που προκύπτουν. Εξίσου σημαντική είναι και η εκπόνηση μίας συνολικής πολιτικής κυβερνοαασφάλειας των κρίσιμων υποδομών, η οποία θα περιλαμβάνει τα απαραίτητα μέτρα ασφάλειας, αλλά και τον μηχανισμό ελέγχου συμμόρφωσης των διαχειριστών υποδομών, τόσο του δημοσίου, όσο και του ιδιωτικού τομέα.

ΚΑΤΑΛΗΚΤΙΚΑ, ΠΑΡΑΤΙΘΕΝΤΑΙ ΟΡΙΣΜΕΝΕΣ ΠΡΟΤΑΣΕΙΣ ΠΟΛΙΤΙΚΗΣ:

ΑΣΦΑΛΕΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

- **Εκπόνηση** εθνικής στρατηγικής για την κυβερνοασφάλεια και την προστασία των κρίσιμων οντοτήτων, η οποία θα συμβαδίζει με τις τελικές προβλέψεις της Οδηγίας CER για την ανθεκτικότητα των κρίσιμων οντοτήτων.
- **Καθορισμός** των εθνικών κρίσιμων υποδομών ανά τομέα ακολουθώντας τη λογική της Οδηγίας CER.
- **Καθορισμός** ενός φορέα που θα έχει την ευθύνη παρακολούθησης και ελέγχου της πολιτικής προστασίας των κρίσιμων υποδομών.
- **Δημιουργία** ψηφιακής εθνικής βάσης κρίσιμων υποδομών.
- **Έλεγχος** των σχεδίων και των διαδικασιών ασφάλειας των κρίσιμων υποδομών.
- **Συχνές εκπαιδεύσεις** του προσωπικού που απασχολείται σε κρίσιμες υποδομές.
- **Αναζήτηση** και υιοθέτηση βέλτιστων πρακτικών για την ασφάλεια των κρίσιμων υποδομών.
- **Καθορισμός** εθνικών standards ασφάλειας υποδομών και διαδικασιών ελέγχου, και πιστοποίησης της εφαρμογής τους.
- **Καθορισμός** προδιαγραφών ασφάλειας σε όλες τις κρίσιμες υποδομές και έλεγχος εφαρμογής τους.

ΜΕΛΛΟΝΤΙΚΕΣ ΤΑΣΕΙΣ – ΕΓΚΑΙΡΗ ΠΡΟΕΙΔΟΠΟΙΗΣΗ

- **Συνέργειες** με την ακαδημαϊκή και την ερευνητική κοινότητα, τόσο για την ανάδειξη μελλοντικών τάσεων, όσο και για τον καλύτερο σχεδιασμό ασφάλειας.
- **Αξιοποίηση** μεθοδολογιών foresight για τις μελέτες επικινδυνότητας.
- **Χρήση** νέων τεχνολογικών εργαλείων και συστημάτων έγκαιρης προειδοποίησης για την ενίσχυση της ασφάλειας και την αποτροπή των κινδύνων.
- **Ενδυνάμωση** των διαδικασιών διαλειτουργικότητας και συνδεσιμότητας των κέντρων ελέγχου και των επιχειρήσεων των κρίσιμων υποδομών με τα συντονιστικά κέντρα επιχειρήσεων της Ελληνικής Αστυνομίας και της Γενικής Γραμματείας Πολιτικής Προστασίας.
- **Ενίσχυση** των συνεργειών δημοσίου και ιδιωτικού τομέα, με έμφαση στην ανταλλαγή πληροφοριών και βέλτιστων πρακτικών.

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΔΡΑΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ

- **Σχεδιασμός** και υλοποίηση μιας επικοινωνιακής εκστρατείας ενημέρωσης και ευαισθητοποίησης τόσο από το κράτος, όσο και από τις ιδιωτικές εταιρείες, για τις νομοθετικές δικλείδες, τις πολιτικές προστασίας και τα δικαιώματα των πολιτών.
- **Δράσεις** για τη διαμόρφωση μίας ατομικής και συλλογικής κουλτούρας ασφάλειας στο διαδίκτυο, που να δίνει έμφαση στη λήψη μέτρων προστασίας, αλλά και για την ενημέρωση των αρμοδίων δημοσίων φορέων σε περιπτώσεις κινδύνου.
- **Σχεδιασμός** και διεξαγωγή ασκήσεων και stress tests.
- **Σχεδιασμός** και υλοποίηση προγραμμάτων εκπαίδευσης για την ενίσχυση των δεξιοτήτων κυβερνοασφάλειας των πολιτών.
- **Δημιουργία** εκπαιδευτικών δομών που θα παρέχουν τόσο γενικές, όσο και στοχευμένες εκπαιδεύσεις για τους πολίτες, αλλά και για τις διάφορες κατηγορίες επαγγελματιών και επιχειρήσεων.

ΕΝΙΣΧΥΣΗ ΤΗΣ ΕΡΕΥΝΑΣ – ΔΗΜΙΟΥΡΓΙΑ ΓΝΩΣΗΣ

- **Διεξαγωγή** τακτικών ποιοτικών και ποσοτικών ερευνών για τη χαρτογράφηση των προτιμήσεων, αλλά και των απειλών που θεωρούν πως αντιμετωπίζουν οι Έλληνες στο διαδίκτυο, οι οποίες πρέπει να συνδυαστούν με τον σχεδιασμό και την αξιοποίηση σύγχρονων εργαλείων για την ασφαλή πλοήγηση και την προστασία των προσωπικών δεδομένων.
- **Περαιτέρω ανάπτυξη** του επιστημονικού και ερευνητικού τομέα για την κυβερνοασφάλεια, με στόχο και τη δημιουργία περισσότερων ειδικών στον τομέα, που θα καλύψουν και τις ανάγκες που έχει η αγορά.

ΕΝΙΣΧΥΣΗ ΤΩΝ ΣΥΝΕΡΓΕΙΩΝ ΜΕ ΤΟΝ ΙΔΙΩΤΙΚΟ ΤΟΜΕΑ – ΥΠΟΣΤΗΡΙΞΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

- **Υποστήριξη** των επιχειρήσεων, κυρίως των μικρών, για να αξιοποιήσουν εθνικές και ευρωπαϊκές χρηματοδοτήσεις για θέματα κυβερνοασφάλειας.
- **Απλοποίηση** και κωδικοποίηση της νομοθεσίας γύρω από θέματα κυβερνοασφάλειας.
- **Δημιουργία** Εθνικού PPP (Public–Private Platform) για θέματα κυβερνοασφάλειας.

ΤΑΥΤΟΤΗΤΑ
-POLICY PAPER

Το policy paper **«Κυβερνοασφάλεια: Πώς θωρακίζουμε το ψηφιακό μέλλον της χώρας;»** συνοψίζει και εμβαθύνει στα βασικά συμπεράσματα της συζήτησης στρογγυλής τραπέζης που είχε διοργανώσει τον Μάρτιο του 2024 το Center for Cyber Resilience του Οικονομικού Φόρουμ των Δελφών, σε συνεργασία με τον ΕΛΙΑΜΕΠ και με την υποστήριξη της Vodafone Ελλάδας.

Στη συζήτηση στρογγυλής τραπέζης συμμετείχαν οι: Μιχάλης Χρυσοχοΐδης – υπουργός Προστασίας του Πολίτη, Δημήτριος Παπαστεργίου – υπουργός Ψηφιακής Διακυβέρνησης, Δημοσθένης Αναγνωστόπουλος – γενικός γραμματέας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης, Θεμιστοκλής Δεμίρης – διοικητής Εθνικής Υπηρεσίας Πληροφοριών, Βασίλειος Παπακώστας – διευθυντής Δίωξης Ηλεκτρονικού Εγκλήματος, Θωμάς Δομπρίδης – προϊστάμενος της Γενικής Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης, Ιωάννης Πανολίας – διευθυντής Στρατηγικού Σχεδιασμού / Εθνική Αρχή Κυβερνοασφάλειας, Θάνος Ντόκος – σύμβουλος Εθνικής Ασφάλειας του πρωθυπουργού, Σπύρος Παπαγεωργίου – διευθυντής Κυβερνοάμυνας (ΔΙΚΥΒ/ΓΕΕΘΑ) / Υπουργείο Εθνικής Άμυνας, Παρασκευή Δραμαλιώτη – γενική Γραμματέας Συντονισμού, Δημοσθένης Οικονόμου – επικεφαλής Τμ. Ασφάλειας Πληροφοριών και Προστασίας Δεδομένων (ENISA), Στέλλα Τσίτσουλα – πρόεδρος Ελληνικού Ινστιτούτου Κυβερνοασφάλειας, Φαίη Μακαντάση – διευθύντρια Ερευνών / διαΝΕΟσις, Στέφανος Ζήσης – ICT Risk & Cybersecurity Audit and Supervision / Τράπεζα της Ελλάδος, Παναγιώτης Παπαγιαννακόπουλος – εταίρος, αναπληρωτής επικεφαλής υπηρεσιών κυβερνοασφάλειας της EY στην περιοχή της Κεντρικής, Ανατολικής, Νοτιοανατολικής Ευρώπης και Κεντρικής Ασίας (CESA), Χρήστος Βιδάκης – εταίρος, cyber leader / Deloitte, Νίκος Δημάκος – εταίρος & head of Consulting / KPMG, Βασίλειος Κουτεντάκης – ανώτερος γενικός διευθυντής / Τράπεζα Πειραιώς, Νίκος Γιαννακάκης – γενικός διευθυντής Πληροφορικής Motor Oil, Γεωργία Αναστασίου – Cyber & Information Security director / ΟΠΑΠ, Καρώνης Άγγελος – Information Security Senior manager / Kaizen Gaming (Stoiximan/Betano), Δημήτριος Γιάντσης – γενικός διευθυντής Έργων / Κ.Τ.Π. Μ.Α.Ε., Μιχάλης Κασιμιώτης – διευθύνων σύμβουλος / Hewlett Packard Enterprise Ελλάδος και Κύπρου, Δημήτριος Πατσός – Senior Cuber Security specialist / Microsoft, Χρήστος Κοντέλλης – γενικός διευθυντής Ιδιωτικού Τομέα / Netcompany–Intrasoft, Αντώνης Τζωρτζακάκης – διευθύνων σύμβουλος / 5G Συμμετοχές Α.Ε. και επενδυτικού ταμείου Φαιστός, Ευγενία Μπόζου – επικεφαλής Κυβερνητικών Υποθέσεων και Δημόσιας Πολιτικής Google Ελλάδας, Κύπρου, Μάλτας, Δημήτριος Γκρίτζαλης – καθηγητής Κυβερνοασφάλειας στο Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών, Στέφανος Γκρίτζαλης – καθηγητής Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, διευθυντής του Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο και Τεχνολογίες, Πληροφορικής και Επικοινωνιών» (MSc in Law and ICT), Λίλιαν Μήτρου – πρόεδρος Ινστιτούτου για το Δίκαιο Προστασίας της Ιδιωτικότητας, των Προσωπικών Δεδομένων και την Τεχνολογία & καθηγήτρια στο Πανεπιστήμιο Αιγαίου, Κώστας Πατσάκης – αναπληρωτής καθηγητής, Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς, Γιάννης Θωμάτος – διευθύνων σύμβουλος στην Εταιρεία Δημοσίων Σχέσεων και Επικοινωνίας Tsomokos, Χάρης Μπρουμίδης – πρόεδρος και διευθύνων σύμβουλος Vodafone Ελλάδας, Στράτος Φαναράς – πρόεδρος και διευθύνων σύμβουλος της Metron Analysis S.A., Τριαντάφυλλος Καρατράντος – κύριος ερευνητής του ΕΛΙΑΜΕΠ (θεματικές: ριζοσπαστικοποίηση, τρομοκρατία, μοντέλα αστυνόμευσης, ασφάλεια και εξωτερική πολιτική), Απόστολος Μαγγηριάδης – παρουσιαστής ειδήσεων, δημοσιογράφος, Μαρία Σκάγκου – διευθύντρια Νομικών και Κανονιστικών Θεμάτων, Εταιρικής Ασφάλειας & Εταιρικών Σχέσεων Vodafone Ελλάδας.

Το policy paper επιμελήθηκε ο Δρ Τριαντάφυλλος Καρατράντος, κύριος ερευνητής του ΕΛΙΑΜΕΠ, και υποστηρίχθηκε από Ομάδα Έργου αποτελούμενη από τη Δρ Ελένη Καψοκόλη, υποψήφια μεταδιδάκτωρ του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς, και την Ξένια Σταμάτη.

ΟΜΑΔΑ ΕΡΓΟΥ ΕΛΙΑΜΕΠ

Δρ ΤΡΙΑΝΤΑΦΥΛΛΟΣ ΚΑΡΑΤΡΑΝΤΟΣ, συντονιστής Ομάδας Έργου

Είναι διδάκτωρ Ευρωπαϊκής Ασφάλειας και Νέων Απειλών του Πανεπιστημίου Αιγαίου. Είναι κύριος ερευνητής σε ζητήματα ριζοσπαστικοποίησης, τρομοκρατίας, μοντέλων αστυνόμευσης, ασφάλειας και εξωτερικής πολιτικής στο Ελληνικό Ίδρυμα Ευρωπαϊκής και Εξωτερικής Πολιτικής (ΕΛΙΑΜΕΠ). Τον Σεπτέμβριο του 2021, με απόφαση της Ευρωπαϊκής Επιτροπής, ορίστηκε μέλος της Συμβουλευτικής Ομάδας Ερευνητών Υψηλού Επιπέδου (Advisory Board of Researchers) για την έρευνα και την εξέλιξη της πολιτικής ως προς την πρόληψη της ριζοσπαστικοποίησης και την αντιμετώπιση του βίαιου εξτρεμισμού. Από τον Σεπτέμβριο του 2023 έχει οριστεί εθνικός εκπρόσωπος στο High Level Risk Forum του ΟΟΣΑ. Τον Ιούλιο του 2019 μέχρι τον Αύγουστο του 2021 διετέλεσε σύμβουλος Πολιτικής Ασφάλειας του Υπουργού Προστασίας του Πολίτη, ενώ από τον Σεπτέμβριο του 2021 είναι σύμβουλος Πολιτικών Ασφάλειας του υπουργού Επικρατείας.

Δρ ΕΛΕΝΗ ΚΑΨΟΚΟΛΗ, μέλος Ομάδας Έργου

Η Ελένη Καψοκόλη είναι υποψήφια μεταδιδάκτωρ του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς. Το 2022 ολοκλήρωσε τη διδακτορική της διατριβή σχετικά με την ισλαμική τρομοκρατία στον κυβερνοχώρο από το ίδιο τμήμα. Είναι πτυχιούχος Πολιτικών Επιστημών και Δημόσιας Διοίκησης από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, και κάτοχος μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις και Στρατηγικές Σπουδές από το Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών. Είναι απόφοιτη της Διδακτορικής Σχολής του Ευρωπαϊκού Κολλεγίου Ασφάλειας και Άμυνας, και ερευνήτρια στο Εργαστήριο Πληροφόρησης και Κυβερνοασφάλειας του Τμήματος Διεθνών & Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς.

ΞΕΝΙΑ ΣΤΑΜΑΤΗ, μέλος Ομάδας Έργου

Η Ξένια Σταμάτη είναι πτυχιούχος Διεθνών, Ευρωπαϊκών και Περιφερειακών Σπουδών, του Παντείου Πανεπιστημίου, και κάτοχος μεταπτυχιακού διπλώματος στη Διεθνή και Ευρωπαϊκή Διακυβέρνηση και Πολιτική από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. Εργάζεται στον ιδιωτικό τομέα με εξειδίκευση στη διαχείριση έργων, χρησιμοποιώντας εργαλεία όπως το Jira και το Confluence. Τον τελευταίο χρόνο εργάζεται στην Alpha Bank, ως Project & Facilities Manager των 4.500 ακινήτων της. Έχει άριστες γνώσεις αγγλικών και γαλλικών, αλλά και γνώσεις ισπανικών και κινεζικών.

DELPHI ECONOMIC FORUM

CENTER FOR CYBER RESILIENCE

ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ:
Αμερικής 21
Αθήνα 106 72
+30 210 7289000
info@delphiforum.gr

FOLLOW US:
Facebook: /delphiforum
TikTok: /delphieconomicforum
Instagram: /delphieconomicforum.
Linkedin: /delphi-economic-forum

ΓΙΑ ΕΓΓΡΑΦΗ ΣΤΟ NEWSLETTER:
www.delphiforum.gr

OFFICIAL HASHTAG:
#delphiforum