Περιεχόμενα

Αντί προλόγου

Όταν ξεκίνησα την επιμέλεια αυτού του βιβλίου, δίδασκα ήδη τέσσερα χρόνια το μάθημα «Κανονιστικό Πλαίσιο Ασφάλειας Επικοινωνιών και Πληροφοριών» στο πέμπτο έτος προπτυχιακών σπουδών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής, καθώς και μεταπτυχιακά μαθήματα της γνωστικής περιοχής της *κυβερνοασφάλειας* σε άλλα πανεπιστήμια της ημεδαπής για οκτώ χρόνια. Αποφάσισα να επιμεληθώ το βιβλίο του καθηγητή Amos N. Guiora αφενός για να υποστηρίξω τη διδασκαλία ενός μέρους αυτών των μαθημάτων με ελληνική βιβλιογραφία που δεν αναφέρεται σε τεχνικά θέματα και αφετέρου για να δοθεί η δυνατότητα σε ακροατήρια πέραν εκείνων των Τμημάτων Μηχανικών ή Πληροφορικής να προσεγγίσουν τα θέματα αυτής της γνωστικής περιοχής από μια εξαιρετικά ενδιαφέρουσα σκοπιά. Στην ερώτηση *Τι πραγματεύεται αυτό το βιβλίο*, ατάκτως θα απαντούσα ως εξής: Η επιστήμη και η τεχνολογία, ως γεννήματα της κοινωνικής εξέλιξης, επιδρούν καθοριστικά στις ισορροπίες της παγκόσμιας σφαίρας αλλά δεν μπορούν να αναπτύσσονται ανεπηρέαστες τόσο από σχέσεις διεκδίκησης (*δηλαδή* πολιτικής) όσο και από τα υλικά συμφέροντα που εξυπηρετούνται μέσω των κανόνων δικαίου. Στο πλαίσιο αυτό, το βιβλίο συζητά πώς η κυβερνοασφάλεια επηρεάζει τις σχέσεις μεταξύ κρατών, οικονομικών συμμαχιών και εταιρειών και πώς το πολιτικό και νομικό αυτό εποικοδόμημα ανατροφοδοτεί την εξέλιξη της κυβερνοα-

σφάλειας ως κλάδου των επιστημών. Σύμφωνα με τη ρήση του Benjamin Franklin, «όσοι θυσιάζουν στοιχειώδεις ελευθερίες για λίγη προσωρινή ασφάλεια δεν αξίζουν ούτε ελευθερία ούτε ασφάλεια». Θεώρησα, λοιπόν, σκόπιμο να αναδειχθούν κάποιες πτυχές αυτής της φράσης μέσα από τις γραμμές του βιβλίου.

Παρότι, στην πάροδο των χρόνων, ο όρος *κυβερνοχώρος* έχει χρησιμοποιηθεί κατ' επανάληψη από επίσημα κείμενα επιστημονικών φορέων, καθώς και διακρατικών ανακοινώσεων και συμφωνιών, δεν υπάρχει ενιαία, καθολική περιγραφή του. Ενδεικτικά ως προς τη χρήση του όρου, να αναφέρουμε την έκδοση της Διεθνούς Ένωσης για τις Τηλεπικοινωνίες (International Telecommunication Union – ITU) για το φαινόμενο του κυβερνοεγκλήματος,[1] το πρότυπο οδηγιών ISO/SEC 27032 του Διεθνούς Οργανισμού Προτύπων (International Standards Organisation – ISO) για την κυβερνοασφάλεια,[2] την Απόφαση 2010/18 του Οργανισμού Ηνωμένων Εθνών για την πρόβλεψη του εγκλήματος και την απονομή δικαιοσύνης,[3] το κείμενο προτάσεων της ομάδας εργασίας Cyber Security Coordination Group (CSCG) προς την Ευρωπαϊκή Επιτροπή σχετικά με τη στρατηγική της κυβερνοασφάλειας,[4] τη Σύμβαση για το Έγκλη-

1. International Telecommunication Union – ITU (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Telecommunication Development Sector of ITU-T.

http://handle.itu.int/11.1002/pub/80c0b5e9-en

2. International Standards Organisation – ISO (2012). *Information technology – Security techniques – Guidelines for cybersecurity*.

https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

3. United Nations – UN (2010). *Resolution 2010/18 on on Crime Prevention and Criminal Justice*.

https://www.un.org/en/ecosoc/docs/2010/res%202010-18.pdf

4. CEN/CENELEC/ETSI Cyber Security Coordination Group – CSCG. (2014). *Recommendations for a Strategy on European Cyber Security Standardisation*. http://kigeit.org.pl/FTP/PRCIP/Literatura/079_CEN-CENELEC-ENSI-White_paper-Strategy_european_cybersecurity_standardisation.pdf

μα στον κυβερνοχώρο, γνωστή και ως Σύμβαση της Βουδαπέστης[5] κ.ά. Η μελέτη αυτών των κειμένων οδηγεί στη σύγκλιση ότι ο κυβερνοχώρος είναι *ο σύνθετος χώρος ο οποίος προκύπτει από τη διασύνδεση και διάδραση υπολογιστών, δικτύων, συστημάτων, πληροφοριών, λογισμικού, υπηρεσιών, ανθρώπων και εικονικών οντοτήτων στο Διαδίκτυο*. Για τον ορισμό της ασφάλειας στον κυβερνοχώρο ή, διαφορετικά, της κυβερνοασφάλειας, επίσης δεν έχει υιοθετηθεί μια ενιαία διατύπωση. Για λόγους απλότητας, υιοθετούμε τη διατύπωση από το κείμενο του Κανονισμού (ΕΕ) 2019/881: «Κυβερνοασφάλεια: οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων».

Για να διαπιστώσουμε ποιους αφορά η κυβερνοασφάλεια, αρκεί να αναλογιστούμε ότι το 1996 μόνο το 1% του παγκόσμιου πληθυσμού είχε πρόσβαση στις υπηρεσίες του Διαδικτύου, ενώ στις αρχές του 2023 το ποσοστό ήδη ανέρχεται στο 64%. Δεν αναφερόμαστε μόνο στους χρήστες κοινωνικών δικτύων (Facebook, Instagram, TikTok, WeChat, SnapChat, Twitter, Telegram κ.ά), οι οποίοι αριθμούν περίπου το 60% του πληθυσμού, αλλά και στα συστήματα εκείνα –που αποκαλούνται Κρίσιμες Υποδομές[6]– τα οποία υποστηρίζουν τις ανθρώπινες κοινωνίες (ενέργεια, τηλεπικοινωνίες, μεταφορές, οικονομία, υγεία, βιομηχανία, υδάτινοι πόροι κ.ά). Εντούτοις, η ανάγκη ανάπτυξης κοινών νορμών για την αντιμετώπιση των περιστατικών στον κυβερνοχώρο συγκρούεται με την ύπαρξη πολλαπλών *ενδιαφερόμενων μερών* (stakeholders / non-state actors), τα οποία λειτουργούν αντίθετα με τις εκφρασμένες αποφάσεις του πλειοψηφικού μέρους των κοινωνιών. Είναι βέβαιο ότι τα ενδιαφερό-

5. Council of Europe (2001). *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

6. *Δείτε επίσης* Ευρωπαϊκή Οδηγία 2008/114/ΕΚ και Προεδρικό Διάταγμα 39/2001 (ΦΕΚ 104/Α/2011).

μενα μέρη δεν πράττουν από αυθορμητισμό ή αυταρέσκεια, αλλά πάνω στις ράγες των στρατηγικών επιλογών τους.

Για να φέρουμε στο προσκήνιο ένα παράδειγμα, να θυμηθούμε το πρώτο περιστατικό επίθεσης με την ονομασία *Logic Bomb*, στο μακρινό 1982, και την ανατίναξη ενός αγωγού φυσικού αερίου στη Σιβηρία. Μεσούντος του Ψυχρού Πολέμου, η ΕΣΣΔ προμηθεύεται από τον Καναδά ένα πρόγραμμα υπολογιστή (λογισμικό) για τον έλεγχο και τη διαχείριση των υποδομών της. Η αμερικανική υπηρεσία πληροφοριών CIA έχει φροντίσει να μετατρέψει το λογισμικό αυτό σε κακόβουλο λογισμικό τύπου *δούρειου ίππου* (trojan horse), με αποτέλεσμα την καταστροφή του αγωγού αερίου. Δεν έχει σημασία να αναλύσουμε εδώ αν νόμιμα οι ΗΠΑ και η ΕΣΣΔ προέβαιναν σε εκατέρωθεν πράξεις που θα μπορούσαν να οδηγήσουν σε σύρραξη. Εξάλλου, μια ίδιου τύπου επίθεση ήταν εκείνη που αποκαλύφθηκε το 2010, η οποία πήρε την ονομασία Stuxnet και απείλησε τις πυρηνικές υποδομές του Ιράν με άγνωστες, τότε, συνέπειες. Αυτό που έχει μείζονα σημασία είναι η αναδυόμενη σχέση της γεωπολιτικής με τον κυβερνοχώρο και ο τρόπος τον οποίο θα επιλέξουν οι κοινωνίες προκειμένου να παραμείνουν ασφαλείς τόσο στο επίπεδο των πληροφοριακών συστημάτων, και εν γένει των υποδομών, όσο και σε εκείνο των ανθρώπινων ζωών. Όπως ορθά συμπεραίνουν οι E. Tikk και M. Kerttunen,[7] η ανάγκη για την ανάπτυξη συλλογικής στρατηγικής για τα ζητήματα αυτά δεν μπορεί να περιορίζεται στο δίκαιο του ισχυρού ή σε συνομιλίες υπό την επαπειλούμενη συνθήκη *jus in bello*.[8]

Μολονότι η συμβολή των κυβερνοπεριστατικών στα πεδία των στρατιωτικών επιχειρήσεων και της κατασκοπείας πάντα

7. Tikk, E. and Kerttunen, M. (eds) (2020). *Routledge Handbook of International Cybersecurity*. Abingdon, Oxon: Routledge.

8. Ένα παράδειγμα τέτοιας συνθήκης είναι το Διεθνές Ανθρωπιστικό Δίκαιο, που αφορά τη συμπεριφορά των εμπλεκόμενων μερών σε μια ένοπλη σύρραξη.

κατέχει τη μερίδα του λέοντος επί των θεμάτων του δημόσιου διαλόγου, τα περιστατικά αυτά έχουν σημαντικό μέρισμα στις δραστηριότητες της εφοδιαστικής αλυσίδας, στη λειτουργία των νοσοκομειακών μονάδων, στη διάχυση πληροφοριών για την ενημέρωση ομάδων πολιτών, αλλά και στις συλλογικές διεργασίες των κοινοβουλίων παγκοσμίως. Δεν επιλέγουμε τυχαία ούτε την αναφορά σε αυτά τα πεδία ούτε τη χρονική περίοδο της πανδημίας COVID-19, εντός της οποίας καταγράφονται περιστατικά που πλήττουν τις δραστηριότητες εφοδιασμού φαρμάκων, εμβολίων και ατομικού προστατευτικού εξοπλισμού, καθώς και τη λειτουργία πληροφοριακών συστημάτων τα οποία αναλαμβάνουν την ανάλυση δεδομένων νόσησης του γενικού πληθυσμού και συμβάλλουν στην επιστημονική έρευνα ομάδων ιατρών, βιολόγων και μηχανικών. Τα μέσα δελεασμού που χρησιμοποιούνται στα κυβερνοπεριστατικά παραλλάσσονται ανάλογα με το στάδιο της πανδημίας και εντοπίζονται στην εκμετάλλευση ατόμων που αναζητούν πληροφορίες για την παρακολούθηση και τη θεραπεία ασθενών, στην αντιποίηση ιατρικών φορέων, όπως του Παγκόσμιου Οργανισμού Υγείας και των αμερικανικών Κέντρων Ελέγχου και Πρόληψης Νοσημάτων (Centers for Disease Control and Prevention – CDC), καθώς και σε κυβερνητικά πακέτα οικονομικής βοήθειας. Σε ό,τι αφορά την ύπαρξη παραπληροφόρησης (misinformation) και δυσφήμισης (disinformation), τα περιστατικά κυβερνοεπιθέσεων καταγράφονται επίσης αυξημένα κατά την πανδημική περίοδο με στόχο τη δημιουργία εντυπώσεων και τάσεων στην κοινή γνώμη, οι οποίες θα λέγαμε με σχετική βεβαιότητα ότι έφτασαν σε σημείο να πλήττουν σημαντικά την εμπιστοσύνη των πολιτών για τις επιστήμες. Το φαινόμενο «ηχώ θαλάμου» (echo chamber) γιγαντώνεται την ίδια περίοδο και επικουρεί στη διασπορά δογματικών, αντιεπιστημονικών και ρατσιστικών απόψεων, οι οποίες ανοίγουν πλατύ δρόμο στην εκλογική άνοδο φασιστικών και φονταμενταλιστικών κομμάτων στην Ευρώπη και παγκοσμίως.

Όπως σημειώνει ο K. Okereafor,[9] ανθρώπινα χαρακτηριστικά, όπως η ευσπλαχνία, η πειστικότητα, η απελπισία και η σύγχυση, η τιμιότητα, ο σεβασμός, ο θυμός και η θλίψη, χρησιμοποιούνται κατά κόρον ως μέσα χειραγώγησης και, τελικά, ως εφαλτήρια κυβερνοεπιθέσεων. Στην ίδια περίοδο, χαρακτηριστικό παράδειγμα κυβερνοεπίθεσης που οδήγησε σε απώλεια ανθρώπινης ζωής είναι εκείνο στο πανεπιστημιακό νοσοκομείο του Ντίσελντορφ, τον Σεπτέμβριο του 2020, ύστερα από επίθεση τύπου *λυτρισμικού* (ransomware), με τα πληροφοριακά συστήματα σταδιακά να παραλύουν και το νοσοκομείο να ανακοινώνει ότι δεν μπορεί να δεχτεί νέους ασθενείς στο τμήμα επειγόντων περιστατικών. Έτσι, όταν κάποιος ασθενής μεταφέρεται σε άλλο νοσοκομείο, σε απόσταση πολλών χιλιομέτρων, το απευκταίο δεν μπορεί να αποτραπεί. Για να κλείσουμε την παρένθεση της περιόδου COVID-19 και παρότι δεν είναι καινοφανείς οι κυβερνοεπιθέσεις που έχουν στόχο την παρέμβαση στις δημοκρατικές διαδικασίες κρατών παγκοσμίως (ας θυμηθούμε τον ρόλο των εταιρειών Facebook και Cambridge Analytica[10] στο δημοψήφισμα για το Brexit), να αναφέρουμε τα περιστατικά[11] που εμπλέκουν τη Λευκορωσία, τη Λετονία, τη Λιθουανία, την Πολωνία και το ΝΑΤΟ τον Σεπτέμβριο του 2021, καθώς και τις γαλλικές και τις γερμανικές προεδρικές εκλογές την ίδια περίοδο.

Κλείνοντας, επιλέγω να αναφέρω την εκτεταμένη συζήτηση που διεξάγεται στο βιβλίο σχετικά με την αναλογία συμβατικού πολέμου και κυβερνοπολέμου. Ο καθηγητής Amos N. Guiora

9. Okereafor, K. (2021). *Cybersecurity in the COVID-19 Pandemic*. Abingdon, Oxon: CRC Press.

10. European Union Agency for Cybersecurity – ENISA (2018). *The Value of Personal Online Data*.

https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data

11. European Union Agency for Cybersecurity – ENISA (2022). *Cybersecurity Threat Landscape 2022*.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

λαμβάνει υπόψη τον Καταστατικό Χάρτη των Ηνωμένων Εθνών, και συγκεκριμένα το άρθρο 51 αναφορικά με το δικαίωμα των κρατών στη νόμιμη άμυνα, και συμπεραίνει ότι, παρότι κάποια κυβερνοεπίθεση μπορεί να καταστρέψει υποδομές και να οδηγήσει σε απώλεια ανθρώπινων ζωών, η ένοπλη απάντηση (*jus ad bellum*) δεν αποτελεί ανάλογο και νόμιμο μέσο εκ μέρους του αμυνόμενου έως ότου το Συμβούλιο Ασφαλείας να αποφασίσει για την αποκατάσταση της διεθνούς ειρήνης και ασφάλειας. Παρότι συμφωνώ με αυτό το συμπέρασμα, έχοντας κατά νου τον διεθνή συσχετισμό δυνάμεων, διατηρώ επιφυλάξεις σχετικά με την ανάγκη που διατυπώνει ο συγγραφέας για τη διαμόρφωση κοινής, παγκόσμιας στρατηγικής σε αυτά τα ζητήματα, καθώς δεν λαμβάνει υπόψη του την εμπειρία των χωρών του *Οργανισμού Συνεργασίας της Σαγκάης* και τα συμπεράσματά τους από την ιστορική περίοδο των σοσιαλιστικών δημοκρατιών. Εξάλλου, όπως συζητούν οι S. Abaimov και M. Martellini[12] προς ένα ανάλογο συμπέρασμα, το *Εγχειρίδιο του Ταλίν*,[13] η *Σύμβαση της Βουδαπέστης*, άλλες αποφάσεις και κείμενα συμπερασμάτων στο πλαίσιο του ΟΗΕ, καθώς και εκτός αυτού, πρέπει να ληφθούν υπόψη για τη συγκρότηση παγκόσμιας στρατηγικής στο πεδίο του κυβερνοπολέμου και της κυβερνοασφάλειας.

Η παρουσία της Μάτας, στην ολότητά της, με την αβασάνιστη επιρροή και την άνευ ορίων έμπνευση, ήταν που με όπλισε με την επιμονή και τη δύναμη που χρειαζόμουν για αυτό το βιβλίο. Της το αφιερώνω, εκ βαθέων.

Δημήτριος Ν. Καλλέργης
Πειραιάς, Ιούνιος 2023

---

12. Abaimov, S. and Martellini, M. (2017). *Cyber Arms: Security in Cyberspace*. Boca Raton: CRC Press.

13. NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE (2021). *Tallinn Manual on the International Law*.
https://ccdcoe.org/research/tallinn-manual/