*

‘’Η επίθεση σε δίκτυα ηλεκτρονικών υπολογιστών (computer network attack) και η χρήση βίας κατά το διεθνές δίκαιο. (Η επίθεση σε δίκτυα η/υ με τη χρησιμοποίηση των η/υ και δικτύων ως όπλων.)’’

Υπό ***Βασιλείου Γ. Μακρή,*** *Στρατιωτικού Δικαστή Β΄*

*

(Νοέμβριος 2011, ***Πτυχιακή Εργασία*** για το Α’ Επίπεδο του Προγράμματος Μεταπτυχιακών Σπουδών του Τμήματος Νομικής του Τομέα Διεθνών Σπουδών του Δημοκρίτειου Πανεπιστημίου Θράκης, Ακαδημαϊκά Έτη 2008 – 2009 & 2009 – 2010.)

*

Περιεχόμενα

5. Η δυσκολία εξεύρεσης της πραγματικής πηγής της ηλεκτρονικής επίθεσης. — Οι επιθέσεις από μη-κρατικές οντότητες

6. Πώς μπορεί να αντιδράσει το κράτος που γίνεται στόχος μίας CNA

7. Ζητήματα 'ανασχετικής' αυτοάμυνας, αυτοάμυνας εναντίον 'επικείμενης' επίθεσης, καθώς και 'προληπτικής' αυτοάμυνας, στην περίπτωση των CNAs

8. Πώς προσεγγίζονται σήμερα οι CNAs από την πρακτική κρατών και Οργανισμών. — Υπάρχει ανάγκη νέου συμβατικού διεθνούς δικαίου ;

V. Συμπεράσματα

VI. Παράρτημα

1. Ο ηλεκτρονικός υπολογιστής (πρόσθετες πληροφορίες)

2. Το διαδίκτυο (internet) και ο 'παγκόσμιος ιστός' (πρόσθετες πληροφορίες)

*

Συντομογραφίες

Β' ΠΠ	Β' Παγκόσμιος Πόλεμος
ΓΕΕΘΑ	Γενικό Επιτελείο Εθνικής Άμυνας [της Ελλάδος]
Δ.Δ.Χ..	Διεθνές Δικαστήριο της Χάγης
ΔΙΚΥΒ	Διεύθυνση Κυβερνοάμυνας [του ΓΕΕΘΑ]
ΔΠΔ	Διεθνές Ποινικό Δικαστήριο
ΕΥΖΣ	Ευρωπαϊκές Υποδομές Ζωτικής Σημασίας
Η.Ε.	Ηνωμένα Έθνη
Η.Π.Α.	Ηνωμένες Πολιτείες Αμερικής
η/υ	Ηλεκτρονικός υπολογιστής, ηλεκτρονικοί υπολογιστές
Ο.Η.Ε.	Οργανισμός Ηνωμένων Εθνών
Σ.Α.	Συμβούλιο Ασφαλείας
ΥΕΘΑ	Υπουργός Εθνικής Άμυνας
ΥΠ.ΕΘ.Α.	Υπουργείο Εθνικής Άμυνας
ΥΠΕΞ	Υπουργείο Εξωτερικών
ΦΕΚ	Φύλλο Εφημερίδας της Κυβέρνησης

ARPA	Advanced Research Project Agency [Υπηρεσία των Η.Π.Α.]
bot	robot (software)
botnet	robot network
CCD COE	Cooperative Cyber Defence Centre of Excellence [του NATO στην Εσθονία]
CCW	Convention on Certain Conventional Weapons
CIA	Central Intelligence Agency [Υπηρεσία των Η.Π.Α.]
CNA	Computer Network Attack
CNE	Computer Network Exploitation
C4I	Command, Control, Communications, Computers, and (military) Intelligence
DARPA	Defense Advanced Research Projects Agency [Υπηρεσία των Η.Π.Α.]
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service

F.B.I.	Federal Bureau of Investigation [Υπηρεσία των Η.Π.Α.]
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Criminal Court
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the former Yugoslavia
IEEE	Institute of Electrical and Electronics Engineers [Η.Π.Α.]
ILC	International Law Commission
I.O.	Information Operations
IP	Internet Protocol
M.I.T.	Massachusetts Institute of Technology [Η.Π.Α.]
NATO	North Atlantic Council Organization
PDoS	Permanent Denial of Service
SCADA	Supervisory Control And Data Acquisition systems
UN	United Nations
UNCLOS	UN Convention on the Law of the Sea
'worm'	Write Once Read Many [κακόβουλο 'ηλεκτρονικό σκουλήκι' (λογισμικό)]
www	World Wide Web

*

Π η γ έ ς

[Στο κείμενο της εργασίας, οι αναφορές στις πηγές που ακολουθούν γίνεται με την απλή παράθεση του ονόματος του συγγραφέα και της σελίδας του έργου]

- **Β ι β λ ί α**

—Ιωάννου Κρατερός, *Δίκαιο Διεθνούς Ευθύνης,* Κομοτηνή 2003, Εκδ. Εταιρείας Αξιοποίησης & Διαχείρισης Περιουσίας Δημοκρίτειου Πανεπιστημίου Θράκης

—Ρούκουνας Εμμανουήλ, *Διεθνές Δίκαιο*, Τεύχος Πρώτο, 3η έκδ., Α.Ν. Σάκκουλας, 2004

—Antonopoulos Constantine, *The unilateral use of force by states in international law,* 1997 (εκδ. A.N. Σάκκουλα, Publications of the Seminar of International Law and International Relations, Democritos University of Thrace, Faculty of Law, Series A', Papers on International Law 21)

—Brownlie Ian, *International Law and the Use of Force by States,* 1963

—Carr Jeffrey, *Inside Cyber Warfare – Mapping the Cyber Underworld*, O'Reilly, 2010 (on line edition)

—Dinstein Yoram, *War, Aggression and Self-Defence,* 3rd ed., Cambridge University Press (Virtual Publishing) 2003

—Gray Christine, *"International Law and the Use of Force"*, Oxford University Press, 2008 (repr. 2009)

——*The Use Of Force And The International Legal Order,* σε Evans Malcolm D., *International Law,* 2nd ed., Oxford University Press, 2006, σελ. 589 et seq.

—Higgins Rosalyn, *Problems & Process – International Law and How We Use it,* Clarendon Press – Oxford, 1994 (repr. 1995)

—Harris DJ, *Cases and Materials on International Law,* 6th ed., Sweet & Maxwell, 2004

—Kamal Ahmad, *The Law of Cyber-Space – An Invitation to The Table of Negotiations*, United Nations Institute of Training and Research (UNITAR), 2005

—Libicki Martin C., *Cyberdeterrence and cyberwar*, RAND Corporation, 2009 (μελέτη που εκπονήθηκε για λογαριασμό της Πολεμικής Αεροπορίας των Η.Π.Α. (USAF))

—Owens William A., Dam Kenneth W. & Lin Herbert S., eds, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Committee on Offensive Information Warfare Computer Science and

Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, The National Academies Press, Washington D.C., 2009, http://www.nap.edu

—Schmitt Michael N. & O'Donnell Brian T., eds, *Computer Network Attack and International Law,* US Naval War College, International Law Studies, Vol. 76, 2002

—Shaw Malcolm N. QC, *International Law*, 6th ed., Cambridge University Press, 2008, e-Book (EBL)

— Tanenbaum Andrew S., *Structured Computer Organization*, Prentice–Hall International, 4th ed., 1999

—Tikk E., Kaska K., Vihul L., *International Cyber Incidents – Legal Considerations,* Cooperative Cyber Defence Centre of Excellence (CCDCOE) – Estonia, 2010

—Tikk Eneken, *Frameworks For International Cyber Security,* CCDCOE (Estonia), 2010

—Tikk E., Kaska K., Rünnimeri K., Kert M., Talihärm A.-M., Vihul L., *Cyber Attacks Against Georgia: Legal Lessons Identified*, CCDCOE (NATO), Ver. 1.0, November 2008

—United States Air Force Law Review, *Cyberlaw Edition*, vol. 64, 2009

- **Ά ρ θ ρ α**

—Νταϊλιάνης Ευάγγελος, Φυσικός M.Sc., *Πόλεμος στον κυβερνοχώρο – οδεύοντας προς τον ψηφιακό όλεθρο*, περιοδική έκδοση ''Περισκόπιο της επιστήμης'', τ. 348, Μάρτιος 2011, 54 – 69

—Barkham Jason, *Information Warfare And International Law On The Use Of Force,* International Law and Politics, vol. 34 (2001), 57 – 113

—Brown Davis, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, Harvard International Law Journal, Vol. 47, Winter 2006, 179 – 221

— Clark Wesley K. & Levin Peter L., *Securing the Information Highway – How to Enhance the United States' Electronic Defenses*, Foreign Affairs, Nov./Dec. 2009, Vol. 88, numb. 6

—Hollis Duncan B., *Why States Need an International Law for Information Operations*, Lewis & Clark Law Review, Vol. 11:4, 2007, 1023 – 1061

—Ophardt Jonathan A., *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, Duke Law & Technology Review No. 3, 2010

—Roscini Marco, *World Wide Warfare – Jus ad bellum and the Use of Cyber Force,* Max Planck Yearbook of United Nations Law, Vol. 14, 2010, 85 – 130

—Shackelford Scott J., *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law, Vol. 27:1, 2009, 191 – 250

—Schmitt Michael N., *Computer Network Attack and Use of Force in International Law : Thoughts on a Normative Framework*, Columbia Journal of Transnational Law 37 (1998 – 1999), 885 et seq.

——, *Cyber Operations in International Law : The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, Proceedings of a Workshop on Deterring Cyber Attacks : Informing Strategies and Developing Options for U.S. Policy, Committee on Deterring Cyberattacks : Informing Strategies and Developing Options; National Research Council, 2010 (διαθέσιμο στην ιστοσελίδα http://www.nap.edu/catalog/12997.html)

——, *Wired warfare: Computer network attack and jus in bello,* **IRRC,** June 2002, Vol. 84, No 846, 365 – 399

—Theiler Olaf, Dr., *New threats: the cyber-dimension*, στην ηλεκτρονική έκδοση του 'NATO Review', στην ηλεκτρονική διεύθυνση http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm

—Walker Paul A., *Rethinking Computer Network "Attack", Implications for Law and U.S. Doctrine,* 2009

—Watts Sean, *Combatant Status and Computer Network Attack,* Virginia Journal of International Law, Vol. 50:2, 2010, 391 – 447

—Waxman Matthew C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* Columbia Law School, Public Law & Legal Theory Working Paper Group, Paper Number 10-246 (electronic copy from http://ssrn.com/abstract=1674565, Oct. 12, 2010 – to be published in the Yale Journal of International Law, 2011)

—Weisbord Noah, Conceptualizing Aggression, Duke Journal of Comparative & International Law, vol. 20:1, 2009

—Vatis M.A., *The Council of Europe Convention on Cybercrime*, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, http://www.nap.edu/catalog/12997.html, 207 – 223

- **Δ ι α δ ί κ τ υ ο**

—http://ssrn.com

—http://www.rand.org

—http://www.nap.edu/catalog/12997.html

—http://www.techweb.com

—http://webopedia.com

—http://internetsecurityzone.com

—http://www.nato.int

—http://www.un.org/en

—http://www.geetha.mil.gr

—http://www.mod.mil.gr

—http://en.wikipedia.org

—http://el.wilipedia.org

—http://www.isoc.org

*

Αποφάσεις Διεθνών Δικαστηρίων

—ICJ, Corfu Channel Case (U.K. v. Albania), 1949

—ICJ, Case Concerning United States Diplomatic and Consular Staff in Tehran (U.S.A. v. Iran), 1980

—ICJ, Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.A.), 1986

—ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996

—ICJ, Indonesia /Malaysia case, 2002

—ICJ, 'Oil Platforms' case (Iran v. US), 2003

—ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2005

—ICJ, Armed Activities on the Territory of the Congo (DRC v. Uganda), 2005

—ICJ, Bosnia & Herzegovina v. Serbia & Montenegro, Merits, 2007

—ICTY, Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber, 1999

*

"You can't say that civilization don't advance, however, for in every war they kill you in a new way" (Will Rogers, The New York Times, December 23, 1929)

"Cyber-attacks pose difficult line-drawing problems, but we must avoid missing the strategic forest in thinking about the legal trees. Some problems of cyber-warfare for regulating force are at the same time novel yet familiar" (M.C. Waxman)[1]

[1] Waxman, σελ. 24.

Ι. Εισαγωγή

Αυτό που αποκαλούμε σήμερα *'ηλεκτρονικό υπολογιστή'* εμφανίστηκε για πρώτη φορά στη δεκαετία του 1940 και το πρώτο *δίκτυο η/υ* λειτούργησε πειραματικά το έτος 1969.

Σύμφωνα με εξακριβωμένες πληροφορίες, *ήδη* το έτος 1982 η Κεντρική Υπηρεσία Πληροφοριών (CIA) των Η.Π.Α. εκτέλεσε μία *κυβερνο-επιχείρηση* που είχε ως σκοπό —τον οποίο και τελικά πέτυχε— να προμηθεύσει στους Σοβιετικούς ηλεκτρονικό εξοπλισμό με συγκεκριμένες *εκ κατασκευής τρωτότητες* για τη λειτουργία του υπερ-Σιβηρικού αγωγού φυσικού αερίου, ο οποίος (εξοπλισμός) θα προερχόταν, φαινομενικά, από την ελεύθερη αγορά. Το αποτέλεσμα ήταν η πρόκληση *έκρηξης* τρομακτικής ισχύος…[2] Έξι χρόνια μετά, το έτος 1988 —και ήδη πριν από 22 – 23 χρόνια από τη σημερινή εποχή—, κυκλοφόρησε, απ' ό,τι φαίνεται, το πρώτο δείγμα *κακόβουλου λογισμικού* που σήμερα μας απασχολεί καθημερινά, γνωστό ως 'ηλεκτρονικό σκουλήκι' (worm)˙ συγκεκριμένα, στις 02 Νοεμβρίου 1988 ένας φοιτητής του Πανεπιστημίου Cornell μόλυνε με κακόβουλο λογισμικό τύπου 'worm' το δίκτυο η/υ του M.I.T.[3]

Το 2008, στη Γεωργία, εκδηλώθηκαν ηλεκτρονικές επιθέσεις μεγάλου εύρους εναντίον των δικτύων η/υ της χώρας, οι οποίες απέκοψαν επικοινωνιακά και 'ιντερνετικά' τη Γεωργία από τον υπόλοιπο κόσμο για τρεις εβδομάδες περίπου. Όπως είναι γνωστό, την 9η Αυγούστου 2008 η Γεωργία εισέβαλε στην ημιαυτόνομη Νότια Οσετία˙ η Ρωσική Ομοσπονδία απάντησε αμέσως ένοπλα. Συγχρόνως με την προσβολή επί του εδάφους, η Γεωργία έγινε στόχος συστηματικών και εκτεταμένων κυβερνο-επιθέσεων (: επιθέσεις τύπου DDoS, εισαγωγή κακόβουλου λογισμικού στα δίκτυα η/υ, παραποίηση ιστοσελίδων (defacement) κ.λπ.[4]). Η πρώτη φάση των επιθέσεων αυτών πιστεύεται ότι είχε ξεκινήσει ήδη από τις 19 Ιουλίου 2008, δηλαδή δύο εβδομάδες νωρίτερα-! Το πιο εντυπωσιακό στοιχείο των κυβερνο-επιθέσεων κατά

[2] Επ' αυτού βλ. και παρακάτω, στο σημείο όπου παρουσιάζονται τα όπλα και οι μέθοδοι του σύγχρονου 'πολέμου των δικτύων', με τις απαραίτητες βιβλιογραφικές παραπομπές.
[3] Shackelford, 223, αλλά και παρακάτω, στο *τμήμα ΙΙ.* — Άλλα είδη κακόβουλου κώδικα, τα οποία θα αναφερθούν παρακάτω, είναι οι 'ιοί', οι 'δούρειοι ίπποι', οι 'λογικές' και οι 'χρονικές' βόμβες (λογισμικού), οι 'κερκόπορτες' κ.λπ.
[4] Για όλ' αυτά βλ. εκτενέστερες αναφορές παρακάτω.

της Γεωργίας είναι το γεγονός ότι απέκοψαν *αναίμακτα* σχεδόν όλες τις επικοινωνίες της χώρας με τον υπόλοιπο κόσμο για αρκετές ημέρες και με τον τρόπο αυτό πέτυχαν να προκαλέσουν ό,τι ακριβώς κατάφερε και το ΝΑΤΟ με την προσβολή του τηλεοπτικού πύργου του Βελιγραδίου στην πρώην Γιουγκοσλαβία με όπλα κινητικής ενέργειας, μόνο που σ' αυτή την τελευταία περίπτωση σκοτώθηκαν δεκαέξι άνθρωποι και τα αποτελέσματα της προσβολής διήρκεσαν μόνον για μερικές ώρες…[5] Μέχρι σήμερα —και παρά την εκτεταμένη και σε βάθος μελέτη του τρόπου και των τεχνικών των επιθέσεων— δεν έχει αποδειχθεί πέραν πάσης αμφιβολίας ότι οι συγκεκριμένες κυβερνο-επιθέσεις μπορούν να αποδοθούν στην κρατική οντότητα της Ρωσικής Ομοσπονδίας.

Πριν από αυτά, το 2007, η Εσθονία είχε γίνει στόχος της πιο σφοδρής και εκτεταμένης ηλεκτρονικής προσβολής που έχει σημειωθεί μέχρι σήμερα σε βάρος κρατικής οντότητας. Με ημερομηνία έναρξης την 27η Απρ. 2007 και για τρεις εβδομάδες, η Εσθονία[6] έγινε στόχος 'κυβερνο-επιθέσεων' τεράστιου εύρους (κυρίως επιθέσεις τύπου DoS και DDoS, αλλά και παραποίηση ιστοσελίδων, επιθέσεις σε εξυπηρετητές του συστήματος ονοματοδοσίας τομέων του διαδικτύου (DNS servers),[7] μαζική αποστολή μηνυμάτων *spam* κ.λπ.). Όλοι οι διαδικτυακοί ιστότοποι και τα δίκτυα η/υ της κυβέρνησης (συμπεριλαμβανομένου και του Γραφείου του Πρωθυπουργού της χώρας) τέθηκαν εκτός λειτουργίας και την ίδια μοίρα είχαν λίγο αργότερα οι ιστότοποι και τα δίκτυα των εφημερίδων, των τηλεοπτικών σταθμών, των τραπεζών, των επιχειρήσεων κοινής ωφέλειας κ.λπ. Το ίδιο συνέβη και με τους ιστότοπους του κοινοβουλίου, των νοσοκομείων, των ηλεκτρονικών μέσων ενημέρωσης, των πανεπιστημίων, αλλά και τους ιστότοπους και τα δίκτυα των

[5] Walker, σελ. 33. — Εξαιτίας, ακριβώς, των κυβερνο-επιθέσεων, κατέστη εξαιρετικά δύσκολο έως αδύνατο για τη Γεωργία να διανείμει πληροφορίες στο διεθνές κοινό, αλλά και στον ίδιο τον πληθυσμό της, για την εν εξελίξει σύγκρουση με τη Ρωσική Ομοσπονδία, ειδικά κατά τις πρώτες κρίσιμες ημέρες των συγκρούσεων, και έτσι απέτυχε πλήρως να αμυνθεί ή να επιτεθεί επικοινωνιακά-! (Για τις κυβερνο-επιθέσεις εναντίον της Γεωργίας, βλ. Tikk, Kaska & Vihul, σελ. 67 et seq. και Owens, Dam & Lin, eds, σελ. 172 et seq.)

[6] Η χώρα αυτή ήταν ήδη το 2007 μία από τις περισσότερο δικτυωμένες και ηλεκτρονικά προηγμένες της Ευρώπης , με πλήρη ηλεκτρονική διακυβέρνηση˙ για το λόγο αυτό ήταν γνωστή και ως 'eStonia'. Ενδεικτικά αναφέρεται ότι το 90% όλων των τραπεζικών συναλλαγών γίνονταν δικτυακά, όπως και η δήλωση και πληρωμή των φόρων, ενώ και οι βουλευτικές εκλογές διεξάγονταν μέσω internet˙ ακόμη και η πληρωμή της στάθμευσης των αυτοκινήτων γινόταν μέσω κινητών τηλεφώνων. (Shackelford, σελ. 192.)

[7] Και γι' αυτό βλ. αμέσως παρακάτω στην *Εισαγωγή*, όπου παρατίθενται ορισμένα τεχνικά και πληροφοριακά στοιχεία για το διαδίκτυο (αλλά και τους ηλεκτρονικούς υπολογιστές γενικά).

εταιρειών παροχής υπηρεσιών internet, των εταιρειών τηλεφωνίας κ.λπ.[8] Υπολογίζεται ότι περισσότεροι από… *ένα εκατομμύριο* η/υ από 178 χώρες(!) χρησιμοποιήθηκαν εναντίον της Εσθονίας, συνδεδεμένοι μεταξύ τους με την τεχνική των *'botnets'*, αρκετοί απ' αυτούς μάλιστα από το εσωτερικό της ίδιας της Εσθονίας και άλλοι ακόμη και από τις Η.ΠΑ. Οι επιθέσεις προκάλεσαν σοβαρές *οικονομικές* και *κοινωνικές* συνέπειες, αλλά όχι υλικές ζημίες σε αντικείμενα ή απώλειες ζωών· προκλήθηκαν, ωστόσο, σύγχυση και ταραχές, με επακόλουθο τον τραυματισμό 150 ανθρώπων και το θάνατος ενός ακόμη, ρωσικής εθνικότητας.[9]

> Οι έννοιες 'bot' και 'botnet' και οι τεχνικές που συνδέονται με αυτές είναι κρίσιμες για την κατανόηση μίας μεγάλης μερίδας επιθέσεων σε δίκτυα η/υ και για το λόγο αυτό *θεωρούμε απαραίτητη την αποσαφήνισή τους σ' αυτό το σημείο του κειμένου :* **' B o t '** ονομάζεται ένα πρόγραμμα για η/υ (a piece of software) το οποίο εκτελεί αυτοματοποιημένα και επαναλαμβανόμενα στον η/υ εργασίες και ρουτίνες, πολύ πιο γρήγορα από οποιονδήποτε άνθρωπο – χειριστή του η/υ (ο όρος προέρχεται από τη λέξη (ro)bot)· ένα πρόγραμμα 'bot' δεν είναι κατ' ανάγκη πάντοτε κακόβουλο. Στη γλώσσα των 'κυβερνο-επιχειρήσεων' (αλλά και των hackers) ο όρος αναφέρεται ειδικά σε ένα *παρασιτικό* και *κακόβουλο* λογισμικό το οποίο 'υφαρπάζει' έναν η/υ συνδεδεμένο σε δίκτυο και τον χρησιμοποιεί —*χωρίς ο χειριστής ή ο κάτοχός του να το γνωρίζουν καν*— για την εκτέλεση αυτοματοποιημένων κυβερνο-επιθέσεων για λογαριασμό τρίτων. — **' B o t n e t '** (ή 'bot army' – ο όρος προέρχεται από τη σύντμηση των λέξεων (ro)bot net(work)) ονομάζεται ένα δίκτυο η/υ που αποτελείται από διάφορους υπολογιστές των οποίων ο έλεγχος έχει αναληφθεί κρυφίως και παρανόμως με τη χρήση λογισμικού τύπου 'bot'. Τα 'botnets' 'χτίζονται' με τη χρήση κακόβουλου λογισμικού ('bot herder' ή 'bot wrangler') το οποίο αναπαράγει και διαμοιράζει αυτοματοποιημένα τα 'bots' και ελέγχει τους υπολογιστές – στόχους και το οποίο αναπαράγει και τον ίδιο του τον εαυτό-! Με τον τρόπο αυτό μπορούν να δημιουργηθούν τεράστια 'botnets' στα οποία τα bot herders λειτουργούν ως *κόμβοι*. Όταν δημιουργηθεί ένα botnet, συνήθως είναι

[8] Αφορμή (ή αιτία…) για τις επιθέσεις θεωρείται η απόφαση της Εσθονικής κυβέρνησης να μεταφέρει από το κέντρο της πρωτεύουσας Tallinn σε άλλη τοποθεσία ένα μνημείο της σοβιετικής εποχής (γνωστό ως 'Bronze Soldier'), το οποίο είχε ανεγερθεί για να τιμήσει τους νεκρούς της Σοβιετικής Ένωσης κατά την απελευθέρωση της περιοχής από τους Γερμανούς κατά τον Β' ΠΠ.
[9] Shackelford, σελ. 193.

εξαιρετικά δύσκολο (και χρονοβόρο) να διαλυθεί ή να αντιμετωπιστεί, διότι η δομή του και ο τρόπος δράσης του είναι αποκεντρωμένα.[10]

Εσθονοί αξιωματούχοι ισχυρίστηκαν αμέσως ότι η χώρα τους ήταν το θύμα ενός *νέου είδους πολέμου* και υπέδειξαν ως υπεύθυνη για την επίθεση αυτή τη Ρωσική Ομοσπονδία (η κατηγορία αυτή μέχρι σήμερα δεν έχει καταστεί δυνατό να επιβεβαιωθεί πλήρως, παρά τις εκτεταμένες ηλεκτρονικές έρευνες και την σε βάθος μελέτη των επιθέσεων)· ο Υπουργός Άμυνας Jaak Aaviksoo έκανε λόγο για 'national security emergency' και για 'blockade'. Η Εσθονία, επίσης, ως χώρα – μέλος του NATO ζήτησε βοήθεια από τον Οργανισμό αυτό· στα ανώτατα πολιτικά και στρατιωτικά κλιμάκια του NATO επικράτησε η άποψη ότι οι ηλεκτρονικές επιθέσεις ήταν μεν σοβαρές αλλά δεν ξεπερνούσαν τα επίπεδα της ενόχλησης και της 'δυσάρεστης' συμπεριφοράς και έτσι *δεν* υπήρχε έδαφος εφαρμογής του άρθρου 5 του Χάρτη της Συμμαχίας·[11] σ' αυτό, βέβαια, πρέπει, κατά την εκτίμησή μας, να έπαιξε ρόλο και το γεγονός ότι δεν μπορούσε να τεκμηριωθεί γρήγορα και με ασφάλεια σύνδεση των 'επιθέσεων' με τις πράξεις συγκεκριμένης κρατικής οντότητας. Το NATO απλά απέστειλε στην Εσθονία ειδικούς για τη μελέτη των επιθέσεων και την παροχή τεχνικής βοήθειας.[12] Αξίζει επίσης να σημειωθεί ότι ο Ο.Η.Ε. δεν ασχολήθηκε με τις κυβερνο-επιθέσεις εναντίον της Εσθονίας.[13]

Η εργασία αυτή θα προσπαθήσει να απαντήσει στο ερώτημα εάν μία επίθεση στα δίκτυα η/υ μίας χώρας (computer network attack – CNA) που εκδηλώνεται σε *περίοδο ειρήνης* με τη χρήση των η/υ και των δικτύων η/υ ως *όπλων* και μπορεί να

---

[10] Tikk, Kaska & Vihul, σελ. 111.

[11] Βλ. και Owens, Dam & Lin, eds, σελ. 172 et seq. και Theiler σε 'NATO Review'. — Το άρθρο 5 της Συνθήκης του Βορείου Ατλαντικού (Ουάσιγκτον, 04 Απρ. 1949) ως γνωστόν ορίζει ότι "[t]he Parties agree that an *armed attack* against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the *right of individual or collective self-defence* recognised by *Article 51 of the Charter of the United Nations*, will assist the Party or Parties so attacked…" (η έμφαση δική μας – το πλήρες κείμενο της Συνθήκης διαθέσιμο στην ιστοσελίδα του NATO στη δνση http://www.nato.int/cps/en/natolive/ official_texts_17120.htm).

[12] Το συμβάν, ωστόσο, λειτούργησε ως 'προειδοποιητικό καμπανάκι' για το NATO (Owens, Dam & Lin, eds, ibid)· τον Ιούνιο του 2007 οι Υπουργοί Άμυνας των χωρών – μελών του NATO, προφανώς και εμφανώς θορυβημένοι από τα γεγονότα στην Εσθονία, αποφάσισαν την ίδρυση, από τη Συμμαχία, ενός "Cooperative Cyber Defence Centre of Excellence" (CCD COE) με έδρα την Εσθονία και με αποστολή τη μελέτη των απειλών στον κυβερνοχώρο, τη διατύπωση προτάσεων και την ανάπτυξη τεχνικών αντιμετώπισής τους.

[13] Shackelford, 237. — Για το περιστατικό των επιθέσεων σε βάρος της Εσθονίας βλ. γενικά Shackelford (ιδίως σελ. 192 et seq. και 202 et seq.) και Tikk κ.λπ., op. cit., σελ. 15 et seq. Ο Shackelford, 200, επίσης αναφέρει ότι ήδη το 2002 δεκαεννέα εκατομμύρια ιδιώτες είχαν την τεχνογνωσία για τη διεξαγωγή 'κυβερνο-επιθέσεων' και (σελ. 225) ότι το 2009, 439 εκατομμύρια υπολογιστές ήταν συνδεδεμένοι στο internet.

αποδοθεί σε συγκεκριμένο κράτος (άσχετα εάν διενεργείται από τα όργανα του κράτους αυτού, ή από κάποια μη-κρατική οντότητα, ή ακόμη και από ιδιώτες για λογαριασμό κάποιου κράτους), είναι δυνατόν να έχει —και υπό ποίες προϋποθέσεις— τα χαρακτηριστικά της *χρήσης βίας* του άρθρου 2(4) του Χάρτη ή της *ένοπλης επίθεσης* του άρθρου 51, έτσι ώστε να είναι δυνατή η λήψη από το κράτος-στόχο όλων εκείνων των 'νόμιμων' μέτρων που επιφυλάσσονται από το διεθνές δίκαιο και ιδίως από το *jus ad bellum* γι' αυτές τις περιπτώσεις.[14]

Προκειμένου να διευκολυνθεί η καθαρά νομική προσέγγιση του ζητήματος, αμέσως μετά την *Εισαγωγή* —η οποία συμπληρώνεται από ορισμένα ιστορικά και τεχνικά στοιχεία για τους η/υ, τα δίκτυα και το internet—, στο *τμήμα ΙΙ* της εργασίας, θα εξηγηθεί τι ακριβώς είναι από *τεχνική άποψη* μία 'επίθεση σε δίκτυα η/υ', θα δοθούν οι απολύτως απαραίτητοι ορισμοί, ιδίως όσον αφορά το πεδίο αντιπαράθεσης στο οποίο λαμβάνουν χώρα οι επιθέσεις αυτές (: στον 'κυβερνοχώρο') και θα παρουσιαστούν, με συνοπτική ακρίβεια, οι τεχνικές και τα 'όπλα' των 'κυβερνο-επιθέσεων' (επιθέσεις DoS και DDoS, κακόβουλο λογισμικό, επιθέσεις σε επίπεδο ολοκληρωμένων κυκλωμάτων κ.λπ.). — Στο *τμήμα ΙΙΙ* θα παρατεθεί η βασική θεωρία του διεθνούς δικαίου για τη χρήση βίας και την ένοπλη επίθεση (στο σημείο εξέλιξης που έχει φθάσει σήμερα το δίκαιο αυτό), με έμφαση στα σημεία εκείνα τα οποία, κατά την κρίση του γράφοντος, μπορούν να αποτελέσουν ασφαλείς βάσεις για τη μορφοποίηση απαντήσεων στα παραπάνω βασικά ερωτήματα. — Στο *τμήμα ΙV* θα γίνει η προσπάθεια *αναγωγής* των ιδιαίτερων χαρακτηριστικών, των ιδιαιτεροτήτων, του τρόπου εκδήλωσης και των αποτελεσμάτων των CNAs, στο νομικό πλαίσιο του σύγχρονου διεθνούς δικαίου για τη χρήση βίας και την ένοπλη επίθεση στις σχέσεις μεταξύ των κρατών. Στο τμήμα αυτό ο γράφων διατυπώνει, σε γενικές γραμμές, την άποψη ότι τα 'ηλεκτρονικά όπλα' που απαριθμούνται στο τμήμα ΙΙ, *είναι* 'όπλα' σαν κι αυτά που είχαν στο μυαλό τους οι συντάκτες των άρθρων 2(4) και 51 του Χάρτη των Η.Ε. και ότι η χρήση των όπλων αυτών και οι μέθοδοι χρησιμοποίησής τους, *μπορεί* να συνιστούν χρήση βίας και ένοπλη επίθεση, όπως οι έννοιες αυτές γίνονται δεκτές από το γραπτό και εθιμικό *jus ad bellum*, στο στάδιο εξέλιξης που έχει φθάσει σήμερα. Διατυπώνει, επίσης, την άποψη

[14] Ως εκ τούτου από το σκοπό της εργασίας αυτής ε κ φ ε ύ γ ε ι η ενασχόληση με επιθέσεις CNA που εκδηλώνονται *κατά τη διάρκεια* μίας (ήδη διαπιστωμένης) ένοπλης σύγκρουσης και, πολύ περισσότερο, η ενασχόληση με τα ζητήματα που τίθενται από τη διάπραξη εγκλημάτων στον κυβερνοχώρο ή τη διάπραξη ηλεκτρονικών εγκλημάτων ή εγκλημάτων που σχετίζονται με υπολογιστές ή διαπράττονται με τη βοήθεια η/υ, όπως αυτά προσδιορίζονται στα ποινικά δίκαια των διαφόρων χωρών.

ότι αυτή τη στιγμή υπάρχει ήδη ανιχνεύσιμη πρακτική κρατών και διεθνών οργανισμών περί του ότι βία στις διακρατικές σχέσεις μπορεί να ασκηθεί και με τη μορφή των CNAs, καθώς και την άποψη ότι οι διατάξεις των άρθρων 2(4) και 51 του Χάρτη και το διεθνές εθιμικό δίκαιο που ισχύει σήμερα αναφορικά με το δικαίωμα αυτοάμυνας, μπορούν να λειτουργήσουν ικανοποιητικά και στα ζητήματα άσκησης βίας και εκδήλωσης 'ένοπλων επιθέσεων' στον κυβερνοχώρο και δεν έχουν καταστεί *ακόμη* 'ανεπανόρθωτα ακατάλληλες', αν και οι δυνατότητες και οι ιδιαιτερότητες των CNAs και των πληροφοριακών επιχειρήσεων γενικότερα, πιέζουν αφόρητα, μέχρι τα όριά της, τη ρυθμιστική τους ικανότητα. Διαπιστώνεται επίσης ότι εκείνο που απαιτείται άμεσα και σε πρώτη φάση, είναι η θωράκιση του (ιδιωτικού) internet με ένα *minimum* κανόνων και τεχνολογιών ασφαλείας, χωρίς να θίγονται τα δικαιώματα των τρίτων προς απόλαυση του κυβερνοχώρου, και η περισσότερο αποφασιστική και ρωμαλέα εφαρμογή των υφισταμένων διατάξεων και του κεκτημένου του Χάρτη των Η.Ε. — Στο *τμήμα V*, τέλος, θα παρατεθούν ορισμένα συμπεράσματα από αυτή την ενασχόλησή μας με τις επιθέσεις σε δίκτυα η/υ ως μορφή χρήσης βίας στις διακρατικές σχέσεις των τελευταίων δύο δεκαετιών τουλάχιστον. — Μετά τα συμπεράσματα, θα παρατεθούν σε *Παράρτημα* ορισμένα *πρόσθετα* στοιχεία για τους η/υ και τα δίκτυα, για τα οποία, αν και είναι απαραίτητα για την κατανόηση του συνόλου της εργασίας, κρίθηκε ότι η παράθεσή τους στην Εισαγωγή θα διασπούσε τη δομή μίας καθαρά νομικής εργασίας.

Στο σημείο αυτό —και πριν από τα κύρια τμήματα της εργασίας— παρατίθενται ορισμένα απολύτως απαραίτητα ιστορικά και τεχνικά στοιχεία για τους η/υ και το διαδίκτυο (internet) γενικά, τα οποία θα βοηθήσουν στην κατανόηση των προσεγγίσεων που θα ακολουθήσουν :

Ο ηλεκτρονικός υπολογιστής

> Ως η/υ (computer)[15] γενικά, νοείται μία *προγραμματιζόμενη* μηχανή, σχεδιασμένη να εκτελεί κατά στάδια και με αυτοματοποιημένο τρόπο μία σειρά αριθμητικών ή λογικών λειτουργιών· η σειρά των λειτουργιών μπορεί να μεταβάλλεται, ώστε να είναι δυνατό ο η/υ να επιλύει περισσότερα είδη

[15] Η πρώτη χρήση της λέξης 'computer' καταγράφηκε το 1613 και αναφερόταν σε ένα πρόσωπο το οποίο εκτελούσε αριθμητικές πράξεις και υπολογισμούς. Από το τέλος του 19ου αιώνα η λέξη άρχισε σταδιακά να λαμβάνει το σημερινό της περιεχόμενο, να περιγράφει, δηλαδή, μία *μηχανή* πια, η οποία μπορεί να εκτελεί υπολογισμούς.

προβλημάτων.[16] *'Ηλεκτρονικός υπολογιστής'*, κατά την τρέχουσα έννοια του όρου, είναι ένα αυτοματοποιημένο, ηλεκτρονικό, ψηφιακό επαναπρογραμματιζόμενο σύστημα γενικής χρήσης (: μια 'μηχανή'), κατασκευασμένο κυρίως από ψηφιακά ηλεκτρονικά κυκλώματα και δευτερευόντως από ηλεκτρικά και μηχανικά συστήματα, που έχει ως σκοπό να επεξεργάζεται πληροφορίες βάσει ενός συνόλου προκαθορισμένων οδηγιών (: εντολών) που συνολικά ονομάζονται 'πρόγραμμα'. Κατ' ελάχιστον ένας η/υ αποτελείται από κάποιο είδος μνήμη για την αποθήκευση δεδομένων, από τουλάχιστον μία μονάδα που εκτελεί αριθμητικές και λογικές λειτουργίες και από μία μονάδα ακολουθίας (αλληλουχίας) και ελέγχου, η οποία μπορεί να μεταβάλει τη σειρά των λειτουργιών που πρέπει να εκτελεστούν με βάση τις αποθηκευμένες πληροφορίες.[17] Η ανάπτυξη των πρώτων πραγματικών ηλεκτρονικών η/υ άρχισε στη δεκαετία του 1940˙ είχαν μέγεθος ενός μεγάλου… δωματίου και η ενέργεια που κατανάλωναν αντιστοιχούσε στην ενέργεια που καταναλώνουν σήμερα μερικές εκατοντάδες προσωπικοί ηλεκτρονικοί υπολογιστές. Οι βάσεις για τις τεχνολογίες που χρησιμοποιήθηκαν σ' αυτούς, ωστόσο, και τη θεωρητική θεμελίωσή τους, τέθηκαν στη δεκαετία του 1930.[18] Στην επιστήμη των σύγχρονων η/υ συνδυάζονται με εντυπωσιακό τρόπο δύο διαφορετικές τεχνολογίες : ο αυτοματοποιημένος υπολογισμός και ο προγραμματισμός (automated calculation and programmability).

Πέρα από τα διάφορα είδη προσωπικών η/υ (personal computers – PCs) που αποτελούν την κατ' εξοχήν εικόνα της πληροφοριακής εποχής του 20ού και του

---

[16] Για να χαρακτηριστεί κατ' αρχήν μία μηχανή ως 'ηλεκτρονικός υπολογιστής', δεν απαιτείται να λειτουργεί απαραίτητα με ηλεκτρικό ρεύμα, ούτε να διαθέτει επεξεργαστή, μνήμη ή σκληρό δίσκο. Ως 'η/υ' χαρακτηρίζεται οποιαδήποτε συσκευή μπορεί να μετατρέψει τις εισαγόμενες σ' αυτήν πληροφορίες, θεληματικά και με βάση κάποιους λογικούς κανόνες. Σήμερα, ωστόσο, ο όρος η/υ παραπέμπει πλέον σε μία συσκευή που λειτουργεί με ηλεκτρικό ρεύμα και διαθέτει μνήμη, επεξεργαστή, αποθηκευτικό μέσο, και διατάξεις εισόδου και εξόδου δεδομένων˙ ο,τιδήποτε άλλο δεν θα είναι (πλήρης) 'η/υ' αλλά απλά ένας επεξεργαστής.

[17] Κάθε υπολογιστικό σύστημα ή η/υ, ανεξάρτητα από το μέγεθός του, αποτελείται από το υλικό μέρος (***hardware***), δηλαδή όλα εκείνα τα μέρη που έχουν υλική υπόσταση (: ηλεκτρονικά κυκλώματα, οθόνη, τροφοδοτικά, καλώδια, πληκτρολόγια, εκτυπωτές κ.λπ.) και το λογισμικό (***software***), δηλαδή τα άυλα μέρη του υπολογιστικού συστήματος (: λειτουργικό σύστημα, εφαρμογές, αποθηκευμένα δεδομένα, πρωτόκολλα επικοινωνίας με τα περιφερειακά ή τα διάφορα δίκτυα κ.λπ.). Όταν το software αποθηκεύεται στο hardware με τρόπο που καθιστά ανέφικτη ή εξαιρετικά δύσκολη την τροποποίησή του (όπως για παράδειγμα το BIOS (: **B**uilt **I**n **O**perating **S**ystem), η μνήμη ROM κ.λπ.), γίνεται λόγος για '***firmware'***.

[18] Τα ψηφιακά ηλεκτρονικά, για παράδειγμα, θεωρούνται σε μεγάλο βαθμό ανακάλυψη του Claude Shannon του έτους 1937, ενώ ως ο 'πατέρας' της σύγχρονης επιστήμης των η/υ θεωρείται ο Άγγλος μαθηματικός Alan Turing, ο οποίος με τη διατριβή του και τις άλλες εργασίες του της δεκαετίας του 1930 αναδιατύπωσε τα αποτελέσματα των εργασιών του 1931 του Αυστριακού μαθηματικού Κούρτ Γκέντελ για τα όρια της απόδειξης και του υπολογισμού, επινόησε τις αφηρημένες λογικές 'μηχανές Τούρινγκ' και απέδειξε ότι μια τέτοια 'μηχανή' θα ήταν σε θέση να υπολογίσει οποιοδήποτε κατανοητό μαθηματικό πρόβλημα εάν ήταν δυνατό το πρόβλημα αυτό να αναπαρασταθεί από έναν *αλγόριθμο* (algorithm, δηλ. λεπτομερειακές οδηγίες που καθορίζουν το πώς εκτελείται μία εργασία). Οι μηχανές Τούρινγκ είναι μέχρι σήμερα το κεντρικό αντικείμενο μελέτης της θεωρίας του υπολογισμού.

21ου αιώνα, αλλά και τα μεγάλα υπολογιστικά συστήματα των τραπεζών, των δημοσίων οργανισμών, των ενόπλων δυνάμεων, των κάθε είδους εταιρειών κ.λπ. (minicomputers, mainframes, supercomputers, servers κ.λπ.), δεν πρέπει να λησμονούμε ότι μικροί ηλεκτρονικοί υπολογιστές (στο μέγεθος μίας πλακέτας ηλεκτρονικών) υπάρχουν πλέον *σχεδόν σε κάθε ηλεκτρική συσκευή* (φορητή ή μη) *και σύστημα*, από τα κινητά τηλέφωνα, τα παιχνίδια και τις συσκευές MP3, μέχρι τα εμπορικά και τα μαχητικά αεροσκάφη, τα βιομηχανικά ρομποτικά συστήματα, τις τηλεπικοινωνίες, τα δορυφορικά συστήματα, τα οπλικά συστήματα κ.λπ.

Ορισμένες πρόσθετες πληροφορίες για τους υπολογιστές βλ. στο Παράρτημα.

Το διαδίκτυο (internet)[19]

Το διαδίκτυο ή *internet*, όπως είναι ευρέως γνωστό, είναι ένα *δίκτυο δικτύων*, δηλαδή ένα παγκόσμιο (πλέον) δίκτυο στο οποίο συνδέονται εκατοντάδες χιλιάδες άλλα δίκτυα διαφόρων μεγεθών και το οποίο επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε *διασυνδεδεμένου* (δικτυωμένου) η/υ. Ως μέσο έχει διπλή υπόσταση : υλική (αφού αποτελείται από περισσότερα δίκτυα που βασίζονται σε hardware και software) και άυλη (αφού αυτό που προσφέρει στην κοινωνία ως μέσο μαζικής επικοινωνίας —και ιδίως ο αμφίδρομος χαρακτήρας του— προστίθεται στην (και ξεπερνά κατά πολύ την) ούτως ή άλλως υπερμεγέθη υλική του υπόσταση. Η τεχνολογία του βασίζεται στη *διασύνδεση επιμέρους δικτύων* ανά τον κόσμο, με τη χρήση πολυάριθμων πρωτοκόλλων μεταγωγής πακέτων δεδομένων (data packet switching), με κυρίαρχο το πρωτόκολλο TCP/IP.[20] Το internet προσφέρει διάφορες διαδικτυακές υπηρεσίες —και μάλιστα σε πραγματικό χρόνο—, όπως *η άμεση επικοινωνία και ο έλεγχος μεταξύ η/υ και δικτύων η/υ*, το ηλεκτρονικό ταχυδρομείο (e-mail), οι ομάδες συζητήσεων (news /chat groups), η *διαμοίραση και μεταφορά αρχείων* (file sharing /transfer), ο *παγκόσμιος ιστός* (world wide web[21]), το δικτυακό ραδιόφωνο και τηλεόραση, η διαδικτυακή τηλεφωνία κ.λπ.

[19] Ο αγγλικός αυτός όρος προκύπτει από τη σύνθεση των λέξεων '*inter' και 'network'*.
[20] Μερικά από τα άλλα λιγότερο ή περισσότερο γνωστά διαδικτυακά πρωτόκολλα επικοινωνίας είναι το UDP, το DNS, το PPP, το SLIP, το ICMP, το POP3, το IMAP, το SMTP, το HTTP, το HTTPS, το SSH, το Telnet, το FTP, το LDAP και το SSL.
[21] Παγκόσμιος ιστός και internet συχνά θεωρούνται το ίδιο πράγμα. *Η αντίληψη αυτή είναι λανθασμένη* καθώς ο 'παγκόσμιος ιστός' αποτελεί μία μόνο υπηρεσία (facility) ή προσφερόμενη εφαρμογή του internet και για την ακρίβεια την δημοφιλέστερη και περισσότερο διαδεδομένη (ακολουθούμενη από το ηλεκτρονικό ταχυδρομείο).

Πρέπει να επισημανθεί, ότι *το internet λειτουργεί σε πολύ μεγάλο ποσοστό με κονδύλια και εξοπλισμό του ιδιωτικού τομέα και δεν έχει κεντρική διοίκηση, διεύθυνση ή 'διακυβέρνηση'*, ούτε όσον αφορά τις χρησιμοποιούμενες *τεχνολογίες*, ούτε όσον αφορά τις πολιτικές *πρόσβασης* και *χρήσης*· κάθε επιμέρους δίκτυο (το οποίο συνδέεται στο internet) καθορίζει *το ίδιο* τους δικούς του κανόνες και τα πρότυπα.[22] Σε αυτό το ιδιαίτερο και μοναδικό χαρακτηριστικό του internet οφείλεται και το γεγονός ότι αφενός μεν το διαδίκτυο προσφέρεται για τη διάπραξη 'ηλεκτρονικών' εγκλημάτων και 'κυβερνοεγκλημάτων',[23] αφετέρου δε ότι *ο 'κυβερνοχώρος' μετατράπηκε πολύ γρήγορα —και με καταπληκτική ευκολία— σε πεδίο ανθρώπινης αντιπαράθεσης*, στο οποίο είναι εξαιρετικά δύσκολο να ασκηθεί έλεγχος και να τεθούν κανόνες.

> Κεντρική διεύθυνση και συντονισμός ασκούνται αποκλειστικά και μόνο σε θέματα 'ονοματοδοσίας', δηλαδή στις διευθύνσεις internet (internet protocol addresses – IP adresses) που απονέμονται και στις ονοματοδοσίες DNS (βλ. στο *Παράρτημα*), από τον διεθνή μη-κερδοσκοπικό οργανισμό ICANN (Internet Corporation for Assigned Names and Numbers).[24]

Η *εμπορικοποίηση* του internet —το οποίο ήταν ήδη παγκόσμιο— κατά τη δεκαετία του 1990, οδήγησε στην εξαιρετικά ευρεία διάδοσή του, στην εκλαΐκευσή του και στη χρησιμοποίησή του *σε κάθε πτυχή της σύγχρονης ζωής στον πλανήτη και σχεδόν σε κάθε κρατική λειτουργία*.[25]

Πρόσθετες πληροφορίες για το internet και τον παγκόσμιο ιστό ('www') βλ. στο Παράρτημα.

II. Τι είναι οι 'επιθέσεις σε δίκτυα η/υ' (Computer Network Attacks – CNAs)

---

[22] Αυτή η 'ανοικτή φιλοσοφία' είναι συγχρόνως και η Αχίλλειος πτέρνα του συστήματος… (Shackelford, 199).
[23] Οι δύο αυτές έννοιες δεν ταυτίζονται, ωστόσο η υπόδειξη των διαφορών δεν εμπίπτει στο αντικείμενο της εργασίας μας αυτής.
[24] Για όλα τα παραπάνω, καθώς και τις πρόσθετες πληροφορίες του *Παραρτήματος*, πηγή : wikipedia, λήμματα ''διαδίκτυο'' και ''παγκόσμιος ιστός'', τελευταία πρόσβαση : 04.10.2011.
[25] Εκτιμάται, για παράδειγμα, ότι το **2009** πάνω από το ¼ του συνολικού πληθυσμού της γης χρησιμοποιούσε υπηρεσίες του internet και στο διαδίκτυο ήταν συνδεδεμένοι περισσότεροι από… 439 εκατομμύρια η/υ(!)· είναι εντυπωσιακό ότι μόλις πριν από 22 περίπου χρόνια, το **1988**, το 'internet' αποτελούνταν μόνο από 60.000 περίπου συνδεδεμένους η/υ, οι περισσότεροι από τους οποίους ανήκαν σε ερευνητικά κέντρα και πανεπιστήμια στις Η.Π.Α. (βλ., π.χ., Shackelford, σελ. 223 & 225).

1. Ορισμοί

Ως *'κυβερνοχώρος'* (cyberspace)[26] ορίζεται η νοητή εκείνη περιοχή (ο νοητός 'τομέας') που χαρακτηρίζεται από τη χρήση ηλεκτρονικών, καθώς και του ηλεκτρομαγνητικού φάσματος, για την αποθήκευση, τροποποίηση και ανταλλαγή δεδομένων, μέσω δικτυωμένων συστημάτων και των υλικών υποδομών που σχετίζονται με αυτά και τα υποστηρίζουν.[27] Κατ' αυτόν τον τρόπο *ο κυβερνοχώρος είναι ευρύτερος από το internet* και περιλαμβάνει όλες τις 'δικτυωμένες' ψηφιακές δραστηριότητες (και όχι μόνο τις 'ιντερνετικές').[28] Λόγω της φύσης και των ιδιοτήτων του, αλλά και της παγκόσμιας εμβέλειας του, ο κυβερνοχώρος έχει αρχίσει να *'διαβρώνει'* τη σύνδεση μεταξύ εδαφικής επικράτειας και κρατικής κυριαρχίας.[29]

Οι *'κυβερνοεπιθέσεις'* είναι χρήση βίας (με την καθημερινή έννοια του όρου) στον κυβερνοχώρο ('κυβερνο-βία') με εχθρική πρόθεση, δηλαδή επιχειρήσεις που αναλαμβάνονται από ένα κράτος σε βάρος άλλου (με αμυντικές ή επιθετικές προθέσεις και επιδιώξεις) με τη χρήση πληροφοριών αποθηκευμένων σε μεμονωμένους η/υ, σε ορισμένους από τους η/υ ενός δικτύου ή σε ολόκληρα δίκτυα η/υ, με *σκοπό* την εξουδετέρωση των η/υ – στόχων, ορισμένων από τους η/υ ενός δικτύου ή ολόκληρου του δικτύου ή ιστοσελίδων ή /και την πρόκληση ζημιών που ξεπερνούν, όμως, αυτή καθ' εαυτή την υλική καταστροφή των η/υ και των δικτύων – στόχων. Από την πλευρά του 'επιτιθέμενου' *οι η/υ και τα δίκτυα η/υ χρησιμοποιούνται ως όπλα.* Δεν καλύπτονται,

---

[26] Η ελληνική λέξη 'κυβερνοχώρος' είναι μεταφραστικό 'δάνειο' από την αγγλική λέξη 'cyberspace', την οποία επινόησε ο συγγραφέας έργων επιστημονικής φαντασίας *William Gibson*, στην προσπάθειά του να περιγράψει το όραμά του για ένα παγκόσμιο δίκτυο η/υ που θα συνέδεε ανθρώπους, μηχανές και πληροφορίες. Βέβαια, η λέξη 'cyberspace' είναι εμπνευσμένη από την επιστήμη των cybernetics (κυβερνητική), η οποία με τη σειρά της ετυμολογικά βασίζεται στο ελληνικό ρήμα 'κυβερνώ' που μεταφέρει ως κυρίαρχες τις ιδέες της *πλοήγησης* και του *ελέγχου*. (Βλ., αντί άλλων, http://pcp.lanl.gov/CYBSPACE.html.)

[27] United States National Military Strategy for Cyberspace Operations, U.S. Department of Defense, Δεκέμβριος 2006, διαθέσιμο στην ιστοσελίδα www.dod.gov/pubs/foi/ojcs/07-F-2105doc.pdf. — Παρομοίως, κατά τον Todd, USAF, Law Review, vol. 64, σελ. 68, ο κυβερνοχώρος είναι "…an evolving man-made domain for the organization and transfer of data using various wavelengths of the electromagnetic spectrum. The domain is a combination of private and public property governed by technical rule sets designed primarily to facilitate the flow of information. The key feature of cyberspace is that it is a man-made domain designed to transfer data and information."

[28] Ήδη αρκετοί μελετητές και επιστήμονες (μεταξύ αυτών και νομικοί) θεωρούν ότι ***ο κυβερνοχώρος αποτελεί παγκόσμια κληρονομιά της ανθρωπότητας*** (common heritage of mankind) και θα πρέπει να τεθούν σε ισχύ ειδικοί κανόνες διεθνούς δικαίου για τη ρύθμιση και την προστασία του. (Kamal, σελ. 8, Shackelford, σελ. 210 et seq.)

[29] Πράγματι, αυτή τη στιγμή, για παράδειγμα, μία κλήση με δορυφορικό τηλέφωνο μπορεί να γίνει από την Ανταρκτική ή τη Γη του Πυρός, μία ελληνική εταιρεία μπορεί να έχει τους servers της στην Κίνα, ενώ ένας έφηβος από το Ισραήλ και μερικοί φοιτητές από την Καλιφόρνια μπορούν να διεισδύσουν στο δίκτυο του Υπουργείου Άμυνας των Η.Π.Α. με τη χρήση ενός server στα… Ηνωμένα Αραβικά Εμιράτα (: η περίπτωση αυτή είναι γνωστή ως "Solar Sunrise attack" και έλαβε χώρα το 1998 – Roscini, σελ. 97).

όπως είναι φανερό, οι επιθέσεις με όπλα κινητικής ενέργειας εναντίον εγκαταστάσεων και υποδομών η/υ /δικτύων. Καλύπτονται, αντίθετα, οι επιθέσεις με όπλα ηλεκτρονικού παλμού (electro-magnetic pulse wave weapons)·[30] η χρήση αυτού του είδους όπλων, ωστόσο, *δεν* θα μας απασχολήσει στα πλαίσια αυτής της εργασίας, διότι προκαλούν *υλική* καταστροφή των τυπωμένων ηλεκτρονικών κυκλωμάτων (: του hardware) που χρησιμοποιούνται σε η/υ και δίκτυα.

Οι κυβερνοεπιθέσεις (cyber attacks) ή επιθέσεις στον κυβερνοχώρο, αποτελούν τμήμα ή είδος μίας πολύ ευρύτερης κατηγορίας επιχειρήσεων οι οποίες είναι γνωστές ως 'πληροφοριακές επιχειρήσεις' (information operations – I.O.)· είδος πληροφοριακών επιχειρήσεων αποτελούν και οι *'επιχειρήσεις δικτύων η/υ'*.[31] Οι επιχειρήσεις δικτύων η/υ (ως έννοια γένους), με τη σειρά τους, περιλαμβάνουν τις *επιθέσεις* σε δίκτυα η/υ (CNAs), τις επιχειρήσεις για την άμυνα (των φίλιων) δικτύων, καθώς και τις επιχειρήσεις αθέμιτης εκμετάλλευσης δικτύων η/υ (computer network exploitation enabling operations – CNE). Αν και οι τελευταίες αναφέρονται συνήθως (ιδίως) στον τύπο ως 'κυβερνοεπιθέσεις',[32] στην πραγματικότητα *δεν* είναι, από μόνες τους, 'επιθέσεις' ή 'χρήση βίας' κ.λπ., έτσι όπως οι έννοιες αυτές προσεγγίζονται στα πλαίσια του *jus ad bellum* και του *jus in bello*,[33] καθώς με αυτές απλά *συλλέγονται πληροφορίες* ή γίνονται λεπτομερείς *παρατηρήσεις* για τα συστήματα του αντιπάλου (port scanning, application mapping, network mapping κ.λπ.), ή διαδίδονται πληροφορίες για προπαγανδιστικούς σκοπούς (για παράδειγμα, με την τεχνική της

---

[30] Kamal, σελ. 80 και http://www.fas.org/irp/threat/cyber/docs/npgs/ch2.htm (τελευταία πρόσβαση : 13 Οκτ. 2011). Η τεχνολογία των όπλων ηλεκτρονικού παλμού έχει προχωρήσει αρκετά και ήδη τέτοιου είδους συστήματα μπορούν να έχουν το μέγεθος μίας βαλίτσας ταξιδίου-!

[31] Πολύ γενικά, πληροφοριακές επιχειρήσεις είναι η χρήση κατά τρόπο ενιαίο, συνολικό και ολοκληρωμένο των δυνατοτήτων του ηλεκτρονικού πολέμου, των ***επιχειρήσεων δικτύων η/υ***, των ψυχολογικών επιχειρήσεων, της στρατιωτικής παραπλάνησης και των διαφόρων μεθόδων ασφάλειας επιχειρήσεων, με σκοπό τον επηρεασμό, τη ρήξη, τη διατάραξη, τη φθορά /αλλοίωση, ή ακόμη και τον 'σφετερισμό' /ιδιοποίηση των διαδικασιών λήψης αποφάσεων του αντιπάλου (τόσο των ανθρώπινων όσο και των αυτοματοποιημένων), με παράλληλη προστασία των φίλιων διαδικασιών. (US National Military Strategy for Cyberspace Operations, U.S. DoD, op. cit.) — Εδώ ανήκει, ως υποκατηγορία, και ο *'πληροφοριακός πόλεμος'* (information warfare), δηλαδή τέτοιου είδους επιχειρήσεις όταν διεξάγονται στα πλαίσιο (ήδη διαπιστωμένης) ένοπλης σύγκρουσης, έτσι όπως αυτή ορίζεται σήμερα στο σύγχρονο διεθνές δίκαιο (βλ., π.χ., Schmitt (1999), 889- 891).

[32] Βλ., για παράδειγμα, στην *ηλεκτρονική 'Καθημερινή'* της 07-03-2011, άρθρα με τίτλο ''Ηλεκτρονική επίθεση κατά του γαλλικού υπουργείου Οικονομικών'' και ''Κινέζοι χάκερ «επιτέθηκαν» στο νοτιοκορεατικό υπουργείο Αμύνης'', τα οποία στην πραγματικότητα περιγράφουν επιχειρήσεις αθέμιτης 'εκμετάλλευσης' δικτύου και όχι επιθέσεις.

[33] Είναι δυνατόν, όμως, να αποτελούν *προπαρασκευαστικές* πράξεις χρήσης βίας ή επίθεσης (βλ., π.χ., Watts, 392 et seq.).

παραποίησης ιστοσελίδων (web-page defacement)), υφαρπάζονται δεδομένα[34] κ.λπ. παρόμοια.

Στα πλαίσια της εργασίας αυτής *δεν* ενδιαφέρουν οι επιχειρήσεις CNE αλλά *μόνο* οι CNAs, δηλαδή εκείνες οι επιχειρήσεις κατά δικτύων η/υ που συνοδεύονται από εχθρική πρόθεση, υπερβαίνουν την (με οποιονδήποτε τρόπο) 'αθέμιτη εκμετάλλευση' και έχουν ως επιδίωξή τους την τροποποίηση ή την καταστροφή των πληροφοριών που περιέχονται στους η/υ ή τα δίκτυα – στόχους, με απώτερο σκοπό την αχρήστευση των συστημάτων διοίκησης, ελέγχου και επικοινωνιών του αντιπάλου ή /και την πρόκληση απωλειών σε ζωές και ζημιών που ξεπερνούν αυτή καθ' εαυτή την υλική καταστροφή των η/υ ή των δικτύων που γίνονται στόχος.[35]

Ένας αρκετά διαδεδομένος ορισμός των CNAs είναι αυτός του Υπουργείου Άμυνας των Η.Π.Α., σύμφωνα με τον οποίο οι CNAs είναι ''επιχειρήσεις που σκοπό έχουν να αποδιοργανώσουν και να καταστρέψουν πληροφορίες που είναι αποθηκευμένες σε η/υ και δίκτυα η/υ, ή να απαγορεύσουν τη χρήση ή να μειώσουν την αξία αυτών των πληροφοριών, ή να προκαλέσουν όλα τα παραπάνω στους ίδιους τους η/υ και τα δίκτυα''.[36] Ο ορισμός αυτός φαίνεται ότι καλύπτει τις επιθέσεις σε η/υ και δίκτυα η/υ και τις επιθέσεις κατά των ίδιων των πληροφοριών που περιέχονται στους η/υ και τα δίκτυα η/υ˙ είναι ασαφές όμως εάν καλύπτει και τη *μετατροπή* των δεδομένων λειτουργίας του δικτύου έτσι ώστε αυτό να εκτελέσει κάποιες εργασίες ή λειτουργίες που δεν ήταν μέσα στους σκοπούς των σχεδιαστών του ή δεν είναι αποδεκτές από αυτούς.[37] Για το λόγο αυτό ορισμένοι μελετητές προτείνουν τη συμπλήρωση του ορισμού έτσι ώστε να καλύπτει και τις επιχειρήσεις που αποσκοπούν στην *παραποίηση* (: αθέμιτη μετατροπή) των πληροφοριών με σκοπό την απόκτηση του ελέγχου του η/υ ή του δικτύου. Και οι δύο αυτές προσπάθειες ορισμών, ωστόσο, θεωρητικά περιλαμβάνουν και τις επιθέσεις σε η/υ ή δίκτυα η/υ με συμβατικά όπλα

---

[34] Με τη χρήση κακόβουλου λογισμικού του τύπου των 'trap doors' και των 'sniffers'. Η κατασκοπεία, όπως είναι γνωστό, δεν απαγορεύεται, σαν τέτοια, από κανόνα του διεθνούς δικαίου και απλά αποτελεί ποινικό αδίκημα κατά τις εσωτερικές νομοθεσίες των κρατών (βλ., π.χ., Roscini, σελ. 93). Για παράδειγμα, φαίνεται ότι την περίοδο 2009 – 2010 κάποιες επιχειρήσεις κυβερνο-κατασκοπείας με προέλευση την Κίνα (;) υφάρπασαν διαβαθμισμένα έγγραφα από την Ινδία και απέκτησαν πρόσβαση σε e-mails του γραφείου του Dalai Lama (T. Branigan, *The Guardian,* 06 April 2010 – αναφέρεται στον Roscini, υποσημ. 31).

[35] Όπως λέγεται χαρακτηριστικά στην ευρύτερη πληροφοριακή κοινότητα : «οι hackers έχουν ως στόχο τα πληροφοριακά συστήματα˙ οι CNAs, αντίθετα, έχουν τελικά ως στόχο τους ανθρώπους».

[36] Βλ. σε http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf. — Ο ορισμός αυτός επικρίνεται από τον Roscini (σελ. 94, υποσημ. 37) και τον Dinstein (σε Schmitt /O'Donnell, eds, vol. 76, 101).

[37] Σε αντίθεση, δηλαδή, με την καταστροφή του δικτύου ή την περιέλευσή του σε κατάσταση αναστολής λειτουργίας. Βλ. και Silver D., σε Schmitt /O'Donnell, eds, vol. 76, σελ. 76.

(π.χ. όπλα κινητικής ενέργειας), περίπτωση η οποία, όπως είναι αυτονόητο, δεν μπορεί να αποτελέσει αντικείμενο έρευνας της εργασίας αυτής.[38] Θα πρέπει επίσης να σημειωθεί ότι στόχος μίας CNA μπορεί να είναι —πέρα από ένα δίκτυο ή δίκτυα η/υ— και μεμονωμένοι η/υ ή ορισμένοι η/υ ενός δικτύου, καθώς επίσης και ιστοσελίδες.

Στο σημείο αυτό πρέπει να γίνουν οι ακόλουθες επισημάνσεις :

Ο *κυβερνοχώρος* χαρακτηρίζεται από μία συγκεκριμένη και μοναδική ιδιαιτερότητα : ενώ είναι ένας 'χώρος' και άρα μοιάζει με τις άλλες περιοχές ανθρώπινης αντιπαράθεσης (: ξηρά, θάλασσα, αέρας, διάστημα), είναι συγχρόνως και ο μόνος *τεχνητός* χώρος ανθρώπινης αντιπαράθεσης, ένα πεδίο αντιπαράθεσης που φτιάχτηκε από τον ίδιο τον άνθρωπο. Έχοντας αυτή τη διαπίστωση κατά νου, ίσως είναι πιο εύκολο να προσεγγίσουμε το πρόβλημα των κανόνων που ισχύουν ήδη στα άλλα πεδία των ανθρωπίνων συγκρούσεων και θα μπορούσαν, ενδεχομένως, να ισχύσουν, ή ισχύουν (και σε ποιο βαθμό), και στον κυβερνοχώρο. Ο κυβερνοχώρος είναι ένα *εικονικό* πεδίο, πολύ λιγότερο απτό σε σχέση με την ξηρά και τον εναέριο χώρο, για παράδειγμα, αλλά και πολύ λιγότερο απτό και συγκεκριμένο ακόμη και σε σχέση με το διάστημα ή σε σχέση ακόμη και με το φάσμα των ραδιοσυχνοτήτων. Ένας τρόπος για να κατανοήσουμε πληρέστερα τον κυβερνοχώρο και κατ' επέκταση να κατανοήσουμε και την άσκηση βίας στον κυβερνοχώρο, είναι να συνειδητοποιήσουμε ότι *διαρθρώνεται σε τρία επίπεδα ή στρώματα* :[39] το *φυσικό* επίπεδο (physical layer), το *συντακτικό* επίπεδο (syntactic layer) και το *σημασιολογικό* επίπεδο (semantic layer) :[40]

Όλα τα πληροφοριακά συστήματα (άρα, τόσο οι μεμονωμένοι η/υ, όσο και τα δίκτυα η/υ) βασίζονται (ή 'χτίζονται', ή 'στήνονται', για να χρησιμοποιήσουμε δύο πιο αγοραίες λέξεις), κατ' αρχάς επάνω σε ένα επίπεδο ή 'στρώμα' *φυσικού* εξοπλισμού, δηλαδή σε μεταλλικά κουτιά, καλώδια, κυκλώματα τυπωμένα σε πλακέτες ηλεκτρονικών, οθόνες κ.λπ. Χωρίς αυτό το φυσικό επίπεδο, όπως είναι αυτονόητο, δεν υπάρχει καν μεμονωμένος η/υ ή σύστημα άξιο λόγου. Το φυσικό αυτό επίπεδο μπορεί

---

[38] Η προσβολή ενός υπολογιστικού, δικτυακού ή επικοινωνιακού κέντρου με όπλα κινητικής ενέργειας, μπορεί να είναι 'πληροφοριακή επιχείρηση', όπως αυτή ορίστηκε παραπάνω, αλλά *όχι* συγχρόνως και CNA. Το *jus ad bellun* και το *jus in bello* όπως τα γνωρίζουμε σήμερα, αντιμετωπίζουν επαρκώς τέτοιες περιπτώσεις με την κλασσική νομική ανάλυση περί βίας, ένοπλης επίθεσης και ένοπλης σύγκρουσης.

[39] Γενικά, στην αρχιτεκτονική δικτύου 'στρώμα' ή 'επίπεδο' (layer) αποκαλείται μια ομάδα υπηρεσιών, λειτουργιών και πρωτοκόλλων, η οποία θεωρείται πλήρες σύνολο από εννοιολογική άποψη, ανήκει σε ένα σύνολο ιεραρχικά διευθετημένων ομάδων και εκτείνεται σε όλα τα συστήματα, τα οποία συμμορφώνονται προς την αρχιτεκτονική του δικτύου.

[40] Libicki, RAND, 2009, σελ. 11 et seq.

να γίνει αντικείμενο επίθεσης ή άλλων συναφών πράξεων, αλλά κάτι τέτοιο δεν μας ενδιαφέρει στα πλαίσια αυτής της εργασίας, για τους λόγους που ήδη επισημάνθηκαν παραπάνω (: ενδιαφέρει *η 'καταστροφή' ή αλλοίωση της πληροφορίας*, με ό,τι αυτό συνεπάγεται)˙ πρέπει όμως να επισημάνουμε ότι *ένας η/υ ή ένα δίκτυο δεν είναι δυνατόν να εξαπατηθεί με τη φυσική καταστροφή των εξαρτημάτων του, μπορεί όμως να εξαπατηθεί με την υποκατάσταση ενός εξαρτήματος με κάποιο άλλο*.[41] — Το *συντακτικό* επίπεδο περιέχει τις οδηγίες και τις εντολές τις οποίες οι σχεδιαστές και οι χρήστες δίνουν στα μηχανήματα, καθώς και τα πρωτόκολλα με τα οποία οι μηχανές επικοινωνούν μεταξύ τους (: device recognition, packet framing, addressing, routing, document formatting, database manipulation κ.λπ.). Ορισμένα συστήματα έχουν περισσότερο ανεπτυγμένο το στρώμα αυτό, αλλά ο κανόνας είναι ότι οποιοσδήποτε η/υ ή δίκτυο η/υ κ.λπ., όσο απλό ή απλοϊκό και αν είναι, πρέπει να διαθέτει ένα ελάχιστο σύνολο οδηγιών που ανήκει στο επίπεδο αυτό.[42] Αυτό το επίπεδο —δηλαδή τα σύνολα των οδηγιών και των κανόνων που ανήκουν σ' αυτό— *αποτελεί συνήθως στόχο των hackers*, οι οποίοι, ως 'τρίτοι' (outsiders) επιδιώκουν την υποκατάσταση των νόμιμων χρηστών και των σχεδιαστών των συστημάτων και την ανάληψη του ελέγχου αυτών.

Επάνω και από τα δύο προηγούμενα 'στρώματα' ή 'επίπεδα', υπάρχει και λειτουργεί το *σημασιολογικό* επίπεδο, δηλαδή αυτές καθ' εαυτές οι *πληροφορίες* που περιέχουν τα μηχανήματα (: οι μεμονωμένοι η/υ, τα δίκτυα, τα δίκτυα δικτύων κ.λπ.) και των οποίων η τήρηση, η επεξεργασία, η μεταφορά, η διαχείριση κ.λπ., είναι ακριβώς και ο λόγος ύπαρξης των η/υ και των δικτύων τους-! Ένα ποσοστό των πληροφοριών αυτού του επιπέδου προορίζονται για τον έλεγχο του ίδιου του συστήματος και άρα είναι σημασιολογικές ως προς τη μορφή, αλλά συντακτικές ως προς το σκοπό (π.χ. address lookup tables, printer control codes). Ένα άλλο ποσοστό προορίζεται αποκλειστικά και μόνο για τον έλεγχο άλλων μηχανών που ελέγχονται μέσω η/υ ή δικτύων (π.χ. έλεγχος και λειτουργία του δικτύου διανομής ηλεκτρικής ενέργειας, ή των χρηματιστηριακών και τραπεζικών συναλλαγών μίας χώρας, έλεγχος και λειτουργία του συστήματος εναέριας κυκλοφορίας ή αεράμυνας κ.λπ.). Το υπόλοιπο ποσοστό που είναι και το μεγαλύτερο, είναι πληροφορίες που έχουν νόημα μόνο για τα ανθρώπινα όντα – χρήστες των η/υ και των δικτύων και προορίζεται γι'

[41] Ibid, σελ. 12.
[42] Κατά τον Libicki, ibid, σελ 12, "… every system more complex than two cans and a string has to have some [syntactic level]".

αυτά.[43] Είναι νοητό και τεχνικά εφικτό η επίθεση σε η/υ /δίκτυα να γίνει *απευθείας* στο *σημασιολογικό* επίπεδο, με την εισαγωγή σ' αυτούς ψευδών[44] πληροφοριών. Μια τέτοια επίθεση μοιάζει με την 'εξαπάτηση' ενός θερμοστάτη χώρου, ο οποίος βρίσκεται σ' ένα ψυχρό δωμάτιο αλλά μπροστά του κάποιος ανάβει ένα κερί, με αποτέλεσμα ο θερμοστάτης αυτός να εκλαμβάνει λανθασμένα ότι η θερμοκρασία έχει αυξηθεί σε ολόκληρο το δωμάτιο(!), ή με την διασπορά ψευδών ειδήσεων που προέρχονται από μία φαινομενικά αξιόπιστη πηγή.[45] Κατά βάση, ωστόσο, μόνο τα συστήματα τα οποία δέχονται αθέμιτες παρεμβάσεις σε *συντακτικό* επίπεδο, μπορούν στη συνέχεια να τροφοδοτηθούν με ψευδείς πληροφορίες.

2. 'Ηλεκτρονικά όπλα' και τεχνικές[46]
(Τα 'όπλα' και οι τεχνικές που χρησιμοποιούνται στη διεξαγωγή CNAs)

2.1. 'Άρνηση υπηρεσιών' (Denial of Sevice (DoS), DoS attack)

Μία επίθεση άρνησης υπηρεσιών συνίσταται στον κατακλυσμό ενός δικτύου η/υ με τόσο πολλά αιτήματα παροχής υπηρεσιών (για παράδειγμα με το 'αίτημα' να έχουν πρόσβαση ή να 'βλέπουν' μία ιστοσελίδα δεκάδες ή εκατοντάδες χιλιάδες υποτιθέμενοι χρήστες ταυτόχρονα), ώστε η φυσιολογική ηλεκτρονική κίνηση του δικτύου αυτού να καταστεί εξαιρετικά αργή ή ακόμη και να διακοπεί. Αυτό που χαρακτηρίζει αυτού του είδους την επίθεση είναι η σαφής πρόθεση και επιδίωξη να αποκλειστούν όλοι οι 'νόμιμοι' και φυσιολογικοί χρήστες μίας υπηρεσία δικτύου, από την υπηρεσία αυτή. Πλεονέκτημα του τρόπου αυτού επιθέσεων αποτελεί το γεγονός ότι μπορεί να εκτελεστεί με πολύ περιορισμένα μέσα εναντίον σύγχρονων, τεχνολογικά εξελιγμένων και πολύπλοκων δικτύων και υπολογιστικών συστημάτων. Ένας επιτιθέμενος, με έναν προσωπικό η/υ (το γνωστό μας 'PC') και με τη χρήση του κατάλληλου λογισμικού και ενός σχετικά αργού *modem*, μπορεί, θεωρητικά, να θέσει εκτός λειτουργίας πολύ ταχύτερους και προηγμένους η/υ αλλά και δίκτυα.

---

[43] Τα όρια μεταξύ 'πληροφοριών' (information) και 'οδηγιών' ή 'εντολών' (instructions) που περιέχουν τα συστήματα, αρκετές φορές είναι θολά και ασαφή˙ πράγματι, αρκετές τεχνικές hacking εισάγουν *οδηγίες* στο σύστημα, *μεταμφιεσμένες* ως πληροφορίες προς αποθήκευση ή επεξεργασία, για παράδειγμα ιστοσελίδες που περιέχουν τμήμα κώδικα λογισμικού, αρχεία συνημμένα σε e-mail τα οποία περιέχουν υιούς ή εξαιρετικά μεγάλου μήκους διευθύνσεις που προκαλούν κορεσμό στις προσωρινές μνήμες (buffer overflow), με αποτέλεσμα τμήματα αυτών (των διευθύνσεων) να εισέρχονται στον όγκο των πληροφοριών που τυγχάνουν επεξεργασίας από το σύστημα, κ.λπ.

[44] Ο όρος 'ψευδής', εδώ, νοείται ως μία λογική τιμή που μπορεί να αποδοθεί σε μεταβλητές λογικού τύπου.

[45] Παράδειγμα από τον Libicki, RAND, 2009, σελ. 13.

[46] Schaap, USAF Law Review, vol. 64, σελ. 134 et seq., Roscini, σελ. 93, 94., Kamal, σελ. 40 et seq.

Τον Φεβρουάριο του 2000, για παράδειγμα, επιθέσεις τύπου DoS αχρήστευσαν προσωρινά ορισμένα από τα δημοφιλέστερα sites στο internet, μεταξύ των οποίων το eBay, το Amazon.com και το Yahoo!.[47]

2.2. 'Κατανεμημένη άρνηση υπηρεσιών' (Distributed denial of service (DDoS), DDoS attack)

Στις επιθέσεις που γίνονται με την τεχνική αυτή, ένας μεγάλος αριθμός (ένας 'στρατός') ηλεκτρονικά μολυσμένων η/υ ή συστημάτων, επιτίθενται εναντίον άλλων η/υ, δικτύων ή συστημάτων. Ο επιτιθέμενος χρησιμοποιεί χιλιάδες ή και εκατομμύρια μολυσμένους (με το κατάλληλο λογισμικό) η/υ —οι οποίοι συνήθως αναφέρονται ως "zombies" ή "bots"[48]— και τους ενορχηστρώνει στο να επιτεθούν συγχρόνως σε ένα δίκτυο[49]. Αυτού του είδους οι επιθέσεις είναι δύσκολο να αντιμετωπιστούν διότι τα δεδομένα που κατακλύζουν το δίκτυο – στόχο προέρχονται από πολλούς διαφορετικούς η/υ και από πολλές διαφορετικές γεωγραφικές τοποθεσίες (δηλαδή από … εκατομμύρια διαφορετικές διευθύνσεις internet – IP addresses).[50]

2.2.1. Μόνιμη άρνηση υπηρεσιών (Permanent denial of service – PDoS)

Μία παραλλαγή της επίθεσης κατανεμημένης άρνησης υπηρεσιών προκαλεί *μόνιμα* αποτελέσματα στο σύστημα – στόχο και συγκεκριμένα επιφέρει τόσο βαρείες ζημίες ώστε για την επαναφορά του συστήματος απαιτείται πλέον *η αντικατάσταση ή η επανεγκατάσταση τμημάτων του φυσικού εξοπλισμού* (hardware)· πρόκειται για επιθέσεις PDoS.[51] Οι συνήθεις επιθέσεις DoS ή DDoS αποσκοπούν στην αναστολή των λειτουργιών ή υπηρεσιών ενός δικτύου ή ενός ιστότοπου ή στο να αποκρύψουν την εισαγωγή στο σύστημα κακόβουλου λογισμικού (malware), ενώ οι επιθέσεις PDoS

---

[47] Barkham, 63.

[48] Για τις έννοιες 'bot' και 'botnet' βλ. αναλυτικά παραπάνω στην *Εισαγωγή*. Εδώ αναφέρουμε επιπλέον ότι, για παράδειγμα, το botnet 'Mariposa', το οποίο δημιουργήθηκε το 2008 και κατέστη δυνατό να διαλυθεί μόλις στις αρχές του 2010, σε κάποια φάση της λειτουργίας του ήλεγχε… **12,7 εκατομμύρια η/υ**-! (Arthur C., *The Guardian,* 03 Μαρ. 2010).

[49] Δηλαδή να κατακλύσουν το δίκτυο με έναν τεράστιο αριθμό αιτημάτων πρόσβασης, παροχής πληροφοριών, διαβίβασης πληροφοριών και στοιχείων και με λοιπά κατ' αρχήν 'νόμιμα' ή 'νομιμοφανή' αιτήματα, κατά τρόπο ώστε η διαχείρισή τους να καθίσταται απολύτως αδύνατη, *με αποτέλεσμα το σύστημα ή δίκτυο – στόχος να κορέννυται, να μην μπορεί να λειτουργήσει και να μετατρέπεται σ' ένα σύνολο από μεταλλικά κουτιά, πλαστικό και καλώδια…*

[50] Ο Roscini, 94 (και άλλοι) αναφέρει ότι τον Ιανουάριο του 2009 το Kyrgyzstan έγινε αντικείμενο επίθεσης τύπου DDoS, η οποία έθεσε εκτός λειτουργίας το 80% των επικοινωνιών internet της χώρας με τη Δύση.

[51] Βλ., π.χ., Kelly Jackson Higgins, Senior Editor, ηλεκτρονικό περιοδικό *'Security Dark Reading'*, στη διεύθυνση http://www.darkreading.com/security/client-security/211201088/permanent-denial-of-service-attack-sabotages-hardware.html (τελευταία πρόσβαση : 09 Οκτ. 2011).

αποτελούν καθαρή προσβολή του *υλικού* υπόβαθρου των συστημάτων, αλλά με τη χρήση λογισμικού (με 'ηλεκτρονικό' τρόπο, με την ευρύτερη έννοια του όρου).[52]

2.3. Κακόβουλο λογισμικό (malicious programs /software)

*(Αναφέρεται και ως **'malware'**, από τη σύντμηση των λέξεων malicious software.)*

Το κακόβουλο λογισμικό επιτίθεται διαταράσσοντας και αποδιοργανώνοντας τις φυσιολογικές λειτουργίες των η/υ και των δικτύων (: διαγραφή, τροποποίηση, μετατροπή, ή καταστροφή αρχείων και πληροφοριών κ.λπ.) ή δημιουργώντας αφύλακτες 'κερκόπορτες' (electronic back doors), μέσω των οποίων τρίτοι μπορούν να αναλάβουν τον έλεγχο του η/υ ή του δικτύου. Η επίθεση με κακόβουλο λογισμικό μπορεί είτε άμεσα να αχρηστεύσει ή να διαταράξει έναν η/υ ή ένα δίκτυο, είτε να είναι έτσι σχεδιασμένη ώστε να ενεργήσει με *χρονική καθυστέρηση*, μετά την αρχική εγκατάσταση του κακόβουλου λογισμικού, αχρηστεύοντας τον η/υ ή καθιστώντάς τον ενεργούμενο, μετά την παρέλευση ενός χρονικού διαστήματος, είτε αυτοματοποιημένα είτε με τη διαβίβαση εντολής εκ του μακρόθεν. Οι πιο συνηθισμένες μορφές κακόβουλου λογισμικού είναι οι ιοί, τα ηλεκτρονικά 'σκουλήκια' και οι 'δούρειοι ίπποι'

2.3.1. Ιός (virus)

Ο ιός είναι ένα μικρό πρόγραμμα το οποίο προσκολλά τον εαυτό του σε άλλα προγράμματα ή αρχεία και μεταδίδεται από η/υ σε η/υ, σε δίκτυα, συσκευές αποθήκευσης κ.λπ., φτιάχνοντας αντίγραφα του εαυτού του. Εκτός από αυτό, ένας ιός είναι συνήθως εφοδιασμένος και με ένα εκτελέσιμο κομμάτι λογισμικού (payload), το οποίο μπορεί να προγραμματιστεί έτσι ώστε να προκαλέσει κακόβουλα αποτελέσματα, όπως διαγραφές αρχείων, αλλοίωση δεδομένων, διαταραχή λειτουργιών κ.λπ. Σχεδόν όλοι οι ιοί προσαρτώνται σε εκτελέσιμα αρχεία, πράγμα που σημαίνει ότι ο ιός μπορεί να υπάρχει για ένα διάστημα σε κάποιον η/υ, χωρίς να είναι ανιχνεύσιμος, μέχρι τη στιγμή που το μολυσμένο εκτελέσιμο αρχείο θα εκτελεστεί (ή θα 'τρέξει', όπως λέγεται).[53]

---

[52] Αντίθετα, τα όπλα ηλεκτρονικού παλμού, όπως εξηγήθηκε παραπάνω, μπορούν να προκαλέσουν *υλική* καταστροφή των η/υ και των δικτύων με *ακτινοβολία* και χωρίς τη χρήση άλλων η/υ ή δικτύων ως όπλων.

[53] Ένας υιός μπορεί να είναι εξαιρετικά επικίνδυνος ακόμη και για αμυντικά συστήματα. Βλ., π.χ., πρόσφατο δημοσίευμα σύμφωνα με το οποίο εξαιτίας ενός ιού που έπληξε κέντρο ελέγχου στη Νεβάδα των Η.Π.Α., όλα τα μη επανδρωμένα εναέρια οχήματα (UAVs – unmanned aerial vehicles) των Η.Π.Α.,

2.3.2. Ηλεκτρονικά σκουλήκια (λογισμικά σκουλήκια) (worms)[54]

Τα 'σκουλήκια' λογισμικού λειτουργούν με τρόπο που μοιάζει με αυτόν των ιών, επειδή μεταδίδονται από η/υ σε η/υ. Σε αντίθεση, όμως, με τους ιούς, τα 'σκουλήκια' λογισμικού έχουν την ικανότητα να ταξιδεύουν χωρίς (έστω και την ακούσια) βοήθεια προσώπων· αυτό επιτυγχάνεται επειδή αυτού του είδους το κακόβουλο λογισμικό εκμεταλλεύεται τα δεδομένα μεταφοράς και κινήσεως των αρχείων εντός του δικτύου.[55] Ωστόσο, ο μεγαλύτερος κίνδυνος που παριστούν τα 'σκουλήκια' συνίσταται στο γεγονός ότι έχουν την ιδιότητα και την ικανότητα να αναπαράγουν τον εαυτό τους εντός του συστήματος· έτσι ένας μολυσμένος η/υ μπορεί να διαβιβάζει σε άλλους (και κατ' επέκταση σε ολόκληρα δίκτυα ή συστήματα) εκατοντάδες ή και χιλιάδες αντίγραφα ενός ηλεκτρονικού 'σκουληκιού'. Το τελικό αποτέλεσμα στις περισσότερες περιπτώσεις είναι ότι τα ηλεκτρονικά 'σκουλήκια' καταναλώνουν μεγάλα ποσοστά της διαθέσιμης μνήμης ή ακόμη και του εύρους (bandwidth) των γραμμών επικοινωνιών των δικτύων, με συνέπεια μεμονωμένοι υπολογιστές, εξυπηρετητές ιστοσελίδων (web servers) ή και εξυπηρετητές δικτύων (network servers), απλά να μην μπορούν να εκτελέσουν ούτε ένα ποσοστό της φυσιολογικής λειτουργίας τους. Τελευταία έχει παρατηρηθεί και η ύπαρξη σκουληκιών, σχεδιασμένων να εισέρχονται σε δίκτυα η/υ και τελικά να επιτρέπουν την εκ του μακρόθεν ανάληψη της λειτουργίας και διαχείρισης των δικτύων αυτών από τρίτους.

2.3.3. Δούρειοι ίπποι (Trojan horses)

Ο δούρειος ίππος είναι ένα φαινομενικά μη βλαβερό πρόγραμμα, το οποίο, ωστόσο, περιέχει —κατά τρόπο μη εμφανή— κακόβουλο ή επιβλαβή κώδικα λογισμικού και μπορεί να προκαλέσει ζημία ή να εκτελέσει οποιαδήποτε άλλη (κακόβουλη) εργασία για την οποία είναι προορισμένος. Οι χρήστες η/υ που λαμβάνουν έναν δούρειο ίππο, παρασύρονται διότι χρησιμοποιούν ένα φαινομενικά αβλαβές πρόγραμμα ή ανοίγουν αρχεία από φαινομενικά 'νόμιμη' και γνωστή πηγή προέλευσης. Οι δούρειοι ίπποι μπορούν να προκαλέσουν σοβαρά προβλήματα διαγράφοντας αρχεία ή καταστρέφοντας πληροφορίες· μπορούν επίσης να δημιουργήσουν ηλεκτρονικές

ακόμη και αυτά που δρουν στο Πακιστάν, την Υεμένη και τη Λιβύη, κινδυνεύουν να καθηλωθούν-! (βλ. http://www.defencenet.gr/defence/index.php?option=com_content&task=view&id=25207&Itemid=46, τελευταία πρόσβαση : 09 Οκτ. 2011).

[54] Η λέξη 'worm' σ' αυτήν την περίπτωση προέρχεται στην πραγματικότητα από τη φράση '**W**rite **O**nce **R**ead **M**any'.

[55] Για τα πακέτα δεδομένων και τον τρόπο κίνησής τους στα δίκτυα, βλ. στο *Παράρτημα.*

'κερκόπορτες' στο σύστημα. Σε αντίθεση με τους ιούς και τα ηλεκτρονικά 'σκουλήκια' δεν προσκολλώνται σε αρχεία ή προγράμματα για να τα μολύνουν ούτε αναπαράγουν τους εαυτούς τους.

2.3.4. Μικτές απειλές

Στην πράξη έχει παρατηρηθεί και η εκδήλωση *'μικτών απειλών'* πολύ προηγμένου τύπου, δηλαδή επιθέσεων στις οποίες χρησιμοποιούνται με συνδυασμένο και συνδυαστικό τρόπο —και χρονικά ταυτόχρονο ή/και συγχρονισμένο— τα πλέον επικίνδυνα χαρακτηριστικά των ιών, των δούρειων ίππων, των ηλεκτρονικών 'σκουληκιών' και άλλων ειδών κακόβουλου λογισμικού, όλα σε μια απειλή· εκμεταλλεύονται τις τρωτότητες των η/υ – εξυπηρετητών και του internet για ταχεία και εκτεταμένα αποτελέσματα.

2.3.5. Πολυμορφικό κακόβουλο λογισμικό (polymorphic malware)

Είναι κακόβουλο λογισμικό που έχει την ιδιότητα και τη δυνατότητα να μεταβάλλει κατά τρόπο τυχαίο την 'ηλεκτρονική του υπογραφή' (τα ηλεκτρονικά του ίχνη) κάθε φορά που αναπαράγει τον εαυτό του. Με τον τρόπο αυτό αποφεύγει την ανίχνευση από το λογισμικό που είναι σχεδιασμένο να το ανιχνεύει και να το εξουδετερώνει (anti-spyware programes). Στην περίπτωση του πολυμοφικού malware, μόνον η εμφάνιση του κακόβουλου κώδικα λογισμικού μεταβάλλεται, όχι και οι λειτουργίες του.

2.3.6. 'Λογικές βόμβες' (logic bombs) και 'βόμβες' χρονικής καθυστέρησης (time bombs)

Πρόκειται για κώδικα κακόβουλου λογισμικού, σχεδιασμένο να τίθεται σε εφαρμογή (να εκτελείται αυτοματοποιημένα) όταν πληρωθούν ορισμένες προϋποθέσεις, ή όταν συντρέξουν ορισμένα κριτήρια, ή, τέλος, σε μία δεδομένη χρονική στιγμή στο μέλλον. Μόλις συμβεί αυτό, ο κακόβουλος κώδικας μπορεί να διακόψει ή να καταστήσει δυσχερή τη λειτουργία ενός η/υ ή δικτύου, να διαγράψει δεδομένα, ή ακόμη και να ξεκινήσει μία επίθεση τύπου DoS /DDoS.

2.4. Παραπλάνηση (IP spoofing)

Με την *τεχνική* αυτή (γνωστή και ως IP address forgery ή host file hijack) ο επιτιθέμενος παρίσταται ψευδώς ως ο κατασκευαστής και διαχειριστής νόμιμων και ακίνδυνων ιστοσελίδων και ιστότοπων˙ ο επισκέπτης που πληκτρολογεί στον η/υ του μία διεύθυνση ορισμένης ιστοσελίδας στο διαδίκτυο,[56] οδηγείται σε μία άλλη ιστοσελίδα, παραποιημένη. Κατά την επικοινωνία του με αυτήν τη φαινομενικά νόμιμη και φυσιολογική —αλλά στην πραγματικότητα κατασκευασμένη από τρίτους—, ιστοσελίδα, όλα τα στοιχεία που τυχόν εισάγει ο χρήστης καταλήγουν στους 'πλαστογράφους', οι οποίοι *μπορούν ακόμη και να αναλάβουν τον έλεγχο του η/υ του ή του δικτύου* στο οποίο αυτός ανήκει, με ό,τι αυτό συνεπάγεται…

2.5. Chip-level actions ή chipping[57]

(Κακόβουλες ενέργειες σε επίπεδο ολοκληρωμένων κυκλωμάτων)

Μία από τις παλαιότερες μεθόδους δράσης εναντίον πληροφοριακών συστημάτων και δικτύων, είναι η διάθεση προς χρήση ολοκληρωμένων κυκλωμάτων (chips) στα οποία έχουν ενσωματωθεί τρωτότητες *εκ κατασκευής* (compromised microprocessor chips).[58] Ήδη το **1982** η CIA των Η.Π.Α. εκτέλεσε μία κυβερνο-επιχείρηση κατά την οποία ελαττωματικά ολοκληρωμένα κυκλώματα και λογισμικό που επίσης περιείχε τρωτότητες[59] και τα οποία είχαν διατεθεί με κατάλληλο τρόπο στην ελεύθερη αγορά, τοποθετήθηκαν στον εξοπλισμό που ήλεγχε τη λειτουργία του υπερ-Σιβηρικού αγωγού φυσικού αερίου,[60] με απευθείας απόκτηση από τους Σοβιετικούς από την ελεύθερη αγορά.[61] Το αποτέλεσμα ήταν ότι κάποια στιγμή, *ακριβώς σαν συνέπεια αυτού*, προκλήθηκε στον αγωγό έκρηξη ισχύος τριών κιλοτόνων˙[62] η σκέψη ότι το ίδιο αποτέλεσμα θα μπορούσε εναλλακτικά να επιτευχθεί με την οργάνωση μίας ολόκληρης επιχείρησης βομβαρδισμού μακράς ακτίνας, ή με την εκτόξευση ενός διηπειρωτικού πυραύλου, ή με την εκτέλεση κάποιας καταδρομικής

---

[56] Οι διευθύνσεις αυτές συχνά αναφέρονται απλά ως διευθύνσεις 'URL' (: uniform recourse locator).
[57] Roscini, 93, Walker, 36 et seq., Clark & Levin.
[58] Παραδόξως, αυτή η μέθοδος δράσης ή 'επίθεσης' εναντίον η/υ, συστημάτων και δικτύων έχει συζητηθεί ελάχιστα, τόσο από την πληροφοριακή όσο και από τη νομική κοινότητα και τη σχετική βιβλιογραφία.
[59] Δηλαδή *σκόπιμα σφάλματα* στον πηγαίο κώδικα (στο λογισμικό), γνωστά ως 'bugs' στην ορολογία της πληροφορικής.
[60] Trans-Siberian natural gas pipeline.
[61] Αντίθετα, η πρώτη περίπτωση ευρείας διάδοσης ενός 'ηλεκτρονικού σκουληκιού' (the Morris worm) στο τότε περιορισμένο internet, αναφέρεται ότι συνέβη το **1988** (έξι ολόκληρα χρόνια μετά…), στα πλαίσια ενός πειράματος με απρόβλεπτα και ανεπιθύμητα αποτελέσματα (United States v.Morris, 928 F.2d 504 (2d Cir. 1991)).
[62] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War*, εκδ. Ballantine Books, 2004, Clark & Levin, σελ. 4.

επιχείρησης, προκαλεί κατ' ελάχιστον ανησυχία… Η συγκεκριμένη μέθοδος παρουσιάζει ορισμένα πλεονεκτήματα σε σχέση με τη χρήση των παραπάνω αναφερόμενων 'ηλεκτρονικών όπλων' και μεθόδων : είναι σαφώς αρκετά πιο 'διακριτική' και *αδύνατο να εντοπιστεί με τη χρήση αντι-ιικών προγραμμάτων*.

> Η μέθοδος αυτή μπορεί να υλοποιηθεί με δύο τρόπους : Κατ' αρχάς το εκ κατασκευής προβληματικό ολοκληρωμένο κύκλωμα μπορεί να λειτουργήσει ως 'χρονοδιακόπτης' (kill switch), διακόπτοντας τη λειτουργία του συστήματος στο οποίο έχει εγκατασταθεί, ή προκαλώντας δυσλειτουργία —είτε με τρόπο τυχαίο είτε σε προκαθορισμένο χρονικό σημείο. Ο πιο εύκολος τρόπος να γίνει κάτι τέτοιο είναι με την ενσωμάτωση στο κύκλωμα ενός τυπωμένου ελαττωματικού μικροκαλωδίου. Επίσης, είναι δυνατόν το ολοκληρωμένο κύκλωμα να έχει 'πειραχθεί' με την προσθήκη επιπρόσθετου —και φυσικά μη ανιχνεύσιμου— λογισμικού·[63] αυτό μπορεί να γίνει με την προσθήκη επιπλέον τυπωμένων transistors στο κύκλωμα κατά τη διαδικασία κατασκευής του,[64] ή κατά τη διαδικασία σχεδιασμού του.[65] Δεύτερον, είναι δυνατόν να έχει προστεθεί στο ολοκληρωμένο κύκλωμα επιπρόσθετο λογισμικό, που δημιουργεί μία ηλεκτρονική 'κερκόπορτα', μέσω της οποίας τρίτοι μπορούν να ενεργοποιούν ή να απενεργοποιούν συγκεκριμένες λειτουργίες.

Οι αθέμιτες επεμβάσεις στα ολοκληρωμένα κυκλώματα (στους επεξεργαστές, τις κάρτες δικτύων, τις κάρτες γραφικών κ.λπ.) είναι εξαιρετικά δύσκολο να ανιχνευθούν εκ των προτέρων. Επειδή ένα ολοκληρωμένο κύκλωμα μπορεί να αποτελείται, σήμερα πλέον, μέχρι και από δύο δισεκατομμύρια(!) transistors,[66] τα περισσότερα *διαγνωστικά προγράμματα* ελέγχουν μόνον την ύπαρξη συγκεκριμένων λειτουργιών των κυκλωμάτων και όχι όλο το εύρος των δυνατοτήτων ή των αδυναμιών τους. Για παράδειγμα, ο κατασκευαστής ενός κινητού τηλεφώνου ή ενός ασυρμάτου για

---

[63] Θα πρόκειται για λογισμικό τύπου 'firmware', δηλαδή για 'ενσυρματωμένο' λογισμικό που αναπαριστάται απευθείας με τυπωμένα μικρο-κυκλώματα επάνω στην πλακέτα των ηλεκτρονικών.

[64] Η διαδικασία αυτή, δηλαδή η διαδικασία ενσωμάτωσης των τυπωμένων κυκλωμάτων στις πλακέτες των ηλεκτρονικών, αποτελείται από περίπου … *τετρακόσια* (400) κατασκευαστικά στάδια-! (Clark & Levin, σελ. 5).

[65] Η ύπαρξη περισσότερων κυκλωμάτων ή περισσότερων δυνατοτήτων σ' ένα μικροτσίπ απ' ό,τι συνήθως χρειάζονται, δεν είναι κατ' ανάγκην κάτι 'κακό'˙ αντίθετα είναι σύνηθες στην αγορά. Τα προγραμματιζόμενα μικροτσίπ γενικών χρήσεων χρησιμοποιούνται σε διάφορες συσκευές και σε διάφορες εργασίες, ακόμη και από την αμυντική βιομηχανία και τους κατασκευαστές αμυντικών συστημάτων. Για το σχεδιασμό αυτών των μικροτσίπ χρησιμοποιούνται σχεδιαστικά προγράμματα, διαθέσιμα και στο internet, και αυτό αυξάνει τις πιθανότητες και τις δυνατότητες εισαγωγής στα κυκλώματα κρυφών δυνατοτήτων και κακόβουλου λογισμικού.

[66] Πρόκειται για 'ολοκλήρωση πολύ μεγάλης κλίμακας' (VLSI – very large scale integration). Περί αυτού βλ. και στο *Παράρτημα*.

στρατιωτική χρήση μπορεί να αγοράσει από την ελεύθερη αγορά ένα ολοκληρωμένο κύκλωμα συγκεκριμένων προδιαγραφών, να το υποβάλλει σε διαγνωστική δοκιμασία (με τη χρήση κατάλληλου λογισμικού) για να διαπιστώσει εάν εκτελεί τις επιθυμητές λειτουργίες και τελικά να το εγκαταστήσει στο τελικό προϊόν της εταιρείας του· κάθε τυχόν επιπρόσθετη λειτουργία ή δυνατότητα του κυκλώματος αυτού, δεν θα φανεί στις διαγνωστικές δοκιμασίες, απλά γιατί *κάτι τέτοιο δεν απαιτείται*. Εάν το κύκλωμα αυτό, ωστόσο, είναι εφοδιασμένο με μία συγκεκριμένη τρωτότητα, είναι δυνατόν να παρακάμπτει το λογισμικό κρυπτογράφησης του τηλεφώνου ή του ασυρμάτου και να παρέχει σε τρίτους τη δυνατότητα ανοικτής ακρόασης των συνομιλιών ή πρόσβασης στα δεδομένα που ανταλλάσσονται· είναι επίσης δυνατό να επιτρέπει σε τρίτους τον εντοπισμό της θέσης του χρήστη του τηλεφώνου ή του ασυρμάτου, για την περίπτωση που αυτοί θα ήθελαν να αντλήσουν κάποια πληροφορία από τη θέση αυτή ή να χρησιμοποιήσουν εναντίον του, για παράδειγμα, όπλα κινητικής ενέργειας…

> Με την αξιοποίηση σημάτων που εκπέμπονται από κινητά τηλέφωνα (χωρίς οι κάτοχοί τους να το γνωρίζουν), φαίνεται ότι έχουν εντοπιστεί και εξολοθρευτεί σε αρκετές περιπτώσεις (με τη χρήση μη επανδρωμένων ιπταμένων οχημάτων) ηγέτες των Ταλιμπάν και της al Qaeda σε επιχειρήσεις στο Αφγανιστάν.[67]

Αλλά και η ενσωμάτωση ‘χρονοδιακοπτών’ στα ολοκληρωμένα κυκλώματα μπορεί να λειτουργεί με ποικίλους τρόπους. Ένα κατάλληλα σχεδιασμένο ολοκληρωμένο κύκλωμα μπορεί να ρυθμιστεί έτσι ώστε να δυσλειτουργήσει και κατά συνέπεια να διακόψει, ή να μεταβάλλει /τροποποιήσει, τη λειτουργία του συστήματος στο οποίο έχει ενταχθεί, όταν συντρέξουν κάποιες προϋποθέσεις.[68] Νοητός, αν και δύσκολος (αλλά όχι ανέφικτος), είναι και ο σχεδιασμός και η εγκατάσταση σε ηλεκτρονικά συστήματα ολοκληρωμένων κυκλωμάτων στα οποία είναι δυνατόν να ενεργοποιηθούν (ή, αντίστοιχα, να απενεργοποιηθούν) ορισμένες δυνατότητες ή λογικές λειτουργίες εκ του μακρόθεν, με την παρέμβαση τρίτου.[69]

---

[67] Βλ., π.χ., http://news.rediff.com/slide-show/2009/aug/14/slide-show-1-everything-you-wanted-to-know-about-drones.htm.

[68] Για παράδειγμα, να αχρηστέψει το σύστημα κατεύθυνσης ενός πυραύλου, μόλις αυτός εκτοξευθεί και οπλιστεί, ή —ακόμη χειρότερα— να εκτρέψει το όπλο αυτό σε διαφορετικό στόχο-!

[69] Φημολογείται έντονα, για παράδειγμα, ότι η επίθεση του *Ισραήλ* τον *Σεπτέμβριο του **2007*** εναντίον τοποθεσίας στη *Συρία* όπου κατά πληροφορίες κατασκευάζονταν πυρηνικές υποδομές, έγινε δυνατή επειδή τα ισραηλινά αεροσκάφη δεν έγιναν εγκαίρως αντιληπτά από τη συριακή αεράμυνα, εξαιτίας της προσωρινής απενεργοποίησης με ‘τηλεχειρισμό’ ορισμένων λειτουργιών του ηλεκτρονικού εξοπλισμού των συστημάτων αεράμυνας, στον οποίο είχαν εγκατασταθεί *εμπορικού τύπου* ολοκληρωμένα κυκλώματα που είχαν αγοραστεί από την ελεύθερη αγορά (altered commercial off-the-shelf microprocessors) (Clark

Όλες οι επιθέσεις τύπου DoS /DDoS έχουν λίγο ως πολύ παρόμοια αποτελέσματα, ιδίως όσον αφορά την έλλειψη υλικής καταστροφής στους ίδιους τους υπολογιστές και τα δίκτυα.[70] Αντίθετα, οι συνέπειες από τις *ενέργειες σε επίπεδο ολοκληρωμένων κυκλωμάτων* ποικίλουν, από τη δημιουργία μίας κερκόπορτας σ' έναν η/υ ή ένα δίκτυο, που επιτρέπει τη μόνιμη πρόσβαση σε τρίτους και την εκμετάλλευση πληροφοριών και δεδομένων απ' αυτούς,[71] έως την πρόκληση πραγματικής υλικής καταστροφής (physical destruction) στο σύστημα. Ανάμεσα σ' αυτά τα δύο 'άκρα', με επέμβαση, ακριβώς, στα ολοκληρωμένα κυκλώματα ένα σύστημα μπορεί να είναι δυνατόν να καταστεί (ανά πάσα στιγμή) αναποτελεσματικό ή μη-λειτουργικό.

III. Τι θεωρείται 'use of force' και 'armed attack' κατά το διεθνές δίκαιο σήμερα

Μετά το τέλος της οδυνηρής εμπειρίας του Β' Παγκοσμίου Πολέμου, η διεθνής κοινότητα προσπάθησε να ρυθμίσει την προσφυγή στη βία από τα κράτη στις μεταξύ τους σχέσεις και έθεσε σε ισχύ ένα μοντέρνο (για τα δεδομένα της εποχής) θεσμικό πλαίσιο, με τη μορφή του Χάρτη του Ο.Η.Ε.[72] Το πλαίσιο αυτό προβλέπει αφενός μεν την κατ' αρχήν απόλυτη απαγόρευση της χρήσης βίας στις διεθνείς σχέσεις μεταξύ των κρατών, αφετέρου δε ένα σύστημα για την τήρηση στην πράξη της απαγόρευσης αυτής. Έτσι σήμερα ο Χάρτης και οι σχετικοί με τον τομέα αυτόν κανόνες του διεθνούς εθιμικού δικαίου, ορίζουν, με περιοριστικό τρόπο, το *πότε* και το *πώς* μπορεί να χρησιμοποιηθεί βία από τα κράτη στις διεθνείς τους σχέσεις.

Ο Χάρτης στο *άρθρο 2(4)* ορίζει ότι "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the

& Levin, σελ. 4). (Σύμφωνα με άλλες πληροφορίες, όμως, η 'τύφλωση' της συριακής αεράμυνας έγινε με επέμβαση στο φέρον κύμα των ραντάρ.)

[70] Μπορούν, όμως, να προκαλέσουν —όπως θα έχει γίνει πια κατανοητό μέχρι τώρα— υλικές καταστροφές και απώλειες ζωών εξ αιτίας της παύσης ή της αποδιοργάνωσης του ελέγχου που τα δίκτυα αυτά ασκούν σε διάφορα συστήματα ή υποδομές κοινής ωφελείας, συστήματα ελέγχου κυκλοφορίας κ.λπ.

[71] Δηλαδή είδος *espionage*, που δεν ενδιαφέρει στα πλαίσια της εργασίας αυτής.

[72] Για την Ελλάδα : κυρωτικός αναγκαστικός νόμος 585/1945, ΦΕΚ 242 τ. Α'/29-09-1945. (Ο Χάρτης υιοθετήθηκε την 25-06-1945 (τότε, ακόμη, ο πόλεμος με την Ιαπωνία δεν είχε τερματιστεί …) και τέθηκε σε ισχύ την 24-10-1945.)

Purposes of the United Nations"[73] και στο *άρθρο 51* ότι "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security….".[74] Για τα ακρότατα όρια της αυτοάμυνας του άρθρου 51 η συζήτηση είναι ευρεία και ακόμη ανοικτή. Παρ' όλ' αυτά γίνεται από όλους δεκτό ότι το άρθρο 51 συνιστά μία από τις εξαιρέσεις της απαγόρευσης του άρθρου 2(4), υπό την έννοια ότι η (στρατιωτική) χρήση βίας την οποία 'επιτρέπει' το άρθρο 51 δεν απαγορεύεται από το άρθρο 2(4).

Πέρα από τη σκόπιμη μη αναφορά του όρου 'πόλεμος' στο άρθρο 2(4),[75] το άρθρο αυτό ήταν καινοτόμο και για τον πρόσθετο λόγο ότι απαγορεύει και την *απειλή* χρήσης βίας˙ απαγορευμένες απειλές είναι όμως μόνον αυτές με τις οποίες εξαγγέλλεται χρήση βίας που θα είναι 'παράνομη' κατά τον Χάρτη.[76] Εξάλλου, η φράση "against the territorial integrity… or in any other manner inconsistent…", γίνεται πλέον δεκτό ότι συνιστά μία πρόβλεψη σχεδιασμένη να καλύπτει όλες τις περιπτώσεις χρήσης βίας οι οποίες δεν είναι ανεκτές από τις διατάξεις του Χάρτη —ήτοι κάθε χρήση βίας εκτός από την άσκηση βίας κατόπιν εξουσιοδοτήσεως από το Σ.Α. ή στα πλαίσια άσκησης του δικαιώματος αυτοάμυνας— και να *διευρύνει* το πλαίσιο εφαρμογής της απαγόρευσης του άρθρου 2(4) και όχι το αντίθετο-! Πράγματι, από τις προπαρασκευαστικές εργασίες της διάσκεψης του San Francisco προκύπτει ότι οι φράσεις "against the territorial… …" δεν είχαν τεθεί από την αρχή στο κείμενο αλλά

---

[73] Κατά την ελληνική μετάφραση στον αναγκαστικό νόμο 585/1945 «[π]άντα τα Μέλη θα απέχωσι εις τας διεθνείς αυτών σχέσεις της απειλής ή χρήσεως βίας κατά της εδαφικής ακεραιότητος ή της πολιτικής ανεξαρτησίας οιουδήποτε Κράτους ή καθ` οιονδήποτε άλλον τρόπον ασυμβίβαστον προς τους σκοπούς των Ηνωμένων Εθνών.» — Η απαγόρευση αυτή δεν έχει αποτρέψει, ωστόσο, το ξέσπασμα 100 και πλέον 'μεγάλων συγκρούσεων' από το 1945 μέχρι σήμερα και το θάνατο περισσότερων από 20 εκατομμυρίων ανθρώπων εξ αιτίας αυτών. (*Gray* σε Evans, 589.)

[74] Κατά την ελληνική μετάφραση στον αναγκ. νόμο 585/1945 «[ο]υδέν εκ των διαλαμβανομένων εν τω παρόντι Χάρτη θα παρεμποδίζη το φυσικόν δικαίωμα ατομικής ή συλλογικής νομίμου αμύνης εις περίπτωσιν καθ` ήν Μέλος τι των Ηνωμένων Εθνών υποστή επίθεσιν ένοπλον, μέχρις ου το Συμβούλιον Ασφαλείας λάβη τα αναγκαία μέτρα προς διατήρησιν της διεθνούς ειρήνης και ασφαλείας..».

[75] Ο Dinstein (Dinstein, e-book, σελ. 80) σημειώνει ότι το άρθρο 2(4) αποφεύγει τη χρήση του όρου 'war', αλλά η απαγόρευση της χρήσης βίας κατά το άρθρο αυτό καλύπτει, βέβαια, και τον (κλασσικό) πόλεμο, ωστόσο τον ξεπερνά και καλύπτει και άλλα είδη καταναγκασμού /εξαναγκασμού στις διακρατικές σχέσεις που δεν φθάνουν στο κατώφλι του πολέμου ("forcible measures short of war").

[76] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ Rep. 226, (246, §47). Ορισμό της 'απειλής χρήσης βίας' παραθέτει ο Roscini, σελ. 104 (: "άμεση ή έμμεση εξαγγελία, με δηλώσεις ή διάφορες άλλες ενέργειες, για τη μελλοντική άσκηση παράνομης βίας…" κ.λπ.), όπου γίνεται και παραπομπή στο άρθρο *"Threats of Armed Force and Contemporary International Law"*, NILR 54 (2007), 229 et seq. (235), του ιδίου.

προστέθηκαν αργότερα με σκοπό την *έμφαση* και *όχι* με σκοπό περιορισμού του εύρους της γενικής απαγόρευσης "inconsistent with the Purposes of the United Nations".[77]

Η απαγόρευση της απειλής ή της χρήσης βίας στις διεθνείς σχέσεις των κρατών αποτελεί και κανόνα του διεθνούς *εθιμικού* δικαίου και μάλιστα κανόνα *jus cogens*[78] και κατά συνέπεια δεσμεύει όλα τα κράτη, ανεξάρτητα από το εάν έχουν, συγχρόνως, και την ιδιότητα του Μέλους του Ο.Η.Ε.[79] Πάντως τόσο ο κανόνας του άρθρου 2(4) του Χάρτη όσο και ο αντίστοιχός του κανόνας του διεθνούς εθιμικού δικαίου, έχουν αποκλειστικά απαγορευτικό περιεχόμενο και δεν περιέχουν ρυθμίσεις για την αποκατάσταση των πραγμάτων στην προτέρα κατάσταση˙ η φύση και το εύρος των ενεργειών που μπορούν να αναληφθούν σε περίπτωσή παραβίασής τους, καθορίζονται από τους κανόνες που διέπουν τη λειτουργία και τις εξουσίες του Σ.Α., τους κανόνες που διέπουν την άσκηση του δικαιώματος αυτοάμυνας των κρατών και το δίκαιο της διεθνούς ευθύνης των κρατών.

Αν και η διατύπωση της απαγόρευσης είναι εξαιρετικά απλή, το περιεχόμενό της είναι αρκετά σύνθετο και δημιουργεί περισσότερα προβλήματα απ' αυτά που επιχειρεί να επιλύσει-! Στα πλαίσια της εργασίας αυτής —και προκειμένου να κριθεί εάν, και υπό ποίες προϋποθέσεις, τελικά η εκδήλωση CNAs αποτελεί χρήση βίας και ένοπλη επίθεση—, ενδιαφέρει ιδιαίτερα η απάντηση στο ερώτημα «τι είναι, εν τέλει, 'χρήση βίας'», εν όψει του γεγονότος ότι την εποχή που συντάχθηκε και τέθηκε σε ισχύ η συγκεκριμένη απαγόρευση, οι έννοιες των η/υ, του διαδικτύου, του κυβερνοχώρου και του 'κυβερνοπολέμου' (για να αναφέρουμε μόνον μερικές από αυτές τις 'εξωτικές' νέες έννοιες) δεν υπήρχαν ούτε καν στη *φαντασία* των συντακτών του Χάρτη-!

Τα γενικά κριτήρια για την ερμηνεία των διεθνών συνθηκών καθορίζονται στο άρθρο 31 §1 της Συνθήκης της Βιέννης του 1969.[80] Ο Χάρτης υιοθετήθηκε και τέθηκε σε ισχύ *πριν* από την Συνθήκη της Βιέννης και η Συνθήκη, κατά το άρθρο 4

---

[77] Randelzhofer A., 'Article 2(4)', *The Charter of the United Nations: A Commentary* 106, 118 (B. Simma ed., 1995).

[78] ICJ, Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.A.), 1986 ICJ Rep. 14, 187 – 191. Επίσης, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ Rep. 2005, 136 et seq.

[79] Ως γνωστό, το ICJ κατά το άρθρο 38(1) του Καταστατικού του εφαρμόζει, εκτός από το διεθνές γραπτό συμβατικό δίκαιο, και το *διεθνές έθιμο* "as evidence of a general practice accepted as law".

[80] 1969 Vienna Convention on the Law of Treaties, UN *Treaty Series*, vol. 1155, p. 331 (για την Ελλάδα, κυρωτικό νομοθ. δ/γμα 402/1974, ΦΕΚ 141 τ. Α').

αυτής, *δεν* εφαρμόζεται σε προγενέστερα συμβατικά κείμενα, ωστόσο οι κανόνες ερμηνείας των άρθρων 31 και 32 που αυτή περιλαμβάνει θεωρούνται κατά βάση ότι συνιστούν κωδικοποίηση διεθνούς *εθιμικού* δικαίου.[81] Εάν εφαρμόσουμε τα κριτήρια της γραμματικής ερμηνείας και του γενικότερου συμφραζομένου προσπαθώντας να προσδιορίσουμε με τη μεγαλύτερη δυνατή ακρίβεια το περιεχόμενο του όρου 'force' του άρθρου 2(4), τα αποτελέσματα δεν είναι και τόσο ενθαρρυντικά : Κατ' αρχάς η έννοια της λέξης 'force' είναι αρκετά ευρεία και το γλωσσικό της πεδίο φαίνεται ότι καλύπτει τόσο την κλασσική στρατιωτική χρήση βίας όσο και άλλες μορφές καταναγκασμού.[82] Από την πλευρά του γενικότερου συμβατικού 'περιβάλλοντος' και των συμφραζομένων του Χάρτη (: context), η λέξη *force,* η οποία στο άρθρο 2(4) δεν συνοδεύεται από τον επιθετικό προσδιορισμό *'armed'*, απαντάται και στο Προοίμιο και στα άρθρα 41 και 46, όπου όμως συνοδεύεται από τον επιθετικό προσδιορισμό *'armed'*, ενώ στο άρθρο 44 είναι σαφές ότι γίνεται αναφορά σε *στρατιωτική* βία και *μόνο*. Με βάση αυτή την παρατήρηση αρκετοί μελετητές υποστηρίζουν ότι επειδή στα άλλα σημεία του Χάρτη η λέξη 'force' σημαίνει 'armed force', αυτό πρέπει να θεωρηθεί ότι ισχύει και για το άρθρο 2(4), ενόψει της ανυπαρξίας άλλου ειδικού προσδιορισμού. Αν και το επιχείρημα αυτό μπορεί άνετα να αντιστραφεί (: όπου οι συντάκτες του Χάρτη θέλησαν να αναφερθούν σε 'armed force' το διατύπωσαν έτσι ακριβώς και αυτή δεν είναι η περίπτωση του άρθρου 2(4)˙ έτσι, μπορεί να θέλησαν στο άρθρο αυτό ο όρος 'force' να έχει ευρύτερο περιεχόμενο), ωστόσο, η *στενότερη* ερμηνεία του όρου, κατά τρόπο ώστε να καλύπτει μόνον την *ένοπλη* /στρατιωτική βία (armed force), φαίνεται ότι είναι περισσότερο συμβατή με την *τελολογική* ερμηνεία του άρθρου 2(4) : Ο *σκοπός* του Χάρτη, όπως αυτός αποτυπώνεται στο Προοίμιό του, είναι "to save succeeding generations from the scourge of war"[83] και όχι να απαγορεύσει ή να εξοβελίσει όλες τις μορφές και τους τρόπους καταναγκασμού που θα μπορούσαν να χρησιμοποιηθούν μεταξύ των κρατών στις διεθνείς τους σχέσεις.[84] Επίσης, οι προπαρασκευαστικές

[81] ICJ, the *Genocide Convention (Bosnia* v. *Serbia)* case, ICJ Reports, 2007, paras. 160 ff.; Επίσης, ICJ, *Indonesia/Malaysia* case, ICJ Reports, 2002, pp. 625, 645–6. Βλ. και Shaw, e-book, 6th ed., σελ. 933 και τις εκεί παραπομπές, Ρούκουνα, σελ. 177 et seq.

[82] Κατά το *Black's Law Dictionary*, εκδ. 2009, 'force' σημαίνει «δύναμη, βία ή πίεση που κατευθύνεται εναντίον ενός προσώπου ή πράγματος» ("power, violence, or pressure directed against a person or thing" —αναφέρεται από τον Roscini, σελ. 104).

[83] Ενδιαφέρον, βέβαια, είναι ότι εδώ χρησιμοποιείται η λέξη 'war'. — Κατά τη μετάφραση του αντίστοιχου εδαφίου από τον έλληνα κυρωτικό νομοθέτη : «[ό]πως σώσωμεν τας επερχομένας γενεάς από την μάστιγα του πολέμου, ήτις δις εις το διάστημα μιας γενεάς επεσσώρευσεων άφατον θλίψιν εις την ανθρωπότητα».

[84] Έτσι Randelzhofer A., *'Article 2(4)'*, op. cit., 112–113.

εργασίες[85] της διάσκεψης του San Francisco αποκαλύπτουν ότι στη βούληση (της πλειοψηφίας) των συμβαλλομένων μερών δεν συμπεριλαμβανόταν και η απαγόρευση του οικονομικού καταναγκασμού και της βίας που ασκείται με πολιτικές πιέσεις.[86] Τέλος, η προσέγγιση ότι το άρθρο 2(4) αναφέρεται μόνο σε ένοπλη βία υποστηρίζεται και από σημαντικά κείμενα της Γ.Σ. που εκδόθηκαν τις δεκαετίες που ακολούθησαν, όπως η *Declaration on Friendly Relations* του 1970 και η *Declaration on the Non-Use of Force* του 1987. Τις άλλες μορφές καταναγκασμού στις διεθνείς σχέσεις μεταξύ των κρατών ρυθμίζει η αρχή της μη-επέμβασης (principle of non-intervention).[87]

Το επόμενο ερώτημα είναι, βέβαια, τι ακριβώς συνιστά 'ένοπλη' ('armed') βία. Κατά το Black's Law Dictionary, για παράδειγμα,[88] *'armed'* είναι αυτός που είναι εξοπλισμένος με όπλο ή αυτός που χρησιμοποιεί όπλο, *'όπλο'* δε, είναι ένα όργανο, εργαλείο ή σύστημα το οποίο χρησιμοποιείται για να προκαλεί βλάβες ή θάνατο ή είναι σχεδιασμένο για το σκοπό αυτό. *Σχεδόν κάθε αντικείμενο μπορεί να χρησιμοποιηθεί ως 'όπλο', αρκεί η χρήση του σαν τέτοιο να καλύπτεται από τη βούληση αυτού που το φέρει ή το χρησιμοποιεί*.[89]

Η επιλογή των λέξεων στο άρθρο 51 είναι σκόπιμα περιοριστική˙ η φράση 'armed attack' δεν είναι ισοδύναμη με τον όρο 'aggression'. Ο τελευταίος αυτός όρος είναι αρκετά πιο ευρύς και 'χαλαρός'.[90] Στην πραγματικότητα η ένοπλη επίθεση είναι ένα είδος 'aggression'[91] και μάλιστα ένα είδος επίθεσης στα πλαίσια της οποίας γίνεται παράνομη χρήση ένοπλης βίας σε βάρος άλλου κράτους. Η παράνομη χρήση βίας για να λάβει τις διαστάσεις μίας 'ένοπλης επίθεσης' πρέπει να φθάσει και να ξεπεράσει ένα

---

[85] *'Travaux preparatoires'* στα γαλλικά, όπως έχει επικρατήσει ο όρος στην πράξη. Κατά το άρθρο 32 της Συνθήκης της Βιέννης του 1969, οι προπαρασκευαστικές εργασίες που οδηγούν στην σύναψη ενός διεθνούς συμβατικού κειμένου, αποτελούν *"supplementary means of interpretation"*.

[86] Σχετική πρόταση περί του αντιθέτου από την Αντιπροσωπεία της Βραζιλίας στη διάσκεψη, *απορρίφθηκε*.

[87] Η αρχή της μη επέμβασης αναφέρεται στο κείμενο ενός ικανού αριθμού διεθνών συμβάσεων, αλλά *δεν* διατυπώνεται ρητά στον ίδιο τον Χάρτη του Ο.Η.Ε. Το Δ.Δ.Χ.. την προσεγγίζει, ωστόσο, ως κανόνα του διεθνούς εθιμικού δικαίου ("part and parcel of customary international law" – Nicaragua v. United States, ICJ Reports 1986, 106, para. 202).

[88] Op. cit., υποσημ. 82. Χρησιμοποιείται από τον Roscini, σελ. 106.

[89] Για παράδειγμα, το *Oxford Dictionary of Law*, 5th ed., 2002, στο λήμμα *"weapon of offence"* δίνει τον ορισμό : "[a]ny offensive weapon *or any article made, adapted, or intended for incapacitating someone*…" (ή έμφαση δική μας). — Παραδοσιακά, επίσης, στα εγχειρίδια ανορθόδοξων επιχειρήσεων των ενόπλων δυνάμενων όλων των χωρών αναφέρεται ότι ως όπλο μπορεί να χρησιμοποιηθεί *ο π ο ι ο δ ή π ο τ ε* αντικείμενο μπορεί να προκαλέσει τραυματισμό, θάνατο ή απώλειες στον αντίπαλο.

[90] Χρησιμοποιείται, για παράδειγμα, στο άρθρο 39 του Χάρτη, αναφορικά με κάποιες αρμοδιότητες του Σ.Α.

[91] Αυτό αναδεικνύεται ιδίως από τη γαλλική μετάφραση του κειμένου του Χάρτη, όπου ο όρος 'armed attack' αποδίδεται ως "une aggression armée".

ελάχιστο απαιτούμενο ύψος βίας και συνεπειών, δηλαδή ένα 'κατώφλι' (threshold), όπως έχει επικρατήσει να λέγεται. Με δεδομένο ότι το άρθρο 2(4) απαγορεύει τη χρήση βίας και το άρθρο 51 επιτρέπει την εκδήλωση ενεργειών αυτοάμυνας μόνο εναντίον ένοπλης επίθεσης, είναι φανερό ότι οι δύο αυτές προβλέψεις αφήνουν ένα ρυθμιστικό διάκενο.[92] Το διάκενο αυτό οφείλεται στο γεγονός ότι, κατά τη βούληση των συντακτών του Χάρτη, προφανώς, εάν ασκηθεί παράνομη βία από ένα κράτος σε βάρος κάποιου άλλου και η βία αυτή δεν φθάνει στο επίπεδο της 'ένοπλης επίθεσης' ή δεν ισοδυναμεί με τέτοια, τότε το κράτος – θύμα δεν μπορεί να ασκήσει, με τη σειρά του, βία επικαλούμενο αυτοάμυνα. Η σκόπιμη αυτή ανοχή του συγκεκριμένου νομικού κενού στις διατάξεις του Χάρτη, μεταφέρει, ακριβώς, τη βούληση των συντακτών του, να επιτρέπεται η χρήση βίας ως απάντηση στη βία —στα πλαίσια αυτοάμυνας—, *μόνον* όταν η βία του επιτιθέμενου είναι επαρκούς έντασης, ξεπερνά δηλαδή ένα συγκεκριμένο 'κατώφλι'.[93] Εάν η βία που ασκείται παραμένει κάτω από αυτό όριο, τότε το κράτος – θύμα έχει στη διάθεσή του *άλλα* μέσα αντίδρασης, *όχι* όμως και την άσκηση 'αναγκαίας' και 'ανάλογης' βίας στα πλαίσια αυτοάμυνας.

IV. Υπό ποίες προϋποθέσεις και με βάση ποια κριτήρια μπορεί μία CNA να αποτελεί 'use of force' και 'armed attack' κατά το *jus ad bellum*

1. Γενικά

Όταν μία 'επίθεση' CNA μπορεί να αποδοθεί σε συγκεκριμένο κράτος,[94] τότε συνιστά κατ' αρχάς παραβίαση της εθιμικής ισχύος αρχής της μη επέμβασης. Αρκετές από τις περιπτώσεις και τις καταστάσεις που μνημονεύονται στην Διακήρυξη περί Μη-Επέμβασης της Γ.Σ. του Ο.Η.Ε. του 1981,[95] μπορούν να καλύψουν και τις CNA. Μάλιστα και ορισμένες επιχειρήσεις *CNE* μπορούν κάλλιστα να συνιστούν παραβιάσεις της αρχής αυτής, όπως, για παράδειγμα, η (συστηματική) 'κυβερνο-προπαγάνδα' που αποσκοπεί στη δημιουργία κοινωνικής και πολιτικής

[92] Βλ., π.χ., Randelzhofer A., *Article 51*, op. cit., 661, 664.
[93] Βλ. και το άρθρο 2 της "Definition of Aggression", G.A. Res. 3314 (XXIX). — Επίσης, ICJ, 'Oil Platforms' case.
[94] Για την εκδήλωση CNAs από μη-κρατικές οντότητες, καθώς και γενικά για το πρόβλημα απόδειξης της προέλευσης των κυβερνοεπιθέσεων, βλ. παρακάτω.
[95] 1981 General Assembly Declaration on Non-Intervention (A/RES/36/103, 09 Dec. 1981).

αναταραχής στο κράτος –στόχο,[96] ή η προσπάθεια επηρεασμού των ψηφοφόρων του κράτους-στόχου με τον 'βομβαρδισμό' τους με χιλιάδες ή εκατομμύρια e-mails κατάλληλου περιεχομένου. Αντίθετα, είναι αρκετά πιο δύσκολο και απαιτητικό να εξακριβωθεί εάν μία CNA μπορεί να αρθεί στο ύψος της χρήσης βίας μεταξύ κρατών, έτσι όπως η έννοια αυτή προσδιορίζεται δογματικά από το *jus ad bellum*.

Εδώ θα πρέπει κατ' αρχάς να παρατηρήσουμε ότι τα χαρακτηριστικά εκείνα που καθιστούν *'όπλο'* ένα αντικείμενο, μία συσκευή ή ένα σύστημα, δεν είναι τα *εκ κατασκευής* ή *κατά προορισμό* χαρακτηριστικά του, ή η *συνήθης* χρήση του, αλλά οι *προθέσεις* και οι *επιδιώξεις* με τις οποίες χρησιμοποιείται και τα *αποτελέσματα* της χρήσεως αυτής. Το ICJ στην Γνωμοδότησή του για τη νομιμότητα της χρήσης πυρηνικών όπλων διευκρίνισε ότι τα άρθρα 2(4), 51 και 42 του Χάρτη δεν αναφέρονται σε συγκεκριμένα όπλα και ότι εφαρμόζονται σε κάθε είδους χρήση βίας, ανεξάρτητα από το χρησιμοποιούμενο όπλο.[97] Έτσι ένα όπλο δεν είναι απαραίτητο να προκαλεί αποτελέσματα μόνο με την πρόκληση έκρηξης ή γενικότερα με τη μεταφορά και απελευθέρωση κινητικής ή χημικής ενέργειας· η χρησιμοποίηση εναντίον ενός κράτους και οργάνων, εργαλείων, αντικειμένων ή παραγόντων 'διπλής χρήσης', στα οποία δεν χρησιμοποιείται καν κινητική ενέργεια, όπως είναι, για παράδειγμα, οι βιολογικοί ή οι χημικοί παράγοντες —ή άλλα αντικείμενα ή μέσα διπλής χρήσεως (dual use), όπως, για παράδειγμα, οι ακτίνες λέιζερ ή οι ηλεκτρομαγνητικοί παλμοί μεγάλης ισχύος—, μπορούν, αναμφίβολα, να συνιστούν και 'χρήση βίας' κατά το άρθρο 2(4), αλλά και 'armed attack' κατά το άρθρο 51 και έτσι έχουν αντιμετωπιστεί μέχρι σήμερα από τη θεωρία και την πρακτική.[98] Το ICJ, εμμέσως πλην σαφώς, αναγνώρισε ότι η χρήση ενός 'όπλου' μη-κινητικής ενέργειας μπορεί να συνιστά παραβίαση του άρθρου 2(4), όταν αξιολόγησε τον εξοπλισμό και την εκπαίδευση των contras από τις Η.Π.Α. ως απειλή ή χρήση βίας κατά της Νικαράγουα (: 'the arming and training of the Contras as a weapon').[99,] Κατά τον *Brownlie* αυτό είναι δυνατό να συμβαίνει επειδή *και* η χρήση τέτοιου είδους μέσων μπορεί να είναι μέθοδος πολέμου, αλλά και επειδή η χρήση τους

[96] Αυτό μπορεί να γίνει άνετα, για παράδειγμα με τη στοχευμένη και συστηματική παραποίηση ιστοσελίδων (websites defacement).
[97] ICJ Rep. 1996, 244 §39. — Έτσι, π.χ., και ο Dinstein, σε Schmitt & O'Donnell eds, vol. 76, σελ. 103.
[98] Για τα πρόσθετα χαρακτηριστικά που απαιτούνται σ' αυτήν την περίπτωση, ώστε να καλυφθεί το 'διάκενό' μεταξύ των άρθρων 2(4) και 51, βλ. παρακάτω.
[99] ICJ Rep. 1986, 118 §228 — Προβλ. και τη Συνθήκη για την απαγόρευση *χρήσης τεχνικών επέμβασης στο περιβάλλον ως μέθοδο πολέμου* ('ENMOD' – Convention on the Prohibition of Military or Any Hostile Use of Environmental Modification Techniques, May 18, 1977, 31 U.S.T. 333, 16 I.L.M. 88 (1977)).

μπορεί να προκαλεί καταστροφή περιουσιών και απώλειες ζωών˙[100] πρόκειται για μία 'εκ του αποτελέσματος' προσέγγιση, σύμφωνη, οπωσδήποτε, με τις επιδιώξεις των συντακτών των άρθρων 2(4) και 51 του Χάρτη.

Το σκεπτικό αυτό μπορεί να υιοθετηθεί και στην περίπτωση των CNAs, αφού από καθαρά νομική σκοπιά *δεν* υπάρχει κανείς λόγος να γίνει διάκριση μεταξύ των όπλων που μεταφέρουν και απελευθερώνουν, για παράδειγμα, κινητική ενέργεια και των όπλων και μεθόδων που δρουν ηλεκτρονικά στον κυβερνοχώρο, δηλαδή των μέσων, μεθόδων και τεχνικών που προκαλούν βλάβες ή θάνατο στο φυσικό /πραγματικό κόσμο, λόγω, ακριβώς, *της ευθείας και σχεδόν απόλυτης, πλέον, εξάρτησης του κόσμου αυτού από τον κυβερνοχώρο*. Η ουσία της νομικής αξιολόγησης που θα γίνει σ' αυτήν την περίπτωση, δεν πρέπει να λάβει υπόψη της το *μέσο* που χρησιμοποιείται, ούτε και το είδος ή το επίπεδο της τεχνολογίας που εφαρμόζεται,[101] αλλά τα *αποτελέσματα* της ενέργειας που εκδηλώνεται κάθε φορά.[102] Η σχετική βιβλιογραφία βρίθει σχετικών παραδειγμάτων, *αρκετές φορές δε η πραγματικότητα ξεπερνά και τη φαντασία*˙ ακολουθούν ορισμένα παραδείγματα,[103] στα οποία εννοείται ότι ο δράστης των επιθέσεων CNA επιθυμεί και επιδιώκει την πρόκληση των συγκεκριμένων αποτελεσμάτων : Με αθέμιτη επέμβαση στα υπολογιστικά συστήματα που ελέγχουν τη λειτουργία ενός πυρηνικού εργοστασίου προκαλείται τήξη του πυρήνα του αντιδραστήρα, ακολουθεί έκρηξη, προκαλούνται εκτεταμένες υλικές ζημίες και απώλεια εκατοντάδων ή και χιλιάδων ζωών.[104] — Αντί να πληγεί με ένα όπλο μακρού βεληνεκούς, ένα εργοστάσιο παραγωγής ηλεκτρικής ενέργειας και το σύστημα

---

[100] Brownlie I., 1963, σελ. 362 /363. Μνημονεύεται και από τον Barkham, σελ. 72, ο οποίος σημειώνει : "Ian Brownlie … expanded the analysis *beyond kinetic impact* and moved toward a *result-oriented approach*. He focused on whether there was a *destruction of life or property*. According to this analysis, there is no difference between an attacker firing a missile at a target or spraying it with poison gas; if an action kills people or destroys property, it is a use of force. …" (η έμφαση δική μας).

[101] Η χρήση μίας πυροβολαρχίας για να προκαλέσει καταστροφές και θανάτους, είναι μία αρκετά παλαιά και τεχνολογικά χαμηλού επιπέδου λύση˙ αντίθετα η κατάλληλη και επί τούτου χρήση μερικών servers για να προκαλέσει παρόμοια καταστροφή (π.χ. την επαναδρομολόγηση δύο συρμών που μεταφέρουν στρατεύματα, ώστε να συγκρουστούν και να προκληθούν θάνατοι και ματαίωση της μεταφοράς δυνάμεων σε συγκεκριμένο σημείο), είναι μία τεχνολογικά προηγμένη και 'εξωτική' λύση με ***ισοδύναμο αποτέλεσμα***.

[102] Dinstein, σε Schmitt & O'Donnell eds, vol. 76, σελ. 103.

[103] Μερικά αναφέρονται, για παράδειγμα, από τον Schmitt, 1999, σελ. 8 και τον Dinstein, ibid, σελ. 105.

[104] Το 2010, ως γνωστόν, το εξαιρετικά προηγμένο 'ηλεκτρονικό σκουλήκι' (worm) με την ονομασία 'Stuxnet' έπληξε ορισμένους η/υ (βιομηχανικού τύπου η/υ της Siemens) του πυρηνικού προγράμματος του Ιράν (στον πυρηνικό σταθμό του Μπουσέρ και τη μονάδα εμπλουτισμού ουρανίου της Νατάνζ), καθυστέρησε το όλο πρόγραμμα και προκάλεσε πλήθος άλλων προβλημάτων. Το πρόβλημα επεκτάθηκε (bleed over effect) σε Ινδονησία και Κίνα, όπου μολύνθηκαν έξι εκατομμύρια η/υ. (Βλ., π.χ., εφημερίδα 'Το Ποντίκι' της 07-10-2010 και το ηλεκτρονικό 'Βήμα' της 24-09-2010.) *Η επιχείρηση αυτή <u>δεν</u> συνιστά CNA, είναι ενδεικτική, ωστόσο, για τις δυνατότητες που προφέρουν πλέον σήμερα οι 'ηλεκτρονικές επιθέσεις'.*

κατανομής φορτίων που το εξυπηρετεί, τίθενται εκτός λειτουργίας με κακόβουλη επέμβαση στα υπολογιστικά συστήματα που τα ελέγχουν, με αποτέλεσμα τη διακοπή παροχής ενέργειας και την πρόκληση ζημιών, τραυματισμών και θανάτων. — Με ηλεκτρονική επέμβαση στους η/υ, τα μηχανολογικά συστήματα ενός φράγματος δυσλειτουργούν και προκαλείται διαφυγή μεγάλων ποσοτήτων νερού, με αποτέλεσμα ζημίες, θανάτους, αλλά και αδυναμία κινητοποίησης δυνάμεων για την αντιμετώπιση, για παράδειγμα, εισβολής στρατιωτικών δυνάμεων από γειτονικό σημείο. — Το σύστημα έγκαιρης προειδοποίησης εναέριων απειλών μίας χώρας τίθεται εκτός λειτουργίας εξαιτίας μίας επίθεσης CNA στα δίκτυα η/υ που το ελέγχουν, με αποτέλεσμα να μην μπορούν να αντιμετωπιστούν οι εναέριες επιθέσεις του αντιπάλου που ακολουθούν μετά από μικρό χρονικό διάστημα. — Όλα τα προηγμένα μαχητικά αεροσκάφη μίας χώρας καθηλώνονται λόγω 'ιού' που χτυπά τους η/υ τους, με αποτέλεσμα να μην μπορέσουν να χρησιμοποιηθούν αμυντικά σε επίθεση που ακολουθεί μετά από μερικές ώρες.[105]

> Κατά τον *Silver*,[106] ένα (εμπειρικό) κριτήριο για να διαπιστώσει κανείς εάν μία νέα τεχνολογία ή μέθοδος συνιστά 'μέθοδο πολέμου', είναι και το εάν η τεχνική χρησιμοποίησης της τεχνολογίας ή της μεθόδου αυτής σχετίζεται με τις ένοπλες δυνάμεις ενός κράτους και όχι απλά, για παράδειγμα, με κάποιες άλλες υπηρεσίες ή φορείς του κράτους αυτού, όπως οι υπηρεσίες (εσωτερικής & εξωτερικής) ασφαλείας.

Δεν μπορεί να αγνοηθεί και το γεγονός ότι οι συντάκτες του Χάρτη ακολούθησαν μία προσέγγιση ρητά προβλεπόμενης, στο κείμενο του Χάρτη, απαγόρευσης[107] (: τη διαπίστωση ύπαρξης force /armed attack), προκειμένου να καθιερώσουν τις συγκεκριμένες απαγορεύσεις που αφορούν τον καταναγκασμό στις μεταξύ των κρατών σχέσεις, διότι δεν μπορούσαν και δεν ήθελαν να περιγράψουν διαφορετικά το προς απαγόρευση πεδίο· απαγόρευσαν τη χρήση *στρατιωτικής βίας*, δηλαδή τη χρήση ενός και μόνο συγκεκριμένου οργάνου ή εργαλείου καταναγκασμού στις διακρατικές σχέσεις και όχι παράλληλα και τη χρήση άλλων 'εργαλείων' καταναγκασμού, όπως είναι ο οικονομικός ή ο πολιτικός καταναγκασμός. Τη

---

[105] Σύμφωνα με δημοσιεύματα του 2009, *αεροσκάφη της γαλλικής πολεμικής αεροπορίας* καθηλώθηκαν στο έδαφος (για δύο ημέρες) επειδή ένα 'ηλεκτρονικό σκουλήκι' (the 'Conficker' worm) προσέβαλε τους η/υ από τους οποίους, στη συνέχεια, θα φορτώνονταν δεδομένα (σχέδια πτήσεων, τρισδιάστατοι χάρτες κ.λπ.) στους η/υ των αεροσκαφών. (Ηλεκτρονική 'Daily Telegraph, 07 Φεβ. 2009.)
[106] Σε Schmitt & O'Donnell eds, vol. 76, σελ. 73 et seq.
[107] "Instrument based approach".

συγκεκριμένη χρονική στιγμή που συντάχθηκε ο Χάρτης και υπό τις τότε συνθήκες, αυτό είχε νόημα διότι οι *συνέπειες* τις οποίες ήθελαν να αποφύγουν τότε τα κράτη (: έναν ακόμη παγκόσμιο πόλεμο ή, έστω, έναν πόλεμο μεγάλου εύρους) προσιδίαζαν ακριβώς σε αυτού του είδους την προσέγγιση. Ωστόσο τα κράτη ενδιαφέρονται πρωτίστως όχι για το *μέσο,* όσο για τις *συνέπειες* και τα *αποτελέσματα* της χρήσης βίας.[108] *Δεν είχαν ως σκοπό την απαγόρευση χρήσης συγκεκριμένων όπλων,* των όπλων που ήταν γνωστά την εποχή που γράφτηκε ο Χάρτης, *αλλά κάθε όπλου.*

Η ιδιαιτερότητα των κυβερνοεπιθέσεων, η οποία συνίσταται στο γεγονός ότι οι επιθέσεις αυτές δεν απαιτούν τη χρήση 'παραδοσιακών' όπλων κινητικής ενέργειας, δεν συνεπάγεται αναγκαστικά ούτε και ασυμβατότητα με τις 'προδιαγραφές' της 'ένοπλης επίθεσης' (armed attack) κατά το *jus ad bellum*. Και στην περίπτωση του άρθρου 51 οι συντάκτες του Χάρτη ακολούθησαν την προσέγγιση μίας ρητά προβλεπόμενης, στο κείμενο του Χάρτη, απαγόρευσης και έκαναν λόγο για 'armed attack', έχοντας κατά νου, στην πραγματικότητα, να δώσουν στα κράτη το δικαίωμα αυτοάμυνας (δηλαδή ένα δικαίωμα που θα αποτελούσε εξαίρεση από τη γενική απαγόρευση χρήσης βίας), όταν το *εύρος* και οι *συνέπειες* της χρήσης βίας ξεπερνούν ένα επίπεδο και αδιαφορώντας επί της ουσίας για το *είδος* του όπλου ή των όπλων και των μεθόδων που θα χρησιμοποιούνται για την πρόκληση των συγκεκριμένων αποτελεσμάτων. Έτσι, η χρήση οποιουδήποτε αντικειμένου, συστήματος, τεχνικής, μεθόδου κ.λπ., που έχει ως αποτέλεσμα την απώλεια ζωών ή /και την πρόσκληση ζημιών που ξεπερνούν ένα συγκεκριμένο 'κατώφλι' βίας (threshold), μπορεί να γίνει δεκτό ότι συνιστά 'ένοπλη επίθεση'.[109] Το συμπέρασμα αυτό σχετικά με τη βαθύτερη 'φύση' και την 'ουσία' της σύνδεσης μίας ενέργειας που μπορεί να χαρακτηριστεί ως 'ένοπλη επίθεση' με τα *αποτελέσματα* της χρήσης ενός 'όπλου' και τους σκοπούς /επιδιώξεις του χρήστη του, είναι κατ' αρχήν συμβατό και με τις σχετικά πρόσφατες Αποφάσεις του Σ.Α. για τις επιθέσεις της 11ης Σεπτεμβρίου 2001,[110] όπου το Συμβούλιο αναγνώρισε στη συγκεκριμένη περίπτωση την ύπαρξη του "…inherent right of individual or collective self-defence in accordance with the Charter", ενώ τα 'όπλα' που χρησιμοποιήθηκαν στις επιθέσεις ήταν κυριευμένα πολιτικά αεροσκάφη.

---

[108] Έτσι και ο Dhillon, σελ. 83.
[109] Βλ. και Zemanek K., *"Armed Attack"*, Max Planck Encyclopedia of Public International Law, 2010, §21.
[110] S/RES/1368(2001) της 12ης Σεπ. 2001 και S/RES/1373/(2001) της 28ης Σεπ. 2001.

2. Η κλίμακα και τα αποτελέσματα της επίθεσης

Όπως έχει ήδη επισημανθεί, όλες οι περιστάσεις χρήσεως 'κυβερνο-βίας' και όλες οι CNAs, δεν θα μπορούν να χαρακτηριστούν ως 'ένοπλη επίθεση'. Το ICJ, στην υπόθεση *Νικαράγουα κατά Η.Π.Α.*, διέκρινε τις περισσότερο βαρείες μορφές χρήσεως βίας, αυτές δηλαδή που μπορούν να συνιστούν 'ένοπλη επίθεση', από τις άλλες, δηλαδή εκείνες που δεν χαρακτηρίζονται από την απαιτούμενη βαρύτητα και άρα μπορεί να συνιστούν απλή χρήση βίας,[111] και υιοθέτησε το κριτήριο της κλίμακας και των αποτελεσμάτων (scale and effects) της επίθεσης για να κάνει την διάκριση.

> (Για παράδειγμα, μία επίθεση CNA η οποία παραλύει το στρατιωτικό σύστημα έγκαιρης προειδοποίησης τρίτου κράτους και τις επικοινωνίες του (ενσύρματες, ασύρματες και δορυφορικές) χωρίς ανθρώπινες απώλειες, με σκοπό τον μη εντοπισμό αναγνωριστικών αεροσκαφών σε αποστολή εντός των συνόρων του αντιπάλου, μπορεί να συνιστά —σαν τέτοια— απλή χρήση βίας.)

Στις επιθέσεις με 'κλασικά' όπλα, το γεγονός ότι οι στόχοι είναι στρατιωτικοί ή μη-στρατιωτικοί ή και των δύο αυτών κατηγοριών, δεν έχει ιδιαίτερη σημασία για τον επί της ουσίας χαρακτηρισμό της επίθεσης (για παράδειγμα, βομβαρδίζονται νοσοκομεία, φράγματα, αεροπορικές βάσεις, βιομηχανικές υποδομές, γέφυρες κ.λπ.). Το αυτό μπορεί να ισχύσει και στην περίπτωση των CNAs, ακόμη και όταν τα συστήματα-στόχοι είναι αποκλειστικά 'πολιτικά' συστήματα, υπό την αυτονόητη προϋπόθεση ότι πληρούται το κριτήριο της 'κλίμακας και των αποτελεσμάτων' της επίθεσης· η προσέγγιση δεν αλλάζει ούτε όταν το μη-στρατιωτικό σύστημα ή εγκατάσταση που πλήττεται ηλεκτρονικά, ανήκει νομικά σε νομικό πρόσωπο με ιθαγένεια τρίτης χώρας, αλλά ούτε και όταν οι εξυπηρετητές (servers) και τμήμα του δικτύου του συστήματος που πλήττεται είναι εγκατεστημένοι σε τρίτη χώρα αλλά παρέχουν τις υπηρεσίες τους στη χώρα-στόχο. *Διαφορετική* θα είναι η προσέγγιση του ζητήματος (οπότε και *δεν* θα υπάρχει δικαίωμα αυτοάμυνας), *μόνον* εάν τα αποτελέσματα που προκαλεί μία κυβερνοεπίθεση στο κράτος ή στους υπηκόους του δεν είναι ηθελημένα,[112] ακριβώς επειδή δεν θα υπάρχει το στοιχείο της επιδίωξης ή του σκοπού πρόκλησης βλάβης από την πλευρά του επιτιθέμενου· ως γνωστόν, κατά το

---

[111] The most grave forms of the use of force vis-à-vis the less grave forms.

[112] Αυτό διότι, όπως θα εξηγηθεί και παρακάτω, πέρα από τη δυσκολία ταχέως και ακριβούς προσδιορισμού των πηγών προέλευσης των κυβερνοεπιθέσεων, είναι πολύ εύκολο και σύνηθες στην πράξη οι κυβερνοεπιθέσεις να πλήττουν μη-ηθελημένα και 'παράπλευρους' ή άσχετους στόχους, δηλαδή να έχουν τα λεγόμενα ***'bleed-over'*** αποτελέσματα.

ICJ, μία ένοπλη επίθεση "…[must be carried out] with the specific intention of harming"[113].

> Και το κριτήριο 'scale & effects' έχει επικριθεί αρκετά, βέβαια, κυρίως επειδή έτσι όπως διατυπώθηκε από το Δικαστήριο είναι "…an encouragement for low-grade terrorism because the state at whom it is directed cannot use force in self-defence…". Και ο δικαστής *Schwebel* στη μειοψηφία του σημείωσε ότι "[t]he Court appears to offer… a prescription for overthrow of weaker governments by predatory governments while denying potential victims what in some cases may be their only hope of survival."[114]

Πρέπει πάντως να επισημανθεί, στο σημείο αυτό, ότι οι CNAs μικρότερης έντασης, οι οποίες, ενώ ξεπερνούν το επίπεδο των CNE δεν προκαλούν εμφανείς και επαρκούς κλίμακας υλικές ζημίες ή /και απώλειες ζωών, δημιουργούν σοβαρό πρόβλημα ερμηνείας στα άρθρα 2(4) και 51˙ πράγματι, μία επίθεση σαν κι' αυτή που έγινε σε βάρος της Εσθονίας,[115] ενώ δεν προκαλεί υλικές ζημίες στον φυσικό κόσμο και θανάτους ή τραυματισμούς που να βρίσκονται σε φαινομενική αντιστοιχία προς τις συνέπειες μίας επίθεσης με ήδη γνωστά όπλα 'χαμηλής' τεχνολογίας, ωστόσο μπορεί να μετατρέψει το χρηματιστηριακό και τραπεζικό σύστημα μίας χώρας, ή τα κέντρα ελέγχου της εναέριας κυκλοφορίας της και τα κέντρα διανομής ηλεκτρικής ενέργειας κ.λπ., *σε ένα σύνολο από κτίρια και ηλεκτρομηχανολογικές υποδομές απλά μη χρησιμοποιήσιμες*, το ισοδύναμο, δηλαδή, του βομβαρδισμού τους με όπλα κινητικής ενέργειας κατόπιν προειδοποιήσεως ώστε να αποφευχθούν ανθρώπινες απώλειες-! Έτσι φαίνεται να θολώνουν οι διαχωριστικές γραμμές μεταξύ της βίας όπως εννοείται στα άρθρα 2(4) και 51 και των άλλων μορφών διακρατικού καταναγκασμού και τείνει να εμφανιστεί μία ενδιάμεση, τρίτη, μορφή εξαναγκασμού, η οποία ενώ δεν προκαλεί σε πρώτο επίπεδο ζημιές στον φυσικό κόσμο και απώλειες ζωών, συγχρόνως φαίνεται να έχει αποτελέσματα που 'θυμίζουν' αποκλεισμό σαν κι αυτόν που αναφέρεται στην Απόφαση 3314 (XXIX) της Γ.Σ. του Ο.Η.Ε. του 1974, ή αποτελέσματα επίθεσης με όπλα κινητικής ενέργειας και τα οποία (αποτελέσματα), σε κάθε περίπτωση, φαίνεται να ξεπερνούν τον οικονομικό και πολιτικό καταναγκασμό όπως τον γνωρίσαμε μέχρι

[113] Oil Platforms case (Iran v. US), ICJ Reports 2003, 161 et seq. (191 §64). (Πρέπει, όμως, εδώ να σημειώσουμε ότι κατά την Gray, 2008 (2009), 146, δεν είναι σαφές εάν το Δικαστήριο ήθελε να προσδιορίσει ένα προαπαιτούμενο της (νόμιμης) αυτοάμυνας των κρατών, ή απλά να περιορίσει την απαίτηση αυτή στη συγκεκριμένη υπόθεση.)
[114] Higgins, σελ. 250 /251.
[115] Με την οποία δεν ασχολήθηκαν τα Η.Ε. και την οποία το NATO έκρινε τόσο χαμηλού κατωφλίου ώστε να μην τεθεί ζήτημα εφαρμογής του άρθρου 5 του δικού του Καταστατικού Χάρτη…

σήμερα.[116] Εδώ η θεωρία του είδους και της βαρύτητας των αποτελεσμάτων δεν βοηθά. Σ' αυτό βέβαια συμβάλλει και το γεγονός ότι συνήθως οι CNAs ξεκινούν ως μία ήπια και χαμηλής έντασης δραστηριότητα και κορυφώνονται σταδιακά και σε βάθος χρόνου, όταν δε γίνει φανερή η πλήρης έκτασή τους και τα εν δυνάμει αποτελέσματά τους, η διείσδυση στα συστήματα – στόχος είναι τόσο βαθεία ώστε, ανεξάρτητα από τις συνέπειες, η άμυνα είναι επίπονη, χρονοβόρα και ενδεχομένως ανέφικτη…

3. Οι αρχές που διέπουν το δικαίωμα αυτοάμυνας και οι CNAs

Από τη γενική θεωρία του διεθνούς δικαίου για τη χρήση βίας, γίνεται δεκτό ότι ακόμη και όταν διαπιστώνεται 'ένοπλη επίθεση', η αυτοάμυνα για να είναι 'νόμιμη', πρέπει να πληροί και τα κριτήρια των αρχών της αναγκαιότητας, της αναλογικότητας και της αμεσότητας (necessity, proportionality και immediacy, αντίστοιχα)· η αρχή της *αμεσότητας* είναι στην πραγματικότητα μία πτυχή της αρχής της αναγκαιότητας. Η αρχή της *αναγκαιότητας* (της αυτοάμυνας) επιβάλλει η χρήση βίας (ως απάντηση στην 'ένοπλη επίθεση') να είναι η τελευταία επιλογή του αμυνόμενου, επειδή όλοι οι άλλοι τρόποι άμυνας έχουν αποτύχει ή είναι εξαιρετικά πιθανό και αναμενόμενο ότι θα αποτύχουν· στις περιπτώσεις των CNAs για να συμβαίνει αυτό θα πρέπει να έχει προσδιοριστεί με ασφάλεια η *πηγή* της επίθεσης (: να μην παραμένουν άλυτα 'attribution problems'), να υπάρχουν αποδείξεις ότι η συγκεκριμένη επίθεση καλύπτεται από την απαιτούμενη πρόθεση, έτσι όπως εκδηλώθηκε, και δεν είναι απλά ένα 'bleed-over effect' και, τέλος, η επίθεση να μην μπορεί να αντιμετωπιστεί αποτελεσματικά και έγκαιρα με άλλους, λιγότερο επιθετικούς, τρόπους (αποτελεσματική ηλεκτρονική άμυνα, προσωρινή —και χωρίς περαιτέρω επιβλαβείς συνέπειες— διακοπή των διαύλων του internet, μεταφορά των υποδομών σε άλλους servers σε τρίτη χώρα[117] κ.λπ.). Το σοβαρότερο πρόβλημα εδώ θα είναι η σύνδεση των ηλεκτρονικών επιθέσεων με συγκεκριμένο κράτος ή η απόδοσή τους σε συγκεκριμένο κράτος, αφού *οι μέθοδοι απόκρυψης των ηλεκτρονικών ιχνών και των διαδρομών της επίθεσης είναι εξαιρετικά εξελιγμένες και πολύπλοκες και η*

[116] Βλ. και τον Barkham, 112, ο οποίος αναφέρει χαρακτηριστικά : "[i]f the kinetic impact of an attack is not relevant, the resulting damage may be the same whether the victim suffers a missile attack or economic sanctions."

[117] Αυτό το μέτρο, μεταξύ άλλων, αναγκάστηκε να λάβει η Εσθονία, στην προσπάθειά της να αντιμετωπίσει τις επιθέσεις του Απριλίου /Μαΐου 2007 εναντίον της.

αποκάλυψή τους δύσκολη και χρονοβόρα.[118] Μία 'ανάλογη' απάντηση με CNA μπορεί να μην είναι εφικτή είτε επειδή το κράτος-στόχος δεν διαθέτει την τεχνολογική υποδομή να την πραγματοποιήσει, είτε επειδή το κράτος που πραγματοποίησε την επίθεση ή ευθύνεται άμεσα γι' αυτήν δεν έχει αναπτυγμένα δίκτυα και άρα δεν μπορεί να πληγεί ουσιαστικά με τέτοιου είδους όπλα /επιθέσεις.

Το κράτος-στόχος μπορεί να αντιδράσει διακόπτοντας τις επικοινωνίες του με τον υπόλοιπο κόσμο μέσω του διαδικτύου˙ αυτό, ωστόσο, ίσως είναι δυσανάλογα επιβλαβές για το ίδιο και μπορεί να προκαλέσει και περαιτέρω επιπλοκές και ως εκ τούτου θα συνιστά μία αντίδραση που δεν μπορούν οι τρίτοι να απαιτήσουν και να αναμένουν και μάλιστα ως 'αναλογική' απάντηση. Αναλογική απάντηση, λαμβανομένων υπόψη των περιστάσεων, θα μπορούσε να είναι η άμεση χρήση λογισμικού anti-virus ή άλλου λογισμικού θωράκισης των δικτύων που πλήττονται, ή η μεταφορά των δικτυακών υποδομών που πλήττονται σε τρίτο κράτος (δημιουργία mirrored sites κ.λπ.), αν και η τελευταία αυτή λύση, πέρα από χρονοβόρα ίσως είναι επίσης εξαιρετικά επιβλαβής για το πληττόμενο κράτος. Τέλος, ο 'αμυνόμενος' μπορεί να επιχειρήσει να διακόψει τις δικτυακές επικοινωνίες του μόνον με τον 'επιτιθέμενο', αν και αυτό σε σπάνιες περιπτώσεις θα είναι επαρκές, αφού οι επιτιθέμενοι σχεδόν πάντα εκδηλώνουν τις επιθέσεις τους μέσω των δικτύων πλήθους *τρίτων* κρατών, παροχετεύοντάς τις κατάλληλα και αποκρύπτοντας την πραγματική τους προέλευση.[119]

Τέλος, η αρχή της *αμεσότητας* πηγάζει από το σκοπό της αυτοάμυνας, ο οποίος συνίσταται στην απόκρουση και τη διακοπή της επίθεσης και όχι στην τιμωρία του υπευθύνου. Λόγω της βαθύτερης φύσης και των τεχνικών χαρακτηριστικών των CNAs (: ο εντοπισμός των ηλεκτρονικών ιχνών και της πορείας τους απαιτεί χρόνο, τα αποτελέσματα της επίθεσης μπορεί να φανούν μετά από κάποιο χρονικό διάστημα, ο επιτιθέμενος μπορεί να έχει χρησιμοποιήσει 'λογικές' βόμβες ή κακόβουλο λογισμικό που λειτουργεί με χρονο-καθυστέρηση (time bombs)), η αρχή αυτή πρέπει να γίνει

[118] Για το λόγο αυτό ορισμένοι μελετητές προτείνουν να γίνει δεκτό ότι επιτρέπεται η άμεση απάντηση σε κυβερνο-επιθέσεις εναντίων των κρισίμων υποδομών μίας χώρας, έστω και εάν δεν είναι σαφές ποιος είναι ακριβώς ο επιτιθέμενος (βλ. Roscini, σελ. 119 και σημ. 157). Αυτό, φυσικά, δεν μπορεί να γίνει αποδεκτό, τόσο επειδή αντίκειται σε βασικές αρχές του δικαίου της διεθνούς ευθύνης των κρατών, όσο και επειδή, ούτως ή άλλως, οι έννοιες των 'κρισίμων υποδομών' και της 'εθνικής ασφάλειας' του κράτους που υποτίθεται ότι πλήττεται, είναι εξίσου δύσκολα προσδιορίσιμες και η συζήτηση γι' αυτές είναι ακόμη ανοικτή. Με τη λογική αυτή, όπως παρατηρεί και ο *Roscini* (ibid), θα μπορούσε να υποστηριχθεί ότι είναι επιτρεπτή και η εκδήλωση ενεργούς αυτοάμυνας στις περιπτώσεις τρομοκρατικών επιθέσεων με συμβατικά όπλα, πριν ακόμη συνδεθεί με συγκεκριμένο κράτος η ομάδα που εκτέλεσε την επίθεση, συμπέρασμα που οδηγεί σε παράλογες λύσεις…

[119] Todd, σε USAF Law Review, vol. 64, 105.

δεκτό ότι εφαρμόζεται εδώ με περισσότερο *ελαστικό* τρόπο (αρκεί, βεβαίως, να γίνει άμεσα η επίκληση του δικαιώματος άμυνας όταν οι περιστάσεις δεν επιτρέπουν την άμεση ανάληψη δράσης).

> Για τις κυβερνο-επιθέσεις που δεν προκαλούν με άμεσο και προφανή τρόπο φυσικές ζημίες σε αντικείμενα ή απώλειες ζωών και την διάκρισή τους από τις απλές μορφές καταναγκασμού στις διακρατικές σχέσεις (αυτές, δηλαδή, που δεν μπορούν να αρθούν μέχρι του επιπέδου της 'χρήσης βίας'), ο καθηγητής *Michael Schmitt* έχει προτείνει ήδη από το 1999 την υιοθέτηση και την συνακόλουθη αξιολόγηση σε κάθε περίπτωση, *επτά κριτηρίων*.[120, 121] Τα κριτήρια αυτά είναι τα ακόλουθα : (α) Η δριμύτητα /σφοδρότητα (severity) της επίθεσης (: πρόκληση φυσικών ζημιών και απωλειών ζωών, κλίμακα και εύρος των αποτελεσμάτων, σε σχέση και με τις κρίσιμες εθνικές υποδομές κ.λπ.)˙ κατά τον *Schmitt* ο παράγοντας 'severity' είναι ο σημαντικότερος στην ανάλυσή του. (β) Χρονική αμεσότητα (immediacy) μεταξύ της επίθεσης και των αποτελεσμάτων (: τα κράτη είναι λιγότερο πιθανό να χαρακτηρίσουν ως 'use of force' μία CNA που προκαλεί αργά και σταδιακά τα όποια αποτελέσματά της). (γ) Αιτιακή αμεσότητα (directness) μεταξύ επίθεσης και αποτελεσμάτων (: εάν η ηλεκτρονική επίθεση προκαλεί αποτελέσματα με έμμεσο τρόπο, θα είναι λιγότερο πιθανό να χαρακτηριστεί ως χρήση βίας). (δ) Διεισδυτικότητα της επίθεσης (invasiveness), σε σχέση με τις ηλεκτρονικές άμυνες του κράτους–στόχου. (ε) 'Μετρησιμότητα' (measurability) των ποσοτικών αποτελεσμάτων της επίθεσης (: όσο περισσότερο αισθητά και δεκτικά συγκεκριμένης αποτίμησης είναι τα αποτελέσματα, τόσο πιο πιθανό είναι να συνιστούν και χρήση βίας). (στ) Έλλειψη κατ' αρχήν νομιμότητας (ή έστω νομιμοφάνειας) (presumptive legitimacy) της επίθεσης (: με δεδομένο ότι στο διεθνές δίκαιο (όπως και στο δίκαιο γενικότερα) ό,τι δεν απαγορεύεται ρητά, επιτρέπεται˙ έτσι, για παράδειγμα, οι επιχειρήσεις διαδικτυακής προπαγάνδας, ή η 'κυβερνο-κατασκοπεία', δεν θα μπορούσαν ποτέ να συνιστούν 'χρήση βίας'). (ζ) Κρατική ευθύνη (responsibility) για την επίθεση (όσο περισσότερο στενός είναι ο αιτιώδης σύνδεσμος μεταξύ μίας CNA και ενός κράτους (είτε επειδή την διεξάγουν απευθείας κρατικά όργανα ή υπηρεσίες, είτε επειδή την διεξάγουν, π.χ., μη-κρατικές οντότητες για λογαριασμό του κράτους), τόσο περισσότερο πιθανό είναι η συγκεκριμένη επίθεση να χαρακτηριστεί ως χρήση βίας στις διακρατικές σχέσεις). Τα κριτήρια αυτά γίνονται αποδεκτά και χρησιμοποιούνται εκτεταμένα

[120] Schmitt, 1999, 914 et seq. Τα κριτήρια αυτά παραθέτει ο ίδιος και σε άρθρο του τού έτους 2010 (Schmitt, 2010).

[121] Κατά τον ίδιο (ibid, 2010) τα κριτήρια αυτά "…would likely influence assessments by States as to whether particular cyber operations amounted to a use of force."

από επιχειρησιακούς αξιωματικούς και αναλυτές,[122] σε διάφορα μοντέλα προσομοίωσης, στα πλαίσια ασκήσεων κυβερνοπολέμου κ.λπ., ιδίως τις Η.Π.Α.· *ωστόσο αρκετοί θεωρητικοί και μελετητές του διεθνούς δικαίου τα αντιμετωπίζουν με ιδιαίτερο σκεπτικισμό και επιφυλακτικότητα.*[123]

4. Προσβολή των κρίσιμων (μη-στρατιωτικών) υποδομών ενός κράτους, συμπεριλαμβανομένων και αυτών που δεν αποτελούν κρατική ιδιοκτησία

Το επόμενο ερώτημα που πρέπει να απαντηθεί είναι, βεβαίως, το εάν μπορεί να συνιστά χρήση βίας ή/και 'ένοπλη επίθεση', η επίθεση στα δίκτυα η/υ που ελέγχουν τις υποδομές μη-στρατιωτικής φύσεως (civilian infrastructure) των κρατών.

Τα υπολογιστικά συστήματα που ελέγχουν τις υποδομές 'κοινής ωφελείας' και άλλες παρόμοιες υποδομές (: παραγωγή και διανομή ηλεκτρικού ρεύματος, διανομή πόσιμου νερού, ενσύρματα και ασύρματα δίκτυα επικοινωνιών, δορυφορικά συστήματα, έλεγχος εναέριας κυκλοφορίας, διαχείριση κυκλοφορίας οχημάτων, πυρηνικά εργοστάσια, τραπεζικά και χρηματιστηριακά δίκτυα, δίκτυα υπουργείων και υπηρεσιών κ.λπ.), αναφέρονται διεθνώς ως SCADA (: **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition systems).[124]

Το παραπάνω ερώτημα θέτει και το ζήτημα του προσδιορισμού των 'κρίσιμων υποδομών' (critical infrastructure) κάθε κράτους, δηλαδή των υποδομών οι οποίες εάν στοχοποιηθούν, εκτίθεται σε κίνδυνο η ασφάλεια και η επιβιωσιμότητα του ιδίου του κράτους. Στο σύγχρονο και εξαιρετικά 'ηλεκτρονικό' περιβάλλον στο οποίο ζούμε, το πρόβλημα μπορεί να αποκτήσει εξαιρετική πολυπλοκότητα· ο *Roscini* (σελ. 117 και σημ. 144) αναφέρει χαρακτηριστικά ότι στην εφημερίδα *"The Guardian"* (19 Ιαν. 2010, σελ. 32), διατυπώθηκε ο ισχυρισμός ότι αφού το *Google* είναι μία από τις πιο ισχυρές και εκτεταμένες παρουσίες στο internet, μία 'επίθεση' εναντίον του συνιστά επίθεση εναντίον των κρισίμων υποδομών των Η.Π.Α.-! Η Γ.Σ. του Ο.Η.Ε. αναγνωρίζει

---

122 Βλ., για παράδειγμα, στα πρακτικά του 27th Annual International Computer Software and Applications Conference, IEEE, Dallas, Texas, Nov. 2003, *"Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System"*. — Τα κριτήρια αυτά αποδέχεται κατ' αρχήν και η *Διεύθυνση Κυβερνοάμυνας του* (ελληνικού) *ΓΕΕΘΑ* (για την οποία βλ. παρακάτω), με καθαρά επιχειρησιακή και όχι νομική λογική, ωστόσο.

123 Βλ., π.χ., την κριτική του Roscini, σελ. 108 και σημ. 104 και του Silver, σε Schmitt & O'Donnell eds, σελ. 89 et seq. Ο Barkham, επίσης, θεωρεί τα 'κριτήρια Schmitt' ανεπαρκή και επειδή, μεταξύ άλλων, δεν μπορούν να συλλάβουν τις ηλεκτρονικές επιθέσεις χαμηλότερης έντασης.

124 Σε πείραμα που διεξήχθη το 2007 στις Η.Π.Α. (the Aurora Generator Test) και το οποίο αναφέρεται πολύ συχνά στη συναφή βιβλιογραφία, με κατάλληλο hacking στο λογισμικό SCADA ενός εργοστασίου παραγωγής ηλεκτρικού ρεύματος, μία βιομηχανική τουρμπίνα υπερθερμάνθηκε και τελικά καταστράφηκε ολοσχερώς (Schaap, vol. 64, σελ. 147).

ότι κάθε κράτος θα πρέπει να προσδιορίσει το ίδιο τις δικές του κρίσιμες πληροφοριακές υποδομές,[125] και αυτό έχουν κάνει ήδη αρκετά κράτη, αλλά και η ΕΕ.[126] Ο προσδιορισμός των κρίσιμων υποδομών των κρατών περιπλέκεται από το γεγονός ότι στις περισσότερες περιπτώσεις, η πλειοψηφία των κρισίμων υποδομών ανήκει στον ιδιωτικό τομέα και μάλιστα σε νομικά πρόσωπα με έδρα τρίτες χώρες ή νομικά πρόσωπα που ελέγχονται από νομικά πρόσωπα με έδρα τρίτες χώρες.

Εν τέλει το ζήτημα των κρισίμων υποδομών συνδέεται με την έννοια της 'εθνικής ασφάλειας' και της επιβίωσης του κράτους —και άρα η απάντηση στο παραπάνω ερώτημα θα είναι *θετική* εφόσον πληρούνται και οι ήδη αναφερθείσες προϋποθέσεις. Βέβαια, η 'εθνική ασφάλεια' είναι έννοια επίσης δύσκολα προσδιορίσιμη, τόσο στο πεδίο των εθνικών νομοθεσιών, όσο και στο πεδίο του διεθνούς δίκαιου˙ πάντως τόσο τα όργανα των διαφόρων Διεθνών Οργανισμών όσο και τα Διεθνή Δικαστήρια, όταν απαιτείται να κρίνουν περιπτώσεις απειλών κατά της εθνικής ασφάλειας των κρατών εφαρμόζουν αρκετά ελαστικά κριτήρια και επιδεικνύουν μάλλον 'ευρύτητα σκέψης'.

5. Η δυσκολία εξεύρεσης της πραγματικής πηγής της ηλεκτρονικής επίθεσης. —Οι επιθέσεις από μη-κρατικές οντότητες

Ένα πρόβλημα που πηγάζει από την ίδια τη φύση των κυβερνο-επιθέσεων και του κυβερνοχώρου από τον οποίο προέρχονται και στον οποίο εκδηλώνονται, είναι η μεγάλη δυσκολία ταυτοποίησης της *πηγής* προέλευσής τους και άρα η πλήρης ανωνυμία των επιτιθέμενων, η οποία επιτυγχάνεται σχετικά εύκολα με ένα πλήθος μεθόδων και τεχνολογιών υλισμικού και λογισμικού, όπως είναι η χρήση εκτεταμένων

[125] Για παράδειγμα, A/RES/58/1999 της 23ης Δεκ. 2003, σε Roscini, ibid, 117.

[126] Βλ., π.χ., Roscini, σελ. 117. — Στην Ε.Ε. έχει εκδοθεί η **Οδηγία 2008/114/ΕΚ** του Συμβουλίου της 8ης Δεκεμβρίου 2008 *''σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους''* (Επίσημη Εφημερίδα της Ε.Ε., L 345/75, 23.12.2008). Με βάση την Οδηγία αυτή (την οποία η χώρα μας ακόμη δεν έχει εφαρμόσει), κάθε κράτος – μέλος πρέπει να ορίσει τις δικές του κρίσιμες υποδομές οι οποίες είναι συγχρόνως και ευρωπαϊκές υποδομές ζωτικής σημασίας (ΕΥΖΣ), ως 'ΕΥΖΣ' δε νοούνται ''οι υποδομές ζωτικής σημασίας που βρίσκονται εντός των κρατών μελών και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο σε δύο τουλάχιστον κράτη μέλη. Η σπουδαιότητα των επιπτώσεων εκτιμάται βάσει οριζόντιων κριτηρίων…''. Κατά τα λοιπά στη χώρα μας δεν έχει θεσμοθετηθεί μέχρι σήμερα επίσημα ο,τιδήποτε για τις 'κρίσιμες υποδομές'. Το 2008, ωστόσο, με πρωτοβουλία της 'Κοινωνίας της Πληροφορίας Α.Ε., e-Government Forum', εκπονήθηκε και παραδόθηκε μελέτη με θέμα *''Προστασία Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης: Στρατηγικός Σχεδιασμός''*, με εισηγητή τον Αναπληρωτή Καθηγητή του Οικονομικού Πανεπιστημίου Αθηνών, Τμ. Πληροφορικής, Δημήτρη Γκρίτζαλη (διατέθηκε από τον εισηγητή στον γράφοντα, σε μορφή αρχείου pdf).

botnets, η χρήση της τεχνικής των παραπλανητικών διευθύνσεων internet (IP spoofing), η χρήση ειδικού λογισμικού κ.λπ. *Ακόμη και όταν φαίνεται ότι οι επιθέσεις προέρχονται από υπολογιστές που βρίσκονται σε συγκεκριμένη χώρα, αυτό δεν σημαίνει αναγκαστικά ούτε ότι πράγματι η επίθεση προέρχεται από αυτούς τους υπολογιστές, ούτε ότι οι ιδιοκτήτες ή οι κάτοχοι των συγκεκριμένων η/υ οργάνωσαν, πραγματοποίησαν ή συμμετείχαν στις επιθέσεις ή ότι τις αποδέχονται.* Σε αρκετές περιπτώσεις η ταυτοποίηση εάν δεν είναι ουσιαστικά αδύνατη, θα είναι εξαιρετικά χρονοβόρα.

> Για παράδειγμα, στις επιθέσεις του 2007 κατά της Εσθονίας χρησιμοποιήθηκαν εκατοντάδες χιλιάδες υπολογιστές που βρίσκονταν στις Η.Π.Α., την Αίγυπτο, το Περού, τη Ρωσική Ομοσπονδία και… την ίδια την Εσθονία(!),[127] χωρίς οι κάτοχοι των η/υ να γνωρίζουν τίποτε στη συντριπτική πλειοψηφία των περιπτώσεων.

Ακόμη και όταν προσδιοριστεί ο επιτιθέμενος, ανακύπτει το ζήτημα εάν οι πράξεις του μπορούν να αποδοθούν σε συγκεκριμένο κράτος, με βάση τους κανόνες περί ευθύνης των κρατών, αφού σε αντίθεση με ό,τι αποτελεί τον κανόνα στις επιθέσεις με συμβατικά όπλα και με τη χρήση συμβατικών μεθόδων, *οι κυβερνο-επιθέσεις μπορούν να οργανωθούν και να εκτελεστούν σχετικά εύκολα και από μικρές ομάδες 'ιδιωτών' ή ακόμη και από μεμονωμένα άτομα*,[128] αρκεί αυτοί να διαθέτουν σύνδεση στο διαδίκτυο, το κατάλληλο λογισμικό και ελάχιστους οικονομικούς πόρους.[129] Η απλούστερη περίπτωση είναι, όπως είναι αυτονόητο, να υπάρχει δυνατότητα απόδοσης των επιθέσεων στα όργανα συγκεκριμένου κράτους, ιδίως σε μέλη των ενόπλων δυνάμεων ή των κρατικών υπηρεσιών ασφαλείας ('uniformed hackers', όπως αναφέρονται στην πράξη), ή στα όργανα νομικών προσώπων ή άλλων οντοτήτων που ασκούν κατά παραχώρηση κάποιας μορφής κρατική λειτουργία ή συνδέονται άμεσα ή έμμεσα με το κράτος. Αν και οι λεπτομέρειες είναι διαβαθμισμένες, υπάρχουν ασφαλείς πληροφορίες ότι αρκετές χώρες μέχρι σήμερα έχουν συγκροτήσει *ειδικές* μονάδες κυβερνο-πολέμου (cyber units), έχουν αναπτύξει σχετική υλική και επιτελική υποδομή

---

[127] Ως τμήμα, και αυτοί, του τεράστιου botnet που δημιούργησαν οι επιτιθέμενοι.

[128] Υπολογίζεται αυτή τη στιγμή ότι δυνατότητα εκδήλωσης 'κυβερνοεπιθέσεων' έχουν πάνω από 120 κράτη παγκοσμίως και… *εκατομμύρια* ιδιωτών-! Ως μέτρο σύγκρισης αναφέρεται ότι μόνον 30 κράτη διαθέτουν διαστημική τεχνολογία.

[129] Για παράδειγμα, εκτιμάται ότι οι επιθέσεις οι οποίες το 2007 ουσιαστικά απέκοψαν την Εσθονία από τον υπόλοιπο κόσμο για δύο εβδομάδες, από πλευράς χρήσης του διαδικτύου, των διακομιστών, του κατάλληλου λογισμού κ.λπ., στοίχισαν κάτι περισσότερο από μόλις… 100.000 δολάρια-!

και διαθέτουν αξιόλογη ικανότητα και σημαντικές δυνατότητες εκδήλωσης CNAs·[130] στις χώρες αυτές περιλαμβάνονται ιδίως η Κίνα, οι Η.Π.Α., το Ισραήλ, το Ηνωμένο Βασίλειο, η Γερμανία, η Γαλλία, η Τουρκία, η Ρωσική Ομοσπονδία και η Αυστραλία.[131] Οι πράξεις των οργάνων αυτών θα μπορούν να αποδοθούν στο κράτος "… provided the person or entity is acting in that capacity in the particular instance".[132]

Ο επιτιθέμενος μπορεί, βέβαια, να είναι *de facto* (κατ' αντιδιαστολή προς το *de jure*) όργανο συγκεκριμένου κράτους. Κατά το άρθρο 8 των ILC Articles "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct". Στην απόφασή του στην υπόθεση *Νικαράγουα κατά Η.Π.Α.*, το ICJ, προκειμένου να δεχθεί απόδοση των πράξεων των contras στο κράτος των Η.Π.Α., απαίτησε την ύπαρξη 'πραγματικού /ενεργού ελέγχου' (effective control) των επιχειρήσεών τους από το κράτος των Η.Π.Α.·[133] για 'πραγματικό /ενεργό έλεγχο' έκανε λόγο το έτος 2007 και στην απόφασή του στην υπόθεση της γενοκτονίας στα Βαλκάνια,[134] όπου και σημείωσε ότι πρέπει να αποδειχθεί ότι "… this 'effective control' was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally on the overall actions taken by the persons or groups of persons having committed violations" και παράλληλα ότι οι κανόνες για την απόδοση διεθνούς ευθύνης στο κράτος δεν μεταβάλλονται ανάλογα με το είδος της 'παράνομης' ενέργειας, ελλείψει ειδικού κανόνα δικαίου περί αυτού.[135] Βέβαια το Εφετειακό Τμήμα του ICTY στην *υπόθεση Tadić*,[136] αφού παρατήρησε ότι, κατά την άποψή του, στην κρίση της κάθε περίπτωσης διεθνώς παράνομης πράξης "… [t]he degree of control may … vary according to the factual circumstances of each case", χρησιμοποίησε ένα *ευρύτερο* κριτήριο για να κρίνει το ενδεχόμενος της απόδοσης σε τρίτο κράτος της ευθύνης των πράξεων των στρατιωτικά οργανωμένων ένοπλων ομάδων, όταν έκανε λόγο για 'γενικό έλεγχο' (overall control)· κατά το ICTY για την

[130] Περί αυτών βλ. και παρακάτω, στην παράγρ. 8 του τμήματος αυτού.
[131] Οι χώρες αυτές διαθέτουν, όπως είναι φυσικό, και αξιόλογες δυνατότητες κυβερνο-άμυνας. — Για την Ελλάδα και τη Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του ΓΕΕΘΑ, θα γίνει περιορισμένη αναφορά παρακάτω στην παράγρ. 8 του τμήματος αυτού.
[132] ILC Articles on State Responsibility, art. 5.
[133] *Nicaragua v. United States*, ICJ Reports 1986, 14 et seq. (64 §115).
[134] *Bosnia & Herzegovina v. Serbia & Montenegro*, Merits, Judgment of Feb. 26, 2007, §400 (Application of the Convention on the Prevention and Punishment of the Crime of Genocide).
[135] B. & H. v. S. & M., ibid, para 401.
[136] Prossecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber, Judgement of July 15, 1999, §117.

απόδοση των πράξεων τέτοιων ομάδων στο κράτος, αρκεί ότι το κράτος "… has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group … regardless of any specific instructions by the controlling State concerning the commission of each of those acts". Το κριτήριο αυτό σαφώς *χαμηλώνει* το 'κατώφλι' του απαιτούμενο ελέγχου.

Στην περίπτωση των CNAs που εκδηλώνονται από μεμονωμένα άτομα ή από μη-κρατικές οντότητες, *η εφαρμογή του κριτηρίου του 'πραγματικού ελέγχου' είναι ασφαλέστερη και προτιμητέα*, ακριβώς επειδή οι αποδεικτικές δυσκολίες ανίχνευσης της *πραγματικής* ηλεκτρονικής *πορείας* των επιθέσεων, του τόπου ή των τόπων *προέλευσης* και των *προσώπων* που τις εκτελούν, απαιτεί υψηλότερα επίπεδα κριτηρίων ελέγχου για λόγους αποδεικτικής βεβαιότητας, ιδίως στις περιπτώσεις κατά τις οποίες το κράτος-στόχος θεωρεί ότι η επίθεση είναι δεκτική αυτοάμυνας.[137] Τυχόν αντίθετη προσέγγιση δεν θα είναι συμβατή και με το γεγονός ότι το ICTY εφαρμόζει το κριτήριο του 'overall control' μόνο στις περιπτώσεις *οργανωμένων και ιεραρχικά δομημένων ομάδων*, όπως είναι οι στρατιωτικές /παραστρατιωτικές μονάδες, ή στις περιπτώσεις των ένοπλων οργανωμένων ομάδων ατάκτων ή ανταρτών·[138] με τα στοιχεία που είναι προς το παρόν διαθέσιμα, καμία από τις ανιχνευθείσες μέχρι σήμερα κυβερνο-επιθέσεις (άσχετα από το εάν αυτές έχουν ξεπεράσει το κατώφλι της χρήσεως βίας ή όχι) δεν φαίνεται να έχει προέλθει από μη-κρατική οντότητα με τέτοιου είδους οργάνωση ή έστω με οργάνωση που δεν θα μπορούσε να χαρακτηριστεί 'χαλαρή'.[139] Για περιπτώσεις μεμονωμένων ατόμων που εκτελούν για λογαριασμό τρίτου κράτους συγκεκριμένες παράνομες πράξεις στο έδαφος άλλου κράτους, αλλά και για τις περιπτώσεις ομάδων που δεν είναι στρατιωτικά οργανωμένες και ιεραρχικά δομημένες, και το ίδιο το ICTY χρησιμοποιεί το κριτήριο του 'πραγματικού ελέγχου', δηλαδή απαιτεί την ύπαρξη συγκεκριμένων οδηγιών από την πλευρά του 'υπόπτου' κράτους για

[137] Έτσι ο Roscini, σελ. 100. Διαφορετικά ο Shackelford, 234.
[138] Υπόθεση Tadić, §120.
[139] Έχει αναφερθεί, βέβαια, ότι ορισμένες ένοπλες και ιεραρχικά δομημένες ομάδες, όπως η Hamas ή η Hesbollah, πιθανόν να έχουν αναθέσει επ' αμοιβή την εκδήλωση κυβερνο-επιθέσεων σε άτομα ή ομάδες με την κατάλληλη τεχνογνωσία (Roscini, σημ. 70). Σε μια τέτοια περίπτωση οι πράξεις των συγκεκριμένων 'cyber-hackers' είναι πράξεις της ομάδας που τους προσέλαβε. — Εάν για μία 'κυβερνο-επίθεση' υπάρχουν στοιχεία ή βάσιμες υπόνοιες ότι αυτή οργανώθηκε και εκτελέστηκε από τις ένοπλες δυνάμεις ή της ειδικές υπηρεσίες συγκεκριμένου κράτους, τότε έχουμε να κάνουμε με τη δράση *de jure* κρατικών οργάνων και τα πράγματα είναι επί της αρχής απλά.

την εκτέλεση της παράνομης πράξης, ή την αναδρομική έγκριση των πράξεων στις οποίες προέβη ο μεμονωμένος ιδιώτης ή μία ομάδα.[140]

Συχνά στο χώρο του διαδικτύου, επ' ευκαιρία διαφόρων γεγονότων με έντονη πολιτική χροιά, εμφανίζονται *προτροπές* και συστηματική *υποκίνηση*[141] προς οιονδήποτε θέλει και μπορεί να εκδηλώσει 'ηλεκτρονικές επιθέσεις' εναντίον κρατών, οργανισμών, μεγάλων εταιρειών κ.λπ.

> Αυτό συνέβη, για παράδειγμα το 2001, μετά το επεισόδιο της σύγκρουσης ενός κατασκοπευτικού αεροσκάφους των Η.Π.Α. με κινεζικό μαχητικό στη νότια Κινεζική Θάλασσα, οπότε και εμφανίστηκαν στο διαδίκτυο αρκετές ιστοσελίδες οι οποίες παρείχαν οδηγίες για hacking σε βάρος των δικτύων η/υ των Η.Π.Α.·[142] τα ίδια επαναλήφθηκαν, για παράδειγμα, στα πλαίσια της αντιπαράθεσης της Γεωργίας με τη Ρωσική Ομοσπονδία για το ζήτημα της Ν. Οσετίας το 2008, οπότε σε αρκετές ιστοσελίδες, σε blogs και forums εμφανίστηκαν προτροπές και οδηγίες για τον κατακλυσμό ('ping-flood' στη γλώσσα του κυβερνοχώρου) και αχρήστευση των επίσημων ιστοσελίδων της κυβέρνησης της Γεωργίας, καθώς και λίστες με ευάλωτες κυβερνητικές ιστοσελίδες της χώρας αυτής.[143]

Τα πρόσωπα που διενεργούν τις ηλεκτρονικές επιθέσεις σε περιπτώσεις σαν τις παραπάνω, δεν μπορούν να χαρακτηριστούν *de jure* ή *de facto* κρατικά όργανα. Εάν αποδειχθεί ότι η υποκίνηση αυτή γίνεται από όργανα ή υπηρεσίες συγκεκριμένου κράτους —και με δεδομένο ότι στα άρθρα για την ευθύνη των κρατών της ILC, τα οποία εν πολλοίς αποτυπώνουν κανόνες διεθνούς εθιμικού δικαίου, δεν ρυθμίζονται ειδικά τα περί υποκίνησης[144]—, κρατική ευθύνη θα ανακύψει μόνον εάν, και στο μέτρο που, η υποκίνηση είναι τέτοια κατά περιεχόμενο, τρόπο και κλίμακα, που ισοδυναμεί με κατεύθυνση και έλεγχο των ιδιωτών ή των ομάδων που παρακινήθηκαν, τελικά, σε

---

[140] Υπόθεση Tadić, ibid, §118.

[141] Με τη δημιουργία ειδικών ιστοσελίδων που παρέχουν λεπτομερείς οδηγίες, με την αποστολή χιλιάδων e-mails, με τη συντήρηση συζητήσεων στα chat-rooms κ.λπ.

[142] Weisbord, σελ. 20 —πολλές τέτοιες επιθέσεις πράγματι εκδηλώθηκαν και ο συγγραφέας αυτός αναφέρει ότι σύμφωνα με αξιωματούχους των Η.Π.Α., οι επιθέσεις αυτές *σχεδόν διέκοψαν την παροχή ηλεκτρικού ρεύματος στην πολιτεία της Καλιφόρνια*-!

[143] Πρόσφατα, εξαιτίας της σύλληψης του ιδρυτή της ιστοσελίδας 'wikileaks', ***Τζούλιαν Ασάνζ***, στο Ηνωμ. Βασίλειο, εκδηλώθηκαν ηλεκτρονικές επιθέσεις μεγάλου εύρους από αριθμό hackers από διάφορες χώρες, εναντίον των δικτύων μίας μεγάλης τράπεζας των Η.Π.Α. και μίας εταιρείας που διαθέτει στην αγορά γνωστή πιστωτική κάρτα, επειδή αμφότερες διέκοψαν τις οικονομικές συναλλαγές του Ασάνζ και δέσμευσαν τους λογαριασμούς του. Και οι δύο εταιρείες αντιμετώπισαν σοβαρά προβλήματα λειτουργίας, τα οποία έφθασαν μέχρι τη διακοπή εργασιών, για αρκετές ημέρες.

[144] Η *υποκίνηση* (incitement) σε πράξη ή παράλειψη, είναι *per se* παράνομη πράξη όπου αυτό προβλέπεται *ειδικά*, όπως για παράδειγμα στο άρθρο ΙΙΙ της Σύμβασης του 1948 για την απαγόρευση κ.λπ. της Γενοκτονίας.

επιθέσεις (άρθρο 8 του σχεδίου της ILC). Κρατική ευθύνη θα υπάρχει και στην περίπτωση που το κράτος εκ των υστέρων επιδοκιμάσει δημόσια τις ηλεκτρονικές επιθέσεις των 'παρακινηθέντων' ιδιωτών ή των μη-κρατικών οντοτήτων, υιοθετώντας τις με τον τρόπο αυτό·[145] βέβαια, η δημόσια και εκ των υστέρων επιδοκιμασία και υιοθέτηση από κράτος κάποιας CNA είναι εξαιρετικά απίθανο να συμβεί, αφού ο κυβερνοχώρος είναι το πεδίο ανθρώπινης αντιπαράθεσης που κατ' εξοχήν ενδείκνυται για τη διεξαγωγή *κεκαλυμμένων* επιχειρήσεων…

Ιδιαιτέρα πιθανές είναι στην πράξη και οι περιπτώσεις κατά τις οποίες CNAs ξεκινούν από το έδαφος ενός κράτους, χωρίς κατά τα λοιπά οιαδήποτε εμπλοκή και γνώση οργάνων ή υπηρεσιών του κράτους αυτού. Σ' αυτές τις περιπτώσεις, όπως είναι αυτονόητο, οι πράξεις των διενεργούντων τις επιθέσεις δεν μπορούν να αποδοθούν στο κράτος· κρατική ευθύνη θα ανακύψει μόνον εάν το γεγονός περιέλθει σε γνώση των κρατικών υπηρεσιών αλλά δεν εκδηλωθεί καμία ενέργεια, απ' αυτές που είναι εύλογες και αναγκαίες υπό τις περιστάσεις, για διακοπή και πρόληψη των επιθέσεων (κίνηση των προβλεπόμενων ποινικών διαδικασιών, διακοπή πρόσβασης internet κ.λπ.). Πάντως, σε μια τέτοια περίπτωση η ευθύνη του κράτους θα συνίσταται όχι στην εκδήλωση κυβερνο-επίθεσης με έμμεσο τρόπο (δια παραλείψεως, όπως θα λέγαμε στο πεδίο του ποινικού δικαίου), αλλά στο γεγονός ότι εν γνώσει του επέτρεπε τη χρησιμοποίηση της επικράτειάς του για την εκδήλωση (από τρίτους) πράξεων που προσβάλλουν τα δικαιώματα άλλων κρατών.[146]

6. Πώς μπορεί να αντιδράσει το κράτος που γίνεται στόχος μίας CNA

Εάν το κράτος – στόχος είναι σε θέση να προσδιορίσει την προέλευση μίας CNA εναντίον του και να την αποδώσει με ασφάλεια σε ενέργειες άλλου κράτους, τότε μπορεί κατ' αρχάς να θέσει το ζήτημα ενώπιον του Σ.Α. κατά το άρθρο 35 §1 του

[145] Υπόθεση του Διπλωματικού και Προξενικού προσωπικού των Η.Π.Α. στην Τεχεράνη (US v. Iran), ICJ Reports 1980, 3 et seq. (35 §74)· το Δικαστήριο δέχθηκε ότι η αρχική επίθεση στην πρεσβεία των Η.Π.Α. στην Τεχεράνη δεν μπορούσε να αποδοθεί στο κράτος του Ιράν, αλλά η *επιδοκιμασία* της επίθεσης που ακολούθησε από το κράτος αυτό και η απόφασή του να *παρατείνει* και να διαιωνίσει την κατάληψη της πρεσβείας, μετέβαλλε την κατάσταση. — Κατά το άρθρο 11 των Άρθρων της ILC για την ευθύνη των κρατών, συμπεριφορές που δεν μπορούν να αποδοθούν σ' ένα κράτος "shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own".

[146] Υπόθεση του Στενού της Κέρκυρας (U.K. v. Albania), ICJ Reports 1949, 4 et seq. (22).

Χάρτη.[147] Το Σ.Α. μπορεί να προτείνει τις ενδεικνυόμενες διαδικασίες και μεθόδους για την επίλυση της διαφοράς (άρθρο 36 §1). Το Συμβούλιο έχει τη δυνατότητα, επίσης, να θεωρήσει ότι η συγκεκριμένη περίσταση CNA αποτελεί *απειλή* για την ειρήνη, *διατάραξη* της ειρήνης ή *πράξη επίθεσης* (threat to the peace, breach of peach, act of aggression) και να προβεί σε περαιτέρω ενέργειες κατά το Κεφ. VII του Χάρτη˙ ορισμένες από τις περιπτώσεις που έχουν περιληφθεί στην Απόφαση της Γ.Σ. για τον ορισμό της επίθεσης[148] μπορούν άνετα, υπό το φως των όσων έχουν ήδη εκτεθεί παραπάνω, να καλύψουν και κυβερνοεπιθέσεις ("…attack by the armed forces of a State of the territory of another State", "…the use of any weapon by a State against the territory of another State", "[a]n attack by the armed forces of a State on the… forces… of another State", "[t]he action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State"), ενώ, ούτως ή άλλως, η συγκεκριμένη Απόφαση ούτε είναι δεσμευτική για το Σ.Α. ούτε περιέχει εξαντλητική παράθεση των περιπτώσεων.

Ανεξάρτητα από το εάν μία συγκεκριμένη CNA αίρεται μέχρι του σημείου να μπορεί να χαρακτηριστεί ως διατάραξη της ειρήνης ή ακόμη και πράξη επίθεσης, μπορεί πολύ ευκολότερα —και υπό την προϋπόθεση ότι και το ευρύτερο πολιτικό πλαίσιο και οι γεωστρατηγικές ισορροπίες επιτρέπουν κάτι τέτοιο— να κριθεί ότι συνιστά '*απειλή* για την ειρήνη' ˙ η τελευταία αυτή αξιολόγηση μπορεί σχετικά εύκολα να γίνει και αναφορικά με ορισμένες CNE,[149] εάν υπάρχει ανάλογη πολιτική βούληση. Οι συντάκτες του Χάρτη, απ' ό,τι φαίνεται, είχαν κατά νου ότι η ειρήνη μπορεί να διαταραχθεί και να απειληθεί από τη χρήση συμβατικών όπλων, ωστόσο άφησαν επίτηδες τις έννοιες αυτές ασαφείς.[150] Το Σ.Α. μέχρι σήμερα έχει διαπιστώσει 'διατάραξη' της ειρήνης σε ελάχιστες περιπτώσεις˙[151] αντίθετα, η έννοια της 'απειλής' κατά της ειρήνης είναι περισσότερο ελαστική και μέχρι σήμερα τα άκρα όριά της έχουν διευρυνθεί από την πρακτική του Σ.Α., με αποτέλεσμα σχεδόν ο,τιδήποτε να μπορεί να

[147] Σε μία τέτοια ενέργεια μπορεί, βέβαια, να προβεί και οποιοδήποτε άλλο κράτος – μέλος του Ο.Η.Ε. Ένα κράτος που δεν είναι μέλος του Ο.Η.Ε. μπορεί επίσης να φέρει ενώπιον του Σ.Α. ή της Γ.Σ. μία διαφορά στην οποία εμπλέκεται, υπό τις προϋποθέσεις του άρθρου 35 §2.
[148] A/RES/3314 (XXIX)/ Dec. 14, 1974, άρθρο 3.
[149] Roscini, σελ. 110.
[150] UN Conference on International Organization, Documents, Vol. XII, 1945, 505.
[151] Συγκεκριμένα μόνο σε τέσσερις περιπτώσεις : Κορέα, Νησιά Φώκλαντ, πόλεμος Ιράν – Ιράκ και εισβολή του Ιράκ στο Κουβέιτ. Όλες αποτελούν κλασσικού τύπου μεγάλης κλίμακας συρράξεις μεταξύ κρατών.

κριθεί ότι προκαλεί τέτοια 'απειλή'.[152] Εάν το Σ.Α. κρίνει ότι μία CNA συνιστά απειλή για την ειρήνη, μπορεί να διατυπώσει συστάσεις κατά το άρθρο 39, να υιοθετήσει προσωρινά μέτρα που θα εμποδίσουν τη χειροτέρευση της κατάστασης κατά το άρθρο 40, καθώς και μέτρα κατά τα άρθρα 41 και 42, με ή χωρίς τη χρήση βίας. Με δεδομένο ότι στο άρθρο 41 παρατίθεται ως ένα από τα εκεί ενδεικτικά αναφερόμενα μέτρα και η ''… πλήρης ή μερική διακοπή των … *τηλεγραφικών, ασύρματων και λοιπών μέσων επικοινωνιών*'' (η έμφαση δική μας), το Σ.Α. μπορεί να επιβάλει τη διακοπή των δικτυακών και διαδικτυακών επικοινωνιών του κράτους που κρίθηκε ως υπεύθυνο κυβερνοεπίθεσης.[153] Με αφορμή την επισήμανση αυτή δεν μπορούμε παρά να παρατηρήσουμε ότι είναι εκπληκτικό πώς μία διάταξη που γράφτηκε πριν από εξήντα πέντε και πλέον χρόνια μπορεί, θεωρητικά, να λειτουργήσει ακόμη και σήμερα, την εποχή των οπτικών ινών και του διαδικτύου των διαδικτύων,[154] όταν οι κυβερνοεπιχειρήσεις είναι ήδη πραγματικότητα και όταν, κατά πολλούς, το επόμενο στάδιο αυτού του φαινομένου είναι επίσης ορατό και θα συνίσταται στον κυβερνοπόλεμο μέσω… κινητών τηλεφώνων-![155] Αυτό το μικρό παράδειγμα δείχνει τη μεγάλη προσαρμοστικότητα του *jus ad bellum* που περιέχεται στις διατάξεις του Χάρτη και στο ήδη διαμορφωμένο διεθνές εθιμικό δίκαιο˙ οι διατάξεις αυτές φαίνεται ότι είναι ακόμη ικανές να 'στεγάσουν' όπλα και μεθόδους διακρατικού καταναγκασμού που ήταν αδιανόητα όταν η Διάσκεψη του San Francisco βρισκόταν σε εξέλιξη.[156]

Το κράτος που αποδεδειγμένα πραγματοποίησε την CNA μπορεί επίσης να αχθεί από το κράτος – στόχο ενώπιον ενός διεθνούς δικαστηρίου (και κατ' εξοχήν ενώπιον του ICJ), προκειμένου να παράσχει επανορθώσεις για την παραβίαση του

[152] Οι Schmitt, 1999, 928 και Roscini, σελ. 110 /111, θεωρούν, για παράδειγμα, ότι οποιοδήποτε σοβαρό 'κυβερνο-συμβάν' μεταξύ κρατών με μακρό παρελθόν τεταμένων σχέσεων και παραδοσιακή εχθρότητα (όπως ***Ελλάδα – Τουρκία*** ή Ινδία – Πακιστάν (sic)), μπορεί άνετα να κριθεί ότι συνιστά απειλή κατά της ειρήνης.
[153] Roscini, 111.
[154] Στην αγγλική η διάταξη κάνει λόγο για "telegraphic, radio and ***other means*** *of communication*" (η έμφαση δική μας).
[155] Συνέντευξη του Eugene Kaspersky, προέδρου της γνωστής εταιρείας κατασκευής αντι-ικού λογισμικού που φέρει το όνομά του, διαθέσιμη στην ιστοσελίδα http://www.defencenews.gr/?p=1827 (τελευταία πρόσβαση : 13-10-2011).
[156] Βλ. και Schmitt, 2010, σελ. 177, ο οποίος διαπιστώνει ότι "[t]he prohibition on the use of force [of the Charter] has proven somewhat adaptable to this new reality because it has long been understood to extend beyond the application of kinetic force".

άρθρου 2(4) και της αρχής της μη-επέμβασης. Μπορεί επίσης να ζητηθεί από το ICJ η διατύπωση Γνωμοδότησης, σύμφωνα με το άρθρο 96.[157]

Τα τελευταία χρόνια ορισμένοι μελετητές έχουν προχωρήσει ακόμη ένα βήμα παραπέρα, διατυπώνοντας τον ισχυρισμό ότι οι κυβερνοεπιθέσεις που έχουν τα χαρακτηριστικά και τις προδιαγραφές της επίθεσης (aggression), συνεπιφέρουν και την διεθνή ποινική ευθύνη των ατόμων που είναι υπεύθυνα·[158] τα άτομα αυτά μπορεί, φυσικά, να υπέχουν ποινικές ευθύνες και σύμφωνα με το εθνικό ποινικό δίκαιο της χώρας – στόχου, ή ακόμη και της χώρας – προέλευσης της επίθεσης. Το 2010 η Αναθεωρητική Διάσκεψη για το Καταστατικό του ΔΠΔ (ICC), υιοθέτησε τελικά έναν ορισμό για το έγκλημα της επίθεσης, ο οποίος βασίζεται στον ορισμό που περιέχεται στην Απόφαση 3314 (XXIX) της Γ.Σ. του 1974, χωρίς, όπως ήταν εν πολλοίς αναμενόμενο (και παρά τις αντίθετες απόψεις που είχαν διατυπωθεί στις διάφορες ομάδες εργασίας), την πρόβλεψη του άρθρου 4 εκείνης της Απόφασης περί του ενδεικτικού χαρακτήρα του καταλόγου των περιπτώσεων επίθεσης.[159] Το νέο άρθρο 8 *bis*(1) του Καταστατικού του ICC ορίζει το έγκλημα της επίθεσης ως "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the [UN]", κατά δε τη διάταξη της παραγρ. 2 του ιδίου άρθρου, πράξη επίθεσης είναι η χρησιμοποίηση "*armed force* by a State against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the [UN]" (η έμφαση δική μας). Όπως έχει εκτεθεί αναλυτικά παραπάνω, ο προσδιορισμός 'armed' για το είδος της βίας που απαιτείται, δεν μπορεί πλέον να αποκλείσει τη χρήση των η/υ και των δικτύων ως *όπλων*, ούτε τις CNAs ως *μεθόδων* για την πραγματοποίηση 'επιθέσεων' σαν κι' αυτές που απαιτούνται από την ως άνω διάταξη της παραγρ. 2 του άρθρου 8 *bis*· κατά την άποψή μας, δεν υπάρχει κανένα νομικό έρεισμα για να θεωρηθεί ότι, εν έτει 2010, κατά την Αναθεωρητική Διάσκεψη για το Καταστατικό του ICC, οι συντάκτες των συγκεκριμένων ρυθμίσεων του άρθρου 8 *bis* ήθελαν να περιορίσουν την 'ένοπλη βία' που μπορεί να ασκήσει ένα κράτος σε βάρος άλλου, μόνο σ' αυτήν που μπορεί να

[157] Οι Γνωμοδοτήσεις είναι προαιρετικές και μη δεσμευτικές, συμβάλλουν, ωστόσο, σημαντικά στη διαμόρφωση πρακτικών και κανόνων διεθνούς εθιμικού δικαίου.
[158] Π.χ. Ophardt, §61 et seq., Weisbord, σελ. 39 et seq., Roscini, σελ. 111 et seq.
[159] Resolution RC/Res. 4, June 11, 2010.

ασκηθεί με τη χρήση όπλων κινητικής ενέργειας, ή όπλων χαμηλής τεχνολογίας, ή με τη χρησιμοποίηση μόνο 'παραδοσιακών' μεθόδων καταναγκασμού. — Ενδοιασμούς εκφράζει ο *Roscini* (σελ. 112), λόγω της απαγόρευσης αναλογικής επέκτασης των προβλέψεων του Καταστατικού που καθιερώνεται στο άρθρο 22(2)[160] αυτού.[161] Όπως παρατηρεί όμως ορθά ο *Weisbord* (σελ. 40 /41), δεν παραβιάζεται η απαγόρευση του άρθρου 22(2) διότι δεν πρόκειται για 'αναλογία' αλλά για ευρύτερη ερμηνεία του όρου 'armed'·[162] κατά την άποψή μας, ούτε για ευρεία ή ευρύτερη ερμηνεία πρόκειται, αλλά για την απόδοση στον όρο 'armed' του *πραγματικού* περιεχομένου του, έτσι όπως το θέλησαν ήδη οι συντάκτες του Χάρτη των Η.Ε. κατά της δεκαετίας του 1940, αφού, όπως εκτίθεται παραπάνω, «τα χαρακτηριστικά εκείνα που καθιστούν 'όπλο' ένα αντικείμενο, μία συσκευή ή ένα σύστημα, δεν είναι τα εκ κατασκευής ή κατά προορισμό χαρακτηριστικά του, ή η συνήθης χρήση του, αλλά οι *προθέσεις* και οι *επιδιώξεις* με τις οποίες χρησιμοποιείται και τα *αποτελέσματα* της χρήσεως αυτής».

Το κράτος-θύμα μπορεί επίσης να προβεί σε retortions ('ανταπόδοση'), καθώς και σε αντίμετρα χωρίς τη χρήση στρατιωτικής βίας (non-forceful /non-military countermeasures). Τα αντίμετρα μπορούν να ληφθούν (υπό τις προϋποθέσεις, βέβαια, που γίνονται σήμερα δεκτές από το ειδικό επ' αυτού διεθνές δίκαιο[163]) μόνον εάν η συγκεκριμένη 'κυβερνο-επίθεση' αποτελεί παράνομη πράξη κατά το διεθνές δίκαιο, όταν, δηλαδή, θα ξεπερνά το ελάχιστο απαιτούμενο 'κατώφλι' που απαιτείται για να την διακρίνει από μία παρόμοιας φύσεως επιχείρηση η οποία απλά *ενοχλεί* αλλά δεν είναι παράνομη, όπως, για παράδειγμα, η κυβερνο-κατασκοπεία. Έτσι αντίμετρα μπορούν να αναληφθούν από το κράτος που θίγεται όταν οι κυβερνο-επιθέσεις σε βάρος του παραβιάζουν την αρχή της μη-επέμβασης στα εσωτερικά ζητήματα τρίτων κρατών (: κυβερνο-προπαγάνδα για την πρόκληση κοινωνικών αναταραχών, επηρεασμό του εκλογικού σώματος, κλονισμό της οικονομίας κ.λπ.), η συνιστούν χρήση βίας σαν κι' αυτή που απαγορεύει το άρθρο 2(4) του Χάρτη, κατά τα παραπάνω. Με δεδομένο ότι τα 'αντίμετρα με χρήση βίας' (countermeasures involving the use of

---

[160] "The definition of a crime shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favour of the person being investigated, prosecuted or convicted."

[161] Δεν διστάζει, ωστόσο, να σημειώσει ότι οι hackers (sic) που αναλαμβάνουν ηλεκτρονικά και παράνομα τον έλεγχο ενός πυραυλικού συστήματος και το χρησιμοποιούν για να εκδηλώσουν επίθεση, είναι πιθανώς εφικτό να διωχθούν, κατά τις παραπάνω διατάξεις, ως ''πρόσωπα τα οποία είναι σε θέση να ασκούν πραγματικό έλεγχο επί, ή να κατευθύνουν, … τη στρατιωτική δράση ενός κράτους'' (κατά το παραπάνω άρθρο 8*bis*(1)) (σελ. 113).

[162] Έτσι και ο Ophardt, §65.

[163] Βλ. τα άρθρα 50, 51 και 52 του σχεδίου άρθρων της ILC.

force) δεν γίνονται δεκτά ως νόμιμος τρόπος αντίδρασης από το σύγχρονο διεθνές δίκαιο, το κράτος-θύμα μπορεί να καταφύγει σ' αυτά μόνον εάν η CNA εναντίον του συνιστά 'ένοπλη επίθεση' σαν κι' αυτή που απαιτεί το άρθρο 51 (και της οποίας τις προδιαγραφές έχουμε προσεγγίσει παραπάνω). Στα πλαίσια εφαρμογής του άρθρου 51 το κράτος που δέχεται αυτού του είδους την επίθεση μπορεί να αντιδράσει είτε με τη χρήση κλασσικής στρατιωτικής βίας, είτε με CNA, είτε με συνδυασμό των δύο (και υπό τον όρο, βέβαια, ότι προηγουμένως θα διαπιστωθεί πέρα από κάθε αμφιβολία η πηγή της ένοπλης επίθεσης).

Ο *Roscini* (σελ. 113 /114) παρατηρεί ότι θα ήταν παράλογο (sic) να ισχυριστεί κανείς ότι εάν ένα κράτος δεχθεί κυβερνο-επίθεση σαν κι' αυτή που απαγορεύει το άρθρο 2(4) —αλλά της οποίας το επίπεδο δεν φθάνει σ' αυτό που απαιτεί το άρθρο 51—, δεν θα μπορεί να απαντήσει 'σε είδος' με τον ίδιο τρόπο, στέλνοντας, για παράδειγμα, κακόβουλο λογισμικό στα δίκτυα του επιτιθέμενου ή απαντώντας με κάποιο είδος DDoS επίθεσης σε μία προηγηθείσα DDoS επίθεση και τηρώντας την αρχή της αναλογικότητας. Αν και στη συνέχεια προσθέτει ότι η αναλογικότητα είναι δύσκολο να διασφαλιστεί επειδή το κακόβουλο λογισμικό μπορεί να διασπαρθεί ανεξέλεγκτα, ενώ μία αντεπίθεση DDoS, από τη φύση της, δεν είναι και τόσο αυτονόητο ότι θα πλήξει μόνο τον ίδιο τον επιτιθέμενο, φαίνεται ότι τελικά συμφωνεί με τη γενική ιδέα μίας τέτοιας δυνατότητας. Η σκέψη αυτή δεν μπορεί, κατά την άποψή μας, να γίνει αποδεκτή˙ πράγματι, αφενός μεν παραβιάζει τη βασική αρχή της απαγόρευσης χρήσης ένοπλης βίας[164] κατά την εφαρμογή των αντιμέτρων, αφετέρου δε η αρχή της αναλογικότητας των αντιμέτρων προς την αντιδιεθνή πράξη κατά της οποίας στρέφονται, δεν μπορεί να τηρηθεί αφού τα όπλα του ηλεκτρονικού πολέμου από τη φύση τους προκαλούν *παράπλευρες* απώλειες και *διάχυση* των συνεπειών και αποτελεσμάτων, κατά τρίτο δε, είναι πολύ πιθανό ότι ο χαρακτήρας ενός τέτοιου είδους αντιμέτρου δεν θα μπορεί να είναι αντιστρέψιμος (μη-διαρκής), όπως απαιτεί το σύγχρονο δίκαιο διεθνούς ευθύνης των κρατών. Τέλος, μια σκέψη σαν την παραπάνω, αναλογικά εφαρμοζόμενη, θα επέτρεπε, για παράδειγμα, στο κράτος Α, το οποίο δέχεται από το κράτος Β μερικές μεμονωμένες διασυνοριακές βολές πυροβολικού (: χρήση βίας αλλά όχι επιπέδου 'ένοπλης επίθεσης'), να απαντήσει με τον ίδιο τρόπο και να ισχυριστεί ότι ασκεί το δικαίωμά του στην εφαρμογή (νόμιμων)

[164] Όπως έχουμε δει, το κακόβουλο λογισμικό —ανάλογα με την πρόθεση και τον τρόπο χρήσης του— μπορεί να είναι (ένα τεχνολογικά προηγμένο) όπλο, οι δε επιθέσεις DDoS μπορεί να είναι 'μέθοδος (σύγχρονου) πολέμου'.

αντιμέτρων, σκέψη, όμως, η οποία, όπως είναι αυτονόητο, δεν μπορεί να γίνει αποδεκτή και οδηγεί σε αδιέξοδα.

7. Ζητήματα 'ανασχετικής' αυτοάμυνας, αυτοάμυνας εναντίον 'επικείμενης' επίθεσης, καθώς και 'προληπτικής' αυτοάμυνας, στην περίπτωση των CNAs

Όπως είναι γνωστό, αν και το δικαίωμα αυτοάμυνας του άρθρου 51 του Χάρτη έχει εθιμικές καταβολές, υπάρχει μία ουσιαστική διαφορά στο σημείο αυτό ανάμεσα στο γραπτό και το εθιμικό διεθνές δίκαιο αναφορικά με το εύρος του συγκεκριμένου δικαιώματος : το άρθρο 51 επιτρέπει την αυτοάμυνα μόνον όταν *διαπιστώνεται* ένοπλη επίθεση,[165] ενώ ο αντίστοιχος κανόνας του διεθνούς εθιμικού δικαίου επιτρέπει την αυτοάμυνα και ως ένα προληπτικό μέτρο (preventive measure) επί επιθέσεως που *επίκειται*,[166,] υπό ορισμένες προϋποθέσεις. Το δικαίωμα αυτοάμυνας κατά το διεθνές *εθιμικό* δίκαιο, θα πρέπει να πληροί τα κριτήρια που τέθηκαν για πρώτη φορά το 1842 στα πλαίσια του *επεισοδίου 'Caroline'* :[167] πρέπει να διαπιστώνεται *"a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation"*.[168]

Κατά τον *Dinstein*[169] στο θέμα της επίθεσης, ωστόσο, το κρίσιμο ζήτημα δεν είναι να διαπιστωθεί πότε πέφτει 'ο πρώτος πυροβολισμός' ή, πιο γενικά, πότε

---

[165] Εάν ο Χάρτης ήθελε να επιτρέψει και την προληπτική άσκηση βίας στα πλαίσια αυτοάμυνας, θα έπρεπε να ρυθμίσει κάτι τέτοιο σαφώς και όχι να αφήσει τον υποτιθέμενο σχετικό κανόνα να εξάγεται ερμηνευτικά από τη συγκεκριμένη διατύπωση του άρθρου 51, όπως αυτή τελικά τέθηκε σε ισχύ. (Dinstein, e-book, σελ. 168)

[166] Το ICJ στην υπόθεση Νικαράγουα, στήριξε την απόφασή του στους κανόνες του διεθνούς εθίμου για την αυτοάμυνα ως απάντηση σε *π α ρ ο ύ σ α* ένοπλη επίθεση και δεν αποφάνθηκε επί του ζητήματος της νομιμότητας μίας απάντησης στην απειλή *επικείμενης* ένοπλης επίθεσης˙ έσπευσε, ωστόσο, να διευκρινίσει ότι αυτό οφειλόταν στη φύση και τις περιστάσεις της συγκεκριμένης υπό κρίσιν διαφοράς. Ομοίως στην υπόθεση *Armed Activities on the Territory of the Congo*, το Δικαστήριο επίσης δεν εξέφρασε άποψη επί του ζητήματος αυτού επειδή η Ουγκάντα τελικά ισχυρίστηκε ότι οι ενέργειές της εκδηλώθηκαν επί επιθέσεων που ήδη είχαν λάβει χώρα˙ πάντως το Δικαστήριο σημείωσε ότι κατανοεί ότι οι ανάγκες ασφαλείας που η Ουγκάντα προσπαθούσε να διαφυλάξει ήταν "essentially preventive" και επεσήμανε ότι "[a]rticle 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters". (DRC v. Uganda, ICJ Reports 2005, 168 et seq., 222 §143, 223 §148))

[167] Επιστολή του τότε ΥΠΕΞ των Η.Π.Α. Daniel Webster προς τον ομόλογό του της Μεγ. Βρετανίας, Lord Ashburton, αναφορικά με επεισόδιο που είχε λάβει χώρα το 1837.

[168] Βλ. και Higgins, 248, "for self-defence to be a legitimate response to a threat of force, the threat would have to meet the Webster test in the Caroline". — Διαφορετικά ο Roscini (121 /122), ο οποίος, χρησιμοποιώντας τους ερμηνευτικούς κανόνες των άρθρων 31 και 32 της Συνθήκης της Βιέννης του 1969, θεωρεί ότι το δικαίωμα αυτοάμυνας σε επίθεση που *επίκειται* καλύπτεται *και* από το άρθρο 51 του Χάρτη.

[169] Dinstein, e-book, σελ. 172 et seq.

διαπιστώνεται χρήση του όπλου ή των όπλων που χρησιμοποιεί ο επιτιθέμενος, αλλά πότε ξεκινάει μία *μη-αναστρέψιμη* αλληλουχία γεγονότων και δράσης, δηλαδή πότε μπορούν να ανιχνευθούν τα αρχικά στάδια της επίθεσης (εδώ ο συγγραφέας αυτός κάνει λόγο για *'incipient'* armed attack). Κατά τον συγκεκριμένο συγγραφέα θα ήταν εξωφρενικό (sic) να αναμένουμε από το κράτος-στόχο να δεχθεί το πλήγμα της επίθεσης, μόνο και μόνο για να αποδείξει ότι εφαρμόζει με άμεπτο τρόπο τη θεωρία περί του δικαιώματος αυτοάμυνας·[170] έτσι δέχεται και προτείνει την έννοια της 'ανασχετικής' αυτοάμυνας (*'interceptive'* self defence), η οποία, σε αντίθεση με την άμυνα σε επίθεση που επίκειται ή, ακόμη παραπέρα, σε αντίθεση με τη λεγόμενη προληπτική αυτοάμυνα επί επιθέσεως που αναμένεται,[171] ασκείται όταν, με βάση τα υπάρχοντα στοιχεία, η πλευρά του επιτιθέμενου μπορεί να λεχθεί ότι συνδέεται προς μία ένοπλη επίθεση με έναν τρόπο κατά τα φαινόμενα μη-αναστρέψιμο, η οποία (επίθεση), όμως, τυπικά δεν έχει ξεκινήσει ακόμη. Επίσης κατά τον *Dinstein*, ενώ η προληπτική αυτοάμυνα ασκείται εναντίον επίθεσης που είναι απλά προβλέψιμη (ή ακόμη και νοητή ή πιθανή…), η ανασχετική αυτοάμυνα ασκείται εναντίον επίθεσης που είναι επικείμενη και συγχρόνως πρακτικά μη-αναστρέψιμη ή αναπόφευκτη· πάντοτε κατά τον *Dinstein*, η 'ανασχετική' αυτοάμυνα είναι νόμιμη ακόμη και υπό το άρθρο 51 του Χάρτη.[172]

> (Αρκετές φωνές εσχάτως κάνουν ευθέως λόγο και για την ύπαρξη ενός δικαιώματος καθαρά προληπτικής ή αποτρεπτικής αυτοάμυνας (preemptive /preventive self-defence), το οποίο φθάνει πιο μακριά από την αυτοάμυνα σε επίθεση που *επίκειται* και ξεπερνά και αυτά τα κριτήρια του επεισοδίου 'Caroline', ώστε να ασκείται εναντίον *πιθανών* και *αναμενόμενων* επιθέσεων (με βάση 'σοβαρές' ενδείξεις, πληροφορίες των υπηρεσιών ασφαλείας, γεωστρατηγικούς συσχετισμούς και προβλέψεις κ.λπ.). Στο υπόμνημα των Η.Π.Α. προς τον Ο.Η.Ε. τον Οκτώβριο του 2001, αναφορικά με την αναληφθείσα δράση της χώρας αυτής στο Αφγανιστάν, γραφόταν χαρακτηριστικά ότι "[w]e may find that our self-defense requires further actions with respect to other organizations and other states",[173] ενώ η προσέγγιση αυτή περιλήφθηκε επίσημα στην εθνική στρατηγική

[170] Αναφέρει, μάλιστα, μία χαρακτηριστική σκέψη του *Waldock*, ήδη από το 1952 : "Where there is *convincing evidence* not merely of threats and potential danger but of an attack being *actually mounted*, then an armed attack may be said to have begun to occur, though it has not passed the frontier". (Waldock, *"The Regulation of the Use of Force by Individual States in International Law"*, 81 R.C.A.D.I. 451, 498 (1952), με την έμφαση δική μας.)
[171] Περί αυτής και περί της ενδεχόμενης νομιμότητάς της, βλ. αμέσως παρακάτω στο κείμενο.
[172] Την άποψη αυτή φαίνεται ότι συμμερίζεται και ο Shaw, e-book, σελ. 1137 et seq και ιδίως 1139.
[173] Έγγραφο S/2001/946 (αναφέρεται, για παράδειγμα, από τον Shaw, σελ. 1140).

ασφαλείας (‘δόγμα’) των Η.Π.Α. του έτους 2002 (‘δόγμα Bush’) και επαναβεβαιώθηκε στο αντίστοιχο κείμενο του 2006˙ στα κείμενα αυτά γίνεται προσπάθεια διεύρυνσης του ορισμού της έννοιας ‘imminent’ έτσι ώστε να καλύψει και περιπτώσεις κατά τις οποίες “uncertainty remains as to the time and place of the enemy’s attack”.[174] Στο μέτρο που η προληπτική αυτοάμυνα ξεπερνά ακόμη και αυτό το ‘πλαίσιο ‘Caroline’, δεν μπορεί (φυσικά) να γίνει αποδεκτή ως νόμιμη επιλογή στο σύγχρονο γραπτό και εθιμικό διεθνές δίκαιο.)

Μία CNA που θα συνιστά από μόνη της ένοπλη επίθεση κατά τα παραπάνω, λόγω ακριβώς της φύσης και των ιδιαίτερων χαρακτηριστικών της ως μεθόδου χρήσης βίας (: έλλειψη προειδοποιητικών ενδείξεων, ταχύτητα εκδήλωσης και εξάπλωσης κ.λπ.), αφήνει ουσιαστικά μερικά δευτερόλεπτα ή, στην καλύτερη περίπτωση, μερικά λεπτά αντίδρασης στο κράτος που δέχεται την επίθεση˙ σε μία τέτοια (απλή) περίπτωση —και υπό την αυτονόητη προϋπόθεση ότι ο επιτιθέμενος είναι γνωστός—[175] το κράτος-στόχος θα διαπιστώσει τις συνέπειες και θα έχει τη δυνατότητα να αντιδράσει στα πλαίσια του δικαιώματος αυτοάμυνας του άρθρου 51, τηρώντας τις αρχές της αναγκαιότητας και αναλογικότητας, είτε με ‘ηλεκτρονικά όπλα’, είτε με συμβατικά, είτε με συνδυασμό των δύο. Μάλιστα —και ιδίως αναφορικά με το κριτήριο της ‘αναγκαιότητας’— λόγω των ιδιαίτερων χαρακτηριστικών των CNAs και ιδίως της ταχύτητας εκδήλωσης και εξάπλωσής τους, δεν θα υπάρχει χρόνος για προσπάθεια ειρηνικής επίλυσης από την πλευρά του κράτους-στόχου (: δεν θα διαπιστωθεί ‘συγκέντρωση των δυνάμεων του εχθρού στα σύνορα’, ούτε θα συγκεντρωθεί ο στόλος για να αποπλεύσει προς ανακατάληψη των νήσων Falklands /Malvinas…), ούτε για κινητοποίηση της διεθνούς κοινότητας προτού διαπιστωθούν οι πρώτες απώλειες σε έμψυχο και άψυχο υλικό. Υπάρχουν βέβαια, όπως έχουμε ήδη σημειώσει, και επιθέσεις CNA οι οποίες ξεκινούν ως μια απλή ηλεκτρονική διαταραχή, στη συνέχεια αποκτούν τα χαρακτηριστικά των CNE και κάποια στιγμή κορυφώνονται και προσβάλλουν τα συστήματα του στόχου, αιφνιδιάζοντάς τον ουσιαστικά, παρά το γεγονός ότι το συμβάν ‘παρακολουθείται’ για καιρό˙ και σ’ αυτήν την περίπτωση δεν θα υπάρχει χρόνος για

[174] Κατά τον Schmitt, 2010, 166, το δόγμα ασφαλείας των Η.Π.Α. της κυβέρνησης B. Obama του έτους 2010 δεν υιοθετεί καθαρά το δόγμα προληπτικής αυτοάμυνας, αλλά *ούτε και το απορρίπτει*˙ αναφέρει μάλιστα σαφώς, ότι οι Η.Π.Α. διατηρούν το δικαίωμα να ενεργούν *μονομερώς* όταν απαιτείται [κατά την κρίση τους…].

[175] Υπό τις σημερινές τεχνολογικές συνθήκες και με βάση το στάδιο ανάπτυξης της τεχνολογίας η/υ και δικτύων, αποτελεί πραγματική πρόκληση για οποιοδήποτε κράτος, όσο προηγμένο τεχνολογικά και αν είναι, να ανακαλύψει γρήγορα και με ακρίβεια τους πραγματικούς υπευθύνους πίσω από μία ηλεκτρονική επίθεση. (Βλ. και Dinstein, σε Schmitt & O’Donnell eds, Vol. 76, 107.)

προσπάθειες ειρηνικής επίλυσης. (Βλ. όμως και στην τρίτη περίοδο της αμέσως επόμενης παραγράφου.)

Περισσότερο προβληματική είναι, βέβαια, η περίπτωση κατά την οποία το κράτος-θύμα μίας ένοπλης επίθεσης με κυβερνο-όπλα —η οποία προκάλεσε υλικές & ανθρώπινες απώλειες του επιπέδου που απαιτεί το διεθνές δίκαιο—, ανακαλύπτει το υπεύθυνο κράτος μετά τη διακοπή της επίθεσης και μετά από έρευνες που διαρκούν ικανό χρονικό διάστημα. Εδώ, εάν δεν συντρέχουν και κάποιες άλλες προϋποθέσεις (για παράδειγμα, ανακάλυψη 'λογικών' ή 'χρονικών' βομβών στα δίκτυα του στόχου, ή αποδείξεις για επικείμενη συμβατική επίθεση, για την οποία πληρούνται τα κριτήρια της περίπτωσης 'Caroline'), δεν θα μπορεί πλέον να ασκηθεί το δικαίωμα της αυτοάμυνας, αφού ο απώτατος σκοπός του δικαιώματος αυτού *δεν* είναι η τιμωρία του επιτιθέμενου αλλά η απόκρουση ή διακοπή της επίθεσης μέχρις ότου καταστεί δυνατή η ρύθμιση του προβλήματος από τη διεθνή κοινότητα. (Μπορούν, βέβαια, να ληφθούν αντίμετρα χωρίς τη χρήση βίας.) *Ανασχετική αυτοάμυνα* θα είναι νοητή εάν στα δίκτυα του κράτους-στόχου διαπιστωθούν παράνομες και μη-εξουσιοδοτημένες διεισδύσεις,[176] χωρίς πρόκληση (στα αρχικά στάδια) ζημιών ή ανθρώπινων απωλειών (: εκμετάλλευση και καταγραφή των αδυναμιών και της αρχιτεκτονικής των δικτύων του στόχου, εισαγωγή κακόβουλου λογισμικού προπαρασκευής, χρονικές ή λογικές βόμβες), κατά τρόπον ώστε —σε συνδυασμό, ενδεχομένως, και με άλλα διαθέσιμα στοιχεία—, να προκύπτει ότι το κράτος-στόχος βρίσκεται στην πραγματικότητα αντιμέτωπο με το *εναρκτήριο στάδιο* μιας σαρωτικής ηλεκτρονικής επίθεσης ή ακόμη και με μία ένοπλη επίθεση με 'συμβατικά' όπλα και μεθόδους, η οποία πρόκειται να ακολουθήσει άμεσα.[177]

Αυτό το τελευταίο ενδεχόμενο μας φέρνει σε επαφή με το πιθανότερο σενάριο ενδεχόμενης αυτοάμυνας στο σύγχρονο γεωστρατηγικό περιβάλλον που είναι ένα κράτος να βρεθεί αντιμέτωπο με μία κυβερνο-επίθεση η οποία στην πραγματικότητα αποτελεί *προπαρασκευαστική* πράξη μίας άλλης —κυρίας— επίθεσης με συμβατικά όπλα και μεθόδους, η οποία είναι επικείμενη. Αρκετοί αναλυτές

[176] Σχεδόν πάντοτε, ωστόσο, τα δίκτυα του κράτους-στόχου βρίσκονται υπό παρακολούθηση, 'εκμετάλλευση', καταγραφή αδυναμιών και 'χαρτογράφηση' της δομής τους, για μεγάλα χρονικά διαστήματα, χωρίς ο στόχος να αντιλαμβάνεται το πραγματικό εύρος της ηλεκτρονικής επιχείρησης σε βάρος του.

[177] Κάτι ανάλογο, δηλαδή, με το να διαπιστωθεί ότι ένα σμήνος βομβαρδιστικών βρίσκεται ήδη στον αέρα, καθ' οδόν προς συγκεκριμένο στόχο. (Dinstein, σε Schmitt & O'Donnell eds, Vol. 76, 111.)

αναφέρουν ως παράδειγμα την *καταστροφή των δορυφορικών επικοινωνιών ενός κράτους με ηλεκτρονική επίθεση στα δίκτυα που ελέγχουν τους δορυφόρους* (: θέση των δορυφόρων εκτός τροχιάς, καταστροφή του λογισμικού που βρίσκεται ενσυρματωμένο στα ηλεκτρονικά τους κυκλώματα κ.λπ.), ως πρώτο στάδιο μίας επίθεσης με περισσότερο συμβατικές μεθόδους που πρόκειται να ακολουθήσει.[178] Ένα άλλο αγαπημένο παράδειγμα πολλών είναι *η καταστροφή με ηλεκτρονική (προπαρασκευαστική) επίθεση των στρατιωτικών συστημάτων και δικτύων C4I,*[179] ενόψει της επικείμενης κύριας επίθεσης. Κατά τον *Schmitt* σε μία τέτοια περίπτωση —και προκειμένου να υπάρχει συμβατότητα με τα κριτήρια 'Caroline'—, για την επιβεβαίωση του δικαιώματος αυτοάμυνας ενός κράτους σε επίθεση που επίκειται (anticipatory self-defence), όταν διαπιστώνεται CNA η οποία από μόνη της δεν αίρεται στο επίπεδο που απαιτεί το άρθρο 51, *τρεις* παράγοντες πρέπει να ληφθούν υπόψη :[180] (α) η CNA είναι τμήμα μίας ευρύτερης επιχείρησης που κορυφώνεται σε ένοπλη επίθεση προδιαγραφών άρθρου 51˙ (β) η CNA αποτελεί ένα μη-αναστρέψιμο στάδιο μίας επικείμενης, χρονικά άμεσης και —με βάση τα υπάρχοντα στοιχεία— αναπόφευκτης επίθεσης˙ τέλος, (γ) ο αμυνόμενος ενεργεί μεν κατά τρόπο 'προληπτικό', αλλά η αντίδρασή του βρίσκεται εντός του ύστατου διαθέσιμου χρονικού πλαισίου αντίδρασης (last possible window of opportunity) για την επιτυχή απόκρουση της επίθεσης.[181] Σε μια τέτοια περίπτωση η κρίση περί του 'επικείμενου' της επίθεσης δεν μπορεί να στηριχθεί μόνο στο χρονικό παράγοντα, αλλά —με δεδομένο ότι έχουμε να κάνουμε με ηλεκτρονική (προπαρασκευαστική) επίθεση— και σε άλλους παράγοντες όπως η *ένταση* της επίθεσης και οι *μέθοδοι* με τις οποίες εκδηλώνεται, το *είδος* των δικτύων που πλήττονται, η *ταχύτητα* διάδοσης του προβλήματος στα δίκτυα κ.λπ. Εδώ επίσης, όπως είναι αυτονόητο, η αναλογικότητα της επίθεσης θα πρέπει να κριθεί ως προς τη συνολική επίθεση και όχι ως προς το πρώτο στάδιό της, την CNA. Ωστόσο, όπως παρατηρεί και ο *H. B. Robertson, Jr.,*[182] *οι CNAs ωθούν τα κριτήρια του επεισοδίου 'Caroline' στα όριά τους*, αφού, λόγω της *φύσης* αυτής της μεθόδου επίθεσης

[178] Βλ. και παρακάτω για πληροφορίες στον τύπο περί αχρήστευσης *τουρκικού* δορυφόρου με αυτόν τον τρόπο από το *Ισραήλ*.
[179] Η σύντμηση 'C4I' αποδίδει τη φράση "command, control, communications, computers, and (military) intelligence".
[180] Ο συγκεκριμένος συγγραφέας πιστεύει ότι αυτό πλέον είναι και το πιθανότερο σενάριο στη σύγχρονη πραγματικότητα.
[181] Schmitt, 2010, 165 et seq, Schmitt, 1999, 932 – 933, Roscini, 122, Robertson, σε Schmitt & O'Donnell eds, vol. 76, 139 – 140. – Εννοείται ότι εάν ο αμυνόμενος δεν αντιδράσει εντός αυτού του 'last possible window of opportunity', δεν θα μπορεί πλέον να προβάλει σοβαρή αυτοάμυνα διότι θα έχει καταστραφεί.
[182] Robertson, ibid, σελ. 140.

και των *ταχυτήτων* δράσης των ηλεκτρονικών όπλων, το 'ύστατο διαθέσιμο χρονικό πλαίσιο αντίδρασης' μπορεί να αποδειχθεί εξαιρετικά μικρό και ανεπαρκές για να αποτρέψει καταστροφικά αποτελέσματα για το κράτος που δέχεται μια τέτοια επίθεση…˙ ο ίδιος συγγραφέας καταλήγει στο συμπέρασμα ότι για το πρόβλημα αυτό δεν υπάρχει συγκεκριμένη ικανοποιητική λύση και θεωρεί ότι, τελικά, κάθε ανάλυση θα πρέπει να λαμβάνει υπόψη της ''τον πιο θεμελιώδη και περιεκτικό κανόνα απ' όλους, δηλαδή τη συμμόρφωση προς τις επιταγές της λογικής, υπό το φως των δεδομένων και των ιδιαιτεροτήτων της κάθε συγκεκριμένης περίπτωσης'' (reasonableness in particular context).[183]

> Επ' αυτού η *Higgins* (σελ. 242), αναφερόμενη στο άρθρο 51, σημειώνει χαρακτηριστικά : "…in a nuclear age, common sense cannot require one to interpret an ambiguous provision in a text in a way that requires a state passively to accept its fate before it can defend itself." Και ο *Brownlie* έχει δεχθεί ουσιαστικά ότι οι τεχνολογικές εξελίξεις και η πρόοδος στα μέσα που χρησιμοποιούνται στις επιχειρήσεις, επιβάλλουν επανεξέταση του χρονικού σημείου έναρξης μίας 'επίθεσης', σημειώνοντας ότι "…in certain cases technical means of countering the instrument of aggression will not adequately ensure protection if action is only taken when the object enters the territorial domain."[184]

8. Πώς προσεγγίζονται σήμερα οι CNAs από την πρακτική κρατών και Οργανισμών. — Υπάρχει ανάγκη νέου συμβατικού διεθνούς δικαίου ;

Η Γενική Συνέλευση του Ο.Η.Ε. έχει διαπιστώσει επανειλημμένα ότι η ασφάλεια στον κυβερνοχώρο είναι ζήτημα που απασχολεί τη διεθνή κοινότητα και έχει εκδώσει μία σειρά Αποφάσεων[185] στις οποίες αποτυπώνεται η διαπίστωση ότι η διάδοση και η χρήση μέσων και τεχνολογιών πληροφορικής επηρεάζει τα συμφέροντα της διεθνούς κοινότητας ως σύνολο και ότι η χρησιμοποίηση των τεχνολογιών αυτών με εγκληματικό σκοπό μπορεί να έχει επιβλαβείς συνέπειες για όλα τα κράτη˙ διαπιστώνει επίσης —και αυτό είναι εξαιρετικά σημαντικό για την εξαγωγή ορισμένων συμπερασμάτων για τη νομική φύση και την ενδεχόμενη εξέλιξη του προβλήματος στο άμεσο μέλλον— ότι *αυτές οι τεχνολογίες μπορούν δυνητικά να χρησιμοποιηθούν για*

---

[183] Ibid., με παραπομπή σε M.S. McDougal & F.P. Feliciano, *Law and Minimum World Order* (1961), 218. (Η μετάφραση της πρότασης είναι δική μας.)
[184] Op. cit., σελ. 367.
[185] Βλ. τέτοιες Αποφάσεις σε Tikk, *Frameworks*, 395 – 418.

σκοπούς που δεν είναι συμβατοί με την επιδίωξη της διατήρησης της διεθνούς ασφάλειας και σταθερότητας.[186]

Οι ένοπλες δυνάμεις μεγάλου αριθμού χωρών έχουν συγκροτήσει εδώ και μία δεκαετία, τουλάχιστον, μονάδες και διοικήσεις κυβερνοπολέμου (cyber commands και cyber units, αντίστοιχα), με φανερή αποστολή —στις περισσότερες των περιπτώσεων— τη διεξαγωγή 'αμυντικών' επιχειρήσεων στον κυβερνοχώρο˙ στην πραγματικότητα, βέβαια, όλες αυτές οι μονάδες —στις οποίες διατίθενται σημαντικοί οικονομικοί πόροι και οι οποίες εξοπλίζονται με υψηλού επιπέδου ηλεκτρονικό εξοπλισμό και στελεχώνονται με μεγάλο αριθμό προσωπικού (στρατιωτικούς, πολιτικό και ειδικό επιστημονικό προσωπικό))—, έχουν τη δυνατότητα να εκτελέσουν και επιθετικές επιχειρήσεις στον κυβερνοχώρο[187] και τέτοια σενάρια πράγματι εκτελούνται στα πλαίσια ασκήσεων σε ετήσια ή και εξαμηνιαία βάση ακόμη.[188] Στις χώρες αυτές συγκαταλέγονται ιδίως οι Η.Π.Α., το Ισραήλ,[189] η Κίνα,[190] η Ρωσική Ομοσπονδία, ο Καναδάς, η Γερμανία, η Ιταλία, η Τουρκία, το Ηνωμένο Βασίλειο, η Ολλανδία, η Γαλλία, η Ισπανία, η Πολωνία, η Αυστραλία, η Βραζιλία κ.α. Συνολικά υπολογίζεται ότι αυτή τη στιγμή τουλάχιστον 120 χώρες έχουν αναπτύξει και λειτουργούν επιθετικές

---

[186] Roscini, σελ. 88 και σημ. 7, 8 και 9. Ο συγγραφέας αυτός αναφέρει επίσης ότι η Γ.Σ. —προφανώς ως μία επιπλέον αναγνώριση της σπουδαιότητας του ζητήματος— στήριξε τη διοργάνωση Συνόδου Κορυφής για την Κοινωνία της Πληροφορίας, η οποία έλαβε χώρα σε δύο φάσεις, στη Γενεύη το 2003 και στην Τύνιδα το 2005. (Τα έγγραφα που υιοθετήθηκαν στη Σύνοδο, διαθέσιμα στην ιστοσελίδα www.itu.int/wsis/index.html.)

[187] Στην πολεμική αεροπορία των Η.Π.Α., για παράδειγμα, οι απόφοιτοι του 'Undergraduate Network Warfare Training Course', μετά από έξι μήνες εκπαίδευση "…will be able ***to operate a computer like a weapon system***" (Schaap, USAF Law Review, σελ. 132). Επίσης η πολεμική αεροπορία των Η.Π.Α. από το 2005 έχει υιοθετήσει ως 'mission statement' τη φράση "to fight in air, space ***and cyberspace***" (Shackelford, 250). (Η έμφαση δική μας και στις δύο αμέσως προηγούμενες αναφορές.)

[188] Στις Η.Π.Α. τέτοιες ασκήσεις είναι πράγματι αρκετά συχνές. Το ΝΑΤΟ επίσης διοργανώνει σε ετήσια βάση μία μεγάλη άσκηση 'κυβερνοάμυνας', στην οποία, ωστόσο, δοκιμάζονται και σενάρια επιθετικών ηλεκτρονικών επιχειρήσεων… Οι ελληνικές ένοπλες δυνάμεις συμμετέχουν στις ΝΑΤΟϊκές ασκήσεις κυβερνοπολέμου, πρόσφατα δε λήφθηκε η απόφαση, σε ανώτατο πολιτικό επίπεδο, να διοργανώνεται κατ' έτος και μία καθαρά ελληνική άσκηση 'κυβερνοάμυνας'˙ η αρχή έγινε το έτος 2010, στην δε άσκηση αυτή δόθηκε η διακριτική ονομασία 'Πανόπτης' (πρόκειται για προσωνύμιο δανεισμένο από την ελληνική μυθολογία και ήταν ένα από τα επίθετα με τα οποία χαρακτηριζόταν ο Δίας). (Για τον 'Πανόπτη' και τη συμμετοχή των ελληνικών ενόπλων δυνάμεων σε ασκήσεις κυβερνοπολέμου, βλ., ενδεικτικά, την απάντηση του πρώην ΥΕΘΑ Ευαγ. Βενιζέλου (Φεβρουάριος 2011) σε σχετική Ερώτηση του βουλευτή Παντελή Οικονόμου, στη διεύθυνση http://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/7305902.pdf.)

[189] Σύμφωνα με πληροφορίες που έκαναν την εμφάνισή τους στον τύπο το 2007, το *Ισραήλ* κατάφερε, με ηλεκτρονική επίθεση στα κατάλληλα δίκτυα και εκμετάλλευση των αδυναμιών τους, να θέσει εκτός τροχιάς *τουρκικό δορυφόρο*, ο οποίος χρησιμοποιείται για τη λήψη φωτογραφιών και επικοινωνίες.

[190] Η χώρα αυτή θεωρείται —και όχι άδικα— ως εξαιρετικά επικίνδυνος και ικανός αντίπαλος στον κυβερνοχώρο, με ιδιαίτερα μεγάλες δυνατότητες, τόσο σε προσωπικό όσο και σε μέσα και οικονομικούς πόρους, αλλά και σημαντική εμπειρία και ικανό αριθμό πραγματικών (αν και δύσκολα ανιχνεύσιμων) κυβερνοεπιχειρήσεων.

δομές κυβερνοεπιχειρήσεων (: κατασκευή /δοκιμή /χρήση /διανομή κακόβουλου λογισμικού, 'χαρτογράφηση' και εκμετάλλευση των αδυναμιών δικτύων τρίτων χωρών, δημιουργία και χρησιμοποίηση botnets, αλλοίωση ιστοσελίδων, διανομή μηνυμάτων spam, συλλογή πληροφοριών με 'παράνομη' είσοδο σε δίκτυα και παραμονή σ' αυτά για μεγάλα χρονικά διαστήματα κ.λπ.).[191] Οι ελληνικές ένοπλες δυνάμεις διαθέτουν τη ΔΙΚΥΒ του ΓΕΕΘΑ. Η ΔΙΚΥΒ αρχικά οργανώθηκε ως *Τμήμα* το έτος **2000** και από το 2004 δραστηριοποιείται ως *Διεύθυνση*, με προοπτική να αναβαθμιστεί σε *Διοίκηση* (αξιόλογη 'επίδοση' αν υπολογίσει κανείς ότι το πρώτο επίσημο δόγμα κυβερνοπολέμου των Η.Π.Α. εμφανίστηκε το έτος 1998).[192]

Από την άλλη πλευρά αρκετές χώρες έχουν ήδη εκφράσει με διάφορους τρόπους (: δηλώσεις πολιτικών αξιωματούχων & στρατιωτικών ηγητόρων, έκδοση κειμένων κανονισμών & δογμάτων κυβερνοάμυνας ή κυβερνοπολέμου, κ.λπ.) την πεποίθησή τους —και συγχρόνως την άποψή τους από νομική σκοπιά— ότι η άσκηση βίας στον κυβερνοχώρο —ανάλογα με τις περιστάσεις— συνιστά είδος χρήσης βίας και ένοπλης επίθεσης.[193] Ο *Roscini* (σελ. 108, 109) επ' αυτού μνημονεύει τα εξής : Στο διακλαδικό πρόγραμμα 'Joint Vision 2020' των ενόπλων δυνάμεων των *Η.Π.Α*. ρητά αναφέρεται η χρήση όπλων μη-κινητικής ενέργειας για τη διεξαγωγή πληροφοριακών επιχειρήσεων,[194] ενώ η Εθνική Στρατιωτική Στρατηγική τους του έτους 2004 κάνει λόγο για 'όπλα μαζικών επιπτώσεων' (weapons of mass effect (sic)), των οποίων η λειτουργία βασίζεται περισσότερο στις καταστροφικές *επιπτώσεις* (γενικότερα) παρά στα καταστροφικά αποτελέσματα από την απελευθέρωση κινητικής ενέργειας, και αναφέρει ως παράδειγμα κυβερνοεπιθέσεις σε εμπορικά πληροφορικά συστήματα των

---

[191] Το έτος **2008**, για παράδειγμα, η κ α τ ά τ α ξ η των χωρών διεθνώς με κριτήριο την εκδήλωση πραγματικών 'επιθετικών δραστηριοτήτων' στον κυβερνοχώρο, είχε ως εξής : 1. Η.Π.Α., 2. Κίνα, 3. Γερμανία, 4. Ηνωμένο Βασίλειο, 5. Βραζιλία, 6. Ισπανία, 7. Ιταλία, 8. Γαλλία, 9. Τουρκία και 10. Πολωνία (το έτος 2009 η Τουρκία βρέθηκε στην 3η θέση και η εκτίμηση για το 2010 ήταν ότι θα βρεθεί στην πρώτη θέση). (Πηγή : internet, με στοιχεία που συλλέγει και επεξεργάζεται η εταιρεία λογισμικού Symantec. Παρόμοια στοιχεία, αλλά και στατιστικές αναλύσεις, διαθέτουν όλες οι μεγάλες εταιρείες λογισμικού και ιδίως οι εταιρείες που κατασκευάζουν λογισμικό προστασίας από κακόβουλες επεμβάσεις σε η/υ και δίκτυα.)

[192] Για τη ΔΙΚΥΒ του ΓΕΕΘΑ, αντί άλλων, βλ. την απάντηση του πρώην ΥΕΘΑ Ευαγ. Βενιζέλου (Φεβρουάριος 2011) σε σχετική Ερώτηση του βουλευτή Παντελή Οικονόμου, στη διεύθυνση http://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/7305902.pdf.
Ορισμένες πληροφορίες για τη ΔΙΚΥΒ αναρτώνται επίσης, κατά καιρούς, στις επίσημες ιστοσελίδες του ΓΕΕΘΑ και του ΥΠ.ΕΘ.Α.

[193] Ιδιαίτερη σημασία έχει η πρακτική των πολιτικά και οικονομικά ισχυρών χωρών, καθώς και των χωρών που διαθέτουν τις σχετικές δυνατότητες και την τεχνολογία, όπως έγινε κατά τη διάρκεια του 20ού αιώνα με το δίκαιο του διαστήματος, το θεσμό της υφαλοκρηπίδας κ.λπ.

[194] Για την έννοια των πληροφοριακών επιχειρήσεων, βλ. παραπάνω στο κείμενο, *τμήμα II*.

Η.Π.Α. ή σε δίκτυα μεταφορών·[195] επίσης ο πρόεδρος Β. *Obama*, κατά την ομιλία του με την ευκαιρία της έναρξης λειτουργίας του νέου Γραφείου Κυβερνοασφαλείας του Λευκού Οίκου, αξιολόγησε τις κυβερνο-επιθέσεις σε στρατιωτικά δίκτυα και δίκτυα του υπουργείου άμυνας, ως "weapon of mass disruption". — Ομοίως, ανώτατος *Βρετανός* πολιτικός αξιωματούχος δήλωσε πρόσφατα (2009), για παράδειγμα, ότι μία κυβερνοεπίθεση που θα αχρήστευε μία μονάδα παραγωγής ενέργειας θα συνιστούσε πράξη πολέμου, ο δε Υπουργός Άμυνας της *Εσθονίας*, κατά την Κοινοβουλευτική Σύνοδο του ΝΑΤΟ του 2010, δήλωσε ότι ο αποκλεισμός μίας χώρας στον κυβερνοχώρο ισοδυναμεί, με ναυτικό αποκλεισμό (naval blockade).[196] — Η *Ρωσική Ομοσπονδία* υποστηρίζει εδώ και καιρό τη θέση ότι θα πρέπει να υπογραφεί μία συνθήκη 'αφοπλισμού' για τον κυβερνοχώρο, η οποία θα απαγορεύει την ανάπτυξη, παραγωγή και χρήση ορισμένων ιδιαίτερα επικίνδυνων όπλων του πληροφοριακού πολέμου· κατά την άποψη της Ρωσικής Ομοσπονδίας, επίσης, τα όπλα του πληροφοριακού πολέμου μπορεί να έχουν καταστροφικές συνέπειες ευθέως συγκρίσιμες με τις συνέπειες των όπλων μαζικής καταστροφής (sic)[197] και άρα η εκδήλωση 'πληροφορικού πολέμου' εναντίον της Ρωσικής Ομοσπονδίας ή των ενόπλων δυνάμεων αυτής δεν πρόκειται να αντιμετωπιστεί (από τη Ρωσική Ομοσπονδία) απλά ως μη-στρατιωτική φάση μίας ενδεχόμενης σύγκρουσης, είτε προκαλεί απώλειες είτε όχι(!)

Ήδη από το 1998 η Ρωσική Ομοσπονδία έχει θέσει στα Η.Ε. το ζήτημα της σύναψης μίας διεθνούς συμφωνίας έλεγχου των 'κυβερνο-όπλων' και έχει προτείνει σε διάφορες περιστάσεις συγκεκριμένες ρυθμίσεις, ως περιεχόμενο μίας τέτοιας

---

[195] Στην κινηματογραφική ταινία του 2007 'Die Hard 4.0' του Hollywood (παραγωγή της 20th Century Fox Film Corp.), το σενάριο —αν και δεν αποφεύγει αρκετές υπερβολές— εξιστορεί μία ιδιαίτερα σκληρή και εκτεταμένη κυβερνοεπίθεση στις κρίσιμες υποδομές των Η.Π.Α. από ομάδα hackers (: δίκτυο η/υ του FBI, χρηματιστήριο και τραπεζικό σύστημα, δίκτυα διανομής ηλεκτρικού ρεύματος, δορυφορικές επικοινωνίες, δίκτυα κινητών τηλεφώνων, εναέρια κυκλοφορία, σύστημα διαχείρισης οδικής κυκλοφορίας κ.λπ.). *Η πραγματικότητα δεν απέχει όμως και τόσο πολύ από τα σενάρια :* τον Αύγουστο του 2003 ένα 'ηλεκτρονικό σκουλήκι' (το ' W 3 2 S u s s e r ' worm) που είχε εισέλθει πριν από δύο μήνες στο σύστημα παρακολούθησης και κατανομής φορτίων εργοστασίου παραγωγής ενέργειας στο Ohio των Η.Π.Α., από το προσωπικό laptop ενός τεχνικού (κατά παράβαση, βέβαια, των κανόνων ασφαλείας), προκάλεσε *γενικευμένο blackout* σε επτά πολιτείες της βορειοανατολικής ακτής των Η.Π.Α. και στο Οντάριο του Καναδά· αυτό είχε ως αποτέλεσμα ζημίες της τάξης των επτά εκατομμυρίων δολαρίων, επηρέασε τις υποδομές ενέργειες, ύδρευσης, μεταφορών κ.λπ. και έγινε η αφορμή για τη διάπραξη εκτεταμένων λεηλασιών και πλήθους ληστειών…

[196] Οι αποκλεισμοί, ως γνωστόν, αναφέρονται ως ένα από τα παραδείγματα 'επίθεσης' στην Απόφαση A/RES/3314 (XXIX) της Γ.Σ. του Ο.Η.Ε. της 14ης Δεκεμβρίου 1974, αλλά (πλέον) και στο άρθρο 8*bis* του αναθεωρημένου Καταστατικού του ICC.

[197] Επιστολή με ημερομηνία 23 Σεπ. 1998 του Μόνιμου Εκπροσώπου της Ρωσικής Ομοσπονδίας στα Ηνωμένα Έθνη προς τον Γ.Γ./ΟΗΕ, διαθέσιμη στην ιστοσελίδα http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/53/3&Lang=E (τελευταία πρόσβαση : 07 Ιουνίου 2010). Αναφέρεται από τον Vatis, σελ. 221.

συμφωνίας·[198] προκάλεσε, μάλιστα την έκδοση μίας Απόφασης της Γ.Σ. του 2000 στην οποία διατυπώθηκε έκκληση προς τα κράτη – μέλη να λάβουν υπόψη τους "existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field" και να εξετάσουν "international concepts aimed at strengthening the security of global information and telecommunications systems."[199] Αντίθετα, οι Η.Π.Α. ήταν μέχρι πρόσφατα κάθετα αντίθετες ως προς αυτή την προοπτική και επεδίωκαν, στον αντίποδα, τη διευθέτηση των αναφυομένων περιπτώσεων με την εφαρμογή του (εσωτερικού) ποινικού δικαίου των χωρών και την εντατικοποίηση και διεύρυνση των διακρατικών συνεργασιών για τη συλλογή στοιχείων, εντοπισμό των δραστών, ανταλλαγή πληροφοριών για την τεχνική των επιθέσεων κ.λπ.. Προς αυτή την κατεύθυνση, οι Η.Π.Α. πρωτοστάτησαν στη σύναψη της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Council of Europe Convention on Cybercrime)[200], παρ' όλο που κατά τη διαπραγμάτευση είχαν το *status* παρατηρητή, και ακολούθως υπέγραψαν, κύρωσαν και έθεσαν σ' εφαρμογή τη Σύμβαση αυτή.[201] Από το τέλος του 2009 παρατηρείται μία προσέγγιση Η.Π.Α. – Ρωσικής Ομοσπονδίας στο ζήτημα και η κυβέρνηση B. Obama συμφώνησε με τη Ρωσική πλευρά την έναρξη συνομιλιών για την κυβερνο-ασφάλεια στην Επιτροπή Αφοπλισμού & Διεθνούς Ασφαλείας των Η.Ε. (U.N. Disarmament & International Security Committee)· ωστόσο είναι ελάχιστα πιθανό οι Η.Π.Α. να συμφωνήσουν στο ορατό μέλλον σε οποιοδήποτε συμβατικό κείμενο το οποίο θα απαγορεύει ή θα περιορίζει (ή έστω θα ορίζει…) την επιθετική χρήση 'κυβερνο-όπλων'.[202]

---

[198] Το 2008, μάλιστα, προτάθηκε από ανώτατο αξιωματούχο της Ρωσικής Ομοσπονδίας η σύναψη συμφωνίας που θα απαγορεύει την εισαγωγή κακόβουλου λογισμικού στα υπολογιστικά συστήματα μίας χώρας με σκοπό την ενεργοποίησή του σε δεδομένη στιγμή στο μέλλον, σε περίπτωση εχθροπραξιών (η πρόταση αναφέρεται, όπως θα έχει γίνει κατανοητό, για λογισμικό τύπου 'λογικής' ή 'χρονικής' βόμβας). – Αναφέρεται από τον Vatis, σελ. 222.

[199] U.N. G.A. Resolution 55/28, *Developments in the field of information and telecommunications in the context of international security* (November 20, 2000).

[200] CETS No 185, σε ισχύ από 01 Ιουλίου 2004 (http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm). Η Σύμβαση αυτή αποσκοπεί: (α) στην εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των χωρών αναφορικά με το *κυβερνοέγκλημα* (και όχι, φυσικά, αναφορικά με την διακρατική βία στον κυβερνοχώρο), (β) στη βελτίωση των δυνατοτήτων των χωρών στη διερεύνηση τέτοιων εγκλημάτων και (γ) στην αύξηση του επιπέδου διακρατικής συνεργασίας σε θέματα κυβερνοεγκλημάτων. Απαιτεί από τα συμβαλλόμενα μέρη, μεταξύ άλλων, να λάβουν όλα τα αναγκαία νομοθετικά και λοιπά μέτρα, προκειμένου να ποινικοποιήσουν στην εσωτερική τους νομοθεσία ορισμένες συμπεριφορές που περιγράφονται λεπτομερειακά στο κείμενο της Σύμβασης.

[201] Για τις Η.Π.Α. η Σύμβαση ισχύει από 01 Ιαν. 2007 (την κύρωσαν στις 29 Σεπ. 2006). Αντίθετα η Ελλάδα έχει απλώς υπογράψει τη Σύμβαση αυτή (23 Νοε. 2001) και μέχρι σήμερα δεν την έχει κυρώσει ούτε επικυρώσει.

[202] Vatis, σελ. 222.

> Είναι χαρακτηριστικό, επίσης, ότι στο επίσημο ανακοινωθέν της συνόδου κορυφής του NATO του έτους 2010 στη Λισσαβόνα, περιλήφθηκαν και τα ακόλουθα : "*Cyber threats* are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account *the cyber dimension of modern conflicts* in NATO's doctrine and improve its capabilities to detect, assess, prevent, *defend* and recover in case of a *cyber attack* against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability… to Full Operational Capability… by 2012… To address the security risks emanating from cyberspace, we will work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth *cyber defence policy* by June 2011 and to prepare an action plan for its implementation." (Η έμφαση δική μας.)

De lege lata τα ακρότατα όρια των όρων 'force' και 'armed attack' μπορούν μεν να 'στεγάσουν' τις σύγχρονες εξελίξεις στα όπλα και τις μεθόδους σύγκρουσης και καταναγκασμού στις διακρατικές σχέσεις (εάν ερμηνευθούν με τρόπο ευρύ και σύμφωνο με το σκοπό των συντακτών του Χάρτη και υπό το πρίσμα της σημερινής εξέλιξης της τεχνολογίας και των γεωπολιτικών δεδομένων), αλλά δεν είναι δυνατόν να διαρραγούν, διότι αυτό που θα προκύψει θα είναι ένα νομικό *aliud*. Ήδη όμως έχουν αρχίσει να εμφανίζονται τάσεις διάρρηξης των ορίων αυτών και ερμηνευτικές προσεγγίσεις που μόνο *de lege ferenda* θα μπορούσαν να αποτελέσουν αντικείμενο εξέτασης. Ο *Schmitt* (2010, σελ. 177) αναφέρει, για παράδειγμα, ότι σε έκθεση του 2009 του National Research Council των Η.Π.Α.[203] μνημονεύονται ως παραδείγματα 'ένοπλης επίθεσης', αφενός μεν οι κυβερνοεπιθέσεις στα πληροφοριακά συστήματα που ελέγχουν τις [κρίσιμες] υποδομές ενός κράτους, είτε προκαλούν μεγάλου εύρους απώλειες ζωών και υλικές ζημίες *είτε όχι*, αφετέρου δε οι συνεχείς και επαναλαμβανόμενες κυβερνοεπιθέσεις στα δίκτυα χρηματιστηρίων που έχουν ως αποτέλεσμα [μόνο] τη *διατάραξη των συναλλαγών* για μεγάλο χρονικό διάστημα

---

[203] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* σελ. 254 /255 (Owens William, Dam Kenneth & Lin Herbert eds., National Academies Press, 2009).

(εβδομάδων ή και ημερών ακόμη).[204] Η αξιολόγηση δηλώσεων και προσεγγίσεων κυβερνήσεων και αξιωματούχων (πολιτικών & στρατιωτικών) διαφόρων χωρών και ιδίως εκείνων που είναι ηλεκτρονικά και δικτυακά προηγμένες, δείχνει ότι η τάση αυτή θα εξακολουθήσει να ισχυροποιείται στο άμεσο μέλλον και ότι περιστατικά σαν κι' αυτό της Εσθονίας του 2007 δεν θα αξιολογούνται πλέον από τα κράτη ως απλή παραβίαση της αρχής της μη επέμβασης.[205]

Ωστόσο, η προοπτική κατάρτισης και θέσης σε ισχύ ενός συμβατικού κειμένου που θα διευρύνει κατάλληλα τα όρια των εννοιών της 'χρήσης βίας' και της 'ένοπλης επίθεσης' ειδικά για τον κυβερνοχώρο ή /και θα απαγορεύει ή θα θέτει περιορισμούς σε ορισμένα ηλεκτρονικά όπλα,[206] είναι εξαιρετικά ασθενής έως απίθανη, τόσο για το άμεσο όσο και για το απώτερο μέλλον και οι προσπάθειες για την *infra legem* ερμηνεία του υπάρχοντος πλαισίου θα συνεχιστούν.[207] Αυτό διότι τα ηλεκτρονικά και δικτυακά προηγμένα κράτη είναι μεν περισσότερο ευάλωτα σε κυβερνοεπιθέσεις, αλλά, συγχρόνως, είναι και εξαιρετικά ικανά και αποτελεσματικά στη διεξαγωγή τους (και ιδίως στη διεξαγωγή επιχειρήσεων CNE), με αποτέλεσμα σ' αυτή τη φάση η *ασάφεια* του νομικού πλαισίου να εξυπηρετεί τη δική τους θεώρηση των πραγμάτων.

> Στο σημείο αυτό αξίζει να αναφέρουμε μία εύστοχη παρατήρηση της *Higgins* (σελ. 252) : "…if it is felt that the erstwhile articulation of norms no longer serves community interests, then those norms can properly be subjected to processes for change. *The normal processes for change will include non-compliance.* … But there *is* a distinction between non-compliance, on the one hand, and interpretation *infra legem* to achieve certain outcomes, on the other. …We should, moreover, be very sure that the norms as presently articulated are so

---

[204] Το σχόλιο του *Schmitt* επί των παραδειγμάτων αυτών έχει ως εξής : "[i]n other words the [Council] report has misconstrued the law, ***but accurately identified probable State behavior***" (η έμφαση δική μας).

[205] Μπορούμε να υποθέσουμε βάσιμα ότι σημαντικό ρόλο σ' αυτό διαδραματίζει και το γεγονός ότι οι δικτυακά και ηλεκτρονικά προηγμένες χώρες είναι και οι περισσότερο ευάλωτες σε επιθέσεις προερχόμενες από τον κυβερνοχώρο. Ενδεικτικά αναφέρεται ότι το 90 – 95% των επικοινωνιών των ενόπλων δυνάμεων και των υπηρεσιών ασφαλείας των Η.Π.Α., εξυπηρετείται από ιδιωτικά δίκτυα συνδεδεμένα με το internet (πηγή : http://www.npr.org/templates/story/story.php?storyId=130023318, τελευταία πρόσβαση : 14 Οκτ. 2011). Για το λόγο αυτό ***οι Η.Π.Α. έχουν ήδη ξεκινήσει την εκ του μηδενός φυσική κατασκευή νέων δικτύων, τα οποία δεν θα έχουν οιουδήποτε είδους σχέση ή σύνδεση με το internet*-!**

[206] Βλ. γι' αυτά παραπάνω, ιδίως στο *τμήμα ΙΙ*.

[207] Ελάχιστοι, πιστεύω, θα έχουν αμφιβολίες περί του ότι μία 'ψηφιακή 11η Σεπτεμβρίου' κατά των Η.Π.Α., για παράδειγμα, δεν θα προκαλέσει απάντηση σαν κι' αυτή που δόθηκε στο Αφγανιστάν, *ανεξάρτητα* από το εύρος των υλικών ζημιών και των απωλειών σε ζωές (υπό την αυτονόητη προϋπόθεση, βέβαια, ότι ο επιτιθέμενος είναι γνωστός ή έστω υπάρχουν 'βάσιμες υποψίες' γι' αυτόν…).

irredeemably inappropriate to the factual realities that we do indeed wish to undermine them. …" (Η έμφαση δική μας.)

Κατά την άποψή μας οι διατάξεις των άρθρων 2(4) και 51 του Χάρτη και το διεθνές εθιμικό δίκαιο που ισχύει σήμερα αναφορικά με το δικαίωμα αυτοάμυνας, μπορούν να λειτουργήσουν ικανοποιητικά και στα ζητήματα άσκησης βίας και εκδήλωσης 'ένοπλων επιθέσεων' στον κυβερνοχώρο και δεν έχουν καταστεί *ακόμη* 'ανεπανόρθωτα ακατάλληλες' (όπως επισημαίνεται στην παραπάνω παρατήρηση της *Higgins*)· η λύση αυτή τη στιγμή δεν πιστεύουμε ότι είναι η *infra legem* (και κατά το δοκούν) ερμηνεία των διατάξεων αυτών και η ελάττωση ύψους του ''κατωφλιού'' που απαιτείται κάθε φορά για τη διαπίστωση 'βίας' και 'ένοπλης επίθεσης'. Εκείνο που απαιτείται σε πρώτη φάση και άμεσα, είναι η θωράκιση του (ιδιωτικού) internet με ένα (επιπλέον) *minimum* κανόνων και τεχνολογιών ασφαλείας, χωρίς να θίγεται το δικαίωμα του κάθε 'πολίτη της ανθρωπότητας' για την πλήρη απόλαυση του κυβερνοχώρου ως τμήματος της 'παγκόσμιας κληρονομιάς της ανθρωπότητας', και η περισσότερο αποφασιστική και ρωμαλέα εφαρμογή των υφισταμένων διατάξεων· πράγματι, στο περιστατικό της Εσθονίας του 2007, για παράδειγμα, όπως και σε άλλα παρόμοια που προηγήθηκαν ή ακολούθησαν,[208] θα μπορούσε, εάν όχι να είχε εκδοθεί Απόφαση του Σ.Α. που να κρίνει την κατάσταση ως 'threat to the peace, [or] breach of peach or act of aggression' και να διατάσσει κατάλληλα μέτρα,[209] τουλάχιστον να έχει υποβληθεί σχετική πρόταση στο όργανο αυτό, ή έστω να έχουν ασχοληθεί με κάποιο τρόπο τα Η.Ε. με το ζήτημα.[210]

Όπως παρατηρεί ο *Martin Libicki*,[211] η συμβατική απαγόρευση της άσκησης βίας στον κυβερνοχώρο ή της ανάπτυξης και χρήσης όπλων κυβερνοεπιχειρήσεων, θα πρέπει να θεωρείται ανέφικτη· αντίθετα —και κατ' αρχήν— στη σφαίρα του εφικτού ίσως βρίσκεται η σύναψη ορισμένων συμβατικών κανόνων που θα καθιστούν περισσότερο δύσκολη την εκτέλεση κάποιων κατηγοριών κυβερνοεπιχειρήσεων (και

[208] Ο Roscini, σελ. 88 – 90, για παράδειγμα, αναφέρει ότι [εκτός από την περίπτωση της Εσθονίας] άξιες λόγου κυβερνοεπιθέσεις έχουν εκδηλωθεί κατά των Η.Π.Α., του Ηνωμένου Βασιλείου, της Ταϊβάν, της Ν. Κορέας, της Λιθουανίας, του Κιργιστάν, της Ελβετίας, του Μαυροβουνίου, του Ισραήλ κ.λπ. — Οι 'κυβερνοεπιθέσεις' κατά κρατών, Οργανισμών και εταιρειών, είναι πλέον εδώ και χρόνια *καθημερινό* φαινόμενο.

[209] Για τη λήψη γενικών μέτρων προς διακοπή των επιθέσεων και την αποφυγή παρομοίων καταστάσεων στο μέλλον, δεν θα απαιτείτο, σ' εκείνη τη φάση, να είναι γνωστοί οι δράστες των επιθέσεων και οι διαδρομές των ηλεκτρονικών τους ιχνών.

[210] Ο Ο.Η.Ε. σιώπησε στο ζήτημα των κυβερνοεπιθέσεων εναντίον της Εσθονίας (Shackelford, 237).

[211] Libicki, RAND, σελ. 199 et seq.

ευκολότερη και ταχύτερη τη συλλογή αποδείξεων γι' αυτές). Ο συγγραφέας επισημαίνει επ' αυτών τα ακόλουθα : Με δεδομένο ότι τα κυβερνο-όπλα μπορούν να αναπαράγονται και να διαδίδονται ταχύτατα και ανέξοδα (αφού είναι 'όπλα' λογισμικού), η απαγόρευσή τους είναι ανέφικτη.[212] — Ομοίως και η απαγόρευση των *μεθόδων* κυβερνο-επιχειρήσεων είναι τόσο εφικτή όσο και η απαγόρευση (για παράδειγμα)… των ανώτερων μαθηματικών-![213] Το αυτό ισχύει και για την ενδεχόμενη προσπάθεια απαγόρευσης διάδοσης των γνώσεων αναφορικά με την αποκάλυψη και εκμετάλλευση των τρωτοτήτων (vulnerabilities) των η/υ και των δικτύων. — Η απαγόρευση κατασκευής επιθετικού λογισμικού (attack code /malicious code) είναι επίσης αδύνατη, αφού αυτού του είδους το λογισμικό έχει και πλήθος 'νόμιμων' χρήσεων, όπως η ανάπτυξη ηλεκτρονικής άμυνας για την προστασία από κακόβουλες επιθέσεις κρατικών και μη-κρατικών οντοτήτων και ιδιωτών, καθώς και η διενέργεια επιχειρήσεων CNE και 'κυβερνο-κατασκοπείας' (η οποία, όπως έχουμε ιδεί, προς το παρόν είναι κατ' αρχήν νόμιμη δραστηριότητα από πλευράς διεθνούς δικαίου). Εξάλλου και από τεχνική άποψη, η εξεύρεση του κακόβουλου κώδικα που τυχόν θα έχει απαγορευθεί συμβατικά, είναι ουσιαστικά αδύνατη.[214] — Περισσότερο εφικτή φαντάζει μία συμφωνία στην οποία θα ορίζεται με κάποιο τρόπο η έννοια της κυβερνο-επίθεσης (όχι με καθαρά νομικά κριτήρια) και θα αναλαμβάνονται υποχρεώσεις συνδρομής στην έρευνα περιστατικών και παροχής στοιχείων, θα συμφωνείται η μη χρήση κάποιων *ειδών* κακόβουλου κώδικα, τουλάχιστον στις επιχειρήσεις κυβερνο-κατασκοπείας, θα αναλαμβάνονται υποχρεώσεις κοινοποίησης κάποιων κρίσιμων τεχνολογιών υλισμικού και λογισμικού, θα συμφωνείται η αναβάθμιση της ασφάλειας των πρωτοκόλλων επικοινωνίας στο internet κ.λπ.

Και ο *Shackelford* (σελ. 246 et seq., 250 et seq.) έχει την άποψη ότι περισσότερο εφικτό είναι ένα νέο συμβατικό πλαίσιο το οποίο θα προσπαθήσει να αυξήσει τα επίπεδα ασφάλειας στον κυβερνοχώρο, με την αντιμετώπιση του πεδίου αυτού ως οιονεί αντικειμένου παγκόσμιας κληρονομιάς της ανθρωπότητας, και την υιοθέτηση λύσεων ανάλογων με αυτές που έχουν υιοθετηθεί, για παράδειγμα, από την

---

[212] Και ο Shackelford, 197, παρατηρεί ότι το 'non-proliferation' μοντέλο για τα πυρηνικά όπλα δεν μπορεί να λειτουργήσει εδώ επειδή η τεχνολογία διεξαγωγής 'πληροφοριακών επιχειρήσεων' είναι ήδη εξαιρετικά διαδεδομένη.

[213] Η απαγόρευση αυτή ισοδυναμεί με την απαγόρευση της διάδοσης πληροφοριών του τύπου "how-to", η οποία ως ιδέα είναι αστεία.

[214] Όπως παρατηρεί ο Libicki (op. cit.), εάν ήταν δυνατόν να εφαρμοστεί μία τέτοια απαγόρευση, τότε τα κράτη θα ήταν δυνατόν να απαγορεύσουν και να περιορίσουν και τη διαφθορά˙ τέτοιος κόσμος δεν υπάρχει…

UNCLOS για το διεθνή βυθό (: προτείνει τη δημιουργία ενός "international body with the power to regulate cyber security reminiscent of the United Nations Commission on the Limits of the Continental Shelf ('CLCS') under UNCLOS"), ή ανάλογων με το συμβατικό πλαίσιο για το διάστημα (: απαγόρευση της τοποθέτησης σε τροχιά πυρηνικών όπλων), ή για την Ανταρκτική (: ειδικό καθεστώς, ασύμβατο με κάθε εθνική κυριαρχία και απαγόρευση *όλων* των στρατιωτικών δραστηριοτήτων). Θεωρεί επίσης περισσότερο εφικτή την αύξηση της ασφάλειας από πλευράς τεχνολογίας, την υψηλή εποπτεία της τεχνολογίας που χρησιμοποιείται και την συμφωνία αποχής από κάποιες δραστηριότητες, αντί για την απαγόρευση κάποιων ηλεκτρονικών όπλων και μεθόδων που είναι ουσιαστικά ανέφικτη.

V. Συμπεράσματα

1. Ο 'κυβερνοπόλεμος', με την καθημερινή έννοια του όρου, είναι πλέον μία πραγματικότητα στον εξαιρετικά δικτυωμένο πλανήτη στον οποίο ζούμε και στην ηλεκτρονική και δικτυακή μας καθημερινότητα· *έχει ήδη αρκετά μεγάλο παρελθόν, έχει εντυπωσιακό παρόν και ανησυχητικό μέλλον*. Οι χώρες που έχουν τη σχετική τεχνογνωσία και τα μέσα, ξεπερνούν, όπως είδαμε, τις εκατόν είκοσι (120), ενώ τέτοιες δυνατότητες έχουν πλήθος μη-κρατικών οντοτήτων και εκατομμύρια ιδιωτών. Οι 'κυβερνοεπιθέσεις' σε καθημερινό επίπεδο είναι χιλιάδες·[215] οι επιθέσεις αυτές, βέβαια, είναι στη μεγάλη πλειοψηφία τους επιθέσεις τύπου CNE, ενώ από τις υπόλοιπες, ελάχιστες —τουλάχιστον εξ όσων γνωρίζουμε— θα μπορούσαν να αξιολογηθούν ως επιπέδου 'χρήσης βίας'. Ωστόσο, η τεχνολογία και η τεχνογνωσία της καταστροφής υπάρχει και η ανθρωπότητα αυτή τη στιγμή ουσιαστικά είναι σαν να παρατηρεί 'δοκιμές πυρηνικών όπλων' στον κυβερνοχώρο, χωρίς, προς το παρόν, άξιες λόγου ανθρώπινες απώλειες *αλλά με σημαντικές υλικές ζημίες*· πράγματι, οι ζημίες που υφίστανται κατ' έτος από τις 'επιθέσεις' τα δίκτυα των ενόπλων δυνάμεων, των κρατικών φορέων και οργανισμών, αλλά και διαφόρων εταιρειών, ανέρχονται σε δεκάδες ή και εκατοντάδες εκατομμύρια δολάρια. Το μέλλον πρέπει μάλλον να μας ανησυχεί και τα περιστατικά σαν κι' αυτό της Εσθονίας του 2007 και της Γεωργίας του 2008 να μας προβληματίζουν σοβαρά.

[215] Υπολογίζεται, για παράδειγμα, ότι τα δίκτυα των ενόπλων δυνάμεων των Η.Π.Α. δέχονται καθημερινά περίπου 350 'σοβαρές' επιθέσεις.

2. Τα άρθρα 2(4) και 51 και το σύστημα το οποίο με αυτά προσπάθησαν να θέσουν σε εφαρμογή οι συντάκτες του Χάρτη του Ο.Η.Ε., 'ταλαιπωρήθηκαν' αρκετά από τη θέση τους σε ισχύ μέχρι σήμερα και ταλαιπωρούνται ακόμη, επειδή, όντας βασισμένα σε μια συγκεκριμένη φιλοσοφία αποφυγής μεγάλων διακρατικών πολεμικών συγκρούσεων, δυσκολεύτηκαν εξαιρετικά να αντιμετωπίσουν τις νέες μορφές βίας στις διεθνείς σχέσεις που εμφανίστηκαν στο δεύτερο μισό του 20ού αιώνα, όπως οι πολλές μικρής έντασης στρατιωτικές συγκρούσεις,[216] η δράση των λεγομένων 'rogue states', η δράση μη-κρατικών οντοτήτων για λογαριασμό ή επ' ωφελεία κρατών, η διεθνής τρομοκρατία, η χρήση βίας στα πλαίσια 'ανθρωπιστικών επεμβάσεων' του τύπου της επέμβασης του ΝΑΤΟ στο Κόσοβο κ.λπ.

Οι CNAs πιέζουν ακόμη περισσότερο τα όρια και την παραδοσιακή ερμηνεία των άρθρων αυτών : Τα ηλεκτρονικά όπλα και η σχετική τεχνογνωσία είναι διαθέσιμα σε εκατομμύρια ιδιώτες και σε χιλιάδες κρατικές υπηρεσίες, αλλά και σε πλήθος μη-κρατικών οντοτήτων. — Χιλιάδες ηλεκτρονικές επιθέσεις μικρής ή μεγαλύτερης έντασης και εμβέλειας εκδηλώνονται κάθε χρόνο εναντίον κυβερνητικών δικτύων και συστημάτων, ένα καθόλου ευκαταφρόνητο ποσοστό από τις οποίες δεν είναι απλές επιχειρήσεις CNE˙ οι επιθέσεις αυτές φέρνουν και πάλι στο προσκήνιο το ζήτημα των χαμηλής έντασης συγκρούσεων. — Τα ίχνη και οι διαδρομές των επιθέσεων αποκρύπτονται εξαιρετικά εύκολα και αποτελεσματικά και η αποκάλυψη των υπευθύνων και η συλλογή αποδείξεων, εάν δεν είναι αδύνατες, είναι εξαιρετικά δύσκολες και χρονοβόρες. — Η επικινδυνότητα μίας CNA μπορεί να μην γίνει αντιληπτή από την αρχή˙ η 'επιθετική δραστηριότητα μπορεί να ξεκινήσει με χαμηλή ένταση και σταδιακά να κορυφώνεται σε βάθος χρόνου, όταν δεν γίνει φανερή η πλήρης έκτασή της και τα εν δυνάμει αποτελέσματά της, μπορεί να είναι αργά και η αντιμετώπισή της δύσκολη και μεγάλου κόστους.

3. Τα 'ηλεκτρονικά όπλα' που απαριθμήθηκαν παραπάνω στο *τμήμα II* και των οποίων η λειτουργία και οι συνέπειες στην πράξη παρουσιάστηκαν στο *τμήμα IV*, <u>*είναι*</u> 'όπλα' σαν κι αυτά που είχαν στο μυαλό τους οι συντάκτες των άρθρων 2(4) και 51 του Χάρτη των Η.Ε., αφού και αυτά, ανάλογα με τον τρόπο χρήσης τους —τόσο *αυτοτελώς* όσο και σε *συνδυασμό* με άλλα, πιο 'κλασσικά' όπλα—, *μπορούν* να

[216] Κυρίως λόγω της απειλής ενός πυρηνικού ολοκαυτώματος που απέτρεπε επί δεκαετίες τις μεγαλύτερες συγκρούσεις (βλ., π.χ., McCoubrey H. & White N.D., *International Law and Armed Conflict*, 1992, σελ. 32 /33).

προκαλέσουν ζημίες, απώλειες ζωών και τραυματισμούς στο φυσικό /πραγματικό κόσμο, λόγω, ακριβώς, της *ευθείας* και σχεδόν *απόλυτης*, εδώ και καιρό, *εξάρτησης* του κόσμου αυτού από τον εικονικό κυβερνοχώρο. Η χρήση των όπλων αυτών και οι μέθοδοι χρησιμοποίησής τους, *μπορεί* να συνιστούν χρήση βίας και ένοπλη επίθεση, όπως οι έννοιες αυτές γίνονται δεκτές από το γραπτό και εθιμικό *jus ad bellum*, στο στάδιο εξέλιξης που έχει φθάσει σήμερα.

4. Οι διατάξεις των άρθρων 2(4) και 51 και το συναφές διεθνές έθιμο, εξακολουθούν να επιδεικνύουν αξιοθαύμαστη προσαρμοστικότητα και κατ' αρχήν λειτουργούν ακόμη ικανοποιητικά και γι' αυτά τα όπλα και τις μεθόδους άσκησης βίας που δεν υπήρχαν όταν συντάχθηκε ο Χάρτης. Έτσι, όπως αναλύθηκε παραπάνω, μία επίθεση CNA πράγματι *είναι δυνατόν* να έχει τα χαρακτηριστικά της χρήσης (ένοπλης) βίας που απαιτεί το άρθρο 2(4) του Χάρτη, ή ακόμη και της ένοπλης επίθεσης (armed attack), εάν, σ' αυτή την τελευταία περίπτωση, έχει το απαιτούμενο επίπεδο έντασης και συνεπειών (: πρόκληση σημαντικών απωλειών σε έμψυχο και άψυχο υλικό, ανάλογο με αυτό που γίνεται δεκτό ότι απαιτείται για τις επιθέσεις με όπλα 'συμβατικής' τεχνολογίας (κινητικής ενέργειας), ή με άλλα απαγορευμένα και ήδη γνωστά όπλα, όπως τα βιολογικά, τα χημικά, ή ακόμη και τα πυρηνικά.[217] Χρήση βίας και ένοπλη επίθεση μπορεί να συνιστούν και οι CNAs εναντίον των κρίσιμων μη-στρατιωτικών υποδομών ενός κράτους, συμπεριλαμβανομένων και αυτών που δεν αποτελούν κρατική ιδιοκτησία.

5. Ιδιαίτερη προσοχή και σχολαστική μελέτη όλων των δεδομένων απαιτείται για τη *σύνδεση* των CNAs με συγκεκριμένη *πηγή προέλευσης*, επειδή η μέθοδος αυτή διακρατικού καταναγκασμού, λόγω της φύσεώς της αλλά και της φύσεως του ίδιου του κυβερνοχώρου, ενδείκνυται για την απόκρυψη των διαδρομών επίθεσης και των πραγματικών αυτουργών (attribution problems). Στην περίπτωση των CNAs που εκδηλώνονται από μεμονωμένα άτομα ή από μη-κρατικές οντότητες, για την απόδοση και των 'καταλογισμό' των πράξεών τους σε συγκεκριμένο κράτος (προκειμένου, στη συνέχεια, να εφαρμοστούν οι κανόνες περί ευθύνης των κρατών για παράνομες πράξεις των οργάνων τους) ασφαλέστερη είναι η εφαρμογή του κριτηρίου

[217] Όσο και αν φαίνεται απίστευτο ή απίθανο, για παράδειγμα, σύμφωνα με πληροφορίες που έχουν εμφανιστεί κατά καιρούς στον τύπο, οι Η.Π.Α. εξέταζαν κάποια στιγμή σοβαρά τη χρήση στο Αφγανιστάν *τακτικών* πυρηνικών όπλων, δηλαδή πυρηνικών όπλων μικρής σχετικά ισχύος και τοπικά εντοπισμένων αποτελεσμάτων…

του ‘πραγματικού ελέγχου’ που έθεσε το ICJ στην υπόθεση Νικαράγουα κατά Η.Π.Α. και όχι το κριτήριο του ‘γενικού ελέγχου’ του ICTY στην υπόθεση Tadić.

6. Το κράτος – στόχος μίας επίθεσης CNA μπορεί να θέσει το ζήτημα ενώπιον του Σ.Α. ή να προσφύγει ενώπιον διεθνούς δικαστηρίου, εάν το κράτος – δράστης είναι γνωστό· οι διατάξεις που διέπουν τη λειτουργία του Σ.Α. παρέχουν αρκετές δυνατότητες, οι οποίες όμως δεν έχουν χρησιμοποιηθεί ακόμη —για πολιτικούς λόγους— για τη διευθέτηση των προβλημάτων που ανακύπτουν από τις CNAs και τις CNE στην πράξη. Αρκετοί μελετητές, μάλιστα, θέτουν ήδη και ζήτημα αρμοδιότητας του ICC ως προς το έγκλημα της ‘επίθεσης’ του νέου άρθρου 8*bis* του Καταστατικού του δικαστηρίου αυτού· κατά την άποψή μας (βλ. τις σκέψεις μας επ’ αυτού στο *τμήμα IV.6.*, παραπάνω), μία τέτοια ερμηνεία των νέων άρθρων του Καταστατικού του ICC *είναι* νοητή, ωστόσο η σχετική συζήτηση ουσιαστικά ξεκινάει τώρα και πρέπει να αναμένεται επ’ αυτού ενδιαφέρουσα ανταλλαγή νομικών επιχειρημάτων.

7. Το κράτος – στόχος μπορεί επίσης να προβεί σε πράξεις ανταπόδοσης, καθώς και σε αντίμετρα χωρίς τη χρήση βίας, ή και με τη χρήση βίας εάν η CNA είναι επιπέδου ένοπλης επίθεσης.[218] Επειδή, ωστόσο, οι ιδιαιτερότητες των CNAs πιέζουν το δίκαιο στα όριά του, ορισμένοι μελετητές διατυπώνουν ήδη την άποψη ότι εάν ένα κράτος δεχθεί κυβερνο-επίθεση σαν κι’ αυτή που απαγορεύει το άρθρο 2(4), αλλά της οποίας το επίπεδο δεν φθάνει σ’ αυτό που απαιτεί το άρθρο 51, θα μπορεί, παρ’ όλ’ αυτά, να απαντήσει ‘σε είδος’ με τον ίδιο τρόπο, εφαρμόζοντας ‘αντίμετρα με τη χρήση βίας’· οι απόψεις αυτές, προς το παρόν, δεν γίνονται ευρύτερα δεκτές, κερδίζουν, ωστόσο, σταδιακά έδαφος λόγω, ακριβώς, των προβλημάτων που δημιουργούν οι *καθημερινές* πλέον ‘κυβερνοεπιθέσεις’ σε κρατικά και ιδιωτικά δίκτυα.

8. Εάν η CNA έχει τις προδιαγραφές ένοπλης επίθεσης, το κράτος – στόχος έχει και *δικαίωμα αυτοάμυνας*, με την υποχρέωση, να το ασκήσει τηρώντας τις τρεις θεμελιώδεις αρχές που το διέπουν και το γενικό διεθνές δίκαιο. Εάν, μάλιστα, πληρούνται τα κριτήρια του επεισοδίου ‘Caroline’, δικαίωμα αυτοάμυνας θα υπάρχει και έναντι μίας CNA η οποία δεν αίρεται μέχρι του επιπέδου της ένοπλης επίθεσης

[218] Όπως εκτέθηκε παραπάνω, κατά την άποψή μας στην πράξη είναι τεχνικά εφικτό ακόμη και αυτοτελείς επιθέσεις CNA —δηλαδή CNAs που δεν συνοδεύονται και από τη χρήση ‘κλασσικών’ όπλων κινητικής ενέργειας— να συνιστούν ‘ένοπλη επίθεση’.

αλλά η οποία *αποδεδειγμένα* αποτελεί το προπαρασκευαστικό ή εναρκτήριο στάδιο μίας *επικείμενης* ένοπλης επίθεσης με συμβατικά όπλα και μεθόδους.

9. Η θεωρία και το νομικό κεκτημένο περί αυτοάμυνας φαίνεται ότι λειτουργούν ικανοποιητικά και στις περισσότερες περιπτώσεις CNAs. Πάντως, η φύση, οι ιδιαιτερότητες και τα εξωτικά τεχνικά χαρακτηριστικά των CNAs αναγκάζουν το *jus ad bellum* να φθάσει στα όριά του στην περίπτωση της αυτοάμυνας έναντι επικείμενων επιθέσεων αμιγώς του τύπου των CNAs, αφού, όπως παρατηρείται, το 'ύστατο διαθέσιμο χρονικό πλαίσιο αντίδρασης' μπορεί να αποδειχθεί εξαιρετικά μικρό και ανεπαρκές για να αποτρέψει καταστροφικά αποτελέσματα για το κράτος που δέχεται μια τέτοια επίθεση. Ήδη αρκετές φωνές από την απέναντι πλευρά του Ατλαντικού προτείνουν την άμβλυνση της δογματικότητας των κανόνων της αυτοάμυνας σε τέτοιες περιπτώσεις με γνώμονα ''τον πιο θεμελιώδη και περιεκτικό κανόνα απ' όλους, δηλαδή τη συμμόρφωση προς τις επιταγές της λογικής, υπό το φως των δεδομένων και των ιδιαιτεροτήτων της κάθε συγκεκριμένης περίπτωσης''. Οι θεωρίες αυτές δεν είναι η πρώτη φορά που εμφανίζονται στο χώρο του *jus ad bellum*, γίνονται δε ισχυρότερες όσο η τεχνολογία των όπλων εξελίσσεται…

10. Οι CNAs *χαμηλότερης* έντασης, δηλαδή αυτές οι επιθέσεις που ενώ ξεπερνούν το επίπεδο των απλών επιχειρήσεων CNE ωστόσο δεν προκαλούν (άξιες λόγου) απώλειες ζωών ή πρώτου επιπέδου υλικές ζημίες στον φυσικό κόσμο, δημιουργούν σοβαρό πρόβλημα ερμηνείας στα άρθρα 2(4) και 51, διότι ενώ δεν προκαλούν σε πρώτο επίπεδο ζημιές στον φυσικό κόσμο και απώλειες ζωών, συγχρόνως φαίνεται να έχουν αποτελέσματα που 'θυμίζουν' αποκλεισμό, ή αποτελέσματα επίθεσης με όπλα κινητικής ενέργειας τα οποία (αποτελέσματα), σε κάθε περίπτωση, φαίνεται να ξεπερνούν τον οικονομικό και πολιτικό καταναγκασμό όπως τον γνωρίσαμε μέχρι σήμερα˙ εδώ η θεωρία του είδους και της βαρύτητας των αποτελεσμάτων δεν βοηθά. Σ' αυτό βέβαια συμβάλλει και το γεγονός ότι συνήθως οι CNAs ξεκινούν ως μία ήπια και χαμηλής έντασης δραστηριότητα και κορυφώνονται σταδιακά και σε βάθος χρόνου, όταν δε γίνει φανερή η πλήρης έκτασή τους και τα εν δυνάμει αποτελέσματά τους, η διείσδυση στα συστήματα – στόχος είναι τόσο βαθεία ώστε, η άμυνα είναι επίπονη, χρονοβόρα και ενδεχομένως ανέφικτη. Ήδη, κυρίως στις Η.Π.Α. —οι οποίες λόγω της εξαιρετικά μεγάλης εξάρτησής τους από το internet και τα δίκτυα η/υ είναι συγχρόνως και εξαιρετικά ευάλωτες σε επιθέσεις τύπου CNA—, έχουν

αρχίσει να διατυπώνονται αναλύσεις και *infra legem* προτάσεις για την αναγκαιότητα να χαμηλώσει το 'κατώφλι' των κριτηρίων της ένοπλης επίθεσης, ειδικά στις επιθέσεις κατά δικτύων η/υ.

11. Με δεδομένο ότι αυτή τη στιγμή το συμβατικό (: του Χάρτη των Η.Ε.) και το διεθνές εθιμικό δίκαιο *jus ad bellum* δεν ταυτίζονται απόλυτα —και με δεδομένες τις ιδιαιτερότητες του κυβερνοχώρου ως τεχνητού πεδίου ανθρώπινης αντιπαράθεσης, αλλά και του εξαιρετικά μεγάλου αριθμού CNE και CNAs που εκδηλώνονται παγκοσμίως σε καθημερινή βάση—, εκτιμάται ότι θα συνεχιστούν και στο μέλλον οι πιέσεις και οι *infra legem* ερμηνευτικές προσεγγίσεις, με σκοπό να προκληθούν διαφοροποιήσεις στο ύψος του κατωφλίου των *αποτελεσμάτων* και του *εύρους* της χρήσης βίας που θα απαιτούνται για να έχουμε armed attack, αλλά και των κριτηρίων περί του επικειμένου των επιθέσεων στα δίκτυα η/υ. Προς αυτήν την κατεύθυνση επιδρούν και ορισμένες ιδιομορφίες των όπλων και των μεθόδων που χρησιμοποιούνται για την εκδήλωση CNAs, σε αντίθεση με αρκετά από τα ισχυρά και επίφοβα συμβατικά όπλα[219], αλλά και σε αντίθεση ακόμη και με τα πυρηνικά όπλα :

Τα όπλα των CNAs είναι εξαιρετικά φθηνά και γρήγορα, μπορούν να 'εκτοξευθούν' από οποιοδήποτε σημείο, οι συνέπειές τους εξαπλώνονται ανεξέλεγκτα και είναι δυνατόν να τα αποκτήσει με καταπληκτική ευκολία και με τρόπο μη-ελέγξιμο αόριστος αριθμός προσώπων (ακόμη και άτομα εφηβικής ηλικίας) και ιδίως τρίτοι για λογαριασμό κρατών ή και μη-κρατικών οντοτήτων˙ μπορούν να τα αποκτήσουν και οι τεχνολογικά μη-προηγμένες χώρες, από δε τη χρήση τους κινδυνεύουν περισσότερο οι τεχνολογικά προηγμένες χώρες, διότι τόσο οι στρατιωτικές όσο και οι κρίσιμες κοινωνικές υποδομές τους στηρίζονται σχεδόν αποκλειστικά στη χρήση η/υ και δικτύων˙ τέλος, είναι ιδιαίτερα δύσκολο και χρονοβόρο να εξακριβωθεί η προέλευσή τους και η διαδρομή της δράσης τους, άρα και οι πραγματικά υπεύθυνοι πίσω από τις επιθέσεις, όσο μεγάλης έκτασης και βλαπτικότητας και αν είναι.

12. Αυτή τη στιγμή υπάρχει ήδη ανιχνεύσιμη, πλέον, πρακτική κρατών και διεθνών οργανισμών περί του ότι βία στις διακρατικές σχέσεις μπορεί να ασκηθεί και με τη μορφή των CNAs, δηλαδή με χρήση όπλων και μεθόδων καταναγκασμού στον κυβερνοχώρο, όπως αυτά που περιγράφονται στο *τμήμα ΙΙ*, παραπάνω˙ η δημιουργία

[219] Διηπειρωτικοί πύραυλοι, βόμβες κενού (σαν κι' αυτές που χρησιμοποιήθηκαν στο Αφγανιστάν), όπλα διασποράς, pulse weapons κ.λπ.

από τα κράτη μονάδων και επιτελικών διευθύνσεων κυβερνοάμυνας & κυβερνοπολέμου *στις ένοπλες δυνάμεις* τους και η διάθεση σημαντικών πόρων για την εκπαίδευση προσωπικού, την ανάπτυξη κακόβουλου λογισμικού και την εκδήλωση CNE και CNAs, δείχνει την πεποίθησή τους ότι και τα 'κυβερνο-όπλα' (cyberweapons) είναι όπλα όπως τα υπόλοιπα μέχρι σήμερα γνωστά και η χρησιμοποίησή τους μπορεί να είναι μέθοδος καταναγκασμού και βίας, ακόμη και ένοπλης επίθεσης, στις διακρατικές σχέσεις και αποτελεί επιπρόσθετη σοβαρή ένδειξη για την πορεία των πραγμάτων στο άμεσο μέλλον. Δεν διαπιστώνεται όμως, προς το παρόν, ούτε καν αρχόμενη πρακτική απαγόρευσης ανάπτυξης και χρήσης ορισμένων 'κυβερνο-όπλων' και μεθόδων 'κυβερνοπολέμου'.

13. Πολύς λόγος γίνεται για την ανάγκη σύναψης μίας ειδικής διεθνούς συνθήκης για τη ρύθμιση της αντιπαράθεσης στον κυβερνοχώρο. Παρά την προσέγγιση που παρατηρείται εσχάτως στο θέμα αυτό μεταξύ των Η.Π.Α. του Β. Obama και της Ρωσικής Ομοσπονδίας, είναι ελάχιστα πιθανή, τουλάχιστον για το ορατό μέλλον, οποιαδήποτε διεθνής συμφωνία που θα περιορίζει, έστω, τη χρήση 'όπλων' και τακτικών καταναγκασμού στον κυβερνοχώρο, αφού τα ηλεκτρονικά και δικτυακά προηγμένα κράτη είναι μεν περισσότερο ευάλωτα σε κυβερνοεπιθέσεις, αλλά, συγχρόνως, είναι και εξαιρετικά ικανά και αποτελεσματικά στη διεξαγωγή τους, με αποτέλεσμα σ' αυτή τη φάση η δική τους θεώρηση των πραγμάτων να εξυπηρετείται από την *ασάφεια* του νομικού πλαισίου.

14. Για τους λόγους που σκιαγραφήθηκαν στο *τμήμα IV.8.*, παραπάνω, η συμβατική απαγόρευση της άσκησης βίας στον κυβερνοχώρο και της ανάπτυξης και χρήσης όπλων και τεχνικών κυβερνοεπιχειρήσεων είναι *ανέφικτη*. Αντίθετα, κατ' αρχήν *εφικτή* είναι η σύναψη ορισμένων συμβατικών κανόνων[220] με τους οποίους θα καθίσταται περισσότερο δύσκολη η εκτέλεση κάποιων κατηγοριών κυβερνοεπιχειρήσεων και ευκολότερη και ταχύτερη η συλλογή αποδείξεων γι' αυτές, θα ορίζεται με κάποιο τρόπο η έννοια της κυβερνο-επίθεσης (όχι με καθαρά νομικά κριτήρια) και θα θεσπίζονται υποχρεώσεις συνδρομής στην έρευνα περιστατικών και παροχής στοιχείων, θα συμφωνείται η μη χρήση κάποιων *ειδών* κακόβουλου κώδικα —τουλάχιστον στις επιχειρήσεις κυβερνο-κατασκοπείας και εκμετάλλευσης δικτύων (λόγω του κινδύνου 'bleed-over των αποτελεσμάτων)—, θα αναλαμβάνονται

[220] Έστω και νομικά μη δεσμευτικών για αρχή ('best practices', 'non legally binding norms', code of conduct κ.λπ.).

υποχρεώσεις κοινοποίησης κάποιων κρίσιμων τεχνολογιών υλισμικού και λογισμικού, θα συμφωνείται η αναβάθμιση της ασφάλειας των πρωτοκόλλων επικοινωνίας στο internet, θα τίθενται κάποιοι κανόνες για τον έλεγχο ανάπτυξης και διακυβέρνησής του και θα συμφωνείται ένα είδος υψηλής εποπτείας της τεχνολογίας που χρησιμοποιείται και αποχή από κάποιες δραστηριότητες. Ορισμένοι θεωρητικοί, μάλιστα, κάνουν λόγο και για τη προσέγγιση του κυβερνοχώρου ως αντικειμένου παγκόσμιας κληρονομιάς της ανθρωπότητας και τη ρύθμισή του με τρόπους ανάλογους με αυτούς που χρησιμοποιήθηκαν για τη νομική ρύθμιση του διεθνούς βυθού, του διαστήματος ή και της Ανταρκτικής ακόμη.

15. Ακριβώς επειδή το πρόβλημα είναι κυριολεκτικά τεράστιο και οι δικτυακές και οικονομικές υπερδυνάμεις φοβούνται ανά πάσα στιγμή έναν *Αρμαγεδδώνα* στον κυβερνοχώρο, τέτοιου είδους συμβατικές απόπειρες ρύθμισης του καταναγκασμού στον κυβερνοχώρο σαν τις παραπάνω (σε αντίθεση με τη συμβατική απαγόρευση της άσκησης βίας στο πεδίο αυτό και με την απαγόρευση ανάπτυξης και χρήσης όπλων και τεχνικών κυβερνοεπιχειρήσεων), *δεν* αποκλείεται στο ορατό μέλλον να αποκτήσουν ώθηση και ορμή, σαν κι' αυτή που έχουμε δει να αποκτούν διεθνείς συμφωνίες όπως η Συνθήκη για την κατάργηση των ναρκών κατά προσωπικού[221] ή το Πρωτόκολλο IV στη Συνθήκη CCW για την απαγόρευση της χρήσης τυφλωτικών όπλων laser.

16. Εν κατακλείδι, οι διατάξεις των άρθρων 2(4) και 51 του Χάρτη και το διεθνές εθιμικό δίκαιο που ισχύει σήμερα αναφορικά με το δικαίωμα αυτοάμυνας, μπορούν, κατά την άποψή μας, να λειτουργήσουν ικανοποιητικά και στα ζητήματα άσκησης βίας και εκδήλωσης 'ένοπλων επιθέσεων' στον κυβερνοχώρο και δεν έχουν καταστεί *ακόμη* 'ανεπανόρθωτα ακατάλληλες' (για να δανειστούμε την έκφραση της *Higgins)*. Η λύση αυτή τη στιγμή δεν πιστεύουμε ότι είναι η *infra legem* ερμηνεία των διατάξεων αυτών και η ελάττωση ύψους του κατωφλιού που απαιτείται κάθε φορά για τη διαπίστωση 'βίας' και 'ένοπλης επίθεσης'˙ εκείνο που απαιτείται σε πρώτη φάση και άμεσα, είναι η θωράκιση του (ιδιωτικού) internet με ένα επιπλέον *minimum* κανόνων και τεχνολογιών ασφαλείας, χωρίς να θίγονται τα δικαιώματα πλήρους απόλαυσης του κυβερνοχώρου και η περισσότερο αποφασιστική και ρωμαλέα εφαρμογή των υφισταμένων διατάξεων και του κεκτημένου του Χάρτη.

---

221 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, γνωστή απλά και ως "Mine Ban Treaty".

17. Ανεξάρτητα από τα παραπάνω, η συμβατική επέκταση του ρυθμιστικού εύρους του άρθρου 2(4) και των προϋποθέσεων και ορίων του άρθρου 51, φαντάζει, τουλάχιστον για το ορατό μέλλον, ανέφικτη και για τον πρόσθετο λόγο ότι οποιαδήποτε προσπάθεια προς αυτή την κατεύθυνση θα άνοιγε και πάλι σοβαρά τη συζήτηση για την απαγόρευση ή τον περιορισμό και των μεθόδων πολιτικού & οικονομικού καταναγκασμού.

18. Ο κυβερνοχώρος, τόσο λόγω του γεγονότος ότι είναι το μόνο τεχνητό πεδίο ανθρωπινής αντιπαράθεσης, όσο και λόγω του κυρίαρχου χαρακτηριστικού του που είναι η άμεση διασύνδεση της 'εικονικής πραγματικότητας' με τον φυσικό /πραγματικό κόσμο και η υψηλού βαθμού εξάρτηση του δεύτερου από την πρώτη, έχει παγκόσμια εμβέλεια και διαπλέκεται με κάθε πτυχή της σύγχρονης ζωής στον πλανήτη. Οι πληροφοριακές επιχειρήσεις και οι CNAs που μας ενδιαφέρουν ειδικά εδώ, εκμεταλλεύονται τα χαρακτηριστικά του κυβερνοχώρου και ιδίως την εκτεταμένη, άμορφη, άναρχη και ταχεία εξάπλωση του internet και πιέζουν μέχρι τα όρια της θραύσης το σύστημα 'διεθνής ασφάλεια – κρατική κυριαρχία – εδαφικότητα – διεθνής ευθύνη των κρατών'. Ειδικά οι CNAs αναγκάζουν το *jus ad bellum*, όπως το γνωρίζουμε μέχρι σήμερα, να 'αγκομαχεί' για να κρατηθεί κοντά στις εξελίξεις. Το άμεσο μέλλον αναμένεται εξαιρετικά ενδιαφέρον, τόσο από την πλευρά των τεχνολογικών εξελίξεων και των επιπτώσεών τους στην τεχνική των πληροφοριακών επιχειρήσεων και των CNAs, όσο και από την πλευρά των ενδεχόμενων μέτρων που τυχόν θα ληφθούν ώστε το γραπτό διεθνές δίκαιο να κρατηθεί τουλάχιστον σε επαφή με τις εξελίξεις˙ σε κάθε περίπτωση εκτιμάται ότι θα αυξηθεί και το ενδιαφέρον της επιστήμης του διεθνούς δικαίου για το ζήτημα και η ανταλλαγή νομικών επιχειρημάτων αναμένεται με ενδιαφέρον._

**

VI. Παράρτημα

1. Ο ηλεκτρονικός υπολογιστής (πρόσθετες πληροφορίες)

Χωρίς να παραγνωρίζουμε τον κίνδυνο υπεραπλούστευσης, θα μπορούσαμε να περιγράψουμε τα σημαντικότερα στάδια στην πορεία εμφάνισης και εξέλιξης των πρώτων η/υ

ως εξής : Το 1937 ο George Stibitz, ενώ εργαζόταν στα εργαστήρια της εταιρείας Bell, κατασκεύασε έναν η/υ (τον οποίο ονόμασε "Model K") που χρησιμοποιούσε ηλεκτρονόμους και ήταν η πρώτη μηχανή η οποία χρησιμοποίησε δυαδικά κυκλώματα για να εκτελέσει μία αριθμητική λειτουργία˙ στα επόμενα μοντέλα του η/υ αυτού, ο οποίος θεωρείται ο πρώτος σύγχρονος *ψηφιακός* η/υ, ενσωματώθηκαν και δυνατότητες *προγραμματισμού*. — Το 1941 ο Konrad Zuse παρουσίασε μία ηλεκτρομηχανική μηχανή (την "Z3") που χρησιμοποιούσε δυαδική αριθμητική και μπορούσε να προγραμματιστεί. — Μεταξύ των ετών 1937 – 1941 οι John Atanasoff και Clifford Berry ανέπτυξαν έναν μη προγραμματιζόμενο η/υ που χρησιμοποιούσε δυαδικούς αριθμούς και λυχνίες κενού για να εκτελέσει υπολογισμούς και διέθετε προσωρινή μνήμη (τα ενδιάμεσα αποτελέσματα των υπολογισμών μπορούσαν να αποθηκευθούν προσωρινά και κατόπιν να επανα-τροφοδοτηθούν στην αλυσίδα των υπολογισμών). — Το 1943 λειτούργησαν οι (απόρρητες) υπολογιστικές μηχανές "Colossus' των Βρετανών (Colossus computers) που χρησιμοποιήθηκαν για το σπάσιμο των κρυπτογραφημένων μηνυμάτων των Γερμανών κατά τον Β' ΠΠ (χρησιμοποιούσαν εκατοντάδες λυχνίες κενού και είχαν περιορισμένες δυνατότητες προγραμματισμού). — Το 1944 εμφανίστηκε ο ηλεκτρο-μηχανικός η/υ Harvard Mark I, με περιορισμένες δυνατότητες προγραμματισμού. — Το 1946 λειτούργησε ο η/υ ENIAC του Ballistic Research Laboratory του στρατού ξηράς των Η.Π.Α., ο οποίος χρησιμοποιούσε δεκαδική αριθμητική και θεωρείται ο πρώτος η/υ *γενικής χρήσης* (αφού η μηχανή "Z3" του Konrad Zuse του 1941 χρησιμοποιούσε ηλεκτρομαγνήτες και όχι ηλεκτρονικά). — Ακολούθησαν υπολογιστές στους οποίους αξιοποιήθηκαν (αρχικά στη Μεγάλη Βρετανία) οι εργασίες του Ούγγρου μαθηματικού John von Neumann του 1945 για την αρχιτεκτονική των αποθηκευμένων προγραμμάτων ("stored program architecture" ή von Neumann architecture)˙ το 1948 εμφανίστηκε ο η/υ SSEM του Πανεπιστημίου του Μάντσεστερ και το 1949 ο η/υ EDSAC του Κέιμπριτζ, με τον οποίο έγινε και η πρώτη μη-πειραματική και πρακτικά χρησιμοποιήσιμη αξιοποίηση της αρχιτεκτονικής του von Neumann.[222]

Οι υπολογιστές στη δεκαετία του 1950 χρησιμοποιούσαν τεχνολογία λυχνιών κενού (vacuum tubes). Η τεχνολογία αυτή στη δεκαετία του 1960 αντικαταστάθηκε σταδιακά από την τεχνολογία των *τρανζίστορ*˙[223] οι υπολογιστές που χρησιμοποιούσαν τρανζίστορ ήταν μικρότεροι, ταχύτεροι, φθηνότεροι, περισσότερο αξιόπιστοι και απαιτούσαν πολύ λιγότερη ενέργεια για να λειτουργήσουν. Στη δεκαετία του 1970 εμφανίστηκε η τεχνολογία των

[222] Αν και οι τεχνολογίες των η/υ έχουν αλλάξει δραματικά από τη δεκαετία του 1940, στους περισσότερους υπολογιστές ακόμη και σήμερα ακολουθείται η αρχιτεκτονική των αποθηκευμένων προγραμμάτων του von Neumann.

[223] Transistor ή κρυσταλλολυχνία : πρόκειται για μικρό ημιαγώγιμο ηλεκτρονικό στοιχείο στερεάς κατάστασης, το οποίο μπορεί να εκτελεί σχεδόν όλες τις λειτουργίες ενός ηλεκτρονικού σωλήνα, συμπεριλαμβανομένης της ενίσχυσης και της ανόρθωσης. Ο πρώτος η/υ στον οποίο έγινε χρήση transistors κατασκευάστηκε και επιδείχθηκε στο Πανεπιστήμιο του Μάντσεστερ το 1953.

ολοκληρωμένων κυκλωμάτων και ακολούθησε η κατασκευή των *μικρο-επεργαστών*˙ η ταχύτητα και η αξιοπιστία των η/υ έγινε ακόμη μεγαλύτερη, ενώ το κόστος τους μειώθηκε περισσότερο. Στα τέλη της δεκαετίας του 1970 άρχισαν να εμφανίζονται και ηλεκτρικές και ηλεκτρονικές συσκευές εφοδιασμένες με μικρο-υπολογιστές ειδικών λειτουργιών (dedicated computers) που είναι γνωστοί ως 'μικροελεγκτές' (microcontrollers) (: τηλεοράσεις, συσκευές εγγραφής εικόνας και ήχου, οικιακά πλυντήρια κ.λπ.). Στη δεκαετία του 1980 εμφανίστηκαν οι προσωπικοί υπολογιστές (personal computers – PCs), οι οποίοι στις ημέρες μας, με την εξέλιξη και διάδοση του internet, έχουν γίνει τόσο κοινοί όσο το τηλέφωνο και η τηλεόραση. Τα σύγχρονα 'έξυπνα (φορητά ή 'κινητά') τηλέφωνα' (smart phones) είναι στην πραγματικότητα πλήρως προγραμματιζόμενοι (μικρού μεγέθους) ηλεκτρονικοί υπολογιστές (με επεξεργαστή, μνήμη, λειτουργικό σύστημα, αποθηκευτικά μέσα κ.λπ.) και ήδη από το 2009 θεωρούνται ως το πολυπληθέστερο είδος ηλεκτρονικού η/υ σε χρήση παγκοσμίως.[224]

Πίνακας

Ορόσημα της αρχιτεκτονικής η/υ[225]

Μηδενική γενιά	**Μηχανικοί υπολογιστές**, 1642 – 1945 (Ο πρώτος που κατασκεύασε μία (μηχανική) υπολογιστική μηχανή που λειτουργούσε, ήταν ο Γάλλος Blaise Pascal το 1642. Η μηχανή αυτή λειτουργούσε με γρανάζια, ήταν χειροκίνητη και μπορούσε να κάνει μόνο πρόσθεση και αφαίρεση.)
Πρώτη γενιά	**Λυχνίες κενού**, 1945 – 1955
Δεύτερη γενιά	**Τρανζίστορ**, 1955 – 1965
Τρίτη γενιά	**Ολοκληρωμένα κυκλώματα**, 1965 – 1980
Τέταρτη γενιά	**Ολοκλήρωση πολύ μεγάλης κλίμακας**, 1980 – ; (VLSI – Very Large Scale Integration= ***εκατομμύρια*** [ή και παραπάνω] τρανζίστορ σε ένα μόνο τσιπ)

2. Το διαδίκτυο (internet) και ο 'παγκόσμιος ιστός' (πρόσθετες πληροφορίες)

Η προσπάθειες για τη δημιουργία ενός διαδικτύου η/υ ξεκίνησαν στις Η.Π.Α. κατά τη διάρκεια του ψυχρού πολέμου, στα πλαίσια εξεύρεσης λύσεων για την προστασία των τηλεπικοινωνιών από μια πιθανή πυρηνική επίθεση της Σοβιετικής Ένωσης˙ την περίοδο εκείνη η αμερικανική υπηρεσία ασφαλείας ARPA (γνωστή στις μέρες μας ως DARPA), ξεκίνησε προσπάθειες για την ανάπτυξη ενός κατανεμημένου δικτύου επικοινωνιών για τις ένοπλες δυνάμεις των Η.Π.Α., το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση και θα παρουσίαζε ιδιαίτερη αντοχή στις τεχνικές αστοχίες˙ *στις προσπάθειες αυτές*

[224] Για όλα τα παραπάνω, πηγή : wikipedia, λήμμα : 'computer', τελευταία πρόσβαση : 04 Οκτ. 2011.
[225] Tanenbaum, σελ. 33 et seq.

συνεισέφεραν οικονομικά και αρκετές μεγάλες ιδιωτικές εμπορικές εταιρείες. Το θεωρητικό υπόβαθρο για κάτι τέτοιο είχε δοθεί από τον J.C.R. Licklider, ο οποίος είχε κάνει λόγο σε συγγράμματά του για το 'γαλαξιακό δίκτυο', δηλαδή ένα δίκτυο η/υ που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το δίκτυο αυτό θα έπρεπε να ήταν *αποκεντρωμένο* έτσι ώστε ακόμα κι αν κάποιος κόμβος του δεχόταν επίθεση, να υπήρχε δίοδος επικοινωνίας με τους υπόλοιπους υπολογιστές˙ λύση σε αυτό έδιναν οι εργασίες του Paul Baran. ο οποίος σχεδίασε ένα κατανεμημένο δίκτυο επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων δεδομένων του καθηγητή Leonard Kleinrock, που υποστήριζε ότι πακέτα πληροφοριών, κάθε ένα από τα οποία θα περιείχε συγχρόνως και τις απαραίτητες πληροφορίες για την προέλευση και τον τελικό προορισμό του, μπορούσαν να σταλούν από έναν η/υ σε έναν άλλο.[226] Με βάση αυτές τις θεωρητικές προσεγγίσεις δημιουργήθηκε το πρώτο είδος διαδικτύου, γνωστό ως ARPANET, το οποίο εγκαταστάθηκε και λειτούργησε για πρώτη φορά το **1969** με τέσσερις κόμβους, μέσω των οποίων συνδέονταν τέσσερις μίνι υπερυπολογιστές (mini computers) του πανεπιστημίου της Καλιφόρνια (στη Σάντα Μπάρμπαρα και στο Λος Άντζελες), του πανεπιστημίου SRI στο Στάνφορντ και του πανεπιστημίου της Γιούτα. Η ταχύτητα του δικτύου έφθανε τα 50 kbps και έτσι επιτεύχθηκε η πρώτη dial up σύνδεση μέσω γραμμών τηλεφώνου. Μέχρι το 1972 οι συνδεδεμένοι στο ARPANET υπολογιστές είχαν φτάσει τους είκοσι τρεις˙ τότε εφαρμόστηκε για πρώτη φορά και το σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου (e-mail). Παράλληλα δημιουργήθηκαν και άλλα δίκτυα, που χρησιμοποιούσαν διαφορετικές μεθόδους και τεχνικές διασύνδεσης η/υ (όπως το x.25 και το UUCP), τα οποία συνδέθηκαν με το ARPANET. Το πρωτόκολλο επικοινωνίας που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το οποίο, όμως, είχε το μειονέκτημα ότι λειτουργούσε μόνο με συγκεκριμένους τύπους η/υ. Έτσι, στις αρχές του 1970, διαφάνηκε η ανάγκη για ένα πρωτόκολλο που θα ένωνε όλα τα δίκτυα που είχαν δημιουργηθεί μέχρι τότε. Το 1974 δημοσιεύθηκε η μελέτη των Vint Cerf και Bob Kahn από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol), το οποίο το 1978 έγινε 'TCP/IP', προστέθηκε δηλαδή σ' αυτό το Internet Protocol (IP), και τελικά το 1983 έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET. Το 1984 υλοποιήθηκε το πρώτο *σύστημα ονοματοδοσίας τομέα διαδικτύου* (DNS – Domain Name System), στο οποίο καταγράφηκαν χίλιοι κεντρικοί κόμβοι και οι υπολογιστές του διαδικτύου πλέον αναγνωρίζονταν από *διευθύνσεις κωδικοποιημένων αριθμών*. Ένα ακόμα σημαντικό βήμα στην ανάπτυξη του διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών των Η.Π.Α. (National Science Foundation – NSF), το οποίο το 1986 δημιούργησε την πρώτη μεγάλη διαδικτυακή πανεπιστημιακή αρτηρία επικοινωνίας (δίκτυο-ραχοκοκαλιά – backbone), το NSFNet.

[226] Ο ίδιος, κατά τη διάρκεια της δεκαετίας του 1970 ασχολήθηκε και με την *ιεραρχημένη δρομολόγηση* των πακέτων δεδομένων, η οποία είναι επίσης ζωτικής σημασίας για το internet.

Ακολούθησε η ενσωμάτωση στο ARPANET και άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet, *πολλά από τα οποία ήταν καθαρά ιδιωτικά και μάλιστα εμπορικού χαρακτήρα*. Ο όρος διαδίκτυο /internet άρχισε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το APRANET με το NSFNet και internet σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε το πρωτόκολλο επικοινωνίας TCP/IP.

Η μεγάλη άνθιση του διαδικτύου, ωστόσο, ξεκίνησε με την εφαρμογή της υπηρεσίας του **παγκόσμιου ιστού** (‘www’ – world wide web), εφεύρεση του Tim Berners-Lee του έτους **1989**, ο οποίος εκείνη την εποχή εργαζόταν στο ευρωπαϊκό ερευνητικό κέντρο CERN στη Γενεύη, όπου και λειτούργησε ο πρώτος web-server η/υ. Ο παγκόσμιος ιστός είναι μία πρότυπη μέθοδος παρουσίασης των πληροφοριών με γραφικό τρόπο, με τη μορφή σελίδων διαφόρων μεγεθών στην οθόνη του η/υ˙ ενσωματωμένοι στις σελίδες του www —μαζί με εικόνες, κείμενα και πολυμέσα—, υπάρχουν και οι υπερ-σύνδεσμοι (hyper-links), δηλαδή σημεία επάνω στη σελίδα (συνήθως υπογραμμισμένες λέξεις ή τμήματα εικόνων και γραφικών) που οδηγούν, μέσω ενός απλού *click* του ποντικιού επάνω τους, σε άλλες σελίδες του www.[227, 228]

***

Β.Γ.Μ.
xi/11

[227] Η μεταφορά γίνεται σε άλλες σελίδες, τοποθετημένες είτε στον ίδιο η/υ – εξυπηρετητή (web server), είτε σε κάποιον άλλον που μπορεί να βρίσκεται γεωγραφικά οπουδήποτε στον κόσμο.

[228] Η τεχνική σχεδιασμού κειμένων που κάνουν χρήση υπερ-συνδέσμων (hyper-links) ονομάζεται ‘υπερ-κείμενο’ (hypertext), ενώ η γλώσσα που χρησιμοποιείται για την κατασκευή σελίδων του www ονομάζεται HTML (HyperText Markup Language). Για τη μεταφορά των σελίδων του www στο internet αναπτύχθηκε ένα ειδικό πρωτόκολλο επικοινωνίας η/υ και μεταφοράς πακέτων δεδομένων, το πρωτόκολλο HTTP (Hyper-Text Transmission Protocol). Για το λόγο αυτό όλες οι διευθύνσεις στον παγκόσμιο ιστό αρχίζουν με τη συντομογραφία *‘’http://’’*, για να φαίνεται ότι το αρχείο στο οποίο παραπέμπουμε είναι μία σελίδα υπερ-κειμένου (hypertext page) και πρέπει να ανακτηθεί μέσω του πρωτοκόλλου http.