San Diego International Law Journal

Volume 14 | Issue 1 Article 5

11-1-2012

Cyberterrorism in the Context of Contemporary International Law

Yaroslav Shiryaev

Cyberterrorism in the Context of Contemporary International Law

YAROSLAV SHIRYAEV*

TABLE OF CONTENTS

* Ph.D. Candidate at University of Warwick; L.L.M. 2010, University of Aberdeen; B.A. 2008, University of Tartu. Please feel free to send feedback to yaroslav.law@gmail.com. This Article is dedicated to Melinda Taylor and other lawyers who seek fair and impartial trial for Saif al Islam al Gaddafi.

1. TERRORISM AND CYBERTERRORISM AS LEGAL CONCEPTS

A. Impact of Technology on the Notion of Terrorism

The international law framework surrounding terrorism existed well before 9/11. Out of the eighteen international instruments (including amendments)[1] adopted since 1963, thirteen existed before 2001. Though it seems obvious that the attack on the World Trade Center and other events within the United States served as catalysts for the development of serious international documents such as the 2005 Convention for the Suppression of Acts of Nuclear Terrorism and 2006 United Nations Global Counter-Terrorism Strategy, the documents were built upon previously existing legal foundations.[2]

The extent to which general principles of international law pertaining to terrorism have changed since 9/11 can be described as one-sided, as

1. *International Legal Instruments to Counterterrorism*, U.N. ACTION TO COUNTER TERRORISM, http://www.un.org/terrorism/instruments.shtml (last visited Aug. 21, 2012).

2. *See, e.g.*, Int'l Civil Aviation Org. [ICAO], 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, ICAO Doc. 9960; ICAO, 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft, Sept. 14, 1963, ICAO Doc. 8364; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Jan. 26, 1973, 974 U.N.T.S. 178; U.N. Secretary-General, International Convention for the Suppression of Acts of Nuclear Terrorism, U.N. GAOR (Apr. 13, 2005); Int'l Atomic Energy Agency [IAEA], Convention on the Physical Protection of Nuclear Material, May 1, 1980, IAEA Doc. INFCIRC/274/Rev.1; Int'l Maritime Org. [IMO], 2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, July 28, 2010; IMO, 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Nov. 1, 2005, IMO Doc. LEG/Conf.15/22.

some elements have not changed at all (as evidenced by the failure to adopt the UN Comprehensive Convention on International Terrorism due to a deadlock over the definition of terrorism), while other elements changed drastically (e.g., express recognition by the United Nations Security Council (UNSC) in Resolutions 1368 and 1373 of the right to self-defense in response to a terrorist attack by a non-state actor).[3] If a cyberterrorist-attack would reach at least the same threshold as the 9/11 attacks, there is serious reason to believe that legal approach will be the same as for Al-Qaeda attacks themselves: rapid development of law on the basis of an already-existing base.

Some authors today believe that there is no imminent cyberterrorism threat.[4] It is true that cyber-attacks have not officially set the record in terms of severe casualties yet[5] and on the outside they resemble ordinary cyber-attacks.[6] In fact, there is a great gap between the presumed danger and the known cyberterrorism activities.[7] However, with quick evolution of technologies, it is only a matter of time[8] before the danger of life-threatening cyberterrorism manifests itself.

---

3. *See generally* Derek Jinks, *September 11 and the Laws of War*, 28 YALE J. INT'L. L. 32 (2003).

4. *See* Massimo Mauro, *Threat Assessment and Protective Measures: Extending the Asia–Europe Meeting IV Conclusions on Fighting International Terrorism and Other Instruments to Cyber Terrorism*, *in* CYBERWAR, NETWAR AND THE REVOLUTION IN MILITARY AFFAIRS 219, 221 (Edward Halpin et al. eds., 2006); *see* Dorothy Dennings, *A View of Cyberterrorism Five Years Later*, *in* READINGS IN INTERNET SECURITY: HACKING, COUNTERHACKING, AND SOCIETY (K. Himma ed., 2006), *cited in* Eneken Tikk, *Comprehensive Legal Approach to Cyber Security*, 35 DISSERTATIONES JURIDICAE UNIVERSITATIS TARTUENSIS 22 (2011).

5. Hai-Cheng Chu, Der-Jiunn Deng, Han-Chieh Chao & Yueh-Min Huang, *Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of All Intangible Fears*, 15 J. UNIVERSAL COMPUTER SCI. 2373, 2373–86 (2009).

6. Dorothy E. Denning, *Terror's Web: How the Internet Is Transforming Terrorism*, *in* HANDBOOK ON INTERNET CRIME 198 (Yvonne Jewkes & Majid Yar eds., 2009).

7. Anna-Maria Talihärm, *Cyber Terrorism: in Theory or in Practice?*, 3.2 DEFENCE AGAINST TERRORISM REV. 59, 62 (2010).

8. FBI Director Robert Mueller opines that the cyber terrorism threat is "rapidly expanding." Vineetha Menon, *FBI: Cyber Terrorism Threat Is 'Rapidly Expanding'*, ITP.NET (Mar. 8, 2010), http://www.itp.net/579523-fbi-cyber-terrorism-threat-is-rapidly-expanding, *cited in* Tikk, *supra* note 4, at 25.

B. Lack of a Common Definition

The lack of a universally accepted definition of terrorism is an obstacle in describing the nature of cyberterrorism[9] without referring to conventional terrorism. Generally, a common definition is required for two reasons: firstly, to definitively determine the status of customary law pertaining to the use of force in relation to acts of terror; and secondly, to criminalize such acts,[10] i.e. to prevent terrorism, to condemn it, and to punish it. Worth noting is also that international demand to extradite a terrorist offender far exceeds pressure to extradite a common criminal.[11]

The various suggestions made by academics on how to define this concept are only partially overlapping and range from those including social aspects (terrorism is motivated by "egoism, intolerance, lack of dialogue and inhumanity, greed and accountability")[12] or psychological ones ("terrorism is a tactic to coerce behavioral change in an adversary")[13] to very thorough legal approaches ("one must distinguish between attitude [and] methods"[14] of terrorism).

This is further complicated by the definition recommended by the UN's High-Level Panel in its Report on Threats, Challenges and Change of 2004. The panel concluded that a definition in the upcoming Comprehensive Convention on International Terrorism should include a

> description of terrorism as "any action, in addition to actions already specified by the existing conventions on aspects of terrorism, the Geneva Conventions and Security Council resolution 1566 (2004), that is intended to cause death or

---

9. Jeff Addicott, *Terrorism Law: Materials, Cases, Comments, 6th Edition*, CENTER FOR TERRORISM LAW ISSUES FOR DISCUSSION: CYBER SECURITY 1 (2011), *available at* www.stmarytx.edu/law/pdf/CLEAddicott.pdf.

10. *See also* Clive Walker, *The Legal Definition of "Terrorism" in United Kingdom Law and Beyond*, 2007 PUB. L. 331, 336 (2007).

11. LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 21-33 (1998), *cited in* Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber Attacks from China*, 17 AM. U. INT'L. L. REV. 663 (2002).

12. PAUL MEDHURST, GLOBAL TERRORISM: A COURSE PRODUCED BY THE UNITED NATIONS INSTITUTE FOR TRAINING AND RESEARCH 1 (2000), *cited in* Harry R. Jackson, Understanding Terrorism (unpublished thesis, Peace Operations Training Institute), *available at* http://media.peaceopstraining.org/theses/jackson.pdf.

13. Laurence Andrew Dobrot, *The Global War on Terrorism: A Religious War?*, STRATEGIC STUD. INST. 6 (2007), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/pub822.pdf.

14. Jean-Marc Sorel, *Some Questions About The Definition of Terrorism and The Fight Against its Financing*, 14 EUR. J. INT'L L. 365, 371 (2003); *see also* G.A. Res. 51/210, ¶ 2, U.N. Doc. A/RES/51/210 (Dec. 17, 1996) ("Reiterates that criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable . . . .").

> serious bodily harm to civilians or non-combatants, when the purpose of such an act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act."[15]

In a 2005 Report "In Larger Freedom,"[16] Kofi Annan endorsed this suggestion, noting that "[i]t is time to set aside debates on so-called 'State terrorism' [and] the right to resist occupation must be understood in its true meaning." It is worth noting that although the High-Level Panel explicitly asks for the "definition" contained in the SC Resolution 1566 to be included,[17] Security Council Resolution 1566 itself clearly favors the sectoral approach, i.e. it refers directly to the existing conventions on terrorism.[18]

However, from the legal perspective, the ex-Secretary-General's suggestions are supportive rather than innovative, since a similar core-definition (partially resembling one of the 1937 Convention for the Prevention and Punishment of Terrorism that never entered into force) contained in the draft of the Comprehensive Convention on International Terrorism remained unchanged[19] since 2001:

---

15. U.N. Secretary-General, *A More Secure World: Our Shared Responsibility: Report of the High-level Panel on Threats, Challenges and Change*, ¶ 164(d), U.N. Doc. A/59/565 (Dec. 2, 2004).

16. U.N. Secretary-General, *In Larger Freedom*, ¶ 91, U.N. Doc. A/59/2005 (Mar. 21, 2005), at ¶ 91.

17. U.N. Secretary-General, *A More Secure World: Our Shared Responsibility: Report of the High-level Panel on Threats, Challenges and* Change, *supra* note 15, at ¶ 164(c).

18. *See* S.C. Res. 1566, ¶ 3, U.N. Doc. S/RES/1566 (Oct. 8, 2004) ("*Recalls* that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and *calls upon* all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature.").

19. *Compare* Ad Hoc Comm. established pursuant to resolution 51/210, art. 2, para. 1, U.N. Doc. A/57/37 (2010), *with* U.N. Report of the Working Group, *Measures to Eliminate International Terrorism*, U.N. GAOR, 65th Sess., art. 2, para. 1, U.N. Doc. A/C.6/65/L.10 (Nov. 3, 2010); *see also* ALEX CONTE, HUMAN RIGHTS IN THE PREVENTION AND PUNISHMENT OF TERRORISM 25 (2010).

> Any person commits an offence within the meaning of the present Convention if that person, by any means, unlawfully and intentionally, causes:
>
> a. Death or serious bodily injury to any person; or
> b. Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or to the environment; or
> c. Damage to property, places, facilities or systems referred to in paragraph 1(b) of the present article resulting or likely to result in major economic loss,
>
> when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

The draft also suggests criminalizing threats, attempts, and organization of these acts, as well as assistance and participation in them.[20]

The fact that the core of this definition is not widely disputed (the deadlock is mostly the result of disagreements over applicability of the convention to states and their armed forces, as well as liberation movements),[21] may suggest that this draft reflects the current state of customary international law pertaining to terrorism. This definition is indeed incorporating common elements of self-made legal definitions employed, e.g., by the European Union,[22] African Union,[23] South Asian

20. G.A. Res. 51/210, ¶ 4, U.N. Doc. A/57/37 (2010).

21. *See generally* U.N. Report of the Working Group, *Measures to Eliminate International Terrorism*, U.N. GAOR, 65th Sess., U.N. Doc. A/C.6/65/L.10 (Nov. 3, 2010); *see generally* Report of the Ad Hoc Comm. established pursuant to resolution 51/210 (Dec. 17, 1996), U.N. GAOR, 15th Sess., U.N. Doc. A/66/37 (2011); *see* U.N. GAOR, 66th Sess. Supp. No. 37, U.N. Doc. A/66/37, at 5 n.9 (Apr. 11–15, 2011), *cited in* U.N. GAOR 66th Sess., U.N. Doc. A/66/478 (Nov. 15, 2011), *available at* http://www.eyeontheun.org/assets/attachments/documents/10010reportmterr.pdf.

22. EU Council Framework Decision on Combating Terrorism, art. 1, 2002 O.J. (L 164/3) 2; *see also* Steven Best & Anthony J. Nocella II, *Defining Terrorism*, 2 ANIMAL LIBERATION PHIL. & POL'Y J. 1, 3 (2004), *available at* http://ww.drstevebest.org/Defining Terrorism.pdf.

23. Organization of African Unity [OAU], Convention on the Prevention and Combating of Terrorism art.1, ¶ 3, July 14, 1999, *available at* http://www.au.int/en/sites/default/files/OAU_CONVENTION_PREVENTION_COMBATING_TERRORISM.pdf.

Association for Regional Cooperation,[24] and Commonwealth of Independent States.[25]

However, the question is whether the suggested definition unreasonably loosens the already-existing international law regime criminalizing acts of terror. This is particularly relevant in relation to cyber-attacks.

As mentioned above, there are currently eighteen universal legal documents[26] in force meant to prevent terrorist acts.[27] All of these instruments seem to concentrate on acts perpetrated by non-state actors from a criminal law perspective (aut dedere aut judicare—extradite or

---

24. South Asian Association for Regional Cooperation [SAARC], Regional Convention on Suppression of Terrorism, art. I, Nov. 4, 1987, *available at* http://treaties.un.org/doc/db/Terrorism/Conv18-english.pdf.

25. Treaty on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Terrorism, art. 1, June 4, 1999, *available at* http://treaties.un.org/doc/db/Terrorism/csi-english.pdf.

26. Convention on Offences and Certain Other Acts Committed On Board Aircraft, Sept. 14, 1963, 20.3 U.S.T. 2941, 704 U.N.T.S. 219; Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22.2 U.S.T. 1641, 860 U.N.T.S. 105; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, *supra* note 2; Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, 28.2 U.S.T. 1975, 1035 U.N.T.S. 167; International Convention Against the Taking of Hostages, Dec. 17, 1979, 1316 U.N.T.S. 205; Convention on the Physical Protection of Nuclear Material, Oct. 26, 1979, 1456 U.N.T.S. 101, 18 I.L.M. 1419; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 201, 27 I.L.M. 672; Convention on the Marking of Plastic Explosives for the Purpose of Detection, *opened for signature* Mar. 1, 1991, 2122 U.N.T.S. 359; International Convention for the Suppression of Terrorist Bombings, *opened for signature* Jan. 12, 1998, 2149 U.N.T.S. 256; International Convention for the Suppression of the Financing of Terrorism, *opened for signature* Jan. 10, 2000, 2178 U.N.T.S. 197; International Convention for the Suppression of Acts of Nuclear Terrorism, *opened for signature* Sept. 15, 2005, 2445 U.N.T.S. 89, 44 I.L.M. 815; Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, *supra* note 2; Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, 1678 U.N.T.S. 304, 27 I.L.M. 685; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, 974 U.N.T.S. 177; IMO, Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, *supra* note 2; IMO, Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Oct. 14, 2005, IMO Doc. LEG/CONF.15/14; Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, Sept. 10, 2010, 50 I.L.M. 141.

27. *See also* U.N. Secretary-General, *A More Secure World: Our Shared Responsibility: Rep. of the Secretary-General's High-level Panel on Threats, Challenges and Change*, ¶ 164(b), U.N. Doc. A/59/565 (Dec. 2, 2004) ("Acts under the . . . preceding anti-terrorism conventions are terrorism, and a . . . crime under international law.").

adjudicate[28]), sometimes without and sometimes loosely referring to the intent or purpose of the terrorist conduct[29] (terrorizing general population or compelling a government to perform or abstain from an act).

Introduction of the definition contained in the Draft Comprehensive Convention is unlikely to reverse criminalization of terrorist acts committed without such intent, since the twelve Conventions and their protocols will remain in force[30] (unless explicitly stated otherwise in the Comprehensive Convention). Nevertheless, this definition may damage the notion that seems to exist in customary international law (evidenced by the existence of the conventions on terrorism per se[31]) that certain acts by their very nature are so severe that they can be considered terrorism, even if committed without a global purpose. In effect, this will prevent any other equally grave act (also in or through cyber-space) to be criminalized as terrorism, if it is not subject to the "purpose of conduct" criteria.

Until the Comprehensive Convention is adopted, however, the existing conventions on terrorism, including cyberterrorism, remain in the center of the legal framework. Without these instruments, "terrorism" would indeed be, as Rosalyn Higgins puts it, "a term without any legal significance, . . . merely a convenient way of alluding to activities . . . widely disapproved of . . . ."[32]

C. Defining Cyberterrorism as a Dependent Variable

What distinguishes cyberterrorism from conventional terrorism is the use of (mostly internet-based) computer networks.[33] In essence, it is the use of electronic links in order to carry out terrorist attacks, usually involving programs created for that purpose. These programs can be delivered to their destination either through Internet, portable storage-devices (such as USB cards), wireless radio signals, or other similar means.

---

28. *See* BIBI VAN GINKEL, THE PRACTICE OF THE UNITED NATIONS IN COMBATING TERRORISM FROM 1946 TO 2008: QUESTIONS OF LEGALITY AND LEGITIMACY 11 (2010).

29. Andrew Byrnes, Faculty of Law, Australian National University, *Apocalyptic Visions and the Law: The Legacy of September 11*, Inaugural Lecture, Centre for International and Public Law 11 **(**2002), https://digitalcollections.anu.edu.au/bitstream/1885/41104/3/Byrnes30May02.pdf.

30. Michael A. Newton, *Exceptional Engagement: Protocol I and a World United Against Terrorism*, 45 TEX. INT'L L.J. 323, 373 (2009).

31. *See generally* Curtis A. Bradley & Mitu Gulati, *Customary International Law and Withdrawal Rights in an Age of Treaties*, 21 DUKE J. COMP. & INT'L L. 1 (2010).

32. Rosalyn Higgins, *The General International Law of Terrorism*, *in* TERRORISM & INT'L L. 28 (Rosalyn Higgins & Maurice Flory eds., 1997).

33. *See* S.S. Raghay, *Cyber Security in India's Counter Terrorism Strategy*, INTEGRATED DEFENSE STAFF 2 (Sept. 15, 2012), ids.nic.in/art_by_offids/Cyber security in india by Col SS Raghav.pdf.

Cyberterrorism should be viewed separately from the terrorist use of the Internet, which involves such aspects as communication,[34] recruitment, funding, organization of physical attacks,[35] propaganda (also in the form of "hacktivism"[36]), incitement to terrorism,[37] and apology of terrorism. At the same time, certain cyber-operations (e.g., intrusions into critical infrastructure databases to collect information on vulnerable targets) can further cyberextremists' cause,[38] but are not acts of cyberterrorism on their own. Scholars like Conway (who builds on Anderson's suggestion), also propose dividing cyber-attacks into Internet "use" (expression of ideas and communication), "misuse" (disrupting or compromising websites or infrastructure), "offensive use" (using Internet to cause damage or engage in theft), and "cyberterrorism."[39]

The term "cyberterrorism" itself predates 9/11,[40] although lack of universal definitions of "cyber-attack" and "terrorism" has resulted in every expert having his own understanding of the term.[41] The confusion has been exacerbated by the media which has the tendency of randomly characterizing minor cyber-attacks as "cyberterrorism."[42]

---

34. James A. Lewis, *The Internet and Terrorism*, 99 AM. SOC'Y INT'L L. 112, 114 (2005) ("One of the characteristics of terrorist websites is their ability to manage rapid changes of Internet addresses. When authorities force a site to move, informal networks based on chatrooms or e-mail inform the group's supporters of the new network address."); *see also* TIMOTHY F. O'HARA, CYBER WARFARE: CYBER TERRORISM 114 (2004).

35. *See* Elina Noor, *The Problem with Cyber Terrorism*, 2 SOUTHEAST ASIA REGIONAL CTR. FOR COUNTER-TERRORISM 51, 52 (2011).

36. *See* Varvara Mitliaga, *Cyber-terrorism: A Call for Governmental Action?*, BRITISH AND IRISH LAW, EDUCATION & TECHNOLOGY ASSOCIATION 5 (2001), http://www.bileta.ac.uk/01papers/mitliaga.html (describing hacktivism as "using hacking techniques to disrupt normal functions of systems, without causing serious damage, aiming at dissemination of propaganda and expression of political opinions").

37. *See* Yaël Ronen, *Incitement to Terrorist Acts and International Law*, 23 LEIDEN J. INT'L L., 645, 654 (2010).

38. Roland Heickerö, *Terrorism Online and the Change of Modus Operandi*, SWEDISH DEFENCE RESEARCH AGENCY 7 (Sept. 15, 2012), http://www.unidir.ch/pdf/conferences/pdf-conf334.pdf.

39. Maura Conway, *Terrorism and IT: Cyberterrorism and Terrorist Organisations Online* 6 (2003) (paper prepared for presentation at the International Studies Association Annual International Convention in Portland, Oregon).

40. Sam Berner, *Cyber-Terrorism: Reality or Paranoia?*, 5 S. AFR. J. INFO. MGMT. 1, 1 (2003).

41. Ali Jahangiri, *Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion*, WORLDWIDE SECURITY CONFERENCE 6: BACKGROUND MATERIALS AND SELECTED SPEAKERS NOTES 29 (2009).

42. Talihärm, *supra* note 7, at 63.

As in the case of "terrorism", academics have proposed a wide array of possible definitions that could cover this concept. The suggestions include those concentrating on the disruptive[43] and destabilizing[44] nature of cyberterrorism, limiting it only to individuals and non-state perpetrators,[45] focusing on wider psychological effects (fear),[46] malware writing process,[47] involving attacks on critical national infrastructures,[48] and attacks damaging networks themselves.[49] There have also been opinions expressed that the concept of cyberterrorism has no right to exist at all, since terrorism requires a physical attack.[50]

A lot of these definitions are over-inclusive or under-inclusive. For example, Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism of 2000 defines cyberterrorism as

> intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm.[51]

---

43. Rohas Nagpal, President of Asian School of Cyber Laws, *Cyber Terrorism in the Context of Globalization* 3 (Sept. 2002) (paper presented at World Congress on Informatics and Law), *available at* http://www.barzallo.com/DOCUMENTOS%20WEB/DOCTRINA/General/delitos%20inform_ticos/DocPDF/Nagpal,%20Rohas.II%20Congreso%20Mundial%20Derecho%20Informatico%20Madrid.pdf.

44. Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch: The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 301 (2008).

45. Daniel T. Kuehl, *The National Information Infrastructure: The Role of the Department of Defense in Defending It, in* TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES 151 (Carolyn W. Pumphrey ed., 2000).

46. *See* Christopher Beggs, *Cyber-Terrorism: A Threat to Australia*?, *in* MANAGING MODERN ORGANIZATIONS THROUGH INFORMATION TECHNOLOGY: PROCEEDINGS OF THE 2005 INFORMATION RESOURCES MANAGEMENT ASSOCIATION INTERNATIONAL CONFERENCE 472 (2005); *see* Maura Conway, *Cyberterrorism: Media Myth or Clear and Present Danger?* 5 (2004), http://doras.dcu.ie/505/1/media_myth_2004.pdf.

47. Alistair Kelman, *The Regulation of Virus Research and the Prosecution for Unlawful Research?*, 3 J. INFO. L. & TECH. (1997), *available at* http://elj.warwick.ac.uk/jilt/compcrim/97-3kelm/, *cited in* Mathias Klang, *A Critical Look at the Regulation of Computer Viruses*, 11 INT'L J. L. & INFO. TECH., 162, 167 (2003).

48. Gabriel Weimann, *Cyberterrorsim: The Sum of All Fears?*, 28 STUD. IN CONFLICT & TERRORISM 129, 130 (2005), *cited in* Clive Walker, *Cyber-Terrorism: Legal Principle and Law in the United Kingdom*, 110 PENN ST. L. REV., 625, 634 (2006).

49. Gabriel Weimann, *Cyberterrorsim: The Sum of All Fears?*, 28 STUD. IN CONFLICT & TERRORISM 129, 130 (2005), *cited in* Clive Walker, *Cyber-Terrorism: Legal Principle and Law in the United Kingdom*, 110 PENN ST. L. REV., 625, 634 (2006).

50. J. P. I. A. G. Charvat, *Cyber Terrorism: A New Dimension in Battlespace*, CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM 7 (2009), *available at* http://www.ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf.

51. Abraham D. Sofaer et al., *A Proposal for an International Convention on Cyber Crime and Terrorism* 26 (Aug. 2000) (paper presented at the Stanford Conference at Stanford University), *available at* http://iis-db.stanford.edu/pubs/11912/sofaer goodman.pdf.

According to this definition, an angry employee smashing vital SIS (MI6) computers containing dossiers on its agents with a sledgehammer would be a "cyberterrorist," since he commits intentional violence that disrupts cyber-systems and causes substantial damage to a state. In reality, however, the way violence is carried out in this theoretical example (physically and not through electronic network), would rule out the possibility of cyberterrorism.

At the same time, a virus that causes deliberate release of radioactive material into the environment, but with a low risk of human contamination, would fall outside the scope of the Stanford's definition, while it is explicitly criminalized as a terrorist act by Article 2(1)(b)(ii) of the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism.

Taking all these factors into account, from a legal perspective, the best definition that would describe the notion of (conventional) cyberterrorism today is: the use of electronic networks taking the form of a cyber-attack to commit a) a substantive act criminalized by the existing legal instruments prohibiting terrorism, or b) an act of terrorism under international customary law.

To put this definition into context, it is essential to establish who the possible perpetrators are and what objects are likely to be targeted when it comes to cyberterrorism.

II. POTENTIAL PERPETRATORS

Cyber-attacks are impossible without necessary technology and a minimal knowledge (at least by one person) of how electronic networks operate. Since more than two billion people on Earth have access to the Internet, and hacking and cracking manuals are available online, everyone including self-taught individuals, groups, large non-state actors, corporations, and states,[52] at least in theory, can engage in cyber-attacks.

A. States

Controversy regarding possible direct state involvement in conventional acts of terrorism seems less actual when viewed within the context of cyber-space. While the Draft Comprehensive Convention remains

52. *See* Peter Flemming & Michael Stohl, *Myths and Realities of Cyberterrorism*, *in* COUNTERING TERRORISM THROUGH INTERNATIONAL COOPERATION: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE 70-105 (Alex P. Schmid ed., 2001).

deadlocked on this issue,[53] neither of the eighteen existing legal instruments foresee state responsibility for an act of terrorism, so one must turn to international customary law for guidance.

Initially, state terrorism, which can even be the cause of anti-state extremism, has been included in the discussions regarding the definition for three reasons: firstly, due to a historically different meaning of this concept; secondly, because states cause wider destruction in comparison to non-state actors; and finally, since certain forms of violence against civilians occur as part of the counter-terrorism campaigns.[54]

"State terrorism" may be divided into two categories: internal and external. Within historical context, "internal state terrorism" entailed the use of force against its own civilian population to weaken the morale and destroy willingness to resist the government's will, while "external state terrorism" targeted foreign populations.[55] Situations where a state uses cyber-attacks against its civilians are very unlikely, as they would be very inefficient: firstly, physical "punishment" is easier to carry out and it creates more fear (e.g., it is much easier to order the soldiers to shoot down a civilian airplane than to use cyber-attacks against it), and secondly, a significant part of civilian infrastructure usually belongs to the state itself. In situations where governments do not have effective control over some part of their territory due to foreign occupation or civil war, Geneva Conventions would automatically apply and state violence would have to be viewed within the framework of international humanitarian law (this will be further discussed in a separate sub-chapter below). The notion of "external state terrorism," on the other hand, is unlikely to crystallize in customary law in the future, since customary norms arise from state behavior and require their acceptance. It would seem that a majority of countries today believe a state cannot be a

53. Compare the western draft ("the activities undertaken by the military forces of a State in the exercise of their official duties, inasmuch as they are governed by other rules of international law, are not governed by this Convention") with the OIC version ("The activities undertaken by the military forces of a State in the exercise of their official duties, inasmuch as they are in conformity with international law, are not governed by this Convention."). *See* U.N. Rep. of the Ad Hoc Comm., 6th Sess., Jan. 28–Feb. 1, 2002, U.N. Doc. A/57/37 Annex IV; GAOR, 57th Sess., Supp. No. 37 (2002); *see also* U.N. Rep. of the Ad Hoc Comm., 14th Sess., Apr. 12–16, 2010, U.N. Doc. A/65/37; GAOR, 65th Sess., Supp. No. 37 (2010). For more information, also see previous and subsequent reports. Note that the Maritime Convention as amended by the 2005 Protocol (Article 2bis(2)), 2005 Nuclear Terrorism Convention (Article 4(2)), 2010 New Civil Aviation Convention (Article 6(2)) and the Unlawful Seizure Convention as amended by the 2010 Protocol (Article 3bis(2)) all use the western wording.

54. *See generally* RICHARD JACKSON, LEE JARVIS, JEROEN GUNNING & MARIE BREEN SMYTH, TERRORISM: A CRITICAL INTRODUCTION (2011).

55. DONALD J. HANLE, TERRORISM: THE NEWEST FACE OF WARFARE 164 (Yonah Alexander ed., 1989).

perpetrator of conventional terrorism, as evidenced by the large number of signatories to the existing twelve conventions and their protocols without reservations regarding this matter (with minor exceptions[56]). Therefore, the theory of state terrorism that may be viable in relation to conventional extremism does not apply in cyber-space.

This does not rule out the possibility of indirect state involvement in the form of state-sponsored cyberterrorism. It must be said that allowing their territories to be used for acts against the rights of other states is illegal according to the ICJ,[57] while the Friendly Relations Declaration imposes a duty upon countries "to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in . . . such acts . . . ."[58] If one country organizes, actively supports, or contributes to the commission of one or more terrorist offences through cyber-space, it can be said to be a state-sponsor of cyberterrorism.[59] Some conventions (Convention for the Suppression of Acts of Nuclear Terrorism, International Convention for the Suppression of the Financing of Terrorism, and others) foresee individual criminal responsibility for such acts, and although state leadership enjoys immunity, it should still be possible to prosecute the responsible individuals after they have stepped down from their posts (if the relevant conventions are ratified in those states).

B. Non-State Actors

Non-state actors have been consistently viewed as groups capable of perpetrating acts of terror and this status nowadays stems from the international customary law. This is evidenced by a number of the UN Security Council documents,[60] notably Resolutions 1526 ("Reiterating

56. *See* International Convention for the Suppression of Terrorist Bombings, Dec. 15, 1997, S. TREATY DOC. NO. 106-6 (1998). Cuba refers to "state terrorism" in its respective reservations to the International Convention for the Suppression of Terrorist Bombings (1997). *See id*.

57. *See* Corfu Channel (Merits), 1949 I.C.J. 4, 22 (Apr. 9).

58. *See* Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), Principle 1, ¶ 9, U.N. Doc. A/8082 (Oct. 24, 1970).

59. Allen D. Walker, Applying International Law to the Cyber Attacks in Estonia 13 (Apr. 2008) (unpublished graduation requirement report) (on file with the Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama).

60. *See generally* S.C. Res. 1989, U.N. Doc. S/RES/1989 (June 17, 2011); S.C. Res. 1988, U.N. Doc. S/RES/1988 (June 17, 2011); S.C. Res. 1963, U.N. Doc. S/RES/1963

its condemnation of the Al-Qaida network and other associated terrorist groups for . . . criminal terrorist acts"), 1530 ("Condemns [. . .] the bomb attacks in Madrid, Spain, perpetrated by the terrorist group ETA . . ."), 1963, and 1989 ("Expressing concern at the increase in incidents of kidnapping and hostage-taking committed by terrorist groups . . . .").

Currently there are over one hundred international terrorist organizations ranging from small groups designated as such by a few states (Fianna Éireann, Harkat-ul-Jihad-al-Islami, People's Mujahedin of Iran) to groups widely recognized as terrorist organizations (Al-Qaeda, Lashkar-e-Taiba, Asbat al-Ansar). In the modern world, there are plenty of cyber safe havens where these groups can operate without fear of direct reprisal.[61] The success of counter-terrorist operations is likely to encourage these non-state actors to turn to cyberterrorism[62] and some groups, having lost their physical sanctuary in key areas, have turned to the sanctuary of cyberspace.[63]

In 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey defined three levels of organizations' cyberterrorism capability:

1. Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
2. Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
3. Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target

---

(Dec. 20, 2010); S.C. Res. 1904, U.N. Doc. S/RES/1904 (Dec. 17, 2009); S.C. Res. 1822, U.N. Doc. S/RES/1822 (June 30, 2008); S.C. Res. 1735, U.N. Doc. S/RES/1735 (Dec. 22, 2006); S.C. Res. 1617, U.N. Doc. S/RES/1617 (July 29, 2005); S.C. Res. 1530, U.N. Doc. S/RES/1530 (Mar. 11, 2004); S.C. Res. 1526, U.N. Doc. S/RES/1526 (Jan. 30, 2004); S.C. Res. 1455, U.N. Doc. S/RES/1455 (Jan. 17, 2003); S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

61. *See generally* Kenneth Geers, *Cyber Weapons Convention* 26 COMPUTER L. & SEC. REV. 547 (2010).

62. Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, U.S. INST. OF PEACE, Dec. 2004, at 1, 11.

63. Stuart H. Starr, *Towards and Evolving Theory of Cyberpower*, *in* THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE, 18, 34 (Christian Czosseck & Kenneth Geers eds., 2009).

> analysis, command and control, and organization learning capability.[64]

In 2002 evidence showed that Al-Qaeda considered a cyber-attack against a dam,[65] and in 2005 the group planned to bring down the entire internet traffic in the UK.[66] The Real IRA declared "the future lay in cyberterrorism rather than car bombs"[67] and supporters of the Liberation Tigers of Tamil Eelam in the past have spammed Sri Lankan embassies with emails meant to disrupt their communications.[68] Though cyberterrorism has not yet caused any casualties, these examples demonstrate that existing terrorist groups are interested in inflicting damage through cyber-space and in cyberterrorism per se. The low level of their technical expertise ("simple-unstructured") can be, and sometimes is, compensated by recruiting technically-skilled individuals[69] to improve the terrorists' capabilities in this regard.[70]

Entire groups of cyber-criminals can work together and even merge with known terrorist organizations if they share similar radical views, religious or socio-political interests,[71] in order to engage in cyberterrorism. Alternatively, extremists can obtain knowledge and necessary programs from hacker teams for a fee. Some groups like the "Russian Hacker Association" have been offering one-time services over the Internet;[72]

---

64. BILL NELSON, RODNEY CHOI, MICHAEL IACOBUCCI, MARK MITCHELL & GREG GAGNON, CYBERTERROR: PROSPECTS AND IMPLICATIONS, at IX (1999), *cited with approval in* Dorothy E. Denning, *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*, GEORGETOWN UNIV. (May 23, 2000), http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

65. Shima D. Keene, *Terrorism and the Internet: A Double-Edged Sword*, 14 J. MONEY LAUNDERING CONTROL 359, 364-65 (2011).

66. *Id*. at 363.

67. Simon Finch, *Cyber-Terrorism is Real—Ask Estonia*, TELEGRAPH (May 30, 2007, 12:01 AM), http://www.telegraph.co.uk/comment/personal-view/3640255/Cyber-terrorism-is-real-ask-Estonia.html.

68. Denning, *supra* note 64.

69. Andrew Rathmell, *Cyber-Terrorism: The Shape of Future Conflict?*, 6 J. FIN. CRIME 277, 279 (1999).

70. STEPHEN J. LUKASIK & REBECCA GIVNER-FORBES, DETERRING THE USE OF CYBER FORCE 46 (2009), *available at* http://www.learningace.com/doc/1347649/5e4bd5e592d706f6019865a25bd59160/cyber_deterrencev2.

71. CLAY WILSON, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 18 (2008).

72. NICK ELLSMORE, CYBER-TERRORISM IN AUSTRALIA: THE RISK TO BUSINESS AND A PLAN TO PREPARE 7 (2002).

information about computer vulnerabilities for which no software patch (software designed to fix problems) exists yet can be obtained nowadays on the black market for a sum of $1,000 to $5,000 USD.[73] Arrangements with these groups for modifying existing programs or developing new ones to target a particular object (nuclear reactor, airplane, etc.) are possible.[74]

Some individual cyber-criminal groups can have overlapping goals with the "field-terrorists," but they prefer to act independently, trying to engage in "pure cyberterrorism." For example, the "G-Force Pakistan" group (sympathizers of Al-Qaeda) waged an independent cracking campaign against the internet community (peaking in 2001–2002) with the aim of liberating Kashmir, although its activities mostly consisted of defacing websites[75] and not actual acts of cyberterrorism.

C. Corporations

Corporations have long been objects of cyber-attacks,[76] eventually leading to their heavy investment in information technology (IT) security.[77] This, in turn, resulted in them having the most advanced cyber-defense (and logically, cyber-offense) capabilities, which exceed those of many states. In a world that moves away from "statecentrism,"[78] the know-how, relative autonomy of operations,[79] significant funding and a structured team of experts make corporations a potential perpetrator of cyberterrorist acts. Though their cyber-attacks are likely to target competitors,[80] companies (especially multilateral corporations) may be interested in destabilizing a country's (or the entire world's) economy for profit, or they may be guided by the extremist views of their leadership.

---

73. WILSON, *supra* note 71.

74. David Peter Hansen, Is "Cybterterrorism" a Serious Threat to the Integrity of Computer Networks? 29 (2010) (unpublished dissertation, University of Bradford), *available at* http://files.dave.dk/cyberterrorism.pdf.

75. Namosha Veerasamy, Motivation for Cyberterrorism 3 (Aug. 2010) (unpublished presentation, 9th Annual Information Security for South Africa) (on file with Council for Scientific and Industrial Research Information Services, South Africa).

76. Gaurav Jain, *Cyberterrorism: A Clear and Present Danger to Civilized Society?*, 3 INFO. SYS. EDUC. J. 3, 6 (2005), *available at* http://isedj.org/3/44/ISEDJ.3(44).Jain.pdf.

77. Compare this to smaller enterprises, some of which, in the words of U.S. adviser on cybersecurity Richard Clarke, "spend more on coffee than on cyber-security." *See* Robert Lemos, *Security Guru: Let's Secure the Net*, ZDNET.COM (Feb. 19, 2002, 12:25 PST), http://www.zdnet.com/news/security-guru-lets-secure-the-net/120859.

78. TOBY BLYTH, CYBERTERRORISM AND PRIVATE CORPORATIONS: NEW THREAT MODELS AND RISK MANAGEMENT IMPLICATIONS 24 (1999).

79. Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 104-05 (2001) (discussing information warfare as a new type of weapon).

80. *Id*. at 105.

Unlike terrorist organizations, corporations are often pressured to be more transparent,[81] and to have a legal personality within their host state. Though this does not preclude criminal behavior, this makes them a special category of non-state actors ("any person") that can be held legally responsible for offenses criminalized by existing anti-terrorism conventions. In other words, aside from the leadership of the corporation and members of the IT team that was directly involved in cyberterrorism, it is possible to prosecute the company itself, if the respective legal systems permit it.

D. Individuals

Finally, like the independent cyber-criminal groups, individual persons may engage in acts of terrorism online, if motivated by money, prestige or ideology.[82] These one-man cyberterrorists (so to say, "cyber-Breiviks") who have the knowledge necessary to conduct online attacks[83] work alone, and, like their less sophisticated counterparts, can be divided into categories revealing their motivations: psychopathic terrorists (individuals who seek satisfaction in the need to control), religious and political ethno-geographic terrorists (struggling for a "group-cause"), and retributional terrorists (persons who suffered an atrocity against themselves, their family, or community).[84] In addition, cyberterrorism includes other categories of persons which are not typical to traditional extremism, such as the greed-prompted (offering to wage cyberterrorism for a fee) or "rebels" (who protest against the entire world order; this category includes teenage cyber-criminals as well).[85]

---

81. United Nations Conference on Trade and Development, Geneva, Switz., 2004, *Disclosure of the Impact of Corporations on Society: Current Trends and Issues*, UNCTAD/ITE/TEB/2003/7 (Aug. 26, 2004).

82. Suleyman Ozeren, Global Response to Cyberterrorism and Cybercrime: A Matrix for International Cooperation and Vulnerability Assessment (Aug. 2005) (dissertation prepared for philosophy doctorate, University of North Texas) (on file with author).

83. Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404, 404-06 (2007) (discussing the growing threat of cyber attacks).

84. Raymond H. Hamden, *The Retributional Terrorist: Type 4*, *in* 2 THE PSYCHOLOGY OF TERRORISM: CLINICAL ASPECTS AND RESPONSES 174 (Chris E. Stout ed., Greenwood 2002).

85. Arun Kr. Singh & Ahmad T. Siddiqui, *New Face of Terror: Cyber Threats, Emails Containing Viruses*, 1 ASIAN J. TECH. & MGMT. RES. (2011) (discussing the new face of terror).

As mentioned previously, the existing treaty regime pertaining to terrorism allows for the prosecution of individuals for terrorism (and cyberterrorism as its sub-category). It should be noted though that states may have an interest in avoiding prosecution of "talented" cyberterrorists, if those cyberterrorists act in the interests of the state. Due to the lack of cyber-experts, they can even be seen as limited state assets.[86] Obviously this approach would be a violation of a country's legal obligations, and could possibly be seen as state-sponsorship of cyberterrorism.

III. TARGETS AND AIMS

A. Reasons for Cyberterrorism

Extremists have a lot of secondary reasons to resort to cyberterrorism: it helps weaken "enemy's" operational capabilities; destroys the reputation of an organization, nation, or alliance; demonstrates that terrorists groups are capable of inflicting significant harm on their targets; and even persuades those attacked to change affiliation.[87] However, the main purpose remains to inflict damage on the selected targets and maximize the harmful consequences.

Targets which might be susceptible to cyberterrorism include, but are not limited to: air-traffic controls and navigation computers on board of commercial planes and ships, atomic power plants, and nuclear-material enrichment facilities. Conventional attacks against these targets by non-state actors are already outright criminalized by the existing counter-terrorism agreements and their protocols. Other vulnerable targets comprise power substations, water supply networks and automated food preparation factories, "smart" transportation grids, banks and stock-exchanges, dams, computerized cars, gas and oil pipelines, space-navigation controls, medical institutions, and implanted medical devices. Cyber-strikes against these targets may result in terrorism-like effects and contribute to the creation of restlessness and mob-mentality among the general population.

Some analysts note that acts of cyberterrorism against these targets are less favorable for terrorist organizations, since they would result in less immediate drama and have a lower psychological impact than a conventional attack.[88] Indeed, a carefully-planned physical act of terror

86. JEFFREY CARR, INSIDE CYBER WARFARE 29 (2009).

87. Shamsuddin Abdul Jalil, Counting Cyber Terrorism Effectively: Are We Ready to Rumble? (June 2003) (practical assignment for GIAC security essentials certification) (on file with SANS Institute and author); *see also* Rajeev C. Puran, Beyond Conventional Terrorism. . . The Cyber Assault (Feb. 2003) (practical assignment for GIAC security essentials certification) (on file with SANS Institute and author).

88. CLAY WILSON, COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 18-19 (2005).

can have a tremendous effect on population's feeling of security,[89] as evidenced by the Nord-Ost hostage crisis in Moscow (2002), Madrid bombings (2004), London bombings (2005) and other terrorist attacks. However, unlike traditional terrorism, cyberterrorism does not require substantial financial investments or physical presence to be successful. In fact, the only real prerequisite to carry out an act of cyberterrorism is technical knowledge—once acquired, a free and reusable asset.[90] This makes cyberterrorist attacks a much more convenient option, and thus, very probable in some situations where distance and financial matters may otherwise pose a problem for the extremists.

While the current international treaty regime pertaining to terrorism does not directly mention cyber-attacks, and the majority of the existing conventions were created when cyber-strikes were unimaginable, this does not exclude their application to the acts of cyberterrorism. In addition, the principles enshrined in them help influence the formation of international customary law[91] in relation to these acts.

In the context of cyberterrorism, it is important to distinguish between the real risks and low-probability scenarios, which are close to fiction. For the purposes of this Article, the legal instruments shall be analyzed in the order of increasing possibility of committing terrorist acts, criminalized therein, through cyber-space: from impossible to highly probable.

B. Manufacturing Explosives

The crime of manufacturing unmarked explosives, prohibited by Article 2 of the 1991 Plastic Explosives Convention,[92] cannot be perpetrated through cyber-space even in theory. Even if computers in official facilities are in some manner engaged in the preparation process, and a program malfunction can result in a wrong marking being put on the materials, the explosives are thoroughly checked by humans before they

89. Patrick S. Tibbetts, *Terrorist Use of the Internet and Related Information Technologies: A Monograph*, U.S. ARMY (2002), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA403802.

90. *See generally* Sarah Gordon & Richard Ford, *Cyberterrorism?*, SYMANTEC (2003), https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

91. Matthew J. Skleroy, *Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Negelect Their Duty to Prevent*, 201 MIL. L. REV. 1, 64-65 (2009) (discussing the common principles of *opinio juris* when cyberattacks are used as a terrorist weapon).

92. ICAO, 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection, June 21, 1988, ICAO Doc. S/22393, 30 I.L.M. 721.

are released for sale or use. Moreover, in this case the manufacturing process would not be done by the same persons who are carrying out the cyber-attacks, ruling out criminal responsibility due to the lack of mens rea.

C. Bombings

The 1997 Terrorist Bombing Convention prohibits[93] another crime that is impossible to commit through cyber-space: unlawfully and intentionally delivering, placing, discharging, or detonating "an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility." Article 1(3) of the same convention clarifies that "explosive or other lethal device" means a) an explosive or incendiary weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage; or b) a weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins or similar substances or radiation or radioactive material. "Delivering" and "placing" of these weapons or devices is a physical act that cannot be done through cyber-space; they are also rarely armed before being "delivered" by a legitimate agent (allowing discharge and detonation), and seldom detonated through electronic means (chemical, mechanical, or electrical triggers are used instead).

Looking back at the cyber-attack on the Trans-Siberian natural gas pipeline in 1982, one should consider a more inclusive interpretation of the word "device" in the Convention. The 1982 incident, indeed, proves that a cyber-attack against a non-military device that is part of the oil and gas energy infrastructure can result in an explosion. However, what is being "detonated" and "discharged" in such case is the gas or petrol. Therefore, according to grammatical interpretation of law, the exploited device itself does not have the capacity to explode, since explosive materials are not part of it.

---

93. International Convention for the Suppression of Terrorist Bombings, art. 2(1), Dec. 15, 1997, http://treaties.un.org/doc/db/Terrorism/english-18-9.pdf ("Any person commits an offense within the meaning of this Convention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility:
    a. With the intent to cause death or serious bodily injury; or
    b. With the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss.").

Aviv Cohen notes[94] that computers at nuclear reactors and biological labs may fall under the definition of Article 1(3)(b) (a device that has the capacity to cause death, injury and damage through the release of toxins or radiation), since they control the levels of "temperature, moisture, radiation and other data that is crucial to safety" and as such, upon a cyberterrorist act, can cause a disaster. Cohen further argues[95] that this is supported by Article 31 of the Vienna Convention on the Law of Treaties, according to which the Terrorist Bombing Convention should be interpreted in light of its purpose. What Cohen fails to note, however, is that the same Article 31(1) states that the "terms of the treaty" must be given "ordinary meaning", moreover, taking into account the year when the Terrorist Bombing Convention was created (i.e. "circumstances of its conclusion," in accordance with the Article 32(a) of the Vienna Convention[96]), its purpose and objective could not have been anything else but to prevent traditional bombings and not cyberterrorism. Consequently, cyberterrorists cannot violate the Terrorist Bombing Convention.

D. Hostages

The 1979 Hostages Convention calls for[97] appropriate penalties against "any person who seizes or detains and threatens to kill, to injure or to continue to detain another person . . . in order to compel a third party . . . to do or abstain from doing any acts as an explicit or implicit condition for the release of the hostage . . . ." Nowadays, the possibility of holding persons hostage through "pure" cyber-attacks is close to impossible. The terrorists, with some luck, may be able to capture someone in a confined high-tech contraption, such as an elevator or a computerized car, but the prospect of injuring or continuing to detain him or her is very unlikely—modern cable-borne, hydraulic, and other elevators are employing mechanical devices (including brakes), nullifying any physical danger from cyber-attacks. At the same time, vehicle windows can be broken and elevator doors can be opened manually when the rescue arrives, excluding the possibility of continuous detention.

---

94. Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. & L. 1, 27-28 (2010) (discussing international responses to terrorism).

95. *Id*. at 28.

96. *See also* SIMON CHESTERMAN, JUST WAR OR JUST PEACE? HUMANITARIAN INTERVENTION AND INTERNATIONAL LAW 48 (2001).

97. International Convention Against the Taking of Hostages, art. 1(1) & 2, Dec. 17, 1979, 1316 U.N.T.S. 207.

E. Financing Terrorism

Providing and collecting funds in order to carry out a terrorist act[98] under the 1999 Terrorist Financing Convention hardly fits the notion of cyberterrorist offense: generally, "providing" implies money or other assets are already in possession of the perpetrator, while storing and maintaining them does not require a cyber-attack. At the same time it should be noted that breaking into someone's financial online accounts by means of cyber-attack for the purposes of transferring money to terrorists or acquiring them for further use by extremist organizations would satisfy the narrow overlapping legal requirements to be considered both cyber-strike and an offense under the Terrorist Financing Convention.

F. Protected Persons

The 1973 Diplomatic Agents Convention criminalizes[99] the intentional commission of "a murder, kidnapping or other attack upon the person or liberty of an internationally protected person" or "a violent attack upon the official premises, the private accommodation or the means of transport of an internationally protected person likely to endanger his person or liberty." "Murder" or injuring ("other attack upon the person") is the prohibited conduct which does not depend on the means employed. It can take the form of crashing a protected person's transport, tempering with a hospital computer, infecting his implanted medical device, a computer-triggered explosion, or a similar harmful act. A list of diplomatic agents and information about their cyber-

---

98. International Convention for the Suppressing of the Financing of Terrorism, art. 2(1)

("Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.").

99. Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, art. 2(1), Dec. 14, 1973, 1035 U.N.T.S. 167.

implants, cars, etc. can be provided over the Internet,[100] and a bounty may encourage persons from all over the world to engage in such attacks.

Because injuries have to be a direct consequence of a cyber-strike to be "intentional," acts such as general food or water poisoning through cyber-means do not fall under those prohibited by the present Convention. The same principle applies to cyber-attacks against the premises, accommodation, or means of transport—they have to be direct and threaten the life of the protected person to constitute cyberterrorism. Kidnapping of state officials and their family members[101] is ruled out for the same reasons as ordinary hostage taking (see above), although trapping protected persons in a computerized car or elevator would constitute an "other attack upon liberty."

G. Maritime Vessels

Current technology does not permit taking full control over a ship[102] through cyber-attacks.[103] As mentioned above, "placing" a device or substance is a physical act; and even if a cyber-saboteur onboard a ship uses an infected USB flash-drive, it is not the USB device that would endanger the safe navigation, but the program itself—a virtual object, not substance (physical matter). Breach of Article 3(1)(d)[104] therefore, is also impossible.

Injuring or killing a person with intent to carry out a terrorist attack onboard a ship (prohibited by Article 3(1)(g)[105]) can theoretically be done by tempering with an electronic medical implant, yet it is not

100. Steve Saint-Claire, *Overview and Analysis on Cyber Terrorism*, 3 SCH. DOCTORAL STUD. EUR. UNION J. 85, 89 (2011).

101. *See* Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, *supra* note 100, at art. 1(1)(a) (describing protected persons).

102. *See id*. at art. 1(1)(a) (explaining that warships, naval auxiliary ships, vessels of customs or police authorities and ships withdrawn from navigation are not covered by the Maritime Convention).

103. This does not include violations of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, art. 3(1)(a), Mar. 10, 1988, 1678 U.N.T.S. 224, which reads: "Any person commits an offense if that person unlawfully and intentionally: (a) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation."

104. *See id*. at art. 3(1)(d).

105. *See id*. at art. 3(1)(g), which reads: "injures or kills any person, in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (a) to (f)."

necessary at all to conduct other cyber-attacks. "An act of violence against a person onboard a ship if that act is likely to endanger the safe navigation" (Article 3(1)(b)[106]) would have to be targeted against all persons with crucial knowledge, or in a manner that would devastate a significant part of the ship required for safe navigation, in order to be considered terrorism under the present Convention—an almost impossible prospect. This also applies to an improbable possibility of damaging the ship or its cargo through cyber-attacks, prohibited by Article 3(1)(c).[107] Seriously damaging and interfering with the operation of navigational facilities (illegal under Article 3(1)(e)[108]) and communicating false information to endanger the safety of a ship (criminalized by Article 3(1)(f)[109]) through cyber-strikes, on the other hand, are highly probable in cases where the ship is new and it heavily relies on computer technology for navigation.

Article 3bis(1), added to the Maritime Convention by the 2005 Protocol, sets out a list of additional terrorist offenses involving a ship. Although sub-paragraph 3bis(1)(b) (and Article 3ter as a whole) can be disregarded, since virtual attacks cannot result in "transporting on board a ship" of various dangerous materials, WMDs (or persons), sub-paragraph (1)(a) of Article 3bis merits a closer attention. It reads:

> Any person commits an offence . . . if that person unlawfully and intentionally . . . , when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act:
>
> (i) uses against or on a ship or discharges from a ship any explosive, radioactive material or BCN weapon in a manner that causes or is likely to cause death or serious injury or damage; or
>
> (ii) discharges, from a ship, oil, liquefied natural gas, or other hazardous or noxious substance, . . . in such quantity or concentration that causes or is likely to cause death or serious injury or damage; or
>
> (iii) uses a ship in a manner that causes death or serious injury or damage.[110]

Although this provision specifies the necessary terrorist intent, actus reus is unlikely. The first two sub-paragraphs of 3bis(1)(a) quoted above

---

106. *See id*. at art. 3(1)(b), which reads: "performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship."

107. *See id*. at art. 3(1)(c), which reads: "destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship."

108. *See id*. at art. 3(1)(e), which reads: "destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship."

109. *See id*. at art. 3(1)(f), which reads: "communicates information which he knows to be false, thereby endangering the safe navigation of a ship."

110. *Id*. which reads: "(iv) threatens, with or without a condition, as is provided for under national law, to commit an offence set forth in subparagraph (a)(i), (ii) or (iii)."

criminalize acts that, in theory, could be perpetrated through cyber-attacks, if the hazardous materials are present onboard a ship and they can somehow be destabilized through an electronic network. In reality, however, this is almost impossible since there is no good reason to connect such materials to a complicated computer network.

Breaching sub-paragraph 3bis(1)(a)(iii) is even more unlikely, since, as mentioned previously, no technology exists that would allow a ship to be navigated remotely. Even if it did, cyberterrorists' plans to use the ship for causing death and destruction could be hampered with a simple anchor.

H. Fixed Platforms

Article 2(1)[111] of the 1988 Protocol to the Maritime Convention applies the principles, formulated in Article 3(1) of the latter, to the fixed platforms. For the same reasons as in the case of ships, seizing and controlling a platform (Article 2(1)(a)) and placing a device or substance that can destroy it (Article 2(1)(d)) are ruled out in the context of cyberterrorism. Cyber-violence against a person (Article 2(1)(b)) would have to be carried out in an unlikely wide-spread manner that endangered the safety of the entire fixed platform (Article 2(1)(c)). Though injuring a person in connection with these offenses (Article 2(1)(e)) would also be possible by attacking his or her medical implant, due to the unlikelihood of the offenses in sub-paragraphs (a)-(d) of Article 2(1), this can only be part of a hybrid terrorist attack and not a case of "pure" cyberterrorism.

The offenses in Article 2bis[112] of the 2005 Protocol to the Fixed Platforms Protocol are very similar to those in Article 3bis(1)(a) of the

111. *See* Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, art. 2(1), Mar. 10, 1988, 1678 U.N.T.S. 304, 27 I.L.M. 685 [hereinafter Platforms Protocol], which reads:

> Any person commits an offense if that person unlawfully and intentionally: (a) seizes or exercises control over a fixed platform by force or threat thereof or any other form of intimidation; or (b) performs an act of violence against a person on board a fixed platform if that act is likely to endanger its safety; or (c) destroys a fixed platform or causes damage to it which is likely to endanger its safety; or (d) places or causes to be placed on a fixed platform, by any means whatsoever, a device or substance which is likely to destroy that fixed platform or likely to endanger its safety; (e) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (a) to (d).

112. *See id*. at art. 2bis, which reads:

Maritime Convention. For the same reasons, since dangerous materials and WMDs are not usually connected to conventional computers, a breach of Article 3bis(1)(a) of the Maritime Convention is impossible in reality. In addition, if presence of radioactive or other hazardous materials onboard vessels can be explained by necessity of transportation, there is little reason to keep them on fixed platforms.

I. Nuclear Terrorism

Since nuclear material is a physical entity, out of the acts criminalized by Article 7(1)[113] of the 1980 Nuclear Materials Convention, receipt, possession, use, transfer, alteration, disposal (Article 7(1)(a)), theft, robbery (Article 7(1)(b)), embezzlement, and fraudulent obtaining (Article 7(1)(c)), carrying, sending, or moving (Article 7(1)(d), as amended in 2005[114]) of nuclear material are unlikely in the context of cyberterrorism, though not impossible.[115] A demand for nuclear material by use of cyber-force (Article 7(1)(d)) would constitute a hybrid terrorist

---

> Any person commits an offence within the meaning of this Protocol if that person unlawfully and intentionally, when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act:
>
> (a) uses against or on a fixed platform or discharges from a fixed platform any explosive, radioactive material or BCN weapon in a manner that causes or is likely to cause death or serious injury or damage; or
>
> (b) discharges, from a fixed platform, oil, liquefied natural gas, or other hazardous or noxious substance, which is not covered by subparagraph (a), in such quantity or concentration that causes or is likely to cause death or serious injury or damage; or
>
> (c) threatens, with or without a condition, as is provided for under national law, to commit an offence set forth in subparagraph (a) or (b).

113. *See* The Convention on the Physical Protection of Nuclear Material, art. 7(1), Mar. 3, 1980, 1456 U.N.T.S. 125 [hereinafter Nuclear Materials Convention], which reads:

> The intentional commission of:
>
> (a) An act without lawful authority which constitutes the receipt, possession, use, transfer, alteration, disposal or dispersal of nuclear material and which causes or is likely to cause death or serious injury to any person or substantial damage to property;
>
> (b) A theft or robbery of nuclear material;
>
> (c) An embezzlement or fraudulent obtaining of nuclear material;
>
> (d) An act constituting a demand for nuclear material by threat or use of force or by any other form of intimidation; . . . shall be made punishable offense . . . .

114. *See* Amendment to the Convention on the Physical Protection of Nuclear Material, art. 7(1)(d), Nov. 18, 2010, S. Treaty Doc. No. 110-6, which reads: "an act which constitutes the carrying, sending, or moving of nuclear material into or out of a State without lawful authority."

115. Consider if the US B-52H bomber, that was mistakenly transferring nuclear warheads in 2007, was connected to the internet and hijacked by cyberterrorists.

act. The most probable relevant terrorist act in relation to nuclear material that can be done purely via cyber-space, therefore, is its "dispersal", which is likely to cause death or serious injury or substantial damage to property (Article 7(1)(a)) or the environment (as amended), or as specified in the amended Article 7(1)(e), "an act directed against a nuclear facility,[116] or an act interfering with the operation of a nuclear facility, where the offender causes, or . . . knows that the act is likely to cause, death or . . . injury . . . or substantial damage to property or to the environment . . . ."

Contemporary nuclear reactors run on uranium-235 or plutonium-239 fissile—matter that falls under the definition of "nuclear material" in Article 1(a)[117] of the Nuclear Materials Convention. The Slammer's intrusion into the Ohio nuclear power plant in 2003 and the Stuxnet attacks in 2009–2010 prove that it is indeed possible to damage nuclear facilities with cyber-attacks. These two particular incidents inflicted minor damage and did not cause any "substantial" damage or injury, nor were likely to cause it (despite the unpredictable behavior or infected hardware), and therefore fell short of being criminalized by the present Convention. Nevertheless, attempts to cause destruction through cyber-space continue,[118] and the possibility of substantial damage in the future should not be ruled out.

As in the case of Nuclear Materials Convention, certain physical acts under Article 2(1)[119] of the 2005 Nuclear Terrorism Convention, such as

---

116. "'[N]uclear facility' means a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material." *Id*. at art. 1(d).

117. "'[N]uclear material' means plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; uranium enriched in the isotopes 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue; any material containing one or more of the foregoing." Nuclear Materials Convention, *supra* note 114, at art. 1(a).

118. Michael L. Hummel, *Internet Terrorism*, 2 HOMELAND SECURITY REV. 117, 121 (2008).

119. *See* International Convention for the Suppression of Acts of Nuclear Terrorism, art. 2(1), Apr. 13, 2005, 2445 U.N.T.S. 89, 44 I.L.M. 815 [hereinafter Nuclear Terrorism Convention], which reads:

> Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally:
>
> (a) Possesses radioactive material or makes or possesses a device:
>
> (i) With the intent to cause death or serious bodily injury; or
>
> (ii) With the intent to cause substantial damage to property or to the environment;

possessing radioactive material,[120] making or possessing a nuclear device[121] (Article 2(1)(a)), or using a nuclear device (Article 2(1)(b)) are excluded from the framework of cyberterrorism. The present instrument, however, also prohibits damaging (or using) a nuclear facility[122] in a manner which releases or risks the release of radioactive material (Article 2(1)(b)). Unlike the amended Article 7(1)(e) of the Nuclear Terrorism Convention, aside from being committed with the intent to cause death, injury, or damage, the crime becomes a terrorist act also in the case when the perpetrator(s) intend to compel a natural or legal person, an international organization, or a state to do or refrain from doing any act (Article 2(1)(b)(iii)).

Despite the minor damage that Stuxnet caused, the destruction of centrifuges did risk the release of radioactive material (even if it was in small quantities) and one of its goals seems to have been to make the Islamic Republic of Iran abandon its nuclear program. Therefore, the use of Stuxnet against Iranian nuclear facilities was in breach of the obligations set by the Nuclear Terrorism Convention and, in essence, is the first act of nuclear cyberterrorism in history. Nevertheless, from a legal perspective, this holds true only on a customary level, since neither Iran nor the potential "suspects"—Israel and USA—had signed the Nuclear Terrorism Convention by 2011, absolving them from any criminal responsibility.

J. Aircrafts

Cyberterrorism in the context of offenses against aircrafts do not require presence of a person onboard during flight. Cyber-attacks against

---

(b Uses in any way radioactive material or a device, or uses or damages a nuclear facility in a manner which releases or risks the release of radioactive material:
(i) With the intent to cause death or serious bodily injury; or
(ii) With the intent to cause substantial damage to property or to the environment; or
(iii) With the intent to compel a natural or legal person, an international organization or a State to do or refrain from doing an act.

120. *Id*. at art. 1(2).

121. *Id*. at art. 1(4) (defining "device" as "(a) Any nuclear explosive device; or (b) Any radioactive material dispersal or radiation-emitting device which may, owing to its radiological properties, cause death, serious bodily injury or substantial damage to property or to the environment").

122. *Id.* at art. 1(3) (defining "Nuclear facility" as "(a) Any nuclear reactor, including reactors installed on vessels, vehicles, aircraft or space objects for use as an energy source in order to propel such vessels, vehicles, aircraft or space objects or for any other purpose; (b) Any plant or conveyance being used for the production, storage, processing, or transport of radioactive material").

planes are much more likely to occur through electronic networks (or at least by installing harmful programs before flight), since a person who makes his way to the cockpit can crash a plane much faster manually without any programs, and because the wireless devices nowadays are not capable of taking control over a conventional (manned) aircraft. In addition, there is a risk that suspicious devices onboard that will inevitably cause interference will be noticed, confiscated or destroyed by the crew. These factors exclude the applicability to cyber-attacks of the non-amended version of the 1970 Unlawful Seizure Convention[123] as a whole, although Article 6(1) of the 1963 Aviation Convention still allows the aircraft commander to impose reasonable measures upon persons who are suspected of jeopardizing safety onboard the plane (e.g., those trying to commit a cyber-attack).

On the other hand, Article 1(1)[124] of the Unlawful Seizure Convention, included in its 2010 Protocol, does not require presence of a person inside an aircraft, and criminalizes seizure of an aircraft "by any technical means" (including cyber-attacks). The 2010 Protocol also replaces reference to an aircraft "in flight" in Articles 1 and 3 with an "aircraft in service"[125] (lasting from aircraft preparation to twenty-four hours after landing). As mentioned before, no cyber-attack can establish effective control over a manned aircraft. However, under the amended text of the Convention it is possible to commit an act of cyberterrorism by seizing control over unmanned aerial vehicles (UAVs). Aircrafts such as remote piloted drones that are used for various purposes in more than fifty countries[126] can be "hijacked" by infecting their control stations

123. Convention for the Suppression of Unlawful Seizure of Aircraft, *supra* note 26, at art 1 (criminalizing the act of seizing and exercising control over an aircraft).

124. *See* Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, *supra* note 26, at art. II, which reads: "Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means."

125. Article 3(1) of the Amended Unlawful Seizure Convention reads: "For the purposes of this Convention, an aircraft is considered to be in service from the beginning of the pre-flight preparation of the aircraft by ground personnel or by the crew for a specific flight until twenty-four hours after any landing. In the case of a forced landing, the flight shall be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board." *Id*. at art. V.

126. These countries include the USA, Russia, China, France, Germany, Georgia, India, Israel, Pakistan, Egypt, and others. *See* Jack M. Beard, *Law and War in the Virtual Era*, 103 AM. J. INT'L L. 409, 444 (2009).

and, actually, these stations have been subject to cyber-attacks before.[127] Since Article 3(2) excludes applicability of the Unlawful Seizure Convention to military, customs, and police aircraft, cyberterrorism under the present instrument is possible only when unlawfully exercising control over commercial, civilian, and scientific UAVs.

Placing or causing a device or substance to be placed on board, criminalized by Article 1(1)(c)[128] of the 1971 Civil Aviation Convention, is impossible through cyber-space. As in the case of Maritime Convention, performing an act of cyber-violence against a person on board an aircraft in service, in a manner that endangers the plane's safety (Article 1(1)(a)[129]) would have to target a key person (e.g., a pilot). Constant movement of the airplane at high altitudes will prevent a cyber-attack against this person's medical implant (the only possibility in this case) from the ground, leaving only the option of sneak "attack" from one of the passengers. However, the chances of both pilots having computerized implants and both cyber-strikes from within the aircraft being successful are close to zero.

Violence against a particular individual can also take the form of destroying or causing significant damage to an entire plane (Article 1(1)(b)[130]). In the context of cybeterrorism, such damage can occur as a result of a technical malfunction triggered by a cyber-attack (e.g., detonation of the aircraft's fuel) or upon impact with the ground, due to cyber-interference with the operation of navigational facilities (Article 1(1)(d)[131]) or communicating wrong information to the pilots, air traffic control (in case of a manned plane), or to the UAV control stations (Article 1(1)(e)[132]).

---

127. *See supra* Parts 1.1–1.3; *see also* Noah Shachtman, *Computer Virus Hits US Predator and Reaper Drone Fleet*, ARS TECHNICA (Oct. 7, 2011), http://arstechnica.com/business/news/2011/10/exclusive-computer-virus-hits-drone-fleet.ars.

128. *See* Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, *supra* note 2, at art. 1(1)(c), which reads: "Any person commits an offence if he unlawfully and intentionally . . . [p]laces or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight."

129. *Id*. at art 1(1)(a), which reads: "performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft."

130. *Id*. at art. 1(1)(b), which reads: "destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight."

131. *Id*. at art. 1(1)(d), which reads: "destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight."

132. *Id*. at art. 1(1)(e), which reads: "communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight."

The 1988 Airport Protocol to the Civil Aviation Convention adds two additional offenses: use of a device to perform an "act of violence against a person at an airport serving international civil aviation . . . likely to cause serious injury or death" (Article 1(1bis)(a)[133]) and damaging the facilities of an airport or immobile aircraft or disrupting airport's services (Article 1(1bis)(b)[134]), if they endanger or are likely to endanger safety at that airport. An act of violence in this case can take the form of a cyber-attack against a medical implant, means of transportation, or any other computerized systems within the airport, endangering both the health of the targeted individuals and, if the targeted individuals are working at the flight control facilities, the lives of the passengers on incoming and outgoing flights.

Though the prospect of cyberterrorists damaging the airport or stationary aircrafts is unlikely, disrupting its services is very probable, since basically any interference with the standard operation of the computer systems at the airport,[135] especially those of the air traffic control, could constitute such an offense.

Prohibitions contained in the Civil Aviation Convention's Articles 1(1) and 1(1bis) were entirely incorporated into Article 1 of the 2010 New Civil Aviation Convention. Moreover, according to the UN Action to Counter-Terrorism's website, "[a] cyber-attack on air navigation facilities constitutes an attack."[136] Among the new offenses added by this Convention, transporting (Article 1(1)(i)[137]) and using (Article

133. *See id*. at art. 1(1bis(a)), which reads: "performs an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death."

134. *Id*., which reads: "destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport."

135. Cohen, *supra* note 94, at 23.

136. *International Legal Instruments to Counter Terrorism*, U.N. ACTION TO COUNTER TERRORISM, http://www.un.org/terrorism/instruments.shtml (last visited Oct. 28, 2012).

137. Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, *supra* note 2, art. 1(1)(i) ("Any person commits an offence if that person unlawfully and intentionally . . . transports, causes to be transported, or facilitates the transport of, on board an aircraft: (1) any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, with or without a condition, as is provided for under national law, death or serious injury or damage for the purpose of intimidating a population, or compelling a government or an international organization to do or to abstain from doing any act; or (2) any BCN weapon, knowing it to be a BCN weapon as defined in Article 2; or (3) any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use or

1(1)(h)[138]) dangerous materials and WMDs on board a plane—physical actions—are not relevant in the case of cyberterrorism. Releasing and discharging such hazardous substances (Article 1(1)(g)[139]) through cyber-means are impossible since, as mentioned previously, connecting these materials to electronic networks is illogical and unlikely. However, since civilian UAVs can be seized and controlled by cyberterrorists (see above), they can also use them for "causing death, serious bodily injury or serious damage to property or the environment" on the ground, in breach of Article 1(1)(f)[140] of the New Civil Aviation Convention.

K. Conventional Terrorism in Cyber-Space: Summary

To summarize, a table that reflects the applicability of relevant anti-terrorism instruments in the context of potential cyberterrorism is presented on the next page.

L. Other Targets

Now that the anti-terrorist conventions are thoroughly analyzed, one should consider whether some crimes remain outside the scope of the treaty regime, but can still be considered acts of cyberterrorism under the customary international law.

Human bodies are not directly connected to computers in any way, therefore the majority of cyberterrorist acts (with the exception of those, which result in humans following wrong data, due to a cyber-attack), will chronologically result in property damage (and economic loss) before injury to a person (if any). Growing reliance on technology in the developed countries, coinciding with vulnerability of computer networks, has led to a situation where cyber-criminals can choose between various entities that are susceptible to cyber-attacks—from banking and financial

---

production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to a safeguards agreement with the International Atomic Energy Agency; or (4) any equipment, materials or software or related technology that significantly contributes to the design, manufacture or delivery of a BCN weapon without lawful authorization and with the intention that it will be used for such purpose.").

138. *Id*. at art. 1(1)(h) ("uses against or on board an aircraft in service any BCN weapon or explosive, radioactive, or similar substances in a manner that causes or is likely to cause death, serious bodily injury or serious damage to property or the environment").

139. *Id*. at art. 1(1)(g) ("releases or discharges from an aircraft in service any BCN weapon or explosive, radioactive, or similar substances in a manner that causes or is likely to cause death, serious bodily injury or serious damage to property or the environment").

140. *Id*. at art. 1(1)(f) ("uses an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment").

TREATY	NUMBER OF RATIFICATIONS (OCTOBER 2012)	RELEVANT PROVISIONS	EXAMPLES
Terrorist Financing Convention	180	2(1)	Breaking into online accounts by means of cyber-attack to transfer the money to, or to acquire them by terrorists.
Diplomatic Agents Convention	175	2(1)	Tempering with a hospital computer or diplomatic agent's car or trapping him in an elevator.
Maritime Convention	160	3(1)(e) 3(1)(f)	Infecting navigational facilities with malware that prevents their use or creates a wrong impression of the marine conditions.
Nuclear Materials Convention	Convention: 147 2005 Amendments: 57	7(1)(a) 7(1)(a), as amended (7(1)(e), as amended	A cyber-attack causing a nuclear meltdown at an atomic power plant that contaminates the surrounding environment.
Nuclear Terrorism Convention	82	2(1)(b)	A cyber-attack causing destruction at a uranium enrichment facility with intent to force a government to abandon its nuclear program.
Unlawful Seizure Convention, amendable by the 2010 Protocol	Convention: 185 2010 Protocol: 1 (not yet in force)	1(1)	Infecting a civilian UAV control station with malware, allowing terrorists to control the unmanned aerial vehicle.
Civil Aviation Convention	Convention: 188 Airport Protocol: 171	1(1)(b) 1(1)(d) 1(1)(e) 1(1bis)(b), as amended by the Airport Protocol	A cyber-attack that causes mechanical failure in flight, interferes with the navigational devices or creates a wrong impression of the flying conditions. A cyber-attack on a computerized medical implant of an employee at the air traffic control or on vital airport computers.
New Civil Aviation Convention	1 (not yet in force)	1(1)(b) 1(1)(d) 1(1)(e) 1(1)(f)	Taking control of and flying a civilian UAV into a building.

institutions to military defense systems.[141] However, not all of these attacks would fall under the definition contained in the Draft Comprehensive Convention on International Terrorism, which, as mentioned before, represents a consensus between states, and as such, to a certain degree, reflects customary law. For example, Vitek Boden, while dumping raw sewage during his cyber-attack in 2000 and causing damage to property and environment,[142] was guided by individual motives,[143] and did not desire to "intimidate a population or compel a Government or an international organization to do or to abstain from doing any act," nor did such intent arise from the context of his crime; therefore, his act cannot be characterized as cyberterrorism.

Though the definition in the Draft Convention uses terms which are very subjective, such as "serious damage to public or private property" and "major economic loss," it is possible to draw a list of objects susceptible to cyber-attacks, which might be relevant in this case.

"Purpose" to compel a government to do or abstain from doing something arises entirely from the circumstances of each individual situation. Considerations include whether this is the first terrorist offense of the person or terrorist group, whether there have been any demands, whether the situation involves a political background, and so on. Therefore, one should concentrate on the intent to intimidate a population, which is likely to stem from the nature and context of the criminal act itself.[144]

Due to their virtual nature, and since cyber-attacks more often fail than succeed, they cannot be expected to inflict significant damage to different private properties in a manner that would terrorize ordinary citizens. Therefore, when talking about property and economic loss, the population can be expected to only fear cyber-attacks against objects that are essential for the functioning of the economy and society as a whole (i.e. critical infrastructure). One can conclude from this that cyber-strikes that are likely to seriously damage vital computer facilities responsible for agriculture and food, water, public health, emergency services, government, telecommunications, energy, transportation, banking and

---

141. Ruwantissa Abeyratne, *Cyber Terrorism and Aviation—National and International Responses*, 4 J. TRANSP. SECURITY 337, 340 (2011).

142. Alexandre Kiss, *The International Protection Enviornment*, *in* INTERNATIONAL LAW: CLASSIC AND CONTEMPORARY READINGS 391 (Charlotte Ku & Paul F. Diehl ed., 1998).

143. Susan W. Brenner, *Cybercrime, Cyberterrorism and Cyberwarfare*, 77 REVUE INTERNATIONALE DE DROIT PÉNAL [R.I.D.P.] 453, 458 (2006).

144. Carlos A. Rodriguez, Cyberterrorism: A Rising Threat in the Western Hemisphere (Apr. 2006) (unpublished thesis, Inter-American Defense College), *available at* http://library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf.

finance, chemical industry and hazardous materials, postage and shipping,[145] police, heating (where applicable), and military (depending on the outcome of the definition controversy) should be considered acts of terrorism (and therefore cyberterrorism) under existing customary international law.

Finally, it seems obvious that "death or serious bodily injury" scares an ordinary person regardless of the means employed by terrorists, especially if victims are random. Therefore, aside from the acts criminalized by the existing legal instruments, life-threatening cyber-attacks against dams, water supply networks, automated food preparation factories, ground transport controls, computerized cars, space-navigation controls, medical institutions, medical implants, chemical laboratories, and other facilities should also be considered acts of cyberterrorism under customary norms.

Although not unequivocally globally criminalized, such acts of cyberterrorism, like other acts of terror,[146] can be prosecuted as crimes against humanity[147]—if they are widespread or systematic and satisfy other necessary criteria.

These conclusions demonstrate that the danger of cyberterrorism in peace-time is adequately covered by international law. Now it is essential to review the legal framework surrounding response to this threat to determine whether such acts constitute an "armed attack" and whether states can respond to it with armed force.

IV. CYBERTERRORISM AND JUS AD BELLUM

A. Self-Defense Against Terrorism

Governments today are aware of the vulnerabilities of the domestic infrastructures and of the potential threat that cyberterrorism represents.[148] However, while new ways to conduct cyber-attacks are being shared

145. *See generally* U.S. DEP'T OF DEF., DEPUTY CHIEF OF STAFF FOR INTELLIGENCE, HANDBOOK NO. 1.02, CRITICAL INFRASTRUCTURE THREATS AND TERRORISM § 4 (2006).

146. Michael Byers, *Terrorism, the Use of Force and International Law After 11 September*, 16 INT'L REL. 155, 164 (2002).

147. *See* Michael P. Scharf & Michael A. Newton, *Terrorism and Crimes Against Humanity*, *in* FORGING A CONVENTION FOR CRIMES AGAINST HUMANITY 262, 267-69 (Leila Nadya Sadat ed., 2011); *see also* Roberta Arnold, *Terrorism As a Crime Against Humanity Under the ICC Statute*, *in* INTERNATIONAL COOPERATION IN COUNTER-TERRORISM: THE UNITED NATIONS AND REGIONAL ORGANIZATIONS IN THE FIGHT AGAINST TERRORISM 121, 135 (Giuseppe Nesi ed., 2006).

148. William Gravell, *Some Observations Along the Road to "National Information Power"*, 9 DUKE J. COMP. & INT'L L. 401, 408 (1999).

between crackers around the world,[149] the inter-state cooperation is lagging behind. For example, when the UN Counter-Terrorism Implementation Task Force (CTITF) Working Group on Countering the Use of the Internet for Terrorist Purposes asked countries to make submissions for the 2009 Report, only two states listed cyber-attacks by terrorists as one of the threats that concerned them.[150] This is contrasted by the rapid development of cyber-defensive and cyber-offensive capabilities by the US, China, Russia, Iran, Cuba,[151] Israel, the UK, and others, suggesting that these states favor exercising their right of individual self-defense (against cyberterrorists) over collective action in the future.

In fact, two states stand out for their continuous practice of using force against terrorists and states harboring them—namely Israel and the United States.[152] Both sometimes operate outside legal obligations and both are known to invest heavily in military counter-terrorism campaigns.[153]

Despite the condemnation by the Security Council of its "self-defense" operations against previous terrorist attacks,[154] such as the raid on Beirut airport in 1968 (Resolution 262), raids on Lebanon in 1973 (Resolutions 332 and 337), bombing of PLO Headquarters Tunisia in 1985 (Resolution 573), and assassination of Khalil al-Wazir in 1988 (Resolution 611), Israel continues to stand by its position of interpreting the right to self-defense broadly and is likely to do so in relation to cyberterrorist-strikes as well. One should note that although the international community seems to remain unconvinced by Israeli arguments, after 9/11 states do not explicitly exclude the possibility of acting in self-defense against organizations like Hezbollah and Hamas,[155] and prefer to concentrate instead on issues of proportionality in assessing

149. Lukasz Jachowicz, How to Prevent and Fight International and Domestic Cyberterrorism and Cyberhooliganism 1 (2010) (unpublished essay), *available at* http://honey/7thguard.net/essays/cyberterrorism-policy.pdf.

150. U.N. COUNTER-TERRORISM IMPLEMENTATION TASK FORCE, REPORT ON COUNTERING THE USE OF THE INTERNET FOR TERRORIST PURPOSES 3 (Feb. 2009), *available at* http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_internet_wg_2009_report.pdf.

151. W.P. Strobel, *A Glimpse of Cyberwarfare*, 128 U.S. NEWS & WORLD REP. 32 (2000), *cited in* Joe Wesley Moore, Information Warfare, Cyber-Terrorism and Community Values 24 n.66 (2002) (unpublished LL.M. thesis, McGill University), *available at* http://www.hsdl.org/?view&did=458383.

152. Devika Hovell, *Chinks in the Armour: International Law, Terrorism and the Use of Force*, 27 U. NEW S. WALES L.J. 398, 412 (2004).

153. *See generally, e.g.*, AMY BELASCO, THE COST OF IRAQ, AFGHANISTAN, AND OTHER GLOBAL WAR ON TERROR OPERATIONS SINCE 9/11 (2011).

154. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 116 (2000).

155. Raphaël van Steenberghe, *Self-Defense in Response to Attacks by Non-state actors in the Light of Recent State Practice: A Step Forward?*, 23 LEIDEN J. INT'L L. 183, 193 (2010).

the legality of the airstrike near Damascus in 2003, invasion of Lebanon in 2006,[156] and bombings of Gaza in 2007–2012.

The condemnation of US "self-defense" against terrorists was not likely in the Security Council due to the US veto. Nonetheless, the General Assembly managed to pass Resolution 41/38 condemning the bombings of Libyan Jamahiriya in 1986 carried out in response to the Berlin discotheque bombing. United States' "counter-terrorist" operations in Iraq in 1993, as well as in Sudan and Afghanistan in 1998,[157] continued to raise questions of legality until 2001, when the Security Council in its Resolution 1368 heavily implied that the US has the right to resort to self-defense against a terrorist organization. This was affirmed by the silent approval of the international community of the invasion of Afghanistan in 2001 and also by the legal attitudes adopted in the US itself ("president has both constitutional and statutory authority to use the armed forces in military operations, against terrorists, within the United States"[158]), which inevitably will reflect on cyberterrorism as well.

Other countries have also invoked Article 51 of the UN Charter to justify attacks against terrorist groups with mixed feedback. For example, reactions to numerous Turkish incursions into Northern Iraq in the last two decades to pursue the Kurdistan Workers Party have ranged from understanding[159] to a "mixture of sympathy and concern."[160] Further examples where self-defense arguments were used in relation to terrorists include Russian pursuit of Chechen fighters into Georgia,[161] Iranian attacks on Iraqi bases of People's Mujahedin and Kurdish bands,[162] involvement of Ethiopia in the Somali Civil War in 2006,[163] Colombian

156. Christian J. Tams, *The Use of Force Against Terrorists*, 20 EUR. J. INT'L L. 359, 379 (2009).
157. *See id*. at 359, 380.
158. Memorandum from John C. Yoo, Deputy Assistant Attorney General, and Robert J. Delahunty, Special Counsel, to Alberto R. Gonzales, Counsel to the President, and William J. Haynes II, General Counsel of the Department of Defense 37 (Oct. 23, 2001), *available at* http://www.fas.org/irp/agency/doj/olc/milforce.pdf.
159. Steenberghe, *supra* note 156, at 194; *see also* GRAY, *supra* note 155, at 103.
160. Tams, *supra* note 156.
161. Theresa Reinold, *State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11*, 105 AM. J. INT'L L. 244, 253 (2011).
162. Tams, *supra* note 156, at 380.
163. NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 30 (2010).

invasion of the Ecuadorian territory in 2008 to engage the FARC,[164] and Kenyan pursuit of Al Shabaab in 2011.

Although these examples do not directly involve cyberterrorists, they demonstrate how states might react to serious cyber-strikes from non-state actors. This is particularly important, since not a single country to this day has admitted an attempt to carry out a cyber-attack, and it is expected that non-state actors are more likely to engage in such activity.

From the perspective of international law, branding a group or organization with cyber-offensive capabilities "terrorist" is not enough.[165] In order for a state to exercise its right of self-defense against a cyberterrorist group, the latter should launch (or, arguably, plan to launch) a cyber-strike that would constitute both an illegal "use of force" and an "armed attack."

Although the ICJ concluded in the Wall Case that "Article 51 recognizes the existence of an inherent right of self-defense in the case of armed attack by one state against another state,"[166] the Court did not bother to note that the right to defend itself against aggressive non-state actors has existed in customary international law (i.e. outside Article 51) since ancient times.[167] Furthermore, as pointed out by Judge Higgins, there is nothing in the text of Article 51 stipulating that "self-defense is available only when an armed attack is made by a State."[168]

The massive support for the legality of the US claim to self-defense in Afghanistan, mentioned above,[169] did not necessarily constitute "instant customary international law and an authoritative reinterpretation of the

---

164. Tams, *supra* note 156, at 380.

165. Walker, *supra* note 59, at 627.

166. Legal Consequences of Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J 136, ¶ 128 (July 9) [hereinafter *Wall Case*]. This conclusion can be considered an example of "unhelpful caution in using the judicial tools at its disposal and a reluctance to pronounce clearly on matters of contemporary importance." *Id*.; *see* David McKeever, *The Contribution of the International Court of Justice to the Law on the Use of Force: Missed Opportunities or Unrealistic Expectations?*, 78 NORDIC J. INT'L L. 361, 396 (2009).

167. *See generally* Yaroslav Shiryaev, *Circumstances Surrounding the Separation Barrier and the Wall Case and Their Relevance for the Right of Self-Defense*, 14 GONZ. J. INT'L L. 1 (2010), *available at* http://www.gonzagajil.org/index.php?option=com content&view=article&id=206:circumstances-surrounding-the-separation-barrier-and-the-wall-case-and-their-relevance-for-the-&catid=83:volume-14-issue-1-2010-2011&Itemid=26.

168. *Wall Case*, 2004 I.C.J at ¶ 128 (separate opinion of Judge Higgins).

169. Shiryaev, *supra* note 167; *see generally* Dominika Svarc, *The Military Response to Terrorism and the International Law on the Use of Force*, 1 POL. PERSPECTIVES 1 (2007), *available at* http://www.politicalperspectives.org.uk/wp-content/uploads/2010/08/CIP-2007-01-03.pdf.

UN Charter."[170] In fact, some authors have argued that the US has not asked for legal approval of its military operation in the UNSC[171] and instead chose to invoke self-defense individually, in order to avoid creating a precedent.[172] Nonetheless, one has to acknowledge that enough time has passed to speak of a natural non-instant evolution of the customary norms. Today, the question is no longer whether terrorist (and cyberterrorist) groups can conduct an "armed attack," but rather the degree to which state involvement is necessary "to allow the use of force against the territory of the host state."[173]

Currently there are two opposing views in international jurisprudence. A majority of the ICJ judges in the Armed Activities case agreed that if the attacks by "armed bands" were not attributable to a state, there are no legal circumstances for the exercise of a right of self-defense against that state.[174] On the other hand, Judge Kooijmans[175] and Judge Simma[176] have defended a position that "armed attacks . . . by irregular bands . . . are still armed attacks even if they cannot be attributed to the territorial state." This view is supported, for example, by Leiden Policy Recommendations on Counter-Terrorism and International Law, which reads: "it is now well accepted that attacks by non-state actors, even when not acting on behalf of a state, can trigger a state's right of . . . self-defense."[177] Steenberghe offers a reasonable compromise between the two opinions, which seems to reflect state practice (taking into account the self-defense operations mentioned above): the link between the non-state actors and a host-country should consist at least in unwillingness or inability to stop the attacks.[178]

---

170. CHRISTIAN HENDERSON, THE PERSISTANT ADVOCATE AND THE USE OF FORCE: THE IMPACT OF THE UNITED STATES ON THE JUS AD BELLUM IN THE POST-COLD WAR ERA 158 (2010).

171. Geir Ulfstein, *Terrorism and the Use of Force*, 34 SECURITY DIALOGUE 153, 153-68 (2003).

172. Said Mahmoudi, *Self-Defence and International Terrorism*, 48 SCANDINAVIAN STUD. L. 203, 206 (2005).

173. GRAY, *supra* note 154, at 99.

174. Armed Activities on Territory of Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 146-47 (Dec. 19).

175. *Id.* at 216, ¶ 30-31 (separate opinion of Judge Kooijmans); *see also* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 216 (3d ed. 2001).

176. Armed Activities on Territory of Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168 at 334, ¶ 12 (Dec. 19) (separate opinion of Judge Simma).

177. Nico Schrijver & Larissa van den Herik, *Leiden Policy Recommendations on Counter-terrorism and International Law*, 57 NETH. L. REV. 531, 541-42 (2010).

178. Steenberghe, *supra* note 155, at 197, 202; Andrea Bianchi, *Terrorism and*

In the context of cyberterrorism, this means that countries that control, support,[179] take advantage of, or tolerate cyberterrorist-attacks (reaching significant threshold) originating from their territories can be targeted in self-defense[180] (subject to necessity and proportionality criteria). If strikes emanated from parts of a failed state that the government cannot control, those territories would also be subject to acts of self-defense.

Although this is unlikely, a problem may arise when a government does not want to tolerate acts of cyberterrorism (e.g., it has ratified an anti-terrorist convention that demands extradition or prosecution), but it cannot locate the perpetrators. This is especially relevant if a devastating cyber-attack was carried out by only one person. Military operations against parts of a country in pursuit of only one man are not unheard of (consider Osama bin Laden), yet they will inevitably raise questions of proportionality. Since such situations are not covered by international law, the host-state is left with the only option of turning to the Security Council.

B. Armed Attacks by Cyberterrorists

When it comes to the magnitude of cyberterrorist-attacks necessary to reach the "armed attack" threshold, one can draw parallels with previous cases. For example, taking control of a UAV and flying it into a civilian building resonates with 9/11 and by analogy with the principles in UNSC Resolution 1368, that the victim-state should be entitled to self-defense. Life-threatening attacks upon diplomatic personnel and attacks upon their liberty constituted an "armed attack" in the Tehran Hostages case.[181] An attack against a single ship triggered the right of self-defense in the Oil Platforms case.[182] From the ICJ's attitude in the Nuclear Weapons case also follows that the release of radiation could be an armed attack that "would affect health, agriculture, natural resources and

---

Armed Conflict: Insights from a Law & Literature Perspective, 24 LEIDEN J. INT'L L. 1, 7 (2011); Military and Paramilitary Activities in and Against Nicaragua, Judgment, 1986 I.C.J 14, ¶ 195 (June 27). It follows that supply of software and "other support" by the host-state will not constitute an "armed attack" itself, however this would make a country a state-sponsor of terror, allowing the victim-state to resort to self-defense (possibly preemptively) against it.

179. Military and Paramilitary Activities in and Against Nicaragua, Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

180. T. FRANCK, RECOURSE TO FORCE: STATE ACTIONS AGAINST THREATS AND ARMED ATTACKS 53-54 (2002), *quoted in* Oliver Corten, *The Controversies Over the Customary Prohibition on the Use of Force: A Methodological Debate*, 16 EUR. J. INT'L L. 803, 803 (2006).

181. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶¶ 57, 91 (May 24).

182. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 72 (Nov. 6).

demography over a wide area [and] has the potential to damage the future environment, food and marine ecosystem, and to cause genetic defects and illnesses in future generations."[183]

Some cases of cyberterrorism can also be safely excluded from the self-defense framework—for example, stealing funds for a terrorist organization through the Internet would not even reach the level of "use of force." Merely exercising control over a UAV or destroying centrifuges in a uranium enrichment facility cannot reach the "armed attack" threshold due to their low intensity.

Much will depend on the individual circumstances of each situation and, most likely, political circumstances. However, it is essential to maintain an optimal threshold for invoking the right of self-defense in international law—a very low threshold will blur the lines between armed conflict and criminal law enforcement, while a very high one will put states at risk.[184]

C. Necessity and Proportionality in Context

As in the case of ordinary cyber-strikes, the exercise of self-defense against devastating acts of cyberterrorism requires the response to be necessary and proportional. This is particularly important in light of the legal uncertainty surrounding terrorism[185] (Gazzini notes that terrorist attacks consisted of mostly "unpredictable, sudden and instantaneous acts,"[186] but cyber-attacks take this to a whole new level). Legally controversial "defensive" acts, such as targeted killings[187] may be practiced against cyberterrorists or new "targeted hacking" (taking over

183. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 35 (July 8).

184. Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT'L L. 1, 1–34 (2004).

185. TOM RUYS, "ARMED ATTACK" AND ARTICLE 51 OF THE UN CHARTER 487 (2010); JOHN JANŽEKOVIČ, THE USE OF FORCE IN HUMANITARIAN INTERVENTION: MORALITY AND PRACTICALITIES 103 (2006).

186. Tarcisio Gazzini, *The Rules on the Use of Force at the Beginning of the XXI Century*, 11 J. CONFLICT & SECURITY L. 319, 330 (2006).

187. *See generally* Peter M. Cullen, *The Role of Targeted Killing in the Campaign against Terror*, 48 JOINT FORCE Q. 22 (2008); Mary Ellen O'Connell, *Defining Armed Conflict*, 13 J. CONFLICT & SECURITY L. 393, 400 (2008); Kenneth Anderson, Targeted Killing in U.S. Counterterrorism Strategy and Law 11 (May 11, 2009) (unpublished working paper of the Series on Counterterrorism and American Statutory Law Project with the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution) (on file with author).

or manipulating enemy systems)[188] may be employed in the framework of future "war on cyberterrorism." This is especially relevant since some states started authorizing remote searches of computers of suspected criminals.[189]

Generally, cyberterrorism calls for a reinterpretation of the principles of necessity and proportionality in a new light. Not only will the states be required to present clear and convincing evidence of the need to use force in self-defense[190] to acts that are not easily traceable, but they will also have to explain why persons, some of which never held a gun in their hand, should be targeted militarily. Finally, one should also note that the "luck factor"[191] eliminates the distinction between preemption and prevention in anticipatory self-defense, since the moment of "immediacy" becomes impossible to predict. Resorting to preemptive self-defense legally, therefore, is only possible if cyberterrorist-attacks keep rising in magnitude, possibly reaching the "armed attack" level with the next strike, or if there is a series of identical devastating cyber-attacks and a state learns it is next on the list.

D. Needle-Prick Theory

In 1989 (before the Internet became global) Antonio Cassese claimed that "to qualify as an armed attack, international law requires that terrorist acts form part of a consistent pattern of violent terrorist action rather than just being isolated or sporadic attacks."[192] Modern cyber-

---

188. *See generally* MINISTERIE VAN BINNERLANDSE ZAKEN EN KONINKRIJKSRELATIES, JIHADIS AND THE INTERNET (2007), *available at* http://www.investigativeproject.org/documents/testimony/226.pdf.

189. Juan Carlos Ortiz Pradillo, *Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain*, 19 EUR. J. CRIME, CRIM. L. & CRIM. JUST. 363, 374 (2011).

190. Andrew Garwood-Gowers, *Self-Defence Against Terrorism in the Post-9/11 World*, 4 QUEENSLAND U. TECH. L.J. 1, 16 (2004).

191. Luck-factor cannot be underestimated in terrorist attacks, and will be equally significant in cyberterrorism which is even harder to plan. Consider, for example, the entire auspicious 9/11 operation, or the unlucky Aum Shinrikyo criminal group, which attempted to disseminate botulinum toxin and anthrax at least nine times, failing each time because the agents were not toxic enough or sprayers meant to disseminate the anthrax became clogged and inoperative. Eventually, the successful Sarin attack on the Tokyo subway had to be carried out by disseminating the nerve gas in plastic trash bags and poking them with sharpened umbrella tips. *See* Bruce Hoffman, *Terrorism by Weapons of Mass Destruction: A Reassessment of the Threat*, *in* TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES 85, 92 (Carolyn W. Pumphrey ed., 2000).

192. Niaz A. Shah, *Self-Defence, Anticipatory Self-Defence and Pre-Emption: International Law's Response to Terrorism*, 12 J. CONFLICT & SECURITY L. 95, 107 (2007), *citing* Antonio Cassese, *The International Community's "Legal" Response to Terrorism*, 38 INT'L & COMP. L. Q. 589, 596 (1989).

attacks represent a completely different phenomenon—an ongoing pattern of attempts to gain entry into a system with a relatively low chance of success, mostly against "serious" targets. Although it may very well be easier to sneak explosives on board a plane than to crash it using a computer, cyberterrorism is not impossible and, as mentioned previously, becomes more feasible as technologies develop.

Cyberterrorism can also take the form of multiple cyber-attacks on random targets (e.g., hospital computers of a country). As in the case of traditional terrorism, in this context "account may be taken of a series of attacks emanating from the same territory and the same terrorist group."[193]

The ICJ did imply that attacks can be "cumulative in character" in its Oil Platforms[194] and Armed Activities cases.[195] Also, as Christian J. Tams notes,[196] a large number of states accepted Turkey's and Israel's claims to self-defense "by implication", as they involved constant small-scale terrorist attacks. Nevertheless, the needle-prick theory (or accumulation of events theory) has never been officially endorsed either by the Security Council,[197] a majority of prominent academics, or the ICJ itself. According to this doctrine, instead of measuring the severity of each individual attack, consideration should be given to the cumulative effect of a series of attacks,[198] whereby rather than expiring immediately after a single attack, "the right to self-defense survives it and allows States to take forcible action necessary to put an end to the chain of attacks."[199]

---

193. Schrijver & van den Herik, *supra* note 178, at ¶ 39; *see* Bradley K. Ashley, Anatomy Of Cyberterrorism: Is America Vulnerable? 34 (Feb. 27, 2003) (unpublished research paper submitted for graduation requirements), *available at* http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf (stating that the U.S. Defense Intelligence Agency used five factors in 2003 for assessing the level of cyberterrorist threat: existence, capability, intentions, history, and targeting).

194. Armed Activities on Territory of Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 146 (Dec. 19).

195. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 64 (Nov. 6).

196. Tams, *supra* note 156, at 388.

197. Szabó notes that, although the Security Council has been reluctant to accept the needle-prick theory, the Council became less willing to condemn it in the 1980s (particularly in relation to Israeli self-defense wars). *See* KINGA TIBORI SZABÓ, ANTICIPATORY ACTION IN SELF-DEFENCE: ESSENCE AND LIMITS UNDER INTERNATIONAL LAW 215 (2011).

198. Garwood-Gowers, *supra* note 190, at 7.

199. Tarcisio Gazzini, *The Rules on the Use of Force at the Beginning of the XXI Century*, 11 J. CONFLICT & SECURITY L. 319, 331 (2006).

This theory must be mentioned in the context of cyberterrorism, since at least two of the states that possess serious cyber-offense capabilities—the US and Israel[200]—have resorted to the "cumulative effect" approach in the past, specifically in response to acts of terror.[201] Due to the "luck factor," cyberterrorist-strikes are less intensive in their nature than traditional terrorist attacks, and therefore, it is more probable that a series of damaging attacks (e.g., a pattern of random assassinations via computerized medical-equipment in one state) can provoke the victim-state to resort to the needle-prick doctrine.

As in the case of conventional response, self-defense against cyberterrorism is bound to have the same vices: the response will seem like a reprisal; it will cross the allowed borders of preemptive action (see above),[202] and it will be disproportionate to the cyber-attack in isolation.[203] Even if the needle-prick theory will be recognized in the future in customary international law vis-à-vis cyberterrorism (which this author finds highly unlikely), it will be subject to the same limits that are applicable to traditional self-defense: necessity, proportionality, lack of other means, as well as expiration of the right to continue self-defense after the Security Council has taken action. Until either the UNSC or the ICJ admit the legality of the needle-prick approach, or until there is sufficient evidence to suggest that this theory is incorporated into international customary law, accumulating cyberterrorist-strikes short of "armed attack" for the purpose of invoking self-defense will remain illegal.

V. CYBERTERRORISM AND JUS IN BELLO

A. General Complexities

According to Andrea Bianchi, international humanitarian law is sufficiently well suited to provide a "regulatory framework" and "effective mechanisms" to punish acts of terrorism.[204] Condorelli and Naqvi add that it condemns acts of terrorism in both international and internal conflicts and offers a system for the prosecution and punishment of

200. South Africa and Portugal were among other states that resorted to this doctrine. *See* GRAY, *supra* note 154, at 108.

201. *See* Shiryaev, *supra* note 167, at 17.

202. Jörg Kammerhofer, *Uncertainties of the Law on Self-Defence in the United Nations Charter*, 35 NETH. Y.B. INT'L L. 143, 177 (2004).

203. *Id*; *see also* STANIMIR A. ALEXANDROV, SELF-DEFENSE AGAINST THE USE OF FORCE IN INTERNATIONAL LAW 167 (1996).

204. Bianchi, *supra* note 178, at 21.

those who perpetrate them.[205] Unlike human rights law, humanitarian law takes into account the violent or systematic nature of terrorist acts perpetrated during conflicts,[206] although jus in bello suffers from its own set of deficiencies when it comes to terrorism and, by extension, cyber-terrorism.

The dividing line between use of force and humanitarian law is blurred[207] by the nature of terrorist acts which might or might not initiate an "armed conflict," depending on particular circumstances. In fact, in the Kordić and Čerkez judgment, the ICTY stated that the protraction requirement is "significant in excluding . . . single acts of terrorism."[208] One must therefore assume that single cyberterrorist-strikes cannot initiate a war, though the events after 9/11 paradoxically imply the opposite.

Additional complexities stem also from the controversial nature of the recent counter-terrorism operations ("war on terror"),[209] which only partially correspond to the classic understanding of war.[210] Nevertheless, it remains clear that international humanitarian law would apply in situations where a cyberterrorist-attack is carried out as part of an armed conflict (or armed occupation) with the required nexus,[211] or if it triggers the armed conflict itself.

---

205. Luigi Condorelli & Yasmin Naqvi, *The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of Date?*, *in* ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 37 (Andrea Bianchi ed., 2004).

206. Fionnuala Ni Aoláin, *The No-Gaps Approach to Parallel Application in the Context of the War on Terror*, 40 ISR. L. REV. 563, 579 (2007); *see also* Gabor Rona, *Interesting Times for International Humanitarian Law: Challenges from the "War on Terror"*, *in* TERRORISM AND HUMAN RIGHTS 154, (Magnus Ranstorp & Paul Wilkinson eds., 2008).

207. Neta C. Crawford, *Just War Theory and the U.S. Counterterror War*, 1 PERSPECTIVES ON POL. 5, 20 (2003).

208. Prosecutor v. Kordić & Čerkez, Case No. IT-95-14/2-A, Appeals Chamber Judgment, ¶ 341 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 17, 2004); *see also* Prosecutor v. Martić, Case No. IT-95-11-T, Judgment, ¶ 41 n.60 (Int'l Crim. Trib. for the Former Yugoslavia June 12, 2007).

209. *See generally* Marja Lehto, *War on Terror—Armed Conflict with Al-Qaida?*, 78 NORDIC J. OF INT'L L. 499 (2010).

210. *See* Natasha T. Balendra, *Defining Armed Conflict* 2511 (N.Y.U. Sch. of Law, Pub. Law & Theory Research Paper Series, Working Paper No. 07-22, 2007), *available at* http://lsr.nellco.org/cgi/viewcontent.cgi?article=1062&context=nyu_plltwp; *see also* Matthew C. Waxman, *The Structure of Terrorism Threats and the Laws of War*, 20 DUKE J. COMP. & INT'L L. 429, 429 n.3 (2010).

211. *See* Schrijver & van den Herik, *supra* note 177, at ¶ 60.

B. Special Nature of Terrorism in International Humanitarian Law

Terrorism is equally prohibited in times of internal or international armed conflicts.[212] Like other attacks, violent acts of cyberterror are subject to the principles of necessity, proportionality, humanity, distinction, neutrality, and chivalry. At the same time, Geneva Conventions protocols specifically forbid[213] "all measures of . . . terrorism," "acts of terrorism,"[214] and "acts or threats of violence the primary purpose of which is to spread terror among the civilian population."[215] Acts of terrorism are expressis verbis listed as war crimes in the statutes of the ICTR[216] and Sierra Leone Special Court,[217] as well as the 1996 Draft Code of Crimes against the Peace and Security of Mankind.[218] Though of little relevance in the context of cyber-attacks (for reasons mentioned previously), one should note that international humanitarian law separately prohibits[219] and criminalizes[220] a particular extremist act—hostage taking.

---

212. U.N. Secretary-General, *A More Secure World: Our Shared Responsibility*: *Report of the High Level Panel on Threats, Challenges, and Change*, ¶ 164(b), U.N. Doc A/59/565 (Dec. 2, 2004); *see also* Hans-Peter Gasser, *Acts of Terror, "Terrorism" and International Humanitarian Law*, 84 INT'L REV. RED CROSS 547–68 (2002).

213. ERLING J. HUSABØ & INGVILD BRUCE, FIGHTING TERRORISM THROUGH MULTILEVEL CRIMINAL LEGISLATION 373 (2009).

214. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, art. 4(2)(d), June 10, 1977, 1125 U.N.T.S. 17513 [hereinafter Protocol II].

215. Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, art. 51(2), June 10, 1977, 1125 U.N.T.S. 17512; Protocol II, *supra* note 216.

216. Statute for the International Tribunal for Rwanda, 33 I.L.M. 1602 [hereinafter ICTR Statute], *available at* http://www.ictr.org/ENGLISH/basicdocs/statute.html, adopted by S.C. Res. 955, U.N. SCOR, 49th Sess., U.N. Doc. S/RES/955 (1994).

217. U.N. Secretary-General, *Report of the Secretary-General on the Establishment of a Special Court for Sierra Leone*, art. 3(d), U.N. Doc. S/2000/915 (Oct. 4, 2000).

218. Draft of Crimes Against the Peace and Security of Mankind, art. 20(f)(iv), Rep. of the Intl' Law Comm'n, 48th Sess., May 6- July 26, 1996, UN Doc. A/51/10 (1996).

219. Geneva Convention Relative to the Treatment of Prisoners of War, art. 3, Aug. 12, 1949, 75 U.N.T.S. 135 [hereinafter Common Article 3]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 34 & art. 147, Aug. 12, 1949, 75 U.N.T.S. 287; Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, *supra* note 215, at art. 75(2)(c); Protocol II, *supra* note 214, at art. 4(2)(c).

220. *See* U.N. Secretary-General, *supra* note 217, at art. 3(c); Rome Statute of the International Criminal Court, art. 8, 2187 U.N.T.S. 90, July 17, 1998, *available at* http://www1.umn.edu/humanrts/instree/Rome_Statute_ICC/Rome_ICC_toc.html. Note that negotiations on including "terrorism" as an international crime under the Rome Statute have been underway for more than a decade. *See id*.; PETER J. VAN KRIEKEN, TERRORISM AND THE INTERNATIONAL LEGAL ORDER 109 (2002).

Currently, the archaic notion of terrorism in international humanitarian law differs from the conventional one.[221] The main reason for this paradox is that unlike the latter, the concept of jus in bello terrorism exists in a legal stasis. It has not changed since 1949. When the Geneva Conventions were written, terrorism was perceived as a form of intimidation[222] and collective punishment[223] by a state. Article 33(1) of the Fourth Geneva Convention was therefore aimed at preventing belligerents from the practice of "intimidatory measures to terrorize the population."[224] Building upon this foundation, the 1977 protocols reaffirmed the archaic understanding of terrorism.[225]

A de facto separate legal regime was proclaimed by the ICTY in the Galić case, where the Court noted that although international instruments exist to outlaw terrorism in various forms, the Court had to limit itself to the Geneva framework of conventional armed conflict between states and ignore the "international efforts directed against 'political' varieties of terrorism."[226] However, it is undeniable that some of these political varieties were any way incorporated into the laws of armed conflict by the 1999 Terrorist Financing Convention (currently ratified by 176 states), which suggests that any cyber-attack intended to cause death or

221. Emanuela-Chiara Gillard, *The Complementary Nature of Human Rights Law, International Humanitarian Law and Refugee Law*, *in* TERRORISM AND INTERNATIONAL LAW: CHALLENGES AND RESPONSES 50 (2002), *available at* http://www.iihl.org/iihl/Album/terrorism-law.pdf.

222. *See* INT'L COMM. OF THE RED CROSS, DRAFT RULES FOR THE LIMITATION OF THE DANGERS INCURRED BY THE CIVILIAN POPULATION IN TIME OF WAR (1957). Article 6 reads: "Attacks directed against the civilian population, as such, whether with the object of terrorizing it or for any other reason, are prohibited." *Id*.

223. John B. Bellinger III, *Terrorism and Changes to the Laws of War*, 20 DUKE J. COMP. & INT'L L. 331, 336 (2010) (stating that collective punishment is prohibited by Article 33(1) of the Fourth Geneva Convention, Article 75(2)(d) of Additional Protocol I, and Article 4(2)(b) of Additional Protocol II).

224. Fourth Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287; *see also* CLAUDE PILLOUD ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 1375 (1987), *cited in* VIRGINIA MORRIS & MICHAEL P. SCHARF, ICTR FOR RWANDA 213 (1998).

225. Protocol II, *supra* note 214 (extending to cover "not only acts directed against people, but also acts directed against installations which would cause victims as a side-effect"); *see* INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE 1977 PROTOCOLS ¶ 4538 (Y. Sandoz et al. eds., 1987), *cited in* BEN SAUL, TERRORISM IN INTERNATIONAL LAW (2006); COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, *supra* note 224.

226. Prosecutor v. Stanislav Galić, Case No. IT-98-29-T, Judgment, ¶ 81 (Nov. 30, 2006), http://www.icty.org/x/cases/galic/acjug/en/gal-acjud061130.pdf.

injury to civilians or persons hors de combat[227] during armed conflict should be considered an act of terror not only if carried out to intimidate a population, but also if used to compel a government or an organization to do or abstain from doing any act.[228] At the same time, since mere threats of violence and non-violent acts were left out of the definition contained in the 1999 Terrorist Financing Convention, they cannot be considered jus in bello terrorism if their purpose is to simply coerce a state and not to intimidate its population.

As international humanitarian law is primarily meant to govern the behavior of state armies (see next sub-chapter for the discussion on freedom-fighters), cyber-attacks can be classified as archaic jus in bello terrorism if carried out by military agents of countries (in case of international armed conflict) or of organized groups controlling parts of state territory (in case of internal armed conflicts). Those persons and groups that do not fall under the combatant categories will anyway be covered by the legal regime on conventional terrorism. On the other hand, the activities undertaken by military forces of a state are excluded from this regime by special provisions in the 2005 Protocol to the Maritime Convention,[229] the 2010 Protocol to the Unlawful Seizure Convention,[230] the 2010 Nuclear Terrorism Convention,[231] and the 2010 New Civil Aviation Convention.[232] Therefore, soldiers who hijack a civilian UAV and crash it into a building or cause a nuclear meltdown in another state through cyber-attacks during an armed conflict cannot be held liable for conventional terrorism.

One must note that a similar exception in relation to all armed forces within the meaning of international humanitarian law, suggested by the West in the Draft Comprehensive Convention,[233] is still disputed. There is a lack of sufficient ratification of the four above-mentioned instruments,

---

227. ANTONIO CASSESE, INTERNATIONAL CRIMINAL LAW 173 (Oxford Univ. Press 2d ed. 2008).

228. International Convention for the Suppression of the Financing of Terrorism, *supra* note 98, at art. 21(1)(b).

229. IMO, 2005 Protocol to the 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, *supra* note 2.

230. ICAO, Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, *supra* note 26.

231. Nuclear Terrorism Convention, *supra* note 119, at art. 4(2).

232. Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, *supra* note 2, at art. 6(2).

233. "The activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by this Convention." Rep. of the Ad Hoc Comm. Established by G.A. Res. 51/210, *supra* note 53, at 17.

and, as a result, no solid customary law[234] in this regard exists. Whatever the outcome, such exception does not necessarily represent a legal gap since such acts would still be punishable as war crimes and can be somewhat characterized as terrorism, albeit an archaic form (that of jus in bello).

C. Freedom-Fighters in Cyber-Space

The maxim coined by Gerald Seymour that "one man's terrorist is another man's freedom fighter" accurately reflects one of the most difficult obstacles in coping with terrorism and is no less relevant when discussing cyberterrorism.[235] History knows many examples when the label of "freedom fighters" was earned in resistance to illegitimate actions: colonization, aggression, illegal occupation, tyranny, totalitarianism, and even international crimes and massive human rights violations.[236] Nevertheless, this title is still yet to be recognized in cyber-space.

The 1977 Geneva Conventions Additional Protocol I officially provide freedom fighters with combatant and prisoner-of-war status if they belong to peoples who are "fighting against colonial domination, alien occupation or racist regimes in the exercise of their right of self-determination"[237] Despite making applicability of the Geneva Conventions somewhat dependent upon motivations that inspire guerillas,[238] these three cases are widely recognized as permitting liberation wars. This is partially evidenced by a vast number (170) of state-ratifications of the

234. "The processes of customary international law work best when all international actors realize that there is much at stake" David J. Bederman, *Acquiescence, Objection and the Death of Customary International Law*, 21 DUKE J. COMP. & INT'L L. 31, 44 (2010).

235. *See generally* Boaz Ganor, *Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?*, 3 POLICE PRACTICE & RES. 287 (2002), *available at* http://www.ict.org.il/ResearchPublications/tabid/64/Articlsid/432/Default.aspx; *see also* Zahri Yunos, *Putting Cyber Terrorism into Context*, STAR IN-TECH (2009), *available at* http://www.cybersecurity.my/data/content_files/13/526.pdf.

236. *See* Frédéric Mégret, *Beyond "Freedom Fighters" and "Terrorists": When, If Ever, Is Non-State Violence Legitimate in International Law?*, 6-13 (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1373590.

237. Geneva Convention Relative to the Protection of Victims of International Armed Conflicts, arts. 1(4), 43(1), 43(2) & 44(1), Jan. 23, 1979, 1125 U.N.T.S. 6.

238. Francisco J. Contreras & Ignacio De La Rasilla, *Of War As Law and Law As War*, 21 LEIDEN J. INT'L L. 765, 775 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1616918.

Additional Protocol I,[239] with the notable exceptions[240] of technologically-advanced India, Iran, Israel, Pakistan, Turkey, and the US. The states of the Organization of Islamic Cooperation insist upon excluding applicability of the Comprehensive Convention on International Terrorism in situations of struggle against foreign occupation.[241]

Colonialism, alien occupation and racist regimes can only be maintained in a physical dimension and therefore cannot be established online. Nonetheless, this does not eliminate the possibility of fighting for physical freedom by resorting to cyber-attacks. For example, groups like Islamic Jihad and G-Force Pakistan have engaged in minor cyber-strikes with the purpose of liberating Palestine and Kashmir respectively. Their members can therefore be classified as cyber-freedom-fighters under the existing international humanitarian law. Like other lawful combatants, such cyber-guerillas have a set of obligations they must follow,[242] including "carrying arms openly"[243] (i.e., in reality, warning in advance of an upcoming attack or using encrypted digital signatures) and, if possible, wearing uniforms.

If these requirements are fulfilled, the broad and general definition contained in the Draft Comprehensive Convention cannot be extended to the lawful freedom-fighters without invalidating Article 1(4) of the Additional Protocol I; therefore the suggestion of the Organization of Islamic Cooperation (see above) seems more than reasonable and should be affirmed on the international level.

On the other hand, since the eighteen existing counter-terrorism instruments are not broad in their scope and criminalize specific extremist actions, freedom-fighters and cyber-guerillas remain subject to them. Unlike military forces of a state, they are not excluded from the scope of

---

239. Siobhan Wills, *The Legal Characterization of the Armed Conflicts in Afghanistan and Iraq: Implications for Protection*, 58 NETH. INT'L L. REV. 173, 207 (2011).

240. For some reasons, see Wayne McCormack, *Prosecuting Terrorism—Models for Confronting Organized Violence*, *in* THE PROSECUTOR IN TRANSNATIONAL PERSPECTIVE Part IV (Erik Luna & Marianne Wade eds., 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1623847; Richard D. Rosen, *Targeting Enemy Forces in the War on Terror: Preserving Civilian Immunity*, 42 VAND. J. TRANSNAT'L L. 683, 777 (2009).

241. U.N. Rep. of the Ad Hoc Comm., 6th Sess., Jan. 28–Feb. 1, 2002 at 7, U.N. Doc. A/57/37 Annex IV; GAOR, 57th Sess., Supp. No. 37 (2002), *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/248/17/PDF/N0224817.pdf?OpenElement ("The activities of the parties during an armed conflict, including in situations of foreign occupation, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by this Convention.").

242. *See* ALEX P. SCHMID, THE ROUTLEDGE HANDBOOK OF TERRORISM RESEARCH 68–69 (2011).

243. Geneva Convention Relative to the Protection of Victims of International Armed Conflicts, *supra* note 237, at art. 44(3).

the four newest counter-terrorism instruments (see above). This creates a legal discrepancy where state military is more protected than freedom-fighters, even if they are engaged against each other in the same armed conflict. However, as mentioned before, it does not represent a big problem practically, as both categories can be held liable for war crimes and archaic terrorism. Though maybe a political paradox, under international law, it is possible for one person to be a combatant, a freedom fighter, and a terrorist (both archaic and conventional).

D. Prisoner of War Status

Jean Pictet rightly noted that "there is no intermediate status in jus in bello and nobody in enemy hands can fall outside the law."[244] Since 2002, the US Government contributed to the degradation in protection of the victims of war[245] by defining Taliban and Al-Qaeda detainees as unlawful combatants[246] and denying them the prisoner of war status.[247] Although strict opposition from international organizations and academics did not allow for any change in customary norms,[248] in the future certain states may likewise attempt to deny this status to cyber-combatants (or indefinitely detain civilians who have not participated in hostilities).

Currently, a violation of international law, whether in the form of indiscriminate cyber-attacks or participation in terrorist acts, does not deprive either state forces or freedom-fighters of their combatant and

244. Jean S. Pictet, *Commentary of the Geneva Conventions: Fourth Geneva Convention*, INT'L COMM. OF THE RED CROSS 51 (1958), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-II.pdf.

245. Eric Talbot Jensen, *Applying A Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 726 (2012).

246. *See, e.*g., Avril McDonald, *Terrorism, Counter-terrorism and the Jus in Bello*, *in* TERRORISM AND INTERNATIONAL LAW: CHALLENGES AND RESPONSES 57, 70 (2002), *available at* http://www.iihl.org/iihl/Album/terrorism-law.pdf.

For a similar discussion on Israel, see Henning Lahmann, *The Israeli Approach to Detain Terrorist Suspects and International Humanitarian Law: The Decision Anonymous v. State of Israel*, 169 HEIDELBERG J. INT'L L. 347, 357-58 (2009), *available at* http://www.zaoerv.de/69_2009/69_2009_2_a_347_364.pdf.

247. For discussion on reasons, see Gabor Rona, *Interesting Times for International Humanitarian Law: Challenges from the "War on Terror"*, 27 FLETCHER F. WORLD AFF. 55, 65 (2003). Note that the District Court found that Common Article 3 of the Geneva Conventions was applicable to the Al-Qaeda suspect in Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

248. Noëlle Quénivet, *The "War on Terror" and the Principle of Distinction in International Humanitarian Law*, 3 COLOM. Y.B. INT'L L. 155, 172 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1879133.

prisoner of war status, as long as they abide by the obligations imposed upon them by international humanitarian law.[249] Since jus in bello only prohibits archaic terrorism, in theory, participation in cyber-attacks that constitute non-overlapping conventional terrorism (e.g., acquiring funds through cyber-attacks for terrorist purposes) does not remove prisoner of war privileges.

In determining whether cyber-combatants (or civilians) were involved in acts of archaic terrorism and whether their legal protection should be revoked, one must consider that, as in the case of traditional terrorist organizations, the attackers will belong to a group that consists of cyber-attackers, organizers, donors, facilitators, trainers, colleagues who provided general encouragement but did not participate in the cyber-strikes, and persons who are engaged in non-related services (cooks, for example)—each with a different form of responsibility.[250]

E. Cyberterrorist Acts in War

Jus in bello (archaic) cyberterrorism includes all acts during an armed conflict that injure, attempt to injure, and threaten violence to civilians or persons hors de combat, if their purpose is to intimidate the population. Such acts may include causing incorrect treatment by tempering with medical computers, hijacking an enemy's military UAV and bombarding civilian objects,[251] disrupting drinking water supply, and releasing dangerous chemicals in an urban setting, even if those acts do not create any casualties.[252] There must be a direct intent to intimidate, since incidental spreading of terror among the civilian population is not illegal if acts of violence are pursued against lawful targets.[253] So, for example, American "shock and awe" tactic in the early stages of the 2003 Iraq

249. Geneva Convention Relative to the Protection of Victims of International Armed Conflicts, arts. 44(2) & 44(5), Jan. 23, 1979, 1125 U.N.T.S. 23 1979.

250. Gerald l. Neuman, *Humanitarian Law and Counterterrorist Force*, 14 EUR. J. INT'L L. 283, 289 (2003); *see also* Jean-Philippe Kot, *Israeli Civilians Versus Palestinian Combatants? Reading the Goldstone Report in Light of the Israeli Conception of the Principle of Distinction*, 24 LEIDEN J. INT'L L. 961, 986 (2011).

251. Michael N. Schmitt, *Drone Attacks Under the Jus Ad Bellum and Jus in Bello: Clearing the "Fog of Law"*, 13 Y.B. INT'L HUMAN. L. 311, 320 (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1801179; Ryan J. Vogel, *Drone Warfare and the Law of Armed Conflict*, 39 DENV. J. INT'L L. & POL'Y 101, 124 (2010).

252. *See* CASSESE, *supra* note 227, at 174.

253. Kalliopi Chainoglou, *An Assessment of Jus in Bello Issues Concerning Computer Network Attacks: A Threat Reflected in National Security Agendas*, 12 ROM. J. INT'L L. 25, 32 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1809127.

invasion targeted against Iraqi military was legal, despite being perceived as terrorism by the civilian population.[254]

Directing potentially violent cyber-attacks against civilians or persons hors de combat (in the form of actions and not threats) must also be considered archaic terrorism if carried out to coerce a state or an international organization. In this context one may consider, for example, de-individuated cyber-assassinations of persons[255] with computerized pace-makers which serve as a message to the government. Since a relatively low percentage of the general population would possess such devices, rather than intimidating ordinary civilians, this act would play upon the obligation of states to ensure safety of their citizens.

During armed conflicts, acts of conventional terrorism via cyber-space can only be viewed as an individual crime (see sub-chapter 3) or through a prism of the principles of necessity, proportionality, humanity, distinction, neutrality, and chivalry. However, it is more likely than not that archaic and conventional cyberterrorism will overlap in war.

VI. CONCLUSION

The present Article addressed the legal issues surrounding cyberterrorism. In the first chapter, the author explains why cyberterrorism should be described as "the use of electronic networks taking the form of a cyber-attack to commit a) a substantive act criminalized by the existing legal instruments prohibiting terrorism, or b) an act of terrorism under international customary law." Further, with a special emphasis on existing anti-terrorism conventions and customary international law, it was demonstrated which actors are likely to engage in acts of cyberterrorism (non-state actors, corporations and individuals), as well as which targets are protected by law and which aims are to be pursued by terrorists.

The last two chapters concentrated on permissibility of individual response to cyberterrorism and applicability of this concept to jus in bello. The author noted that although generally self-defense in jus ad bellum is permitted, the controversial legal theories will have trouble adapting to the realities of cyberterrorism without international support. The author also highlights the paradoxical situation of two regimes on

254. Brian Whitaker, *Flags in the Dust*, GUARDIAN, (Mar. 24, 2003, 5:32 EST), http://www.guardian.co.uk/world/2003/mar/24/worlddispatch.iraq.

255. *See* SCHMID, *supra* note 52, at 84.

terrorism (archaic and conventional) coexisting during armed conflicts and its impact on cyberterrorism. Future convergence of these regimes on political level will require legal coordination of international organizations.

This Article demonstrates why conventional terrorism by states should be ruled out as a viable concept in international law. At the same time the author argues in favor of the Organization of the Islamic Conference suggestion to exclude freedom-fighters from the applicability of anti-terrorism conventions. Major legal gaps identified in this Article include preservation of prisoner of war privileges by conventional terrorists during wars, as well as legal discrepancy created by the conventions regime on terrorism which ensures freedom-fighters and cyber-guerillas receive less legal protection than military forces of a state despite their equal status under the Additional Protocol I.