ΣΤΡΑΤΗΓΙΚΟΝ, 2018
ΤΕΥΧΟΣ 2, σελ. 119 - 132

ΣΤΡΑΤΗΓΙΚΟΝ

Οι Κυβερνοεπιθέσεις ως Μέσο Στρατηγικής

Ανδρέας Θεοφίλης

ΣΥΝΟΨΗ

Η χρήση νέων τεχνολογιών και νέων μεθόδων έχει ανέκαθεν αποτελέσει κρίσιμο στοιχείο για την ιστορική εξέλιξη του πολέμου και επομένως και της στρατηγικής σκέψης. Δύναται ο κυβερνοχώρος και οι δυνατότητες που αυτός προσφέρει να ενταχθούν σε κάποια από τις ήδη υπάρχουσες στρατηγικές αντιλήψεις; Ή μήπως ο ψηφιακός χαρακτήρας των κυβερνοεπιχειρήσεων μειώνει τη χρησιμότητα των δράσεων στον κυβερνοχώρο ως εργαλεία στρατηγικής; Σε κάθε περίπτωση, ο κυβερνοχώρος είναι μια πραγματικότητα, και συνεπώς οφείλουμε να λαμβάνουμε υπόψη στο σύγχρονο περιβάλλον τις δυνατότητες και τους περιορισμούς του. Οι σύγχρονοι σχεδιαστές και λήπτες αποφάσεων μπορούν να ιχνηλατήσουν τη στρατηγική σκέψη και να ανακαλύψουν τρόπους υπαγωγής της στις κυβερνοεπιχειρήσεις, επεκτείνοντας τη δράση τους σε μία νέα διάσταση του χώρου.

Λέξεις κλειδιά: Κυβερνοχώρος, κυβερνοεπιχειρήσεις, στρατηγική, στόχοι, απόδοση ευθυνών, ηθικό, επικοινωνία.

Εισαγωγή

Οι τεχνολογικές εξελίξεις επηρέαζαν ανέκαθεν τον τρόπο διεξαγωγής του πολέμου και κατά συνέπεια τα μέσα επίτευξης των τεθέντων στρατηγικών στόχων. Αν και σύμφωνα με τον Clausewitz, όπως παρατίθεται στο Sheehan,[1] η θεμελιώδης φύση του πολέμου που συνίσταται στη χρήση βίας για την επιδίωξη πολιτικών στόχων παραμένει αναλοίωτη, οι μορφές του πολέμου διαφοροποιούνται στο χρόνο.

Τις τελευταίες δεκαετίες η Επανάσταση στις Στρατιωτικές Υποθέσεις (Revolution in Military Affairs—RMA) και οι εξελίξεις στο χώρο των επικοινωνιών έχουν επηρεάσει τον τρόπο που οι διάφοροι δρώντες σχεδιάζουν και υλοποιούν τη στρατηγική τους. Στη σημερινή εποχή, πλήθος καθημερινών δραστηριοτήτων, από τις

[1] Sheehan, M., *Ο Μεταβαλλόμενος Χαρακτήρας του Πολέμου*. στο: J. Baylis, S. Smith και P. Owens, (επιμ), *Η Παγκοσμιοποίηση της Διεθνούς Πολιτικής*. (Θεσσαλονίκη: Επίκεντρο, 2013), 300-318.

Για παραπομπή στο άρθρο: Ανδρέας Θεοφίλης,' Οι Κυβερνοεπιθέσεις ως Μέσο Στρατηγικής', *ΣΤΡΑΤΗΓΙΚΟΝ*, Τ. 2, (Χειμώνας 2018), 119-132.

οικονομικές συναλλαγές έως τη διανομή ηλεκτρικής ισχύος, διεξάγονται μέσα από δίκτυα υπολογιστών. Επομένως, τυχόν ενέργειες που στρέφονται κατά αυτών των δικτύων, όπως οι κυβερνοεπιθέσεις, είναι πιθανό να αποστερήσουν σημαντικούς πόρους από τους πληγέντες. Αυτού του είδους οι ενέργειες, οι επιθέσεις στον κυβερνοχώρο, αποτελούν, λοιπόν, μία νέα μορφή απειλής, θέτοντας νέα ζητήματα ασφαλείας και καταδεικνύοντας την ιστορική εξέλιξη του πολέμου.

Αρκετές χώρες αναπτύσσουν έντονη δραστηριότητα στον κυβερνοχώρο. Χώρες όπως οι ΗΠΑ, η Ρωσία, η Κίνα και η Μ. Βρετανία έχουν ενσωματώσει τον κυβερνοπόλεμο στα στρατιωτικά τους δόγματα.[2] Η ενσωμάτωση αυτή επηρεάζει τις έως τώρα θεωρήσεις περί στρατηγικής, επαληθεύοντας ότι «η σύγχρονη στρατηγική δεν είναι προϊόν κάποιας γενεαλογικής αλυσίδας της στρατιωτικής θεωρίας.»[3] Στο παρόν άρθρο εξετάζεται ο ρόλος του κυβερνοπολέμου στη διαμόρφωση της σύγχρονης στρατηγικής, μελετώντας τη δραστηριότητα της Ρωσίας στον τομέα αυτό. Στο άρθρο υποστηρίζεται ότι στον κυβερνοπόλεμο μπορεί να υπάρξουν σημεία σύγκλισης με ορισμένες προσεγγίσεις της στρατηγικής σκέψης που αφορούν τον συμβατικό πόλεμο, αν και υπάρχει η ανάγκη θεωριών που να αφορούν αμιγώς αυτό το είδος πολέμου.

Το αντικείμενο της ανάλυσης είναι οι κυβερνοεπιθέσεις κατά της Εσθονίας, το 2007, και κατά της Γεωργίας, το 2008. Ιδιαίτερη σημασία θα δοθεί στον ρόλο των κυβερνοεπιθέσεων στις συγκεκριμένες περιπτώσεις, ώστε να εξαχθούν ευρύτερα συμπεράσματα για τη χρήση των κυβερνοεπιχειρήσεων ως εργαλείου προώθησης πολιτικών στόχων και τελικά ως μέσου στρατηγικής.

Το θεωρητικό πλαίσιο

Αν και αρκετοί υποστηρίζουν ότι συχνά σε νεοεμφανιζόμενες τεχνολογίες και ερευνητικά πεδία δεν υπάρχουν κοινά αποδεκτοί ορισμοί, για την κατανόηση του θέματος είναι απαραίτητη η οροθέτηση των εννοιών.[4] Ο κυβερνοχώρος μπορεί να οριστεί ως «*[το] παγκόσμιο πεδίο εντός του περιβάλλοντος πληροφοριών που αποτελείται από αλληλένδετα δίκτυα υποδομών τεχνολογίας της πληροφορίας και αποθηκευμένα δεδομένα, συμπεριλαμβανομένου του Διαδικτύου, τηλεπικοινωνιακών δικτύων, συστημάτων υπολογιστών και ενσωματωμένων επεξεργαστών και ελεγκτών)*»[5].

---

[2] Sheehan, *Ο Μεταβαλλόμενος Χαρακτήρας Του Πολέμου*, 303.

[3] John Shy, "*Ζομινί*", στο Peter Paret (επιμ), *Οι Δημιουργοί της Σύγχρονης Στρατηγικής. Από το Μακκιαβέλλι στην Πυρηνική Εποχή, (Αθήνα: Τουρίκης, 2004)*, 177-228.

[4] Craig Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" στο Jan-Frederik Kremer and Benedict Müller (επιμ), Cyberspace *and International Relations*, (Berlin: Springer, 2013), 21-40.

[5] *([…]including the Internet, Telecommunications networks, Computer systems, and embedded processors and controllers)*, Office of General Counsel, "*Department of Defence. Law of War Manual*", U.S.Department of Defence, 12 June 2015, http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf, τελευταία επίσκεψη στις 26.7.018, 1022.

Το λεξικό της Οξφόρδης ορίζει τον κυβερνοπόλεμο ως «*[τη] χρήση της τεχνολογίας των ηλεκτρονικών υπολογιστών για τη διακοπή των δραστηριοτήτων ενός κράτους ή ενός οργανισμού, ιδίως [τη] σκόπιμη επίθεση των συστημάτων πληροφοριών για στρατηγικούς ή στρατιωτικούς σκοπούς.*»[6] Παράλληλα προς τη χρήση του όρου του κυβερνοπολέμου στη διεθνή βιβλιογραφία συναντάμε και τους όρους κυβερνοεπίθεση (cyber-attack) και κυβερνοεπιχειρήσεις (cyber operations). Οι κυβερνοεπιχειρήσεις

> *χρησιμοποιούν τα χαρακτηριστικά του κυβερνοχώρου, όπως τους υπολογιστές, τα εργαλεία λογισμικού ή τα δίκτυα και έχουν πρωταρχικό σκοπό την επίτευξη στόχων ή επιδράσεων μέσα από τον κυβερνοχώρο. Μπορεί να περιλαμβάνουν ενέργειες που χρησιμοποιούν υπολογιστές με σκοπό να διακόψουν, να αρνηθούν, να υποβαθμίσουν ή να καταστρέψουν [to disrupt, deny, degrade, or destroy] πληροφορίες αποθηκευμένες σε υπολογιστές και δίκτυα υπολογιστών ή τους ίδιους τους υπολογιστές και τα δίκτυα. Μπορεί επίσης να είναι μια μορφή προωθητικών πράξεων βίας, ως προπαρασκευαστική διαδικασία της κύριας επίθεσης*[7].

Ένα από τα πιο σημαντικά χαρακτηριστικά του κυβερνοχώρου και των πληροφοριακών συστημάτων είναι η παντελής έλλειψη συνόρων. Ο διεθνικός και χωρίς σύνορα χαρακτήρας των σύγχρονων συστημάτων πληροφοριών σημαίνει ότι οι επιθέσεις κατά των συστημάτων αυτών έχουν διασυνοριακή διάσταση. Ο εικονικός κόσμος του κυβερνοχώρου δεν γνωρίζει οριοθετήσεις, αντίστοιχες αυτές του φυσικού κόσμου. Συνεπώς, οποιαδήποτε προσπάθεια προβολής και προάσπισης των πραγματικών συνόρων των κρατών στον εικονικό κόσμο του κυβερνοχώρου και των πληροφοριακών συστημάτων είναι προβληματική. Επίσης, προβληματική είναι και η προσπάθεια απόδοσης ευθυνών σε περίπτωση κυβερνοεπίθεσης. Με τον όρο απόδοση ευθυνών εννοείται η δυνατότητα απόδειξης και καταλογισμού ευθυνών βάση του διεθνούς δικαίου του ποιος οργανώνει, διευθύνει και εκτελεί μια επίθεση στον κυβερνοχώρο.

Η σημασία του κυβερνοχώρου στο σύγχρονο διεθνές περιβάλλον έχει αναδειχθεί μέσα από πλήθος διαδικασιών, μελετών και ερευνών. Το «Εγχειρίδιο του Ταλλίν» (Tallinn's Manual) συνιστά μια προσπάθεια του ΝΑΤΟ για την υπαγωγή του κυβερνοπολέμου στο Διεθνές Δίκαιο.[8] Όπως εύστοχα σημειώνεται όμως στο Εγχειρίδιο, δεν υπάρχουν διεθνείς συνθήκες που να ασχολούνται άμεσα με τον κυβερνοπόλεμο. Ομοίως, επειδή η κρατική κυβερνητική πρακτική και οι δημοσίως

[6] English Oxford Living Company, "Definition of Cyberwarfare in English", Oxford University Press, 2018, https://en.oxforddictionaries.com/definition/cyberwarfare τελευταία επίσκεψη στις 26.7.018.

[7] Office of General Counsel, Department of Defence, 2015. *Department of Defence, Law of War Manual*, 1022, http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf, τελευταία επίσκεψη στις 27.7.018.

[8] Το εγχειρίδιο του Ταλλίν ("Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations") είναι η πιο ολοκληρωμένη ανάλυση του τρόπου με τον οποίο εφαρμόζεται το ισχύον διεθνές δίκαιο στον κυβερνοχώρο. Βλ. https://ccdcoe.org/tallinn-manual.html τελευταία επίσκεψη στις 28.7.018.

διαθέσιμες εκφράσεις της opinio juris των κρατών είναι αραιές, είναι δύσκολο να καταλήξουμε οριστικά στο συμπέρασμα ότι υπάρχει οποιοσδήποτε συγκεκριμένος εθιμικός κανόνας για τον κυβερνοχώρο. Οι κανόνες του Εγχειριδίου αντικατοπτρίζουν τη συναίνεση των εμπειρογνωμόνων ως προς το εφαρμοστέο lex lata, αλλά δεν αναφέρονται στο lex ferenda. Η απουσία ακριβώς του lex ferenda καθιστά προβληματική την πλήρη και πανθομολογούμενη εφαρμογή του διεθνούς δικαίου στην περίπτωση των κυβερνοεπιχειρήσεων. Το Εγχειρίδιο, ενώ καλύπτει αποτελεσματικά το jus in bello, δεν κάνει το ίδιο με το jus ad bellum για την περίπτωση του κυβερνοπολέμου. Ουσιαστικά, είναι δυσχερής η νομική αξιολόγηση των κυβερνοεπιχειρήσεων ως βίαιες εφόσον δεν προκαλούν άμεσα θάνατο, σωματικές ή φυσικές υλικές καταστροφές.

Ο Geers εύστοχα σημειώνει ότι σοβαρές επιθέσεις μέσω του κυβερνοχώρου σε κρίσιμες υποδομές είναι μόνο θέμα χρόνου.[9] Επιπλέον, ο Πρόεδρος Barack Obama αναγνωρίζοντας τον κίνδυνο που θέτει ο κυβερνοπόλεμος, σημείωσε σε ομιλία του το 2009 ότι «η ψηφιακή μας υποδομή [...] αποτελεί στρατηγικό εθνικό κεφάλαιο.»[10] Οι Farwell και Rohozinski καταγράφουν τις μεγάλες δυνατότητες επιθέσεως με μικρότερο κίνδυνο, οι οποίες παρέχονται από τις κυβερνοεπιχειρήσεις σε σχέση με τα παραδοσιακά στρατιωτικά μέσα και φανερώνουν την ασυμμετρία αυτών των επιθέσεων.[11] Οι Kremer και Müller αναδεικνύουν το ρόλο του κυβερνοχώρου στις Διεθνείς Σχέσεις.[12] Συνεπώς, οι δυνατότητες που παρέχει ο κυβερνοχώρος αποτελούν ένα σημαντικό συντελεστή ισχύος διαδραματίζοντας καίριο ρόλο στη διαμόρφωση της διεθνούς πραγματικότητας.

Στον παρακάτω πίνακα αποτυπώνονται οι κυριότερες μορφές κυβερνοεπιθέσεων.[13]

[9] Kenneth Geers, "The Cyber Threat To National Critical Infrastructures: Beyond Theory", *Information Security Journal: A Global Perspective*, Vol. 18 (2009), 1-7.

[10] The White House. *Remarks by the President on Securing Our Nation's Cyber Infrastructure.*, 2009,https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure , τελευταία επίσκεψη στις 28.7.018.

[11] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Global Politics and Strategy*, Vol. 53 (2011), 23-40.

[12] Jan-Frederik Kremer and Benedict Müller (επιμ), *Cyberspace and International Relations: Theory, Prospects and Challenges, (*New York: Springer, 2013).

[13] Adam Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies*, Vol. 35.3 (2012), 401-428.

Τύπος Επίθεσης	**Περιγραφή**	**Βασικά Χαρακτηριστικά**	**Πιθανοί Στόχοι**	**Παράδειγμα επιθέσεων**
Δίκτυα Botnets /Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών (DDoS)	Το bot είναι ένα αυτοματοποιημένο κακόβουλο πρόγραμμα που μολύνει ένα εύρος διευθύνσεων δικτύου (IP address - Internet Protocol address) και επηρεάζει ευάλωτους υπολογιστές. Αυτό επιτρέπει στους εισβολείς να παίρνουν τον έλεγχο πολλών υπολογιστών ταυτόχρονα, να τους μετατρέπουν σε «ζόμπι» και να συνθέτουν ένα δίκτυο botnet. Οι μολυσμένοι υπολογιστές μπορεί τότε να χρησιμοποιηθούν σε κατανεμημένες επιθέσεις άρνησης υπηρεσιών (Distributed Denial of Service - DDoS).	Σχετικά χαμηλό κόστος και όχι περίπλοκη υλοποίηση. Τα άμεσα αποτελέσματα της επίθεσης περιορίζονται στη διακοπή της πρόσβασης σε δικτυακές υπηρεσίες.	Οποιοδήποτε δίκτυο (συνηθέστερα δίκτυα συνδεδεμένα στο Διαδίκτυο).	Κατά τη διάρκεια του πολέμου του 2008 μεταξύ της Ρωσίας και της Γεωργίας, οπότε οι Γεωργιανοί δεν είχαν πρόσβαση σε εξωτερικούς ιστοτόπους.
Βασικό Κακόβουλο Λογισμικό	Κακόβουλοι κώδικες/προγράμματα υπολογιστών που χρησιμοποιούν συγκεκαλυμμένα μέσα για να δημιουργήσουν σημεία πρόσβασης, να μεταδώσουν δεδομένα	Χαμηλό κόστος. Χρήσιμος τρόπος εναντίον αδαών χρηστών και συστημάτων που δεν είναι καλά ασφαλισμένα.	Οποιοσδήποτε υπολογιστής ή δίκτυο.	Ιοί,worm, spyware.

	χωρίς αντίστοιχη εξουσιοδότηση ή / και να διαταράξουν τον τρόπο συμπεριφοράς των συστημάτων-στόχων.			
Προηγμένο Κακόβουλο Λογισμικό	Όπως παραπάνω.	Το προηγμένο κακόβουλο λογισμικό μπορεί να επιτεθεί επιτυχώς σε καλά ασφαλισμένα δίκτυα. Απαιτεί υψηλό επίπεδο γνώσης για το σχεδιασμό και την υλοποίηση. Έχει κόστος, τόσο ως προς το χρόνο σχεδιασμού όσο και ως προς τους οικονομικούς πόρους που απαιτούνται για την ανάπτυξή του. Μπορεί δυνητικά να στραφεί εναντίον φυσικών υποδομών.	Κρίσιμες υποδομές.	Ο ιός Stuxnet, που θεωρείται ότι στράφηκε εναντίον των πυρηνικών εγκαταστάσεων του Ιράν.

Ο Λιαρόπουλος[14] κατηγοριοποιεί τις κυβερνοεπιχειρήσεις σε κυβερνοκατασκοπεία (cyberespionage), παραμόρφωση/αλλαγή ιστοσελίδων (website defacement) ή βανδαλισμό (web vandalism), άρνηση παροχής υπηρεσιών και επιθέσεις κατά των κρίσιμων υποδομών, σημειώνοντας ότι τα σενάρια συγκρούσεων στον κυβερνοχώρο περιλαμβάνουν επιθέσεις τόσο στο λογισμικό (λογικές βόμβες, ιούς υπολογιστών κ.λπ.) όσο και στο υλικό (ηλεκτρομαγνητικά όπλα).

Κυβερνοεπιθέσεις στην Εσθονία και στη Γεωργία

Η Ρωσία, μετά την κατάρρευση της ΕΣΣΔ, υιοθέτησε την προσέγγιση του «Εγγύς Εξωτερικού». Αυτός είναι ένας όρος που υπονοεί ότι η «Ρωσία έχει αυξημένο ενδιαφέρον στις περιοχές της πρώην Σοβιετικής Ένωσης, λόγω ιστορικών καταβολών,

[14] Andrew Liaropoulos, "Cyber-security and the Law of War: The Legal and Ethical Aspects of Cyber-conflict." 2011, *Greek Politics Specialist Group Working Paper* 7, http://www.gpsg.org.uk/docs/GPSG_Working_Paper_07.pdf τελευταία επίσκεψη στις 28.7.018.

γεωγραφικής εγγύτητας αλλά και ισχυρής εκεί παρουσίας ρωσικής διασποράς.»[15] Ειδικότερα, κορυφαίας σημασίας για τη Ρωσία έχουν αναδειχτεί η Γεωργία, η Εσθονία και η Ουκρανία, για διαφορετικούς λόγους η καθεμία. Κατά συνέπεια, η Ρωσία μέσα από το δόγμα του «Εγγύς Εξωτερικού», το οποίο αποτελεί την «κορυφαία προτεραιότητα της ρωσικής μετασοβιετικής στρατηγικής,»[16] καταδεικνύοντας τη στρατηγική της, υπό την έννοια «του ορθολογικού προσδιορισμού των ζωτικών συμφερόντων του έθνους, σχετικά με τα ουσιώδη ζητήματα ασφαλείας του, τους θεμελιώδεις σκοπούς του, τις σχέσεις του με τα άλλα έθνη και με την προτεραιότητα ανάμεσα στους διάφορους στόχους του.»[17] Η άνοδος του Vladimir Putin στη ρωσική προεδρία το 2000 κατέστησε τις ισορροπίες της περιοχής πιο περίπλοκες, λόγω της έντονης ρωσικής επιθυμίας προώθησης των συμφερόντων της, κάνοντας πολλούς μελετητές να θεωρούν πλέον τη ρωσική εξωτερική πολιτική ως προϊόν του καθεστώτος Putin [18].

Για την προάσπιση και την προώθηση των συμφερόντων της στο χώρο του Εγγύς Εξωτερικού, η Ρωσία έχει χρησιμοποιήσει ποικίλα μέσα, από την οικονομική διπλωματία έως τη στρατιωτική επέμβαση και τις κυβερνοεπιχειρήσεις. Η χρήση των κυβερνοεπιχειρήσεων ως μέσου επίτευξης στρατηγικών στόχων από την πλευρά της Ρωσίας εξετάζεται στο πλαίσιο των διενέξεών της με την Εσθονία και τη Γεωργία, οι οποίες εντάσσονται και οι δύο στο δόγμα του «Εγγύς Εξωτερικού». Το 2007, οι εσθονικές αρχές αποφάσισαν την μετακίνηση στα περίχωρα ενός Σοβιετικού μνημείου του Β' Παγκοσμίου Πολέμου από το κέντρο του Ταλίν, με τη ρωσική διασπορά να προβάλει σθεναρές αντιρρήσεις σε αυτή την ενέργεια. Η καθαίρεση του μνημείου προκάλεσε αγανάκτηση στο ρωσόφωνο πληθυσμό της Εσθονίας,[19] ενώ η χώρα δέχτηκε κυβερνοεπίθεση τύπου κατανεμημένης άρνησης υπηρεσιών, η οποία ξεκίνησε την 27 Απριλίου 2007 και διήρκεσε 22 ημέρες.[20] Με δεδομένο ότι υποδομές ζωτικής σημασίας για την Εσθονία, όπως το δίκτυο διανομής ηλεκτρικής ισχύος, η λειτουργία των κυβερνητικών επιχειρήσεων, οι τραπεζικές υπηρεσίες, ακόμη και η υδροδότηση του Ταλίν, βασίζονται σε πληροφοριακά συστήματα, το πλήγμα στην

---

[15] Rajan Menon, "*After Empire: Russia and the Southern "Near Abroad*"". Στο: Michael Mandelbaum (επιμ) *The New Russian Foreign Policy (*New York: Council on Foreign Relations, 1998), 100-166.

[16] Θεόδωρος Τσακίρης, "Το Δόγμα του "Εγγύς Εξωτερικού": Η Ρωσική Εξωτερική Πολιτική Έναντι της Ουκρανίας", στο: Μ. Καραγιάννης (επιμ) *Η Ρωσία Σήμερα. Πολιτική, Οικονομία και Εξωτερικές Σχέσεις,(*Αθήνα: Παπαζήσης, 2010), 181-197.

[17] Gordon Craig and Felix Gilbert, "Σκέψεις για τη Στρατηγική Σήμερα και στο Μέλλον» στο Peter Paret (επιμ), *Οι Δημιουργοί της Σύγχρονης Στρατηγικής. Από το Μακιαβέλλι στην Πυρηνική Εποχή, (Αθήνα: Τουρίκης, 2004),* 1021-1030.

[18] Brandon Valeriano and Ryan Maness, "Russia And The Near Abroad: Applying a Risk Barometer For War", *The Journal of Slavic Military Studies,*Vol.25, (2012),125-148.

[19] Damien McGuinness, "*How a Cyber-Attack Transformed Estonia".* BBC News, 27 April 2017, http://www.bbc.com/news/39655415 , τελευταία επίσκεψη στις 28.7.018.

[20] Will *Goodman*, "Cyber Deterrence. Tougher in Theory Than in Practice?" *Strategic Studies Quarterly*, Vol. 4, (2010), 102-135.

εσθονική κοινωνία ήταν ισχυρό.[21] Η επίθεση πραγματοποιήθηκε με τη χρήση υπολογιστών «ζόμπι».[22] Η χρήση της συγκεκριμένης τεχνικής δυσχεραίνει την ανίχνευση της προέλευσής της. Η Εσθονία κατήγγειλε την επίθεση στην ΕΕ και στο ΝΑΤΟ, ζητώντας τη συνδρομή τους. Παρόλο που οι οργανισμοί αυτοί διαθέτουν προσωπικό με κατάλληλη τεχνογνωσία, δεν ήταν σε θέση να επιβεβαιώσουν τη ρωσική συμμετοχή στην επίθεση.[23] Ωστόσο, υπήρχαν έντονες ενδείξεις ρωσικής εμπλοκής, αν όχι ενορχήστρωσης της κυβερνοεπίθεσης. Ρωσόφωνοι ιστότοποι δημοσίευαν οδηγίες σχετικά με το πότε και πώς να εκτελούνται οι επιθέσεις κατανεμημένης άρνησης υπηρεσιών. Επιπλέον, Εσθονοί αξιωματούχοι ισχυρίστηκαν ότι διευθύνσεις του πρωτοκόλλου Διαδικτύου (IP), οι οποίες ανήκαν σε μέλη του γραφείου του Putin, χρησιμοποιήθηκαν στις επιθέσεις. Τέλος, αρκετοί υποστήριξαν ότι ένδειξη ρωσικής εμπλοκής αποτέλεσε το γεγονός πως παρόλο που η Ρωσία και η Εσθονία είχαν υπογράψει συνθήκη αμοιβαίας δικαστικής συνδρομής, την οποία επικαλέστηκε η Εσθονία μετά τις επιθέσεις, η Ρωσία δεν διευκόλυνε τη διεξαγωγή εμπεριστατωμένης έρευνας. Σε κάθε περίπτωση πάντως, δεν υπάρχουν απτές αποδείξεις ότι η ρωσική κυβέρνηση διεύθυνε τις κυβερνοεπιχειρήσεις,[24] αναδεικνύοντας την δυσκολία απόδοσης ευθυνών σε αυτού του είδους τις ενέργειες[25].

Την 8 Αυγούστου 2008 ο ρωσικός στρατός εισέβαλε στη Γεωργία, ενώ πολλές συντονισμένες κυβερνοεπιχειρήσεις έλαβαν χώρα παράλληλα με τις αμιγώς στρατιωτικές ενέργειες. Αν και οι κυβερνοεπιθέσεις δεν αποδείχτηκε ότι καθοδηγούνταν από τη ρωσική κυβέρνηση, είχαν σημαντικό ψυχολογικό αντίκτυπο στη Γεωργία, απομονώνοντάς την από τον έξω κόσμο[26]. Οι κυβερνοεπιθέσεις, οι οποίες ξεκίνησαν στα τέλη Ιουλίου και κορυφώθηκαν την 8η Αυγούστου, δηλαδή την ημέρα της ρωσικής στρατιωτικής επέμβασης, ήταν τριών τύπων. Κατά πρώτον, αφορούσαν σε προπαγανδιστικές ενέργειες, στρεφόμενες κυρίως κατά του τότε προέδρου της Γεωργίας, Mikheil Saakashvili, μέσω παραμόρφωσης (website defacement) ή διαδικτυακού βανδαλισμού γεωργιανών κυβερνητικών ιστοσελίδων. Το δεύτερο είδος επιθέσεων ήταν άρνησης υπηρεσιών εναντίον γεωργιανών δικτυακών τόπων, δημόσιων και ιδιωτικών. Το τρίτο είδος εστίασε στην προσπάθεια διανομής κακόβουλου λογισμικού, κυρίως μέσω ρωσόφωνων δικτυακών τόπων, που παρείχαν

[21] Goodman, "Cyber Defence".

[22] «Υπολογιστής-ζόμπι» είναι ο υπολογιστής που τον έλεγχο του έχει κάποιος τρίτος, χωρίς να το γνωρίζει ο νόμιμος κάτοχος ή εξουσιοδοτημένος χειριστής του. Σε μία τέτοια περίπτωση ο υπολογιστής-«ζόμπι» γίνεται μέρος ενός botnet, ενός δικτύου υπολογιστών-ζόμπι. Οι υπολογιστές αυτοί, μολυσμένοι με κακόβουλο λογισμικό, εξυπηρετούν τους σκοπούς των παράνομων χειριστών τους. Βλ. Craig Schiller and James Binkley, *Botnets: The Killer Web Applications*, (New York: Elsevier,2011).

[23] Herzog, S., "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security,* Vol. 4, (2016), 49-60.

[24] Goodman, "Cyber Defence", 111.

[25] Περισσότερα για τις διαδικασίες ανίχνευσης κυβερνοεπίθεσης (cyber forensics) αναφέρει ο Wei Ren, "Modeling Network Forensics Behavior", *Journal of Digital Forensic Practice,* Vol. 1, ()2006, 57-65.

[26] Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia". *Military Review,* Vol. *T*9:1, (2011), 63.

τεχνικές οδηγίες.[27] Λαμβάνοντας υπόψη ότι η εξάρτηση της Γεωργίας από τις τεχνολογίες διαδικτύου ήταν, και παραμένει, πολύ μικρότερη από την αντίστοιχη της Εσθονίας, ο αντίκτυπος των επιθέσεων στους γεωργιανούς στόχους είχε κυρίως ψυχολογικά αποτελέσματα, συμβάλλοντας καθοριστικά στον περιορισμό της δυνατότητας της γεωργιανής κυβέρνησης να επικοινωνεί διεθνώς προβάλλοντας τις θέσεις της. Όπως και στην περίπτωση της Εσθονίας, το 2007, έτσι και στην περίπτωση των κυβερνοεπιθέσεων στη Γεωργία, ένα χρόνο αργότερα υπήρξε, αδυναμία απόδοσης των ευθυνών.[28]

Κυβερνοεπιχειρήσεις και στρατηγικές προσεγγίσεις

Η χρήση του κυβερνοχώρου ως μέσου προώθησης πολιτικών σκοπών γίνεται εμφανής μέσα από περιπτώσεις όπως αυτές των κυβερνοεπιθέσεων εναντίον της Εσθονίας και της Γεωργίας. Ωστόσο, υπάρχουν διαφορετικές απόψεις σχετικά με τη δυνατότητα των κυβερνοεπιθέσεων να αντικαταστήσουν τα συμβατικά μέσα. Ο Rid, στηριζόμενος στον Clausewitz, αναφέρεται στα τρία θεμελιώδη στοιχεία του πολέμου.[29] Το πρώτο είναι ο βίαιος χαρακτήρας του. Το δεύτερο αφορά στην καθοριστική σημασία του, η οποία συνίσταται στην χρήση βίας ή στην απειλή χρήσης βίας ως μέσου ώστε ο αντίπαλος να αποδεχθεί τη βούληση του επιτιθέμενου. Το τρίτο στοιχείο, συνίσταται στην πολιτική φύση του πολέμου, αφού τελική επιδίωξη των αντιπάλων είναι η επίτευξη πολιτικών σκοπών. Ο Rid, μέσα από τη συλλογιστική του, καταλήγει στο συμπέρασμα ότι οι κυβερνοεπιθέσεις δεν αποτελούν μορφή πολέμου επειδή δεν πληρούν αυτά τα τρία κριτήρια. Οι κυβερνοεπιθέσεις, σύμφωνα με τον ισχυρισμό του, είναι απλώς εκλεπτυσμένες εκδόσεις τριών δραστηριοτήτων που είναι τόσο παλιές όσο και οι ίδιοι οι πόλεμοι: της δολιοφθοράς, της κατασκοπείας και της ανατροπής της νόμιμης εξουσίας.

Ο Stone από τη μεριά του, αντιπαραβάλει την δική του οπτική στην άποψη του Rid.[30] Σύμφωνα με αυτή, οι κυβερνοεπιθέσεις μπορούν να νοηθούν ως βίαιες πράξεις, των οποίων οι συνέπειες πολλαπλασιάζονται από τη χρήση της τεχνολογίας, παραπέμποντας σε ασύμμετρες απειλές. Οι πολεμικές δράσεις συνεπάγονται την άσκηση εξαναγκασμού (force) προκειμένου να παράγουν βίαια (violent) αποτελέσματα. Αυτά τα αποτελέσματα δεν είναι απαραίτητο να είναι θανατηφόρα, αλλά εξακολουθούν να εμπίπτουν στην κατηγορία των πολεμικών πράξεων. Η τεχνολογία, επομένως, αποτελεί μέσο δράσης, μέσω του οποίου μικρή ποσότητα δύναμης μεταφράζεται σε μεγάλη ποσότητα βίας. Όσον αφορά τους ισχυρισμούς του

[27] Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, (2012), 5-32.

[28] Σύμφωνα με το Jeffrey Carr, εμπειρογνώμονα ασφαλείας στον κυβερνοχώρο, οι ρωσικές υπηρεσίες Foreign Military Intelligence Agency (GRU) και Federal Security Service (FSB) πιθανότατα βοήθησαν στο συντονισμό των επιθέσεων, χωρίς πάντως μέχρι σήμερα να έχουν υπάρξει αποδείξεις επί αυτού (Βλ. Rid, "Cyber War Will Not Take Place", 14.).

[29] Rid, "Cyber War Will Not Take Place".

[30] John Stone. "Cyber War Will Take Place! , *Journal of Strategic Studies*, Vol. 36, (2013), 101-108.

Rid, ο Stone αντιπαραθέτει ότι διάφοροι δρώντες, ενεργώντας στρατηγικά, ενδέχεται να προωθήσουν συγκεκαλυμμένους πολιτικούς στόχους μέσω συγκεκαλυμμένων πράξεων βίας. Μέσα από αυτό το συλλογισμό, ο Stone καταλήγει ότι οι επιθέσεις στον κυβερνοχώρο θα μπορούσαν να αποτελούν πράξεις πολέμου.

Σε κάθε περίπτωση, είτε οι κυβερνοεπιθέσεις αποτελούν εκδοχές δραστηριοτήτων όπως η δολιοφθορά και η κατασκοπεία, σύμφωνα με τον Rid, είτε αποτελούν πολεμικές πράξεις, σύμφωνα με τον Stone, ο κυβερνοχώρος έχει αναχθεί σε μέσο προώθησης στρατηγικών στόχων. Οι στρατηγικοί αυτοί στόχοι άλλοτε επιτυγχάνονται και άλλοτε όχι. Στην περίπτωση της Εσθονίας, η επίδραση αυτών των συντονισμένων διαδικτυακών επιθέσεων, οι οποίες διέκοψαν προσωρινά τη ροή πληροφοριών μεταξύ της εσθονικής κυβέρνησης και των πολιτών της, είχε αντίκτυπο στην κοινωνία, αλλά τελικά παρέμεινε ήσσονος σημασίας.[31] Παρόλα αυτά, ο κοινωνικός αντίκτυπος δεν μπορεί να θεωρηθεί αμελητέος, καθώς επέφερε πλήγμα στο ηθικό του αντιπάλου. Ο Γάλλος συνταγματάρχης Charles Ardant du Picq είχε, με σαφήνεια, περιγράψει τη σημασία του ηθικού κατά τη διεξαγωγή πολεμικών επιχειρήσεων,[32] ενώ και ο Paret σημειώνει πως «ήδη από την Αρχαιότητα, οι συγγραφείς τόνιζαν τη σημασία που έχουν τα συναισθήματα κατά τον πόλεμο.» [33]

Η υπόθεση της Εσθονίας του 2007 αποτελεί παράδειγμα επιχειρήσεων που έλαβαν χώρα αμιγώς στον κυβερνοχώρο, ενώ στην περίπτωση της Γεωργίας οι κυβερνοεπιχειρήσεις αποτέλεσαν ενισχυτικό παράγοντα των κύριων στρατιωτικών δράσεων.[34] Μολονότι η «εικονική φύση των κυβερνοεπιχειρήσεων μπορεί να περιορίσει τον αντίκτυπο της βίας,»[35] ο Clausewitz είχε διατυπώσει τη θέση ότι σκοπός του πολέμου μπορεί να είναι η καταστροφή του εχθρού και, όπως παραθέτει ο Paret, αυτό μπορεί να γίνει «[..]αν τον καταστήσουμε (σ.σ. τον αντίπαλο) πολιτικά ανήμπορο ή στρατιωτικά ανίκανο αναγκάζοντάς τον να υπογράψει οποιαδήποτε συνθήκη ειρήνης θέλουμε.»[36] Επομένως, εκλαμβανόμενες οι κυβερνοεπιχειρήσεις ως μέσο άσκησης πιέσεως στον αντίπαλο, μπορούν να θεωρηθούν ως μια, επί το πλείστον αναίμακτη, μετεξέλιξη των θεωρήσεων του Clausewitz. Επιπλέον, μία από τις θέσεις του Clausewitz ήταν ότι «η έλλειψη πληροφοριών μειώνει την ικανότητα των διοικητών και των πολιτικών να ενεργούν αποτελεσματικά.»[37] Υπό αυτή την έννοια, μία κυβερνοεπίθεση που στρέφεται και κατά της δυνατότητας επικοινωνίας του αντιπάλου, όπως με τις κατανεμημένες επιθέσεις άρνησης υπηρεσιών κατά της Εσθονίας ή με την ουσιαστική αδυναμία προβολής των γεωργιανών θέσεων στο

[31] Rid, "Cyber War Will Not Take Place".

[32] Charles Ardant du Picq, *Etudes sur le Combat*, (Paris: 1880), Διαθέσιμο στο https://gallica.bnf.fr/ark:/12148/bpt6k864841/f4.image τελευταία επίσκεψη στις 28.7.018.

[33] Peter Paret,"Κλαούζεβιτς" στο Peter Paret (επιμ), *Οι Δημιουργοί της Σύγχρονης Στρατηγικής. Από το Μακιαβέλλι στην Πυρηνική Εποχή, (Αθήνα: Τουρίκης, 2004),* 229-264.

[34] Goodman, "Cyber Defence", 104.

[35] Kremer and Müller, *Cyberspace and International Relations, 29-30.*

[36] Paret,"Κλαούζεβιτς", 241.

[37] Kremer and Müller, *Cyberspace and International Relations, 30.*

εξωτερικό, φανερώνει την εφαρμογή των απόψεων του Clausewitz στον κυβερνοχώρο. Μια ακόμη σημαντική έννοια που χρησιμοποιεί ο Clausewitz είναι αυτή του κέντρου βάρους, το οποίο μπορεί να νοηθεί σαν ένας σύνδεσμος, η απώλεια του οποίου είναι καταστρεπτική για την ικανότητα των δρώντων να διεξάγουν πόλεμο.[38] Το κέντρο βάρους απαιτεί ενότητα διοικήσεως, η οποία μπορεί κάλλιστα να πληγεί από κυβερνοεπιθέσεις που στρέφονται κατά της ικανότητας της διοίκησης να επικοινωνεί τους στόχους της.[39]

Στην προσέγγιση του Sun Tzu κυρίαρχο ρόλο είχε η «παραπλάνηση (deception)»,[40] η οποία αποτελεί εγγενές στοιχείο των κυβερνοεπιχειρήσεων. Επιπλέον, η δυσκολία απόδοσης ευθυνών σε περιπτώσεις κυβερνοεπιθέσεων ενισχύει το αίσθημα της παραπλάνησης για τον πληγέντα και δίνει πλεονέκτημα στον επιτιθέμενο.[41] Η ιδανική νίκη, σύμφωνα με το Tzu, είναι αυτή που επιτυγχάνεται αν είναι δυνατόν «χωρίς να δώσεις μάχη.»[42] Οι επιχειρήσεις στον κυβερνοχώρο παρέχουν τη δυνατότητα προώθησης πολιτικών σκοπών κατά κανόνα αναίμακτα, με ελάχιστο σχετικό κόστος για τον επιτιθέμενο. Περαιτέρω, ο Greathouse υποστηρίζει ότι οι κυβερνοεπιχειρήσεις δίνουν τη δυνατότητα βαθύτερης γνώσης του αντιπάλου, μέσω πρόσβασης στα πληροφοριακά του συστήματα, που είναι σημαντική σύμφωνα με τον Sun Tzu.[43] Ο τελευταίος υποστήριξε πως «όταν γνωρίζεις καλά τον εχθρό και γνωρίζεις και τον εαυτό σου καλά, μπορεί να δώσεις εκατό μάχες και να κερδίσεις και τις εκατό.»[44]

Ο θεωρητικός της αεροπορικής στρατηγικής Douhet διατύπωσε τη θέση περί μη διάκρισης μαχίμων και αμάχων.[45] Εξετάζοντας τη φύση των κυβερνοεπιχειρήσεων, διαπιστώνουμε ότι αποτελούν ένα είδος επιθέσεων που στρέφονται τόσο κατά στρατιωτικών όσο και κατά μη-στρατιωτικών στόχων, όπως σημειώνει και ο Greathouse.[46] Αυτή η κατάργηση της διάκρισης μεταξύ των στόχων, ασκεί σημαντική επίδραση στο ηθικό του αντιπάλου, επιφέροντας κοινωνική διαταραχή και πλήτωντας την ικανότητα διεξαγωγής πολέμου, αφού «μειώνεται η επιθυμία του λαού για αντίσταση.»[47] Ένα ακόμη στοιχείο που τονίζει ο Douhet, όσον αφορά τις αεροπορικές επιχειρήσεις, είναι αυτό της ταχύτητας, το οποίο είναι εγγενές δομικό χαρακτηριστικό και των σύγχρονων πληροφοριακών συστημάτων. Η ταχύτητα είναι αυτή που καθιστά το «αεροπλάνο ένα επιθετικό όπλο par excelance,»[48] κάτι το οποίο ισχύει και

---

[38] Antulio Echevarria II, *Clausewitz and Contemporary War. (*Oxford: Oxford University Press, 2007), όπως παρατίθεται στους Kremer and Müller.

[39] Greathouse, "Cyber War and Strategic Thought", 30.

[40] Sun Tzu, *Η Τέχνη του Πολέμου, (Αθήνα: Περίπλους, 2003),* 22.

[41] Greathouse, "Cyber War and Strategic Thought",31.

[42] Sun Tzu, *Η Τέχνη του Πολέμου,* 29.

[43] Greathouse, "Cyber War and Strategic Thought",31.

[44] Sun Tzu, *Η Τέχνη του Πολέμου,29*

[45] Giulio Douhet, *The Command of the Air,*(Washington: Office of Air Force History,1983).

[46] Greathouse, "Cyber War and Strategic Thought",31.

[47] Douhet, *The Command of the Air,* viii.

[48] Στο ίδιο, 15.

στην περίπτωση των κυβερνοεπιχειρήσεων όπως φαίνεται και από τις περιπτώσεις κυβερνοεπιθέσεων εναντίον της Εσθονίας και της Γεωργίας.

Οι ιδέες του John Warden αποτέλεσαν τη βάση των αεροπορικών επιδρομών κατά τον Πρώτο Πόλεμο του Κόλπου(1991). Ο Warden συνδύασε στοιχεία από τις προσεγγίσεις που διατυπώθηκαν από τους κλασσικούς θεωρητικούς της στρατηγικής με την κατανόηση της σύγχρονης τεχνολογικής καινοτομίας.[49] Επιπλέον, υπήρξε από τους πρώτους που αναφέρθηκαν ευθέως στη χρήση κακόβουλων λογισμικών ως μέσου στρατηγικής.[50] Υποστήριξε ότι ο αντίπαλος πρέπει να θεωρείται ως ένα σύστημα αποτελούμενο από πέντε υποσυστήματα που δημιουργούν ομόκεντρους δακτυλίους.[51] Οι δακτύλιοι αυτοί είναι η ηγεσία, που βρίσκεται στον πυρήνα, τα είδη ζωτικής σημασίας,[52] οι υποδομές,[53] ο πληθυσμός και ο αμιγώς στρατιωτικός μηχανισμός. Οι επιθέσεις πρέπει να κατευθύνονται από το κέντρο του δακτυλίου, την ηγεσία, προς την περιφέρεια, τους στρατιωτικούς στόχους.[54] Οι κυβερνοεπιθέσεις κατά της Εσθονίας και της Γεωργίας ακολούθησαν τη λογική των ομόκεντρων κύκλων, χωρίς πάντως τελικά να πλήξουν όλους τους δακτύλιους. Στη μεν Εσθονία εστίασαν κυρίως στο δεύτερο δακτύλιο των ειδών ζωτικής σημασίας. Λαμβάνοντας υπόψη τη διασύνδεση της Εσθονίας στον κυβερνοχώρο, τα πληροφοριακά συστήματα αποτελούν είδη ανάλογης σημασίας με τις πετρελαιοπηγές για το Ιράκ. Στη δε Γεωργία, οι κυβερνοεπιθέσεις εστίασαν στην ηγεσία, προσπαθώντας να πλήξουν και να αποκόψουν τον πρόεδρο Saakashvili.

Συμπεράσματα

Αν και οι επιθέσεις στον κυβερνοχώρο δεν συνάδουν, τουλάχιστον έως σήμερα, με τις συμβατικές στρατιωτικές επιχειρήσεις από την άποψη της άσκησης φυσικής βίας, εντούτοις μπορούν να αποτελέσουν εξίσου χρήσιμα εργαλεία επίτευξης στρατηγικών στόχων. Στις περιπτώσεις της Εσθονίας και της Γεωργίας οι κυβερνοεπιθέσεις αποτέλεσαν μέσο προώθησης των ρωσικών συμφερόντων, έστω και αν δεν αποδείχτηκε επίσημη ανάμιξη της ρωσικής κυβέρνησης. Η αδυναμία απόδοσης ευθυνών αποτελεί ένα σημαντικό στοιχείο των κυβερνοεπιθέσεων, αφού ο επιτιθέμενος μπορεί να πλήξει τον στόχο του, εστιάζοντας κυρίως στο ηθικό και στη συνοχή της κοινωνίας, χωρίς να υφίσταται στον ίδιο βαθμό τον έλεγχο, τις νομικές κυρώσεις και τις τυχόν πιέσεις του διεθνούς περιβάλλοντος για τη δράση του. Συνεπώς, ο κυβερνοχώρος αποτελεί πεδίο όπου οι δρώντες μπορούν συγκεκαλυμμένα να προωθήσουν τις επιδιώξεις τους, χωρίς να χρειαστεί να καταφύγουν απαραιτήτως

[49] Greathouse, "Cyber War and Strategic Thought", 35.
[50] John Warden, "The Enemy as a System", *Airpower Journal*, Vol. IX, No. I, 1995, 40-55.
[51] Warden, "The Enemy as a System", 44.
[52] Αυτά αφορούν στα στοιχεία που είναι κρίσιμα για την ύπαρξη του κράτους. Στην περίπτωση του Ιράκ αυτά συνίσταντο στις πετρελαιοπηγές.
[53] Λιμάνια, δρόμοι, τηλεπικοινωνίες.
[54] Warden, "The Enemy as a System", 44-54.

σε στρατιωτικές επιχειρήσεις, οι οποίες σε κάθε περίπτωση είναι περισσότερο κοστοβόρες, τόσο οικονομικά όσο και από άποψη ανθρώπινων απωλειών. Ακόμη, όμως, και σε περιπτώσεις που επιλεγούν τα στρατιωτικά μέσα, οι κυβερνοεπιχειρήσεις μπορούν να χρησιμοποιηθούν ως προπαρασκευαστικά μέσα των κυρίως επιθέσεων, όπως στην περίπτωση της Γεωργίας, ώστε να μειωθεί το κόστος τους και να πολλαπλασιαστούν οι πιθανότητες επιτυχίας.

Όσον αφορά την αξιολόγηση των αποτελεσμάτων των κυβερνοεπιθέσεων, παρουσιάζονται δυσχέρειες λόγω της αδυναμίας απόδοσης ευθυνών. Μη γνωρίζοντας αποδεδειγμένα τους δρώντες, αδυνατούμε να αποσαφηνίσουμε πλήρως και τους τεθέντες στόχους τους. Δεχόμενοι πάντως τους ισχυρισμούς της Εσθονίας και της Γεωργίας περί ρωσικής εμπλοκής, μπορούμε να εξάγουμε χρήσιμα συμπεράσματα. Στην περίπτωση της πρώτης, αν και ο φανερός στόχος της παραμονής του σοβιετικού μνημείου δεν επετεύχθη, υπήρξαν δύο άλλες σημαντικές προεκτάσεις. Αφενός υπήρξε έντονη υπενθύμιση της ισχύος της ρωσικής διασποράς εντός της εσθονικής επικράτειας, αφετέρου δε αποδείχτηκε στην πράξη ότι όσο περισσότερο εξαρτάται ένας δρώντας από τον κυβερνοχώρο, τόσο περισσότερο ευάλωτος σε κυβερνοεπιθέσεις καθίσταται. Στην περίπτωση της Γεωργίας, αναδείχθηκε η σημαντική συνεισφορά των κυβερνοεπιχειρήσεων ως προπαρασκευαστικού μέσου των κυρίως επιχειρήσεων. Τελικά, και στις δύο περιπτώσεις υπήρξε προώθηση των ενταγμένων στο δόγμα του «Εγγύς Εξωτερικού» ρωσικών στρατηγικών συμφερόντων.

Συνδέοντας τις στρατηγικές προσεγγίσεις με τον κυβερνοχώρο, διαπιστώνουμε ότι τα σημαντικότερα σημεία σύγκλισης αφορούν την μη διάκριση μεταξύ στρατιωτικών και μη στρατιωτικών στόχων, τη δυνατότητα προσβολής του ηθικού του αντιπάλου και την πιθανή μείωση των μέσων επικοινωνίας του. Αν και υπάρχουν κοινά σημεία με τις σκέψεις κλασσικών θεωρητικών της στρατηγικής, όπως ο Clausewitz, η αεροπορική στρατηγική προσφέρει την πλειονότητα των προσεγγίσεων που μπορούν να βρουν πεδίο εφαρμογής και στον κυβερνοχώρο. Η αντιστοιχία της ταχύτητας και των επιθετικών δυνατοτήτων των αεροπλάνων, που υποστήριξε ο Douhet, προσομοιάζει με τις χρήσεις του κυβερνοπολέμου. Από τη μεριά του Warden, ο ισχυρισμός του ότι η πραγματική ουσία του πολέμου είναι να κάνουμε στον εχθρό «οτιδήποτε είναι απαραίτητο ώστε αυτός να αποδεχτεί τους στόχους μας» δίνει ώθηση στη χρήση των κυβερνοεπιχειρήσεων, ως μέσου στρατηγικής, είτε κύριου είτε συμπληρωματικού, στο σύγχρονο περιβάλλον.[55] Πέραν των αεροπορικών προσεγγίσεων, η συλλογιστική του Sun Tzu, με την έμφαση στην παραπλάνηση και την επίτευξη των σκοπών με το μικρότερο δυνατό κόστος, φέρνει στο προσκήνιο τα πλεονεκτήματα που παρέχει ο κυβερνοχώρος σε όσους μπορούν τεχνολογικά να τον εκμεταλλευτούν. Ωστόσο, πρέπει να ληφθεί υπόψη ότι όσο περισσότερο τεχνολογικά εξελιγμένος, από την άποψη των δικτυακών και πληροφοριακών υποδομών, είναι ένας δρώντας τόσο περισσότερο ευάλωτος καθίσταται σε ενδεχόμενες κυβερνοεπιθέσεις εναντίον του.

[55] Warden, "The Enemy as a System", 55.

Οι κυβερνοεπιχειρήσεις παρέχουν πλήθος δυνατοτήτων, που εκτείνονται από τη συλλογή πληροφοριών και την επίτευξη στρατιωτικών στόχων έως την καταστροφή κρίσιμων υποδομών, εφόσον τα πληροφοριακά συστήματα αποτελούν τους νευρώνες αυτών των υποδομών σήμερα. Για την πλήρη αξιοποίηση των κυβερνοεπιχειρήσεων οι κλασσικές και οι αεροπορικές στρατηγικές προσεγγίσεις προσφέρουν χρήσιμα στοιχεία. Ωστόσο η ραγδαία αυξανόμενη σημασία του κυβερνοχώρου καθιστά αναγκαία τη διατύπωση στρατηγικών προσεγγίσεων αμιγώς προσαρμοσμένων σε αυτόν. Παράλληλα, η σημασία των κυβερνοεπιθέσεων ως μέσου επίτευξης στρατηγικών στόχων, γίνεται συνεχώς αντιληπτή από ολοένα και περισσότερους διεθνείς δρώντες. Είναι χαρακτηριστική η τοποθέτηση του Προέδρου της Κομισιόν Jean-Claude Juncker, τον Σεπτέμβριο του 2017 στην ετήσια ομιλία του για την Κατάσταση της Ένωσης ενώπιον του Ευρωπαϊκού Κοινοβουλίου,[56] όπου ιεράρχησε ως τέταρτη προτεραιότητα της Ένωσης την προστασία των πολιτών της στην εποχή της ψηφιακής εποχής. Ο Juncker τόνισε ότι

> *οι επιθέσεις στον κυβερνοχώρο μπορούν να είναι πιο επικίνδυνες από τα όπλα για τη σταθερότητα των δημοκρατιών και των οικονομιών[…] Οι επιθέσεις στον κυβερνοχώρο δεν γνωρίζουν σύνορα και κανείς δεν είναι απρόσβλητος από αυτές. Αυτός είναι ο λόγος για τον οποίο σήμερα η Επιτροπή προτείνει νέα μέσα, συμπεριλαμβανομένου ενός ευρωπαϊκού οργανισμού για την ασφάλεια στον κυβερνοχώρο, που θα μας βοηθήσει αμυνθούμε σε τέτοιες επιθέσεις,*

δείχνοντας ότι ο οι κυβερνοεπιχειρήσεις αποτελούν ήδη ένα σημαντικό πεδίο διεθνούς ενδιαφέροντος, ιδιαίτερης στρατηγικής σημασίας.

Ο Ανδρέας Θεοφίλης είναι Σημαιοφόρος Ειδικοτήτων του Πολεμικού Ναυτικού. Αποφοίτησε το 1997 από τη ΣΜΥΝ. Ακολούθως υπηρέτησε επί σειρά ετών σε πολεμικά πλοία. Από το 2010 υπηρετεί στο ΓΕΝ/Α4. Το 2009 αποφοίτησε με άριστα (96%) από τη ΣΠΗΥ, το 2011 παρακολούθησε επιτυχώς την ακαδημία Cisco (CCNA) και το 2018 αποφοίτησε με άριστα (9,5) από το Τμήμα Πολιτικών Επιστημών και Διεθνών Σχέσεων του Πανεπιστημίου Πελοποννήσου. Την παρούσα περίοδο τα ερευνητικά του ενδιαφέροντα εστιάζουν στις δυνατότητες και τους περιορισμούς του κυβερνοχώρου στο σύγχρονο διεθνές περιβάλλον.

[56] Jean-Claude Juncker, "President Jean-Claude Juncker's State of the Union Address 2017." *European Commission Press Release Database*, 13 September 2017, http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm τελευταία επίσκεψη στις 28.7.018.

.