Κείμενο εργασίας No.2

Ιούνιος 2020

Η επίδραση των κυβερνοεπιθέσεων στη μετεξέλιξη της κυβερνοασφάλειας: Η περιπτωσιολογική μελέτη της Εσθονίας

Συγγραφείς: Δέσποινα Βλάχου, Μαρία Ζαμπατή και Χριστίνα Κοντραφούρη

Επιστημονική Επιμέλεια: Α. Λιαρόπουλος


Laboratory of
Intelligence &
Cyber-Security

Εργαστήρι Πληροφόρησης και Κυβερνοασφάλειας

Το *Εργαστήρι Πληροφόρησης και Κυβερνοασφάλειας* ιδρύθηκε το 2015 και σκοπός του είναι η ανάλυση των προκλήσεων ασφάλειας που αφορούν τις έννοιες της πληροφόρησης και του κυβερνοχώρου. Αντικείμενα έρευνας του εργαστηρίου αποτελούν μεταξύ άλλων: η λειτουργία των υπηρεσιών πληροφοριών, η αναδιάρθρωση των υπηρεσιών πληροφοριών, η σχέση πληροφόρησης και ηθικής, η οικονομική κατασκοπεία, η επίβλεψη του έργου των υπηρεσιών πληροφοριών και υπηρεσιών ασφαλείας και η διακυβέρνηση του κυβερνοχώρου.

Οι Συγγραφείς

Η Δέσποινα Βλάχου είναι απόφοιτος του τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς και δόκιμη ερευνήτρια στο Εργαστήρι Πληροφόρησης και Κυβερνοασφάλειας.
Επικοινωνία: dspvlachou@gmail.com

Η Μαρία Ζαμπατή είναι απόφοιτος του τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς και δόκιμη ερευνήτρια στο Εργαστήρι Πληροφόρησης και Κυβερνοασφάλειας.
Επικοινωνία: mariazabati@gmail.com

Η Χριστίνα Κοντραφούρη είναι απόφοιτος του τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς και δόκιμη ερευνήτρια στο Εργαστήρι Πληροφόρησης και Κυβερνοασφάλειας.
Επικοινωνία: christina.kontrafouri@gmail.com

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Ο κυβερνοχώρος έχει αναγνωριστεί ως ο πέμπτος τομέας των πολεμικών επιχειρήσεων μετά την ξηρά, τον αέρα, τη θάλασσα και το διάστημα, με τη διαφορά ότι είναι ο μόνος που έχει δημιουργηθεί εξ' ολοκλήρου από τον άνθρωπο. Η αδιάκοπη εξάρτηση των ανθρώπινων δραστηριοτήτων από τις υποδομές πληροφοριών εγείρει το ζήτημα της ασφάλειας. Οι πιο επιζήμιες επιθέσεις στον κυβερνοχώρο είναι εκείνες κατά των κρίσιμων υποδομών και των πληροφοριακών συστημάτων ενός κράτους. Η παρούσα ερευνητική εργασία εξετάζει τις κυβερνοεπιθέσεις που έλαβαν χώρα το 2007 στην Εσθονία με σκοπό να αναδείξει την επίδραση τους στην μετεξέλιξη της κυβερνοασφάλειας. Αποτελεί την πρώτη ιστορικά, περίπτωση κυβερνοεπίθεσης εναντίον ενός κυρίαρχου κράτους, η οποία μάλιστα κατέδειξε το πρόβλημα απόδοσης ευθύνης και την ανεπάρκεια του Διεθνούς Δικαίου στον τομέα της κυβερνοασφάλειας. Για τη διερεύνηση του ζητήματος θα αναλυθούν παρακάτω τα μέτρα που έχουν ληφθεί και οι στρατηγικές που έχουν υιοθετηθεί τόσο σε κρατικό όσο και σε θεσμικό επίπεδο. Τέλος, θα παρατεθεί μία συγκριτική ανάλυση Ευρωπαϊκής Ένωσης (ΕΕ) και Βορειοατλαντικής Συμμαχίας (ΝΑΤΟ) αναφορικά με τις δυνατότητες των δύο οργανισμών στον τομέα αυτό.

1. Εισαγωγή

Η ραγδαία εξέλιξη της τεχνολογίας σε συνδυασμό με την αυξανόμενη εξάρτηση των ανθρωπίνων δραστηριοτήτων από τα επικοινωνιακά και πληροφοριακά δίκτυα έχουν καταστήσει αναγκαία την επεξήγηση του κυβερνοχώρου. Ο Δρ. Daniel Kuehl ορίζει τον κυβερνοχώρο ως: *έναν παγκόσμιο τομέα μέσα στο πληροφοριακό περιβάλλον του οποίου ο ιδιαίτερος και μοναδικός χαρακτήρας πλαισιώνεται από την χρήση ηλεκτρονικών και του ηλεκτρομαγνητικού φάσματος για να δημιουργήσει, αποθηκεύσει, μετατρέψει, ανταλλάξει και εκμεταλλευτεί πληροφορίες μέσω ανεξάρτητων και αλληλένδετων δικτύων κάνοντας χρήση πληροφοριακών-επικοινωνιακών τεχνολογιών*[1].
Ο κυβερνοχώρος δεν αποτελεί μέρος της φύσης σε αντίθεση με την ξηρά, την θάλασσα, τον αέρα και το διάστημα. Όμως επειδή προϋποθέτει φυσικές υποδομές και μέσα[2], μία ενέργεια στον κυβερνοχώρο μπορεί να έχει επιπτώσεις στον πραγματικό κόσμο, καθώς μπορεί να πλήξει τις υποδομές αυτές και τις δραστηριότητες που διενεργούνται μέσω αυτών. Ενδεικτικά, η περίπτωση του Stuxnet[3] ανέδειξε ότι μια κυβερνοεπίθεση, θα μπορούσε να οδηγήσει σε φυσική καταστροφή. Ο κυβερνοχώρος αποτελεί έναν αχανή χώρο χωρίς σύνορα, στον οποίο ο αποτελεσματικός έλεγχος είναι αδύνατος, καθώς τα κράτη έχουν να αντιμετωπίσουν ποικίλα τεχνικά και πολιτικά ζητήματα λόγω της έλλειψης εδαφικής κυριαρχίας και τάξης σε αυτόν[4]. Το γεγονός αυτό προκαλεί ανασφάλεια και καθιστά ευάλωτα τα κράτη.

2. Οι κυβερνοεπιθέσεις κατά της Εσθονίας το 2007

Μετά την κατάρρευση της Σοβιετικής Ένωσης και την ανεξαρτητοποίηση της Εσθονίας το 1991, η τελευταία για να αντισταθμίσει την ανεπάρκεια της σε φυσικούς πόρους αποφάσισε να δώσει έμφαση στην πληροφοριακή της υποδομή[5]. Ενδεικτικά, το 1997 θεσπίστηκε το σύστημα της ηλεκτρονικής διακυβέρνησης και το 2000

---

[1] Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, Edited by Starr S.H., Wentz L.K. Kramer F.D, 25. University of Nebraska Press, Potomac Books. 2009. Accessed October 14, 2019 https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

[2] Liaropoulos, Andrew. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?" Edited by Douglas Hart. *8th International Conference on Information Warfare and Security.* Denver, Colorado: Regis University, 2013: 138.

[3] Το Stuxnet αποτελεί ένα λογισμικό σχεδιασμένο να διεισδύει σε απομακρυσμένα συστήματα και να αποκτά έλεγχο αυτών, με ημιαυτόνομο τρόπο. Εκπροσωπεί μία νέα γενιά κακόβουλου λογισμικού το οποίο μπορεί να δρα εναντίον επιλεγμένων στόχων στον κυβερνοχώρο. Οι στόχοι του Stuxnet δεν ήταν συνδεδεμένοι στο δημόσιο διαδίκτυο και η διείσδυση προϋπέθετε τη χρήση ενδιάμεσων συσκευών, όπως στικάκια USB, για την απόκτηση της πρόσβασης και του ελέγχου. Η πρώτη του χρήση συνέβη κατά τη διάρκεια της Επιχείρησης «Ολυμπιακοί Αγώνες» εναντίον των πυρηνικών βάσεων του Ιράν το 2010 (βλ. Farwell, James P., and Rohozinski, Rafal. "Stuxnet and the Future of Cyber War." In *Survival: Global Politics and Strategy* 53, no. 1 (2011): 24 και Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." The New York Times, June 1, 2012. Accessed October 14, 2019. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html).

[4] Liaropoulos, Andrew. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?" Edited by Douglas Hart. *8th International Conference on Information Warfare and Security.* Denver, Colorado: Regis University, 2013: 138

[5] Roonemaa, Mari. "Global Lessons from Estonia's tech-savvy Government." In *The UNESCO Courier*, 2017. Accessed October 14, 2019. https://en.unesco.org/courier/2017-april-june/global-lessons-estonia-s-tech-savvy-government

εισήχθη στην Εσθονία το σύστημα ηλεκτρονικής φορολόγησης. Το 2002 οι Εσθονοί πολίτες απέκτησαν ψηφιακές ταυτότητες, οι οποίες παρείχαν νομικά δεσμευτικές ψηφιακές υπογραφές και το 2005 ξεκίνησε η ηλεκτρονική ψηφοφορία στις δημοτικές εκλογές της Εσθονίας. Σήμερα, το 99% των δημόσιων υπηρεσιών παρέχονται ηλεκτρονικά και το 99% των τραπεζικών συναλλαγών διεξάγονται ηλεκτρονικά[6]. Όμως, αυτός ο όγκος ηλεκτρονικών υπηρεσιών έχει οδηγήσει στην υψηλή εξάρτηση από το διαδίκτυο. Οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ)[7] είναι σημαντικές για πολλές επιχειρήσεις καθώς και την εσθονική κυβέρνηση, γι' αυτό χρειάζονται συνεχή και αποτελεσματική προστασία[8].

Στις 26 Απριλίου του 2007, η εσθονική κυβέρνηση μετέφερε το άγαλμα του «Χάλκινου Στρατιώτη» στο στρατιωτικό νεκροταφείο του Ταλλίν. Το άγαλμα αυτό μνημόνευε τη σοβιετική απελευθέρωση της Εσθονίας από τους Ναζί αλλά για τους Εσθονούς συμβόλιζε την σοβιετική καταπίεση. Έτσι, προκλήθηκαν ταραχές στη ρωσική μειονότητα, καθώς θεωρήθηκε ότι η μετεγκατάσταση του, αντιπροσώπευε περεταίρω περιθωριοποίηση της εθνικής τους ταυτότητας, οδηγώντας σε διαδηλώσεις στους δρόμους του Ταλλίν[9]. Μετά τα γεγονότα αυτά, ακολούθησε μία σειρά κυβερνοεπιθέσεων, οι οποίες ξεκίνησαν στις 27 Απριλίου και διήρκεσαν έως τις 18 Μαΐου[10].

Οι κυβερνοεπιθέσεις χτύπησαν τις διαδικτυακές υποδομές της Εσθονίας και τα συστήματα πληροφόρησης, όπως τα DNS[11]. Επίσης, διατάραξαν την πρόσβαση σε διάφορες ιστοσελίδες και τις υπηρεσίες που αυτές προσφέρουν και επηρέασαν την λειτουργία των κυβερνητικών καναλιών λειτουργίας. Αναταραχές προκλήθηκαν μεταξύ των πολιτών, εφόσον πολλές σημαντικές δημόσιες υπηρεσίες ήταν διαθέσιμες μόνο διαδικτυακά, ενώ παράλληλα, παρακωλύθηκαν οι λειτουργίες πολλών τραπεζών και μικρών επιχειρήσεων[12]. Πλήθος ανεπιθύμητης αλληλογραφίας εστάλη από botnet[13]. Ο Εσθονός πρόεδρος, Toomas Hendrik Ilves, ενημερώθηκε ότι το πρόβλημα δεν οφειλόταν σε κάποια εσωτερική αποτυχία, αλλά ήταν μία επίθεση κατανεμημένης

---

[6] "We can built a digital society and so can you (About Us)." n.d. Accessed October 14, 2019. https://e-estonia.com/.

[7] Οι Τεχνολογίες Πληροφοριών και Επικοινωνιών (ICT) αναφέρονται σε τεχνολογίες που παρέχουν πρόσβαση στις πληροφορίες μέσω τηλεπικοινωνιών. Περιλαμβάνουν το υλικό, το λογισμικό, τα δίκτυα και τα μέσα που χρησιμοποιούνται για την συλλογή, αποθήκευση και επεξεργασία δεδομένων, κειμένου εικόνων και συναφών υπηρεσιών (UNHCR. "Glossary of ICT Terms and Equipment." In *UNHCR Manual Chapter 9: Handbook For Emergencies*. 2019. Accessed October 16, 2019. https://emergency.unhcr.org/entry/37435/glossary-of-ict-terms-and-equipment

[8] Cardash, Sharon L., Cilluffo, Frank J., and Ottis, Rain. "Estonia's Cyber Defence League: A Model for the United States?" In *Studies in Conflict and Terrorism* 36, no. 9 (2013): 778.

[9] McGuinness, Damien. "How a cyber attack transformed Estonia." Tallinn, BBC News, April 27, 2017. Accessed September 24, 2019. https://www.bbc.com/news/39655415

[10] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." NATO Cooperative Cyber Defence Centre of Excellence. n.d. Accessed November 21, 2019.

[11] Το Domain Name System (DNS) είναι ο τρόπος με τον οποίο ονόματα τομέα στο διαδίκτυο εντοπίζονται και μεταφράζονται σε διευθύνσεις Πρωτοκόλλου Διαδικτύου. [*SANS Institute*. n.d. Accessed September 24, 2019. https://www.sans.org/security-resources/glossary-of-terms/]

[12] Haataja, Samuli. "The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach." In *Law, Innovation and Technology* 9, no. 2 (2017): 160-161.

[13] Το botnet είναι ένα σύνολο υπολογιστών μολυσμένων από bots. Ένα bot είναι ένα κομμάτι κακόβουλου λογισμικού που λαμβάνει παραγγελίες από έναν «αρχηγό». Μόλις το κακόβουλο λογισμικό bot εισαχθεί σε έναν υπολογιστή, έχει πρόσβαση στους πόρους του υπολογιστή. Τα bots μπορούν στη συνέχεια να διαβάζουν και να γράφουν αρχεία, να εκτελούν προγράμματα, και γενικά να παρεμποδίζουν τον πραγματικό χρήστη από το να χρησιμοποιεί ο ίδιος τον υπολογιστή του. (Κουτσούκου, Ηλέκτρα., Μαρινοπούλου, Αναστασία., και Σπυριδάκης, Μάνος. *Κοινωνία του Κυβερνοχώρου.* Σιδέρης, 2018: 52).

άρνησης υπηρεσίας[14]-DDoS[15]. Ο Εσθονός πρωθυπουργός Andrus Ansip, απέδωσε τις κυβερνοεπιθέσεις στην Ρωσική Ομοσπονδία, εφόσον η πηγή πολλών από αυτές εντοπίστηκε σε ρωσικά IP[16].

Η απόδοση ευθύνης στις κυβερνοεπιθέσεις, ενέχει τεχνικά, νομικά και πολιτικά στοιχεία. Αναφορικά με τα πολιτικά στοιχεία πρέπει να εξετάζεται το πολιτικό κλίμα μέσα στο οποίο συμβαίνει η επίθεση και ποιος επωφελείται από αυτήν[17]. Η συγκεκριμένη απόδοση ευθύνης θεωρείται πολιτική. Η πολιτική απόδοση ευθύνης, προϋποθέτει την κατανόηση του γεωπολιτικού πλαισίου και των κινήτρων του επιτιθέμενου. Ωστόσο τα πολιτικά κίνητρα δεν είναι πάντοτε ξεκάθαρα. Οι μη κρατικοί δρώντες, που χρησιμοποιούνται για τις επιθέσεις συχνά κατευθύνονται και ελέγχονται από ορισμένα κράτη σε διάφορους βαθμούς. Για παράδειγμα, είναι δυνατόν μία κυβέρνηση να έχει γνώση των δραστηριοτήτων αυτών, επομένως και την ευθύνη για την παρεμπόδιση τους, ή άλλοτε συνειδητά να διατηρεί κάποια απόσταση προκειμένου να μην συσχετιστεί[18]. Η θέση των Εσθονών επομένως ενισχύθηκε από τις παρακάτω ενδείξεις.

Εκπρόσωποι της ρωσικής Δούμα[19] σε συζητήσεις που έλαβαν χώρα στην Εσθονία – διαμεσολαβούμενες από την προεδρία της ΕΕ – αρνήθηκαν κάθε εμπλοκή και μίλησαν για ψευδείς δηλώσεις[20]. Εκείνη την περίοδο πολλοί υψηλόβαθμοι πολιτικοί της Ρωσικής Ομοσπονδίας ακολουθούσαν μία επιθετική ρητορική αναφορικά με το άγαλμα. Ταυτόχρονα δεν υπάρχουν αποδείξεις, πως η Ρωσική Ομοσπονδία έλαβε μέτρα για την άμβλυνση των επιθέσεων, μετά τη γνωστοποίηση της κατάστασης. Η έλλειψη συνεργασίας της ρωσικής κυβέρνησης οδήγησε στο συμπέρασμα, πως δεν επιθυμούσε την ταυτοποίηση των επιτιθέμενων κι πιθανόν να προσπαθούσε να τους

[14] Το DoS (Denial of Service) είναι μία μορφή κυβερνοεγκλήματος, το οποίο, αν επιτύχει, αναγκάζει τον ιστότοπο-στόχο να σταματήσει τη λειτουργία του. Αυτό επιτυγχάνεται πλημμυρίζοντας τον στόχο με άχρηστα δεδομένα. Ως αποτέλεσμα, ο στόχος παρεμποδίζεται στην εξυπηρέτηση των κανονικών χρηστών του και αναγκάζεται να κλείσει. Το Distributed DoS (DDoS) είναι μία μορφή επίθεσης DoS στην οποία χρησιμοποιούνται πολλοί υπολογιστές που ζητούν ταυτόχρονη εξυπηρέτηση από τον ιστότοπο στόχο. Αυτοί οι υπολογιστές ανήκουν σε ένα botnet, το οποίο ο κυβερνοεγκληματίας, συνήθως, νοικιάζει από άλλο όμοιο του. (Κουτσούκου, Ηλέκτρα., Μαρινοπούλου, Αναστασία, και Σπυριδάκης, Μάνος. *Κοινωνία του Κυβερνοχώρου.* Σιδέρης, 2018: 53.)

[15] Tamkin, Emily. "10 Years After the Landmark Attack on Estonia. Is the World Better Prepared for Cyber Threats?" Foreign Policy, April 27, 2017. Accessed September 24, 2019. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

[16] Farrell, Michael D., and Tsagourias, Nicholas. "Cyber attribution technical and legal approaches and challenges." n.d. Accessed February 20, 2020. https://sites.tufts.edu/cilg/files/2018/09/attributiondraftsm.pdf

[17] Tsagourias, Nicholas. "Cyber attacks, self-defence and the problem of attribution." In *Journal of Conflict and Security Law* 17, no. 2 (July 24, 2012): 233-234. Oxford University Press. Accessed November 21, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538271

[18] Boudreaux, Benjamin, and Romanosky, Sasha. Working Paper: "Private Sector Attribution of Cyber Incidents:Benefits and Risks to the U.S. Government." Santa Monica: RAND Corporation. February 2019: 5. Accessed November 21, 2019. https://www.rand.org/content/dam/rand/pubs/working_papers/WR1200/WR1267/RAND_WR1267.pdf

[19] Η κρατική Δούμα αποτελεί ένα από τα δύο τμήματα της Ομοσπονδιακής Συνέλευσης, δηλαδή του ρωσικού κοινοβουλίου. Είναι μία νομοθετική αρχή που αποτελείται από 450 μέλη που εκλέγονται κάθε πέντε χρόνια. Το άλλο τμήμα της Συνέλευσης είναι το Ομοσπονδιακό Συμβούλιο. ("Status and Powers, Composition and Regulations of the State Duma." The State Duma. Accessed February 20, 2020. http://duma.gov.ru/en/duma/about/)

[20] Republic of Estonia Government. "Declaration of the Minister of Foreign Affairs of the Republic of Estonia." May 1, 2007. Accessed October 14, 2019. https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia

προστατεύσει[21].

Οι επιθέσεις ξεκίνησαν την ημέρα που ξεκίνησαν οι ανασκαφές, ενώ κορυφώθηκαν την 9η Μαΐου, η οποία είναι εθνική εορτή για τους Ρώσους εις μνήμην της νίκης τους επί των Ναζί. Τέλος, οι κυβερνοεπιθέσεις συνδυάστηκαν με μέτρα οικονομικής φύσεως, όπως την ακύρωση παραγγελιών από ρωσικές επιχειρήσεις και την παράταση των συνοριακών ελέγχων [22].

Η θεωρία του αντανακλαστικού ελέγχου (reflexive control theory) μπορεί να φανεί χρήσιμο εργαλείο στην ανάλυση αυτή, αν θεωρηθεί ότι αφορμή για τις κυβερνοεπιθέσεις αποτέλεσαν οι ρωσικές πολιτικές σκοπιμότητες. Ο αντανακλαστικός έλεγχος ορίζεται ως η διαδικασία μεταφοράς ειδικά προετοιμασμένων πληροφοριών σ' έναν σύμμαχο ή εχθρό, ώστε να ωθηθεί να λάβει εκουσίως την προκαθορισμένη απόφαση που επιθυμεί ο εισηγητής της πράξης[23]. Αν στην περίπτωση αυτή, ο εισηγητής της πράξης θεωρηθεί η Ρωσική Ομοσπονδία, τότε η επιθυμητή πράξη είναι η επανατοποθέτηση του μνημείου. Σύμφωνα με τον αρχιστράτηγο Ιονον, ο αντικειμενικός σκοπός του αντανακλαστικού ελέγχου είναι να εξαναγκάσεις τον εχθρό να λάβει αντικειμενικές αποφάσεις που οδηγούν στην ήττα του, με το να επηρεάσεις ή να ελέγξεις την διαδικασία λήψης αποφάσεων του[24]. Μία μέθοδος του είναι η πληροφοριακή υπερφόρτωση, η οποία δυσχεραίνει ή αποκλείει την πρόσβαση στα πληροφοριακά συστήματα και δίκτυα, όπως στη περίπτωση των επιθέσεων DDoS[25] στην Εσθονία. Ακόμη μία έκφανση της θεωρίας είναι η παράλυση κατά την οποία δημιουργείται η αίσθηση της απειλής ζωτικών συμφερόντων ή τρωτών σημείων[26]. Τα εξελιγμένα πληροφοριακά δίκτυα που χτυπήθηκαν, αποτελούν ένα από τα σημαντικότερα πλεονεκτήματα του εσθονικού κράτους. Ακόμη, οι οικονομικές συναλλαγές που διεξάγονται μέσω αυτών και είναι ζωτικής σημασίας για το κράτος, διεκόπησαν, προκαλώντας οικονομικές ζημίες.

Το γεγονός πως δεν υπάρχει επίσημη αποδοχή της ευθύνης από την Ρωσική Ομοσπονδία καθιστά δύσκολη την απόδοση ευθύνης για τις κυβερνοεπιθέσεις του 2007. Εάν τα κράτη δεν αποκτήσουν την ικανότητα να ταυτοποιούν τους δράστες πίσω από τις κυβερνοεπιθέσεις, κάθε ισχυρισμός για άσκηση κυριαρχίας στον

---

[21] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." NATO Cooperative Cyber Defence Centre of Excellence. n.d. Accessed November 21, 2019. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[22] NATO Strategic Communications Centre of Excellence. "2007 cyber attacks on Estonia." n.d.: 53, 56. Accessed November 22, 2019. https://www.stratcomcoe.org/download/file/fid/80772

[23] Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." In *Journal of Slavic Military Studies* 17, no. 2 (2004): 237. Accessed November 21, 2019. https://www.researchgate.net/publication/248945659_Russia's_Reflexive_Control_Theory_and_the_Military

[24] Ibid, 243.

[25] Jaitner, Margarita L., and Kantola, Harry. "Applying Principles of Reflexive Control in Information and Cyber Operations." Edited by L. Armistead. In *Journal of Information Warfare* 15, no. 4 (2016): 31. Accessed November 21, 2019. https://www.academia.edu/30684046/Applying_Principles_of_Reflexive_Control_in_Information_and_Cyber_Operations

[26] Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." In *Journal of Slavic Military Studies* 17, no. 2 (2004): 248. Accessed November 21, 2019. https://www.researchgate.net/publication/248945659_Russia's_Reflexive_Control_Theory_and_the_Military

κυβερνοχώρο θα είναι εύθραυστος[27].

3. Νομικό πλαίσιο και απόδοση ευθύνης

Η περίπτωση των κυβερνοεπιθέσεων κατά της Εσθονίας αναδεικνύει την δυσκολία απόδοσης ευθύνης στον κυβερνοχώρο, εξαιτίας της μη πρόβλεψης τέτοιων περιπτώσεων από το Διεθνές Δίκαιο. Σύμφωνα με το Άρθρο 2 (4) του Καταστατικού Χάρτη του ΟΗΕ, τονίζεται ότι όλα τα κράτη-μέλη αυτού: *«θα απέχουν από την απειλή ή τη χρήση* βίας*, που εκδηλώνεται εναντίον της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε κράτους είτε με οποιαδήποτε άλλη ενέργεια ασυμβίβαστη προς τους Σκοπούς των Ηνωμένων Εθνών»*[28].
Η αναφορά του άρθρου στην απειλή ή χρήση βίας, αποτελεί μία περιορισμένη αντίληψη αυτής, καθώς προϋποθέτει κάποια μορφή φυσικής καταστροφής περιουσίας, τραυματισμό ή θάνατο ανθρώπων. Κατ' επέκταση, οι κυβερνοεπιθέσεις που δεν έχουν ως αποτέλεσμα υλικές ζημίες, όπως αυτές εναντίον της Εσθονίας, δεν προβλέπονται στο άρθρο. Επομένως εγείρεται το ερώτημα εάν αυτές εμπίπτουν στην υπάρχουσα νομοθεσία και πιο συγκεκριμένα όταν δεν ισοδυναμούν μ' αυτό που είναι παραδοσιακά κατανοητό ως βία[29].
Στο ερώτημα που ανακύπτει αναφορικά με το πότε οι κυβερνοεπιθέσεις αποτελούν περίπτωση χρήσης βίας, το Διεθνές Δίκαιο είναι ελλιπές σ' αυτόν τον τομέα. Το Tallinn Manual προσφέρει ένα σημαντικό μη δεσμευτικό νομικό εργαλείο γι' αυτό το ζήτημα. Το Tallinn Manual 1.0 που εκδόθηκε το 2013 αφορούσε στην εφαρμογή του Διεθνούς Δικαίου στον κυβερνοπόλεμο. Το Tallinn Manual 2.0, που εκδόθηκε το 2017, αφορά στην εφαρμογή του Διεθνούς Δικαίου στις επιχειρήσεις στον κυβερνοχώρο[30]. Σύμφωνα λοιπόν με τον Κανόνα 4 του Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: «Ένα Κράτος δεν πρέπει να διεξάγει επιχειρήσεις στον κυβερνοχώρο, οι οποίες παραβιάζουν την κυριαρχία ενός άλλου Κράτους». Η παραβίαση της κυριαρχίας από κυβερνοεπιθέσεις συνιστά και παραβίαση του Διεθνούς Δικαίου, με εξαίρεση τις περιπτώσεις, στις οποίες υπάρχει εξουσιοδότηση από το Συμβούλιο Ασφαλείας και αφορά μόνο στις σχέσεις μεταξύ των κρατών και όχι σε μη κρατικούς δρώντες, εκτός κι αν υπάγονται στους Κανόνες 15 και 17[31]. Οι Κανόνες 14 και 15 αφορούν στο Δίκαιο της Διεθνούς Ευθύνης και πιο συγκεκριμένα στις διεθνώς παράνομες πράξεις, που μπορούν να συμβούν από ένα κράτος.
Κατά τον Κανόνα 14: «Ένα Κράτος φέρει διεθνή ευθύνη για μία συναφή με τον κυβερνοχώρο ενέργεια η οποία μπορεί να αποδοθεί στο Κράτος και συνιστά παραβίαση μίας διεθνούς νομικής υποχρέωσης». Το κράτος φέρει ευθύνη για τις

---

[27] Liaropoulos, Andrew. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?" Edited by Douglas Hart. *8th International Conference on Information Warfare and Security.* Denver, Colorado: Regis University, 2013: 139.
[28] Οργανισμός Ηνωμένων Εθνών. «Καταστατικός Χάρτης Ηνωμένων Εθνών.» 1945. Accessed October 14, 2019. https://www.unric.org/el/index.php?option=com_content&view=article&id=14
[29] Haataja, Samuli. "The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach." In *Law, Innovation and Technology* 9, no. 2 (2017): 162.
[30] Jensen, Eric T. "The Tallinn Manual 2.0: Highlights and Insights." In *Georgetown Journal of International Law* 48 (March 2017): 735. Accessed October 14, 2019. https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf
[31] International Groups of Experts. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2017: 17.

διεθνώς παράνομες πράξεις σύμφωνα με το Δίκαιο της Ευθύνης του Κράτους[32]. Με τον όρο «συναφείς με τον κυβερνοχώρο ενέργειες», μπορεί να νοηθούν και ενέργειες, οι οποίες δεν διεξάγονται από το κράτος και δεν αποδίδονται σε αυτό, αλλά για τις οποίες το κράτος μπορεί να φέρει ευθύνη, όπως το να αποτύχει να λάβει τα απαραίτητα μέτρα, για να τερματίσει επιχειρήσεις που διεξάγονται από την επικράτειά του, ή να προσφέρει υλικό και λογισμικό για τη διεξαγωγή επιχειρήσεων[33].

Ο Κανόνας 15 ορίζει πως: «Οι επιχειρήσεις στον κυβερνοχώρο, οι οποίες διεξάγονται από όργανα του Κράτους, ή από άτομα ή φορείς εξουσιοδοτημένα από την εσωτερική έννομη τάξη να ασκούν τα στοιχειώδη των κυβερνητικών αρχών, αποδίδονται στο κράτος». Ο όρος «όργανα του κράτους» είναι ευρύς και αναφέρεται σε όλα τα άτομα ή φορείς που έχουν αυτό το καθεστώς υπό την εσωτερική έννομη τάξη, ανεξαρτήτως της λειτουργίας ή της θέσης τους στην κυβερνητική ιεραρχία. Τα όργανα παραδείγματος χάριν, των οποίων οι δραστηριότητες στον κυβερνοχώρο αποδίδονται πλήρως στα αντίστοιχα κράτη είναι τα εξής: US Cyber Command, Netherlands Defence Cyber Command, Estonian Defence League's Cyber Unit, French Network and Information Security Agency, People's Liberation Army cyber unit, Israel's Unit 8200[34].

Για τον ορισμό της χρήσης βίας, ο Κανόνας 69 επισημαίνει πως: «Μία επιχείρηση στον κυβερνοχώρο συνιστά χρήση βίας, όταν η κλίμακα και οι επιδράσεις της είναι συγκρίσιμες με επιχειρήσεις που δεν αφορούν στον κυβερνοχώρο και οι οποίες φτάνουν στο επίπεδο χρήσης βίας»[35].

Τέλος, ο Κανόνας 71 αναφέρεται στην νόμιμη άμυνα έναντι ένοπλης επίθεσης και υπογραμμίζει ότι: «Ένα Κράτος, το οποίο αποτελεί στόχο δραστηριότητας στον κυβερνοχώρο, η οποία φτάνει στο επίπεδο ένοπλης επίθεσης, μπορεί να ασκήσει το αναφαίρετο δικαίωμά του στην νόμιμη άμυνα. Εάν η δραστηριότητα, αποτελεί ένοπλη επίθεση εξαρτάται από την κλίμακα και τις επιδράσεις της». Το εθιμικό δίκαιο αναφορικά με το δικαίωμα της νόμιμης άμυνας ανακλάται στο Άρθρο 51 του Χάρτη των Ηνωμένων Εθνών. Η ένοπλη επίθεση πρέπει να ενέχει το διασυνοριακό στοιχείο[36].

Η περίπτωση της Εσθονίας επομένως, ήταν η πρώτη περίπτωση κυβερνοεπίθεσης η οποία δεν είχε ως επακόλουθο κάποια υλική καταστροφή, τραυματισμό ή θάνατο, αλλά ούτε οδήγησε σε ένοπλη επίθεση και δεν αποδόθηκε τεχνικά ή νομικά σε κάποιο κράτος. Αυτό αποτέλεσε έναυσμα για την Εσθονία και τη διεθνή κοινότητα να λάβουν μέτρα αναφορικά με την ενίσχυση της άμυνας και ασφάλειας στον κυβερνοχώρο. Σήμερα η Εσθονία θεωρείται πρωτοπόρος σε αυτόν τον τομέα.

4. Η μετεξέλιξη της κυβερνοασφάλειας μετά την επίθεση στην Εσθονία

4.1 Εσθονία

Η Εσθονία, ως ένα κράτος που διαπρέπει στον τομέα της ηλεκτρονικής διακυβέρνησης, είχε ήδη κάνει κάποια βήματα στον τομέα της κυβερνοασφάλειας

[32] Για την Διεθνή Ευθύνη του Κράτους βλ. Ρούκουνας, Εμμανουήλ. «Η Διεθνής Ευθύνη του Κράτους.» In *Δημόσιο Διεθνές Δίκαιο - 2η έκδοση* Αθήνα: Νομική Βιβλιοθήκη, 2015: 452-466.

[33] International Groups of Experts. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2017: 84-85.

[34] Ibid, 87.

[35] Ibid, 330.

[36] Ibid, 339-340.

πριν τα γεγονότα του 2007. Πιο συγκεκριμένα, το 2006 ίδρυσε τον CERT-EE (Computer Emergency Response Team-EE), έναν οργανισμό υπεύθυνο να υποβοηθά τους Εσθονούς χρήστες διαδικτύου, ώστε να εφαρμόζουν προληπτικά μέτρα για την αποφυγή ζημίας από διάφορα περιστατικά και απειλές που μπορεί να αντιμετωπίσουν. Επίσης, προσφέρει αρωγή σε θεσμούς και παρόχους διαδικτύου[37]. Το πλήγμα που δέχθηκε, την ώθησε στη δημιουργία της Στρατηγικής Κυβερνοασφάλειας το 2008. Για τη άμβλυνση, λοιπόν, της τρωτότητας της στον τομέα αυτόν τέθηκαν οι εξής στρατηγικοί στόχοι: α) η καθιέρωση ενός πολυεπίπεδου συστήματος μέτρων ασφάλειας, β) η διεύρυνση της τεχνογνωσίας αναφορικά με την πληροφοριακή ασφάλεια και την αντίληψη της, γ) η υιοθέτηση ενός κατάλληλου ρυθμιστικού πλαισίου για την προώθηση της ασφαλούς και εκτεταμένης χρήσης των πληροφοριακών συστημάτων και δ) η εδραίωση της θέσης της Εσθονίας ως ένα από τα εξέχοντα κράτη στις διεθνείς συνεργατικές προσπάθειες για τη διασφάλιση της κυβερνοασφάλειας[38].

Υπάρχει η αντίληψη ότι η κυβερνοασφάλεια μπορεί να διασφαλιστεί μόνο μέσω της συνεργασίας και ότι μία από κοινού συνεισφορά είναι αναγκαία σε όλα τα επίπεδα, κρατικό, ιδιωτικό και ατομικό[39]. Αυτό διαφαίνεται στη δημιουργία της εσθονικής Cyber Defence League (CDL), η οποία είχε ήδη προταθεί από το 2007 και στις αρχές του 2011 αποτελούσε δομική μονάδα της Estonian Defence League[40]. Είναι ένας εθελοντικός οργανισμός και οι δραστηριότητες της περιλαμβάνουν την εκπαίδευση αναφορικά με την πληροφοριακή ασφάλεια, την ενίσχυση της ετοιμότητας κατά τη διάρκεια μίας κρίσης και τη συμμετοχή σε εκπαιδευτικές εκδηλώσεις που αφορούν τη διεθνή κυβερνοασφάλεια[41]. Σκοπός της είναι «η προστασία του υψηλής τεχνολογίας τρόπου ζωής των Εσθονών, μέσω της προστασίας των πληροφοριακών υποδομών και η υποστήριξη των ευρύτερων στόχων της εθνικής άμυνας». Τέλος, σημαντικό της χαρακτηριστικό είναι η δημιουργία ενός δικτύου που διευκολύνει την συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα[42].

Οι κυβερνοεπιθέσεις στην Εσθονία θεωρείται, πως αποτέλεσαν μία προειδοποίηση για το NATO και την ΕΕ, κι έδωσαν ώθηση για μία πιο συνεκτική και ολοκληρωμένη αντιμετώπιση της κυβερνοασφάλειας.

4.2 Ευρωπαϊκή Ένωση (ΕΕ)

[37] Republic of Estonia Information System Authority. *CERT-EE.* n.d. Accessed November 17, 2019. https://www.ria.ee/en/cyber-security/cert-ee.html

[38] Cyber Security Strategy Committee. "Cyber Security Strategy." Tallinn: Ministry of Defence, 2008: 27. Accessed November 22, 2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy

[39] Invest in Estonia. "How Estonia became a global heavyweight in cyber security." June, 2017. Accessed November 17, 2019. https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

[40] Kaska, Kadri., Osula, Anna-Maria., and Stinissen, Jan. "The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis." Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 2013: 5, 7. Accessed November 22, 2019. https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

[41] No author, "Estonian Defence League's Cyber Unit." n.d. Accessed November 22, 2019. http://www.kaitseliit.ee/en/cyber-unit

[42] Kaska, Kadri., Osula, Anna-Maria., and Stinissen, Jan. "The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis." Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 2013: 11. Accessed November 22, 2019. https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

Η ΕΕ άρχισε να μεριμνά για τους κινδύνους του κυβερνοχώρου το 2004 όταν έθεσε σε ισχύ τη Σύμβαση για το Κυβερνοέγκλημα (Convention on Cybercrime), με σκοπό την προστασία της κοινωνίας έναντι του κυβερνοεγκλήματος, υιοθετώντας την κατάλληλη νομοθεσία και προωθώντας την διεθνή συνεργασία[43]. Το ίδιο έτος ιδρύθηκε, με τον κανονισμό 460/2004 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου[44], ένας οργανισμός για την κυβερνοασφάλεια, με στόχο την ανάπτυξη των εθνικών στρατηγικών κυβερνοασφάλειας, την παροχή συμβουλευτικής και λύσεων προκειμένου να βελτιώσουν τα κράτη τις δυνατότητές τους στον τομέα αυτό, αλλά και την εφαρμογή της πολιτικής και του νομικού πλαισίου της ΕΕ σε θέματα ασφάλειας δικτύου και πληροφοριών[45]. Ο ρόλος του οργανισμού αυτού ενισχύθηκε το 2013 και τροποποιήθηκε τον Απρίλιο του 2019 με τον κανονισμό 2019/881[46] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών. Ο ENISA, επίσης, επιβλέπει το πανευρωπαϊκό πρόγραμμα ασκήσεων που ονομάζονται Cyber Europe. Οι ασκήσεις αυτές είναι προσομοιώσεις περιστατικών μεγάλης κλίμακας, οι οποίες κλιμακώνονται σε κρίσεις στον κυβερνοχώρο. Ξεκίνησε το 2010, κι έχει πραγματοποιηθεί πέντε φορές, κάθε δύο έτη. Σκοπός του προγράμματος είναι μεταξύ άλλων η ανάλυση εξελιγμένων τεχνικών περιστατικών και η διαχείριση κρίσεων[47].

Η ΕΕ έλαβε χρήσιμα μαθήματα από τις επιθέσεις εναντίον της Εσθονίας και την αντιμετώπισή τους. Πολύ σημαντική θεωρήθηκε η συνεργασία ιδιωτικού και δημόσιου τομέα, την οποία η Εσθονία υπέδειξε με την σύσταση της Cyber Defence League. Η Ευρωπαϊκή Επιτροπή έχει εκτενώς επενδύσει στις συμπράξεις δημόσιου και ιδιωτικού τομέα, που είναι αρμόδιες κυρίως για την έρευνα και την καινοτομία σχετικά με την διαμόρφωση λύσεων για την κυβερνοασφάλεια[48]. Αντισυμβαλλόμενος της σε αυτό το ζήτημα είναι ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια, που δημιουργήθηκε τον Ιούλιο του 2016[49]. Ακόμη το εσθονικό κράτος θεωρείται πως είναι εκείνο που μπορεί να πείσει ότι το καλύτερο πράγμα για την ευρωπαϊκή κυβερνοασφάλεια, είναι όλοι οι εταίροι της ΕΕ να συμμετάσχουν στην προσπάθεια οικοδόμησης διεθνών δομών και την ανάπτυξη δυνατοτήτων κατάλληλων για την παρεμπόδιση δυνητικών επιθέσεων[50].

---

[43] Council of Europe. "Convention on Cybercrime: Details of Treaty No. 185." 2001. Accessed November 22, 2019. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[44] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Κανονισμός (ΕΚ) αριθ. 460/2004. 10 Μαρτίου, 2004. Accessed November 17, 2019. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32004R0460&from=EN

[45] European Union Agency for Cybersecurity. "About ENISA." n.d. Accessed November 22, 2019. https://www.enisa.europa.eu/about-enisa

[46] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Κανονισμός (ΕΕ) 2019/881. 17 Απριλίου, 2019. Accessed November 17, 2019. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0881&from=EL

[47] European Union Agency for Cybersecurity. "Cyber Exercises: Cyber Europe." n.d. Accessed November 23, 2019. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

[48] European Commission. "Public Private Partnerships." n.d. Accessed November 25 2019. https://ec.europa.eu/digital-single-market/en/public-private-partnerships

[49] European Cyber Security Organisation. "About ESCO." n.d. Accessed November 25, 2019. https://www.ecs-org.eu/about

[50] Tuohy, Emmet. "Toward an EU Cybersecurity Strategy: The Role of Estonia." *Intenational Centre for Defence Studies*. 2012: 10. Accessed November 23, 2019. http://pdc.ceu.hu/archive/00006852/01/ICDS_Toward-EU-Cybersecurity-Strategy-The-Role-of-Estonia.pdf

Τον Σεπτέμβριο του 2012 ξεκίνησε η λειτουργία του CERT-EU (Computer Emergency Response Team – European Union), το οποίο βοηθά στη διαχείριση των απειλών σε συστήματα πληροφορικής των θεσμών της ΕΕ. Επίσης, υποστηρίζει τις ομάδες πληροφοριακής και τεχνολογικής ασφάλειας κάθε θεσμού της ΕΕ και τη συνεργασία με τους ομολόγους των CERT δημοσίου τομέα άλλων χωρών αυτής[51]. Επιπρόσθετα, η Europol τον Ιανουάριο του 2013 ίδρυσε το Ευρωπαϊκό Κέντρο Κυβερνοεγκλήματος (EC3), που στοχεύει στην καταπολέμηση του κυβερνοεγκλήματος, μέσω της νομικής αντιμετώπισης του και της προστασίας των πολιτών, των επιχειρήσεων και των κυβερνήσεων της Ένωσης από το διαδικτυακό έγκλημα[52].

Ένα από τα πιο σημαντικά βήματα ήταν η θέσπιση της Στρατηγικής της ΕΕ το 2013 με τίτλο «An Open, Safe and Secure Cyberspace», για την ασφάλεια στον κυβερνοχώρο με σκοπό τον προσανατολισμό των μέτρων πολιτικής της Ένωσης έναντι των απειλών και των κινδύνων στον κυβερνοχώρο. Βασικό ζήτημα, που η στρατηγική αυτή τονίζει, είναι η ανάγκη να συμπεριλάβει η ΕΕ τα ζητήματα και τις προκλήσεις που αφορούν στον κυβερνοχώρο στην ευρύτερη ατζέντα της[53]. Βασικά σημεία της αφορούν στον περιορισμό των εγκλημάτων στον κυβερνοχώρο, καθώς και στη δημιουργία μιας Πολιτικής Άμυνας στον Κυβερνοχώρο της ΕΕ (EU Cyber Defence Policy) στα πλαίσια της Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ)[54].

Νομικά μέτρα για την ενίσχυση της κυβερνοασφάλειας, μέσω της ετοιμότητας και του σωστού εξοπλισμού των κρατών μελών και την συνεργασία μεταξύ τους[55] παρέχει η Οδηγία αρθ. 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου για την ασφάλεια των δικτύων και των συστημάτων (NIS Directive)[56]. Αποτελεί την πρώτη νομική πράξη της ΕΕ στον τομέα της κυβερνοασφάλειας και τέθηκε σε ισχύ τον Αύγουστο του 2016. Για να ενισχύσει τα δικαιώματα και τις ελευθερίες των ατόμων στον κυβερνοχώρο, η ΕΕ εξέδωσε στις 27 Απριλίου του 2016 τον Κανονισμό 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων). Την περίοδο 2014 - 2019, ο πρώην Εσθονός πρωθυπουργός Andrus Ansip ήταν επικεφαλής της Ενιαίας Ψηφιακής Αγοράς της ΕΕ, που σχετίζεται με την ασφάλεια, τα προσωπικά δεδομένα και τον γενικότερο συντονισμό της ψηφιοποίησης της ΕΕ[57].

Τον Σεπτέμβρη 2017, οι Υπουργοί Άμυνας των κρατών μελών της ΕΕ,

---

[51] Europa. “Interinstitutional bodies.” n.d. Accessed November 17, 2019. https://europa.eu/european-union/about-eu/institutions-bodies/interinstitutional-bodies_en

[52] Europol. “European Cybercrime Centre –EC3 : Combating crime in the digital age.” n.d. Accessed November 23, 2019. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[53]Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Κανονισμός (ΕΕ) 2019/881. 17 Απριλίου, 2019. Accessed November 17, 2019. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0881&from=EL

[54] European Commission. “Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace.” February 7, 2013. Accessed November 17, 2019. https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

[55] European Commission. “The Directive on security of network and information systems (NIS Directive).” n.d. Accessed November 23, 2019. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[56] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Οδηγία (ΕΕ) 2016/1148. 6 Ιουλίου, 2016. Accessed November 17, 2019. http://www.adae.gr/fileadmin/docs/CELEX-32016L1148-EL-TXT.pdf

[57] Gold, Josh. “Estonia as an international cybersecurity leader.” August 2019. Accessed November 17, 2019. https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/

συγκεντρώθηκαν στο Ταλλίν, για την πρώτη στο είδος της, άσκηση άμυνας στον κυβερνοχώρο (EU Cybrid), που οργανώθηκε από την εσθονική προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης, το εσθονικό Υπουργείο Άμυνας και τον Ευρωπαϊκό Οργανισμό Άμυνας. Σκοπός της άσκησης, είναι η αντιμετώπιση των απειλών κατά της Κοινής Πολιτικής Άμυνας και Ασφάλειας, που εντοπίζονται στον κυβερνοχώρο[58].
Καταληκτικά, αξίζει να σημειωθεί, πως από τον Μάιο του 2019 το Συμβούλιο μπορεί να επιβάλλει κυρώσεις για την αποτροπή και την αντιμετώπιση κυβερνοεπιθέσεων που αποτελούν εξωτερική απειλή για την ΕΕ και τα κράτη-μέλη της[59].

4.3 Βορειοατλαντική Συμμαχία (NATO)

Η Συμμαχία ανέκαθεν προστάτευε τα δικά της πληροφοριακά κι επικοινωνιακά συστήματα από κυβερνοεπιθέσεις[60], όπως φάνηκε από την Σύνοδο Κορυφής της Πράγας το 2002, όταν τονίστηκε η ανάγκη ενίσχυσης δυνατοτήτων έναντι των κυβερνοεπιθέσεων[61]. Η Εσθονία το 2004, μόλις έγινε μέλος του NATO, πρότεινε την ίδρυση ενός οργανισμού κυβερνοάμυνας στο πλαίσιο του NATO. Παρ'ολο που η πρόταση εγκρίθηκε το 2006, δεν υλοποιήθηκε αμέσως[62]. Εντούτοις, αυτό άλλαξε μετά το 2007, εφόσον κρίθηκε αναγκαία η ανάπτυξη των αμυντικών δυνατοτήτων στον κυβερνοχώρο για κάθε ένα μέλος ξεχωριστά[63].
Στις 14 Μαΐου του 2008 ιδρύθηκε το Κέντρο Αριστείας του NATO για την Συνεργατική Άμυνα στον Κυβερνοχώρο (CCDCOE) από τα εξής κράτη: Εσθονία, Λετονία, Ιταλία, Γερμανία, Λιθουανία, Σλοβακία και Ισπανία. Μέσα σε δέκα χρόνια από την ίδρυση του έχει διευρυνθεί από τα 7 ιδρυτικά του μέλη σε ένα ισχυρό κέντρο κυβερνοάμυνας με 21 κράτη: Αυστρία, Βέλγιο, Τσεχική Δημοκρατία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιταλία, Λετονία, Λιθουανία, Ολλανδία, Πολωνία, Πορτογαλία, Σλοβακία, Ισπανία, Σουηδία, Τουρκία, Ηνωμένο Βασίλειο και ΗΠΑ. Το CCDCOE, που έχει την βάση του στο Ταλλίν, εστιάζει στην έρευνα, την ανάπτυξη, την εκπαίδευση και την εκμάθηση τόσο σε τεχνικούς όσο και σε μη τεχνικούς τομείς στην άμυνα στον κυβερνοχώρο. Παρ' όλο που ο οργανισμός δεν είναι υπεύθυνος για την κυβερνοασφάλεια του NATO, οι εκδόσεις του, όπως το Tallinn Manual, ένα ετήσιο συνέδριο, όπως το CyCon και ασκήσεις, όπως το Locked Shields, ασκούν σημαντική επιρροή στις αυξανόμενες ικανότητες του NATO αναφορικά με τον κυβερνοχώρο. Η ετήσια άσκηση Locked Shields, οργανώνεται από

[58] European Defence Agency. "First cyber exercise at EU ministerial level focuses on strategic decision-making." 2017. Accessed November 24, 2019. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making
[59] Συμβούλιο της Ευρωπαϊκής Ένωσης. «Κυβερνοεπιθέσεις: Το Συμβούλιο μπορεί πλέον να επιβάλλει κυρώσεις.» 17 Μαΐου 2019. Accessed November 22, 2019. https://www.consilium.europa.eu/el/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/
[60] Laasme, Haly. "Estonia: Cyber Window into the Future of NATO." Joint Force Quarterly: no. 63 (2011): 58. National Defence University Press. Accessed November 23, 2019. https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-63.pdf
[61] NATO. "Prague Summit 2002: Selected Documents and Statements." 2002: 53. Accessed November 23, 2019. https://www.nato.int/docu/0211prague/speeches-e.pdf
[62] NATO Cooperative Cyber Defence Centre of Excellence. "About Us." n.d. Accessed November 21, 2019. https://ccdcoe.org/about-us/
[63] Laasme, Haly. "Estonia: Cyber Window into the Future of NATO." Joint Force Quarterly: no. 63 (2011): 58. National Defence University Press. Accessed November 23, 2019. https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-63.pdf

το 2010 από τον CCDCOE στο Ταλλίν και αποτελεί τη μεγαλύτερη και πιο περίπλοκη, διεθνή άσκηση κυβερνοάμυνας στον κόσμο[64]. Κάθε χρόνο, ομάδες τοποθετούνται υπό έντονη πίεση, ώστε να μπορέσουν να διατηρήσουν τα δίκτυα και τις υπηρεσίες ενός πλασματικού κράτους. Η άσκηση αυτή εστιάζει σε ρεαλιστικές και σύγχρονες τεχνολογίες, δίκτυα και τρόπους επίθεσης. Για παράδειγμα, στην άσκηση του 2017, στην οποία υπήρχαν 900 συμμετέχοντες από 25 χώρες, οι ομάδες έπρεπε να διατηρήσουν τις υπηρεσίες και τα δίκτυα μίας στρατιωτικής, αεροπορικής βάσης ενός πλασματικού κράτους, η οποία σύμφωνα με το σενάριο, θα ερχόταν αντιμέτωπη με έντονες επιθέσεις στο σύστημα ηλεκτροδότησης, σε μη επανδρωμένα αεροπορικά οχήματα, σε στρατιωτικά συστήματα εντολών και ελέγχου, σε κρίσιμες υποδομές πληροφόρησης και σε άλλες λειτουργικές υποδομές[65].

Από το 2008 κι έπειτα λαμβάνει χώρα μία νατοϊκή άσκηση που θεωρείται κορωνίδα των ασκήσεων για την άμυνα στον κυβερνοχώρο κι ονομάζεται NATO Cyber Coalition[66]. Στοχεύει στον έλεγχο και την εκπαίδευση των αμυνόμενων, ως προς την αντιμετώπιση των προκλήσεων στον κυβερνοχώρο σε ρεαλιστικές αμυντικές ασκήσεις. Περιλαμβάνει τόσο επιχειρησιακές όσο και νομικές διαδικασίες. Στην Εσθονία έχει επίσης δημιουργηθεί μία πλατφόρμα για νατοϊκές ασκήσεις κι εκπαίδευση, που ονομάζεται NATO Cyber Range, η οποία συντελεί στην παραπάνω άσκηση[67].

Το 2008 υιοθετήθηκε επίσης η πρώτη πολιτική του NATO για την άμυνα στον κυβερνοχώρο στη Σύνοδο Κορυφής του, στο Βουκουρέστι. Σύμφωνα με το επίσημο κείμενο: *«Το ΝΑΤΟ παραμένει δεσμευμένο στην ενίσχυση των βασικών πληροφοριακών συστημάτων της Συμμαχίας, εναντίον των κυβερνοεπιθέσεων. Η Πολιτική μας αναφορικά με την Άμυνα στον Κυβερνοχώρο, επισημαίνει την ανάγκη για το ΝΑΤΟ και τα έθνη, να προστατεύουν τα βασικά πληροφοριακά τους συστήματα σε συμφωνία με τις ανάλογες υποχρεώσεις τους, να μοιράζονται τις καλύτερες πρακτικές και να παρέχουν την δυνατότητα να βοηθούν τα έθνη της Συμμαχίας, μετά από απαίτηση, ώστε να αντιμετωπίσουν μία κυβερνοεπίθεση»*[68].

Η πολιτική συχνά τροποποιείτο, όπως συνέβη και στην Ουαλία τον Σεπτέμβριο του 2014. Σύμφωνα με την τελευταία έκδοση της, το ΝΑΤΟ αναγνωρίζει ότι το Διεθνές Δίκαιο εφαρμόζεται στον κυβερνοχώρο και ότι η άμυνα σ'αυτόν είναι βασικό καθήκον της συλλογικής άμυνας του ΝΑΤΟ. Ως εκ τούτου, το Άρθρο 5 του Βορειοατλαντικού Συμφώνου για τη συλλογική αυτοάμυνα μπορεί να επικληθεί σε περίπτωση κυβερνοεπίθεσης εάν οι επιδράσεις της ισοδυναμούν με αυτές μίας συμβατικής ένοπλης επίθεσης. Μολαταύτα, δεν τίθενται λεπτομερή κριτήρια για την ενεργοποίηση του Άρθρου 5, τα οποία θα πρέπει να εξετάζονται από τους Συμμάχους σε κάθε περίπτωση ξεχωριστά[69].

---

[64] NATO Cooperative Cyber Defence Centre of Excellence. "About Us." n.d. Accessed November 21, 2019. https://ccdcoe.org/about-us/

[65] Invest in Estonia. "How Estonia became a global heavyweight in cyber security." June, 2017. Accessed November 17, 2019. https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

[66] NATO. "Cyber Coalition 2010 to exercise collaboration in cyber defence." November 16, 2010. Accessed November 24, 2019. https://www.nato.int/cps/en/natohq/news_68205.htm?selectedLocale=en

[67] NATO. "NATO Cyber Defence." 2019. Accessed November 24, 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

[68] NATO. "Bucharest Summit Declaration." Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. Accessed November 24, 2019. https://www.nato.int/cps/en/natolive/official_texts_8443.htm

[69] NATO Cooperative Cyber Defence Centre of Excellence. "NATO Summit Updates Cyber Defence

Στο πλαίσιο της μεταρρύθμισης των οργανισμών και υπηρεσιών του NATO, δημιουργήθηκε το NATO Communications and Information Agency (NCI Agency), τον Ιούλιο του 2012[70]. Σημαντική υπηρεσία του NCI Agency είναι η NCIA Cyber Security Service Line, η οποία είναι αρμόδια για τον σχεδιασμό και την εκτέλεση όλου του φάσματος των δραστηριοτήτων για την κυβερνοασφάλεια. Διευκολύνει την ασφαλή διεξαγωγή των επιχειρήσεων της Συμμαχίας που απαντάται στο NATO C4ISR (NATO's Command, Control, Communications, Computers, Intelligence, Surveillance)[71].

Το 2016 το NATO αναγνώρισε στην Σύνοδο Κορυφής στην Βαρσοβία τον κυβερνοχώρο ως τομέα επιχειρήσεων, στον οποίο πρέπει να υπερασπίζεται αποτελεσματικά τον εαυτό του κι έκτοτε έχει πετύχει σημαντικά ορόσημα[72]. Πιθανώς, το πιο σημαντικό, ανακοινώθηκε στην πιλοτική του μορφή από το NATO τον Οκτώβριο του 2018 και ονομάστηκε Cyberspace Operations Centre (CyOC). Το CyOC αποτελεί το βασικό δομικό στοιχείο για το NATO αναφορικά με τον κυβερνοχώρο και είναι υπεύθυνο για τον κεντρικό προγραμματισμό, για τις επιχειρήσεις, τις αποστολές των Συμμάχων στους τομείς του κυβερνοχώρου καθώς και για την συνεκτική αντιμετώπιση των λειτουργικών προβλημάτων στον κυβερνοχώρο. Τον Ιούνιο του 2018, οι Σύμμαχοι ενέκριναν, επίσης, το «Όραμα και Στρατηγική στον Κυβερνοχώρο ως έναν Τομέα Επιχειρήσεων (Vision and Strategy on Cyberspace as a Domain of Operations)».

Η Δέσμευση για την Άμυνα στον Κυβερνοχώρο (Cyber Defence Pledge), που βασίστηκε στο Άρθρο 3 της Συνθήκης της Ουάσινγκτον, αναφέρει ότι, «οι Σύμμαχοι θα πρέπει να διατηρούν και να αναπτύσσουν τις ατομικές και συλλογικές τους ικανότητες για να αντισταθούν σε ένοπλες επιθέσεις». Καθώς είναι αδύνατον να διαχωριστούν στρατιωτικά, δημόσια και βιομηχανικά ζητήματα στον κυβερνοχώρο, το NATO ενδιαφέρεται εντόνως για την βελτίωση των ικανοτήτων άμυνας σ' αυτόν, όσων οργανώσεων βρίσκονται εκτός του αμυντικού καθεστώτος[73].

Υπάρχει ακόμη ένας λόγος, που καθιστά την Εσθονία άκρως ενεργή και αναπόσπαστο κομμάτι του NATO σε αυτόν τον τομέα. Έχει δεσμευτεί στην κατανομή των βαρών και είναι ένα από τα λίγα κράτη που υπερβαίνουν το ελάχιστο 2% του ΑΕΠ τους, που απαιτείται για την άμυνα του[74]NATO[75].

Οι επιθέσεις αυτές, θα μπορούσαν να χαρακτηριστούν έναυσμα για όλες τις ενέργειες στις οποίες προέβησαν οι οργανισμοί από το 2008 κι έπειτα, ενώ η Εσθονία αναμφισβήτητα διακρίνεται για την συνεισφορά της. Το ερώτημα επομένως που εγείρεται, είναι ποια πλεονεκτήματα αποκομίζει ένα κράτος-μέλος των δύο οργανισμών ως προς την διασφάλισή του στον κυβερνοχώρο.

Policy." n.d. Accessed November 24, 2019. https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/#footnote_1_2663

[70] NATO Communications and Information Agency. "About the NCI Agency." n.d. Accessed November 25, 2019. https://www.ncia.nato.int/About/Pages/Organization.aspx

[71] NATO Communications and Information Agency. "Cyber Security." n.d. Accessed November 25, 2019. https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx

[72] NATO. "Cyber Defence." 2019. Accessed November 24, 2019. https://www.nato.int/cps/en/natohq/topics_78170.htm

[73] Brent, Laura. "NATO's role in cyberspace." NATO, February 12, 2019. Accessed November 17, 2019. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[74] Gold, Josh. "How Estonia uses Cybersecurity to Strengthen its Position in NATO." International Centre for Defence and Security, 2019. Accessed November 26, 2019. https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/

[75] NATO Public Diplomacy Division. "Defence Expenditure of NATO Countries (2012-2019)." 2019. Accessed November 26, 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/20190625_PR2019-069-EN.pdf

5. Σύγκριση ΕΕ – ΝΑΤΟ: Στόχοι και Δυνατότητες

Η ΕΕ αποτελεί πυλώνα της συλλογικής άμυνας του ΝΑΤΟ, ενώ οι δύο οργανισμοί έχουν αρκετά κοινά κράτη-μέλη. Η ευρωατλαντική συνεργασία έχει διευρυνθεί και στον τομέα της κυβερνοασφάλειας, ωστόσο οι δύο κινούνται σε διαφορετικές ταχύτητες, έχοντας διαφορετικά σημεία εστίασης σε πολλές περιπτώσεις. Χαρακτηριστικό παράδειγμα είναι η χρονική απόκλιση υιοθέτησης της επίσημης πολιτικής του ΝΑΤΟ και της επίσημης στρατηγικής της ΕΕ, το 2008 και το 2013 αντίστοιχα. Είναι εμφανές από την παραπάνω ανάλυση ότι το ΝΑΤΟ θέτει ως προτεραιότητά του την άμυνα στον κυβερνοχώρο, εν αντιθέσει με την ΕΕ που δίνει έμφαση στην αντιμετώπιση του κυβερνοεγκλήματος. Πιο συγκεκριμένα, το ΝΑΤΟ εισήγαγε ένα ενισχυμένο σχέδιο δράσης για την άμυνα το 2011 με την τροποποίηση της πολιτικής του. Από μέρους της, η ΕΕ κατέστησε την καταπολέμηση του κυβερνοεγκλήματος ως έναν εκ των τριών πυλώνων της Ευρωπαϊκής Ατζέντας για την Ασφάλεια[76].

Για την διασφάλιση του νατοϊκού και των εθνικών πληροφοριακών δικτύων και υποδομών, το ΝΑΤΟ έχει επικεντρωθεί στην δημιουργία θεσμών, στην ανάπτυξη τεχνικών δυνατοτήτων και στην διεξαγωγή ασκήσεων για την πρόληψη ενδεχόμενων απειλών. Από την άλλη, η ΕΕ έχει εστιάσει στην ανάπτυξη ενός νομοθετικού πλαισίου και παρέχει στα κράτη-μέλη της, κατευθυντήριες γραμμές για την κυβερνοασφάλεια. Σε περίπτωση που κριθεί αναγκαία η παρέμβαση, το ΝΑΤΟ προβλέπει κατά περίπτωση την ενεργοποίηση του Άρθρου 5 από το 2014, ενώ η ΕΕ μπορεί να επιβάλλει κυρώσεις μέσω του Συμβουλίου της ΕΕ από το 2019.

Η ΕΕ και το ΝΑΤΟ λειτουργούν συμπληρωματικά για την άμβλυνση της τρωτότητας στον κυβερνοχώρο. Το 2016, ο Γενικός Γραμματέας του ΝΑΤΟ συναντήθηκε με τους προέδρους του Ευρωπαϊκού Συμβουλίου και της Ευρωπαϊκής Επιτροπής για την υπογραφή Κοινής Δήλωσης για Συνεργασία μεταξύ ΝΑΤΟ και ΕΕ[77]. Παρά τις συνεργατικές πρακτικές υπάρχουν κάποια ζητήματα που δυσχεραίνουν μία εξ ολοκλήρου κοινή πορεία. Η έλλειψη ανταλλαγής πληροφοριών και η μη διεξαγωγή κοινών ασκήσεων αποτελούν καίρια προβλήματα που πρέπει να επιλυθούν για μία πιο συνεκτική συνεργασία[78].

6. Συμπεράσματα

Τα πλεονεκτήματα της πληροφοριακής εποχής είναι αναρίθμητα, συνυπάρχουν, ωστόσο, με απειλές όπως η τρομοκρατία στον κυβερνοχώρο ή ο πληροφοριακός πόλεμος[79]. Οι βασισμένες σε δεδομένα υποδομές, από τις οποίες εξαρτόμαστε για την ασφάλεια μας και οι οποίες είναι πανταχού παρούσες στους χώρους εργασίας και της

---

[76] Lété, Bruno., and Pernik, Piret. "EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions." The German Marhall Fund of the United States 38 (2017): 1. Accessed November 25, 2019. http://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions

[77] Brent, Laura. "NATO's role in cyberspace." NATO, February 12, 2019. Accessed November 17, 2019. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[78] Lété, Bruno., and Pernik, Piret. "EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions." The German Marhall Fund of the United States 38 (2017): 1. Accessed November 25, 2019. http://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions

[79] Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." In *Journal of Strategic Security* 4, no. 2 (2011): 56.

καθημερινότητας των ανθρώπων, έχουν γίνει φορείς επιθέσεων στον πλούσιο σε πληροφορίες τρόπο ζωής[80]. Όσα συνέβησαν το 2007, μαρτυρούν πως ακόμη και το Άρθρο 5 του ΝΑΤΟ ή οι εγγυήσεις της πυρηνικής ομπρέλας των ΗΠΑ δεν διασφαλίζουν την προστασία της εθνικής κυριαρχίας στον κυβερνοχώρο. Έγινε αντιληπτό ότι οι δημοκρατίες έπρεπε να βρουν έναν τρόπο να διατηρούν την ισορροπία ανάμεσα στην διαδικτυακή ελευθερία ενόσω συντηρούν επαρκή συστήματα ελέγχου και έγκαιρης προειδοποίησης. Αυτά τα συστήματα σε συνδυασμό με την διευρυμένη συνεργασία στην κυβερνοασφάλεια, θα είναι ζωτικής σημασίας για τον εντοπισμό ύποπτων ψηφιακών δραστηριοτήτων και την αντιμετώπιση οποιασδήποτε απόπειρας για κυβερνοπόλεμο ή τρομοκρατία στον κυβερνοχώρο. Η αντίδραση των κρατών τόσο σε εθνικό όσο και σε συλλογικό επίπεδο υπέδειξε ότι αυτά δεν θα παρέμεναν αμέτοχα εφόσον απειλείται η κυριαρχία των ίδιων ή των συμμάχων τους από την χρήση του διαδικτύου ως όπλο. Όπως και η παγκόσμια οικονομία έχει προσαρμοστεί στην ψηφιακή εποχή, η περίπτωση της Εσθονίας φανερώνει ότι η εξωτερική πολιτική και πολιτική ασφάλειας των κρατών πρέπει να κάνει το ίδιο, καθώς οι κυβερνοεπιθέσεις, των οποίων η απόδοση ευθύνης είναι δύσκολο έργο, είναι πιθανόν να βλάψουν τα κράτη στο μέλλον[81].

[80] Ryan, Julie. "i-Warfare Some Introductory Remarks." In *Leading Issues in Informational Warfare and Security Research*. acpi, 2011: xv.

[81] Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." In *Journal of Strategic Security* 4, no. 2 (2011): 56.


Laboratory of
Intelligence &
Cyber-Security