Study Group Report

Study Group on Cyber Security, Terrorism and International Law

International Law Association Study Group on Cybersecurity, Terrorism, and International Law; Fidler, D.; Buchan, R.; Crawford, E.; Adhihetty, T.; Harrison Dinniss, H.; Ducheine, P.; Eichensehr, K.; Housen-Couriel, D.; Ivanov, E.; Kim, Sung-Won; Nasu, Hitoshi; Nkusi, F.; O'Connell, M.E.; Sobrinho de Morais Neto, A.; Tsagourias, N.; Ziolkowski, K.

Publication date
2016

Document Version
Final published version

INTERNATIONAL LAW ASSOCIATION

Study Group on Cybersecurity, Terrorism, and International Law

STUDY GROUP REPORT

David P. Fidler (American Branch), Chair
Russell Buchan (British Branch), Co-Rapporteur
Emily Crawford (Australian Branch), Co-Rapporteur

Study Group Members

TJ Adhihetty (Netherlands Branch)
Heather Harrison Dinniss (Swedish Branch)
Paul Ducheine (Netherlands Branch)
Kristen Eichensehr (American Branch)
Deborah Housen-Couriel (Israeli Branch)
Eduard Ivanov (Russian Branch)
Sung-Won Kim (Korean Branch)
Hitoshi Nasu (Australian Branch)
Fred K. Nkusi (Headquarters)
Mary Ellen O'Connell (American Branch)
Arnaldo Sobrinho de Morais Neto (Brazilian Branch)
Nicholas Tsagourias (British Branch)
Katharina Ziolkowski (German Branch)

July 31, 2016

INTERNATIONAL LAW ASSOCIATION

Study Group on Cybersecurity, Terrorism, and International Law

STUDY GROUP REPORT

CONTENTS

Chair's and Co-Rapporteurs' Note

The chair and the co-rapporteurs would like to thank the members of the Study Group for their willingness to participate in this project and for the comments they provided to us as the project developed and moved to completion. The complexity of the Study Group's topic, the challenging nature of our objectives, and the extensive range of international legal issues the report covered made this project difficult to organize and execute. The patience and expertise of Study Group members helped the process move forward effectively and efficiently. We hope the final report does justice to the time and attention the members of the Study Group devoted to this project.

David P. Fidler, Chair (American Branch)
Russell Buchan, Co-Rapporteur (British Branch)
Emily Crawford, Co-Rapporteur (Australian Branch)

Abbreviations

ASEAN	Association of South East Asian Nations
AU	African Union
CENTCOM	Central Command
CIP	Critical infrastructure protection
COE	Council of Europe
EU	European Union
GFCE	Global Forum for Cyber Expertise
GGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICC	International Criminal Court
ICRC	International Committee of the Red Cross
ICTR	International Criminal Tribunal for Rwanda
ICTs	Information and communication technologies
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International humanitarian law
IHR	International Health Regulations
ILA	International Law Association
IMO	International Maritime Organization
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
MLAT	Mutual legal assistance treaty
NSA	National Security Agency
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
SCSL	Special Court for Sierra Leone
UN	United Nations
WHO	World Health Organization
WMD	Weapons of mass destruction

Executive Summary

Introduction

The International Law Association (ILA) established the Study Group on Cybersecurity, Terrorism, and International Law at the end of 2013 to examine international law related to cyber terrorism. The chair and co-rapporteurs invited experts and scholars from ILA branches around the world to participate in the Study Group, and ILA members from eleven countries joined the Study Group. During 2014, the members of the Study Group provided input on the objectives of the project, the structure of the research agenda, and the international legal issues the project needed to address. The chair and co-rapporteurs prepared two full drafts of the report (May 2015, December 2015) and invited Study Group members to comment on the drafts. This report constitutes the Study Group's final draft submitted to the ILA.

The Study Group identified four main objectives for its work:

- Examine the potential threat posed by cyber terrorism, including how technological trends and innovations might affect the threat;
- Develop a definition of "cyber terrorism" to guide its analysis based on international law and state practice;
- Produce and analyze an inventory of international law potentially relevant to cyber terrorism; and
- Assess whether pro-active international legal actions concerning potential acts of cyber terrorism would be worthwhile and feasible.

Examine the potential threat posed by cyber terrorism

The Study Group reviewed primary documents and secondary literature on the threat of cyber terrorism (see Chapters 1-2). It noted the continued gap between concerns expressed by policymakers and experts about cyber terrorism and the lack of cyber incidents widely acknowledged to involve acts of terrorism. Analyses of technological trends and innovations often identify the potential for such changes to facilitate acts of cyber terrorism. Such technological developments, along with threats posed by terrorist groups, such as Al Qaeda and the so-called "Islamic State," ensure that concerns about cyber terrorism have not dissipated, despite the lack of cyber terrorism incidents. The political prominence of these concerns made the Study Group's focus on international law relevant to the policy landscape developing on this issue.

Develop a definition of "cyber terrorism"

The Study Group noted the lack of an agreed definition of "cyber terrorism" in policy, law, and scholarly literature. It reviewed existing international law on terrorism in order to identify what elements a definition of cyber terrorism should include (see Chapter 3). On the basis of this research, the Study Group developed a working definition of cyber terrorism to guide its work:

> "Cyber terrorism" involves acts intentionally committed by any person who uses information and communication technologies unlawfully in ways that cause, or are intended to cause, death or serious bodily injury to persons, substantial damage to public or private property, the economy, or the environment, or serious disruption of public services and that are undertaken with the intent to spread fear in civilian populations or to compel a government, a civilian population, or an international organization to take or abstain from specific acts or courses of action.

Produce an inventory of international law potentially relevant to cyber terrorism

In combatting terrorism, states and international organizations have formulated policies to achieve three strategic objectives: respond to acts of terrorism, protect against terrorism, and prevent terrorist attacks. The Study Group used this "respond, protect, and prevent" framework to organize its analysis of international law relevant to cyber terrorism. Applying this approach, the Study Group analyzed an extensive amount of international law. The bulk of the Study Group's report—Chapters 4, 5, and 6—examines the international law implicated by the threat of cyber terrorism.

The Study Group's analysis of responding to cyber terrorism (see Chapter 4) included examining multilateral and regional anti-terrorism treaties, the draft Comprehensive Convention on International Terrorism, Security Council resolutions on terrorism, the purported crime of international terrorism in customary international law, treaties on cyber crime and transnational organized crime, extradition and mutual legal assistance treaties, international law on the use of force, international humanitarian law, and international criminal law.

In assessing international law relevant to protecting against cyber terrorism (see Chapter 5), the Study Group concentrated on international law connected to critical infrastructure sectors, such as nuclear energy and aviation. This law includes treaties that establish and guide international organizations working on critical infrastructure issues (e.g., International Atomic Energy Agency), as well as treaty law that specifically addresses protection of critical infrastructure from cyber threats. The Study Group also considered areas of international law relevant to: creating resilience in societies against malicious cyber activities (e.g., approaches used in transboundary pollution treaties), securing dangerous materials from terrorists, and using export controls as a counter-terrorism strategy. Finally, international human rights law was analyzed because of the importance electronic surveillance and information sharing have in protecting against terrorism and cyber terrorism.

In terms of preventing cyber terrorism (see Chapter 6), the Study Group focused on Security Council resolutions that impose binding obligations on terrorism prevention, treaties specifically on preventing terrorism, international human rights law and electronic surveillance (including controversies over encryption), and international law on the use of force in connection with anticipatory and pre-emptive self-defense.

Assess whether pro-active international legal actions concerning potential acts of cyber terrorism would be worthwhile and feasible

From its analysis of international law relevant to responding to, protecting against, and preventing cyber terrorism, the Study Group identified options to improve the contributions international law could make against the threat of cyber terrorism. The options fell into two categories: (1) ideas for better utilization of existing treaty and customary international law; and (2) proposals for the development of new international law. The following table summarizes the Study Group's analysis:

Strategic Objective	**Options Analyzed**
Respond (Chapter 4, Section 4.8)	*Better Use of Existing International Law*
	• Where possible, ensure treaties on anti-terrorism, cyber crime, organized crime, extradition, and mutual legal assistance apply to cyber terrorism • Make clear Security Council resolutions on terrorism apply to cyber terrorism
	Creating New International Law
	• Amend, or adopt protocols to, relevant anti-terrorism, cyber crime, and organized crime treaties to cover cyber terrorism expressly • Adoption of a Security Council resolution on cyber terrorism • Negotiate a treaty on cyber terrorism
Protect (Chapter 5, Section 5.8)	*Better Use of Existing International Law*
	• Increase attention on cyber defenses in existing treaty regimes that address critical infrastructure sectors
	Creating New International Law
	• Include strengthening cyber defenses in a treaty on cyber terrorism
Prevent (Chapter 6, Section 6.8)	*Better Use of Existing International Law*
	• Make clear existing Security Council resolutions on terrorism cover cyber terrorism • Make clear existing treaty law on terrorism prevention applies to cyber terrorism
	Creating New International Law
	• Security Council adoption of a resolution on prevention of cyber terrorism • Include prevention of cyber terrorism in a treaty on cyber terrorism

The Study Group also identified where existing controversies in international law continue when cyber terrorism is the focus. Long-standing debates about international law on the use of force, including the rules on using force in self-defense, do not dissipate when cyber terrorism is the topic. Similarly, friction between political desires for expanded counter-terrorism surveillance and the obligations to protect individual rights in international human rights law persists in the context of cyber terrorism.

Finally (see Chapter 7), the Study Group made recommendations to the ILA concerning (1) follow-on work advancing ideas discussed by the Study Group, such as preparing a draft treaty specifically addressing cyber terrorism for states, international

organizations, and non-governmental experts to consider; and (2) additional research focused on other aspects of the relationship between cyberspace and terrorism, such as the international legal issues that arise from how terrorist groups use the Internet to communicate, spread propaganda, recruit and radicalize individuals, and raise funds.

* * *

1

INTRODUCTION

1.1 The Study Group's Objectives

1. The International Law Association (ILA) established the Study Group on Cybersecurity, Terrorism, and International Law to examine international law related to cyber terrorism.[1] Policy documents have frequently identified cyber terrorism as a threat,[2] even though experts do not believe terrorists have, to date, successfully conducted cyber attacks that qualify as terrorism, as opposed to terrorist groups using information and communication technologies (ICTs) and the Internet for other purposes.[3]

2. Even so, governments and experts fear terrorists will eventually use ICTs and the Internet to attack targets, such as cyber-enabled critical infrastructure, in order to terrorize societies by damaging economies and public services or causing injury or death.[4] Cyber attacks by terrorists have the potential to be equally or more devastating than traditional forms of kinetic terrorism. The present gap between often-voiced fears about cyber terrorism and the perceived lack of it has contributed to analyses of cyber terrorism remaining general, speculative, and sporadic.[5]

3. International lawyers have studied and discussed cyber terrorism.[6] For example, a study sponsored by the Council of Europe in 2007 analyzed the applicability of existing

---

[1] ILA, *Study Group on Cybersecurity, Terrorism, and International Law*, http://www.ila-hq.org/en/study-groups/index.cfm/cid/1050.

[2] *See, e.g.,* White House, *National Strategy to Secure Cyberspace* (Feb. 2003), http://georgewbush-whitehouse.archives.gov/pcipb/.

[3] In its research, the Study Group did not identify any cyber incident that experts agree constitutes terrorism, as terrorism has traditionally been understood in policy and law. The lack of acknowledged acts of cyber terrorism flows, in part, from controversies about the definition of "cyber terrorism." Chapter 3 (Defining "Cyber Terrorism") *infra* addresses definitional issues.

[4] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98*, June 24, 2013 [hereinafter *GGE Report* (2013)], ¶ 7 (observing that, if terrorists "acquire attack tools, they could carry out disruptive ICT activities"); *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, July 22, 2015 [hereinafter *GGE Report* (2015)], ¶ 6 (stating that "[t]he use of ICTs for . . . terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility").

[5] For an extended treatment, see *Cyberterrorism: Understanding, Assessment, and Response* (Thomas M. Chen, Lee Jarvis, and Stuart MacDonald, eds.) (New York: Springer, 2014).

[6] *See, e.g.,* Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law* (2010); 43: 57-118; Aviv Cohen, "Cybterterrorism: Are We Legally Ready?" *Journal of International Business & Law* (2010); 9(1): 1-40; Yaroslav Shiryaev, "Cyberterrorism in the Context of Contemporary International Law," *San Diego International Law Journal* (2012); 14: 139-92; Eduard Ivanov, "Combating Cyberterrorism under International Law," *Baltic Yearbook of International Law* (2014): 14: 55-69; Ben Saul and Kathleen Heath, "Cyber Terrorism," in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias and

treaties on terrorism and cyber crime to cyber terrorism.[7] Although helpful, existing international legal literature reflects neither sustained attention nor consensus on how to define and analyze cyber terrorism.[8] Continued warnings about cyber terrorism and the damage it might cause invite more systematic international legal scrutiny of this potential national and international security threat. The increased interest in other aspects of cybersecurity, such as how cyber weapons might affect international law on the use of force and armed conflict,[9] highlight the opportunity to study cyber terrorism more closely under international law.

4. Conceived and initiated by Russell Buchan and Emily Crawford (co-rapporteurs), chaired by David Fidler, and advised by a global group of scholars and experts, the Study Group explored international law associated with potential terrorist use of cyber attacks. Generally, for the Study Group, a terrorist cyber attack involves non-state actors using ICTs to injure or kill persons, damage property, or seriously disrupt public services in order to spread fear among civilians or compel populations or governmental authorities to take or abstain from specific actions.[10]

5. The Study Group excluded from its efforts terrorist use of ICTs and the Internet for other purposes, including communications, propaganda, recruitment, and fundraising. Nor did the Study Group examine how governments conduct counter-terrorism generally in cyberspace, such as engaging in surveillance of electronic communications. These topics are important, but the Study Group limited the scope of its project in order to concentrate on a core component of the relationship between terrorism and cyberspace.

6. The Study Group identified four main objectives for its work:

- Examine the potential threat posed by cyber terrorism, including how technological trends and innovations might affect the threat;
- Develop a definition of "cyber terrorism" to guide its analysis based on international law and state practice;
- Produce and analyze an inventory of international law potentially relevant to cyber terrorism; and
- Assess whether pro-active international legal actions concerning potential acts of cyber terrorism would be worthwhile and feasible.

Russell Buchan, eds.) (Cheltenham: Edward Elgar Publishing, 2015) [hereinafter *Research Handbook on International Law and Cyberspace*], 147-67.

[7] Council of Europe Counter-Terrorism Task Force, *Cyberterrorism—The Use of the Internet for Terrorist Purposes* (Strasbourg: Council of Europe Publishing, 2007), 94-95.

[8] International lawyers are not alone in this respect. The editors of *Cyberterrorism: Understanding, Assessment, and Response* noted a feature of existing analyses "is the absence of any real agreement on the . . . fundamental question of what, exactly, cyberterrorism is."

[9] *See, e.g.,* International Group of Experts, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013) [hereinafter *Tallinn Manual*]; Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New *Tallinn Manual*," *Journal of Conflict & Security Law* (2013); 18(2): 331-51.

[10] *See* Chapter 3 (Defining "Cyber Terrorism") *infra* for detailed analysis.

1.2 The Report's Analytical Framework

7. The absence of cyber attacks widely recognized as acts of terrorism helps explain why, to date, states have not developed much international law specifically on cyber terrorism.[11] In working to achieve its goals, the Study Group examined the ways in which states have used international law to respond to, protect against, and prevent terrorism generally. Using this template, the Study Group organized international legal issues under the strategies of responding to, protecting against, and preventing cyber terrorism. This approach required identifying whether, and to what extent, cyber terrorism might be different from other forms of terrorism. This requirement connected to the objective of assessing cyber terrorism in light of the technological aspects of this threat.

1.2.1 Terrorism and International Law

8. The evolution of international law on terrorism predominantly reflects states reacting to terrorist acts by producing treaties on specific areas or sectors of concern. This pattern emerged before the attacks on the United States on September 11, 2001, as evidenced by treaties on different terrorist activities dating to the 1960s.[12] Reactions to 9/11 and terrorist attacks in Madrid in 2004, London in 2005, Paris in 2015, and Brussels in 2016 continued this pattern as countries responded with, among other things, international legal initiatives.

9. In the wake of these and other terrorist attacks, counter-terrorism policies have emphasized three strategic objectives:

- *Respond* to terrorist attacks through national criminal law and cooperation among national and international law enforcement agencies;
- *Protect* societies from terrorist attacks through "hardening" potential targets, such as critical infrastructure, and developing capabilities for recovery; and
- *Prevent* terrorist attacks through intelligence, information sharing, cutting off financial and other resources, and anticipatory or pre-emptive covert or military action against imminent or emerging terrorist threats.

10. Ideally, the sequencing of these objectives would start with prevention and move through protection and response. However, states have developed more international law with respect to responding to terrorist acts than on protecting against and preventing terrorism. In keeping with this reality, the report focuses first on the response strategy (Part 4) before examining the protection and prevention approaches (Parts 5 and 6).

11. Although distinct, these objectives overlap because actions in each contribute to the other goals. Investigation and prosecution of terrorists can support protection and prevention by creating deterrence. Securing nuclear, chemical, or biological materials

[11] *But see* Section 4.2.3 (Multilateral Anti-Terrorism Treaties Not in Force) *infra* discussing treaties not in force that address cyber attacks in civil aviation.
[12] *See, e.g.,* UN, *UN Action to Counter Terrorism: International Legal Instruments*, http://www.un.org/en/terrorism/instruments.shtml.

protects against and prevents terrorism by ensuring these materials do not fall into terrorists' hands. Preventing terrorist attacks protects societies from suffering harmful consequences. As the terrorist threat continued to grow more dangerous, governments formulated policies against terrorism with these overlapping goals as priorities.

12. Although each category informs counter-terrorism policy, strategies after 9/11 and other major terrorist attacks have emphasized protection and prevention more than previously had been the case. This shift created a broader range of challenges and raised more international legal issues than when treaties criminalizing terrorist offenses and strengthening law enforcement cooperation dominated international law on terrorism.

13. For example, non-proliferation treaties, such as the Biological Weapons Convention,[13] became relevant to counter-terrorism even though they did not specifically address terrorism.[14] The need for intelligence to prevent terrorist attacks implicated international human rights law, particularly the rights to freedom of expression and privacy.[15] Intelligence-driven awareness of terrorist activities fed arguments that international law permitted anticipatory or pre-emptive use of force against terrorists.[16]

14. The heightened concerns about terrorism also attracted the attention of international organizations, resulting in many counter-terrorism initiatives. The United Nations (UN) Security Council issued decisions under Chapter VII of the UN Charter requiring UN member states to fulfill counter-terrorism obligations,[17] and it created a Counter-Terrorism Committee to advance the international counter-terrorism agenda.[18] Other multilateral and regional organizations also generated treaty law, such as new anti-terrorism agreements, and soft-law initiatives designed to improve multilateral cooperation against terrorism.[19]

15. In sum, counter-terrorism efforts produced new international law and "soft" law, applied existing legal instruments in new ways, and created interpretations of international law—with controversies especially appearing with respect to intelligence and military activities—in order to respond to, protect against, and prevent terrorism.

---

[13] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, entered into force Mar. 26, 1975, 1015 UNTS 164.
[14] BioWeapons Prevention Project, *How do Countering Bioterrorism and the BWC Relate to Each Other?*, Dec. 6, 2011, http://www.bwpp.org/documents/revcon/BWPP2010%202011-RevConProject-Conclusion-Bioterrorism.pdf.
[15] Office of the UN High Commissioner for Human Rights, *Human Rights, Terrorism, and Counter-Terrorism*, Fact Sheet No. 32 (2008), http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf.
[16] Anthony Clark Arend, "International Law and the Preemptive Use of Military Force," *Washington Quarterly* (2003), 26(2): 89-103.
[17] *See, e.g.,* UN Security Council, Resolution 1373 (2001), Sept. 28, 2001; UN Security Council, Resolution 2178 (2014), Sept. 24, 2014.
[18] UN Security Council, *Counter-Terrorism Committee*, http://www.un.org/en/sc/ctc/.
[19] *See, e.g.,* UN Office on Drugs and Crime, *(Inter-) Regional Action Against Terrorism* (2015), https://www.unodc.org/tldb/en/regional_instruments.html; Organization for Security and Co-Operation in Europe, *OSCE Anti-Terrorism Reference* (Feb. 2015), http://www.osce.org/secretariat/99765.

1.2.2 Cyber Terrorism and International Law

16. The Study Group's analysis is premised on the widely held position that international law applies to activities in cyberspace,[20] including acts of terrorism.[21] Controversies about whether international law applies in cyberspace, such as those centered on the law of armed conflict,[22] have not arisen in discussions about threats terrorism poses in cyberspace. The Study Group also analyzed the law of armed conflict as an applicable body of international law concerning cyber terrorism.[23]

17. The different ways acts of terrorism and the development of counter-terrorism policy have affected international law constitute starting points for exploring international legal issues related to cyber terrorism. First, the pathways blazed in counter-terrorism form the most likely routes states will take in addressing cyber terrorism. Counter-terrorism policy provides a roadmap for identifying objectives for action against cyber terrorism—respond, protect against, and prevent—and areas and issues relevant to addressing each objective in connection with cyber terrorism.

18. Second, the international law on, and the international legal controversies related to, counter-terrorism applies in various ways to potential acts of cyber terrorism. Certain cyber activities by terrorists could fall within the scope of some existing sector-specific anti-terrorism treaties.[24] Efforts to prevent cyber terrorism through strengthened surveillance or preventive "active defense" measures confront the international legal controversies experienced in counter-terrorism policy associated with expanded intelligence activities[25] and the anticipatory or pre-emptive uses of force.[26]

19. Third, states have engaged in lawmaking when they perceived gaps or weaknesses in international law on terrorism. The lack of specific international law on cyber terrorism makes this pattern relevant in evaluating whether states should develop new international law to support policies against cyber terrorism.

20. Although examining how counter-terrorism efforts have used international law provides guidance, cyber terrorism has features not easily mapped against other types of

[20] *GGE Report* (2013), ¶ 19 (stating that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment").
[21] *GGE Report* (2015), ¶ 6 (noting that "terrorist attacks against ICTs or ICT-dependent infrastructure . . . may threaten international peace and security").
[22] Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica: RAND, 2016), 66-67 (discussing China's resistance to acknowledging the application of the law of armed conflict in cyberspace).
[23] *See* Section 4.6 (International Humanitarian Law and Responding to Cyber Terrorism during Armed Conflict) *infra.*
[24] *See* Section 4.2 (Anti-Terrorism Treaties) *infra.*
[25] *See, e.g., Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UN Doc. A/69/397, Sept. 23, 2014.
[26] *See, e.g.,* Christian J. Tams, "The Use of Force against Terrorists," *European Journal of International Law* (2009); 20(2): 359-97.

terrorism. The international law addressing nuclear, chemical, or biological terrorism does not apply readily to terrorist use of ICTs. Skepticism that states can restrict terrorist access to the means and methods of cyber attack suggests that ICTs and the Internet—as highly accessible technologies that create attribution problems—presents challenges different from those associated with nuclear, chemical, or biological materials. The ways in which the technological attributes of cyberspace affect policy and international law cut across the Study Group's analysis.

1.3 Options for International Legal Action

21. In keeping with its objective of evaluating whether pro-active steps in international law against cyber terrorism would be worthwhile, the Study Group identified options for action described throughout this report. These options fall into two categories. First, the Study Group highlighted ways states could better utilize existing international legal rules and mechanisms against cyber terrorism. For example, states parties to some existing anti-terrorism treaties could publicly declare that the treaties apply to acts of cyber terrorism. States parties to treaties addressing critical infrastructure sectors could pay more attention to cybersecurity and invest resources to protect such infrastructure against cyber terrorism.

22. Second, the Study Group identified options involving the creation of new international law for cyber terrorism. The most prominent of these options would involve adopting a treaty specifically on cyber terrorism. Although much international law is relevant to acts of cyber terrorism, little of this law has been designed with cyber terrorism in mind. Cyber terrorism has sufficiently different features from other forms of terrorism to warrant consideration of developing "fit for purpose" international law.

2

PRELIMINARY CONSIDERATIONS

2.1 Cyberspace and Terrorism

2.1.1 Scope of the Study Group's Analysis

23. The Study Group is aware the relationship between terrorism and cyberspace is broader than terrorists using ICTs to attack governmental or civilian targets with sufficient damage in order to terrorize or coerce. The present paucity of such attacks contrasts with terrorist use of cyberspace for other purposes, including propaganda, recruitment, and fundraising. These terrorist uses of cyberspace explain why references to cyber terrorism, information terrorism, or Internet terrorism often include them.[27]

24. Although long a concern, worries about terrorist use of the Internet increased with the rise of the so-called "Islamic State" and other extremist groups.[28] News stories and analysts have noted the sophistication of such groups in using social media for propaganda and recruitment.[29] These activities support the Islamic State's use of violence to terrorize civilians and intimidate governments.[30] Governments, international institutions, and non-governmental organizations are trying to figure out better approaches to these terrorist uses of cyberspace,[31] including actions taken by the UN Security Council and its Counter-Terrorism Committee.[32]

---

[27] *See, e.g.,* Imran Awan, "Debating the Term Cyber-Terrorism: Issues and Problems," *Internet Journal of Criminology* (Jan. 2014), http://www.internetjournalofcriminology.com/awan_debating_the_term_cyber-terrorism_ijc_jan_2014.pdf.

[28] This report's use of "Islamic State" does not mean the Study Group accepts this terrorist organization's claim to be a state or caliphate. However, use of Islamic State as this group's name has become ubiquitous in the media and in policy and legal analysis of its activities.

[29] *See, e.g.,* J. M. Berger and Jonathan Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter* (Brookings Project on U.S. Relations with the Islamic World Analysis Paper No. 20, Mar. 2015), http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

[30] David P. Fidler, "Cyber War Crimes: Islamic State Atrocity Videos and the Laws of War," *Computer Law Review International* (2015); 16(6): 161-65.

[31] *See, e.g.,* Christina Schori Liang, *Cyber Jihad: Understanding and Countering Islamic State Propaganda* (Geneva Centre for Security Policy Paper 2015/2, Feb. 2015), http://www.gcsp.ch/Emerging-Security-Challenges/Publications/GCSP-Publications/Policy-Papers/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda; David P. Fidler, *Countering Islamic State Exploitation of the Internet* (Council of Foreign Relations Cyber Brief, June 2015), http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-internet/p36644; Jared Cohen, "Digital Counterinsurgency: How to Marginalize the Islamic State Online," *Foreign Affairs* (Nov./Dec. 2015), 52-58.

[32] *See* Security Council Resolution 2178 (2014), ¶ 7 (expressing its "determination to consider listing . . . individuals, groups, undertakings and entities associated with Al-Qaida who are financing, arming, planning, or recruiting for them, or otherwise supporting their acts or activities, including through information and communications technologies, such as the internet, social media, or any other means"). On the Counter-Terrorism Committee, see Special Meeting of the Counter-Terrorism Committee and Technical Sessions of the Counter-Terrorism Committee Executive Directorate on Preventing and

25. The Islamic State has also stoked fears it and other terrorist groups will turn to cyber attacks.[33] In January 2015, the so-called "Cyber Caliphate" affiliated with the Islamic State claimed to have hacked into social media sites of U.S. Central Command (CENTCOM), one of the U.S. military's combatant commands.[34] In April 2015, individuals claiming to be part of the Cyber Caliphate took credit for hacking television channels, websites, and social media operated by TV5Monde, a French public television network.[35] French officials later indicated, however, that Russian hackers might have carried out the TV5Monde attack—another example of the difficulty of attributing acts in cyberspace.[36] Although these incidents were not widely regarded as terrorism, terrorist groups' increased abuse of cyberspace worries policymakers that terrorists might begin to engage in cyber attacks that cause physical damage or injure people.[37]

26. The Study Group decided against taking up all the international legal issues that arise from terrorist activities in cyberspace.[38] The Study Group's focus on potential terrorist cyber attacks exhibiting features associated with terrorism produced enough to explore. However, the Study Group appreciates the need to examine other facets of terrorism and cyberspace, especially given the calls for international cooperation related to the Islamic State's exploitation of the Internet.[39] Thus, it recommends the ILA establish another study group to focus on the international legal issues associated with terrorist use of ICTs and the Internet for purposes other than cyber attacks.

Combating Abuse of ICT for Terrorist Purposes, Dec. 16-17, 2015, http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html.

[33] *See, e.g.,* Sharon Behn, "Could IS Turn Next to Cyber War?," *Voice of America*, Dec. 18, 2015, http://m.voanews.com/a/islamic-state-cyber-war/3109289.html.

[34] Geoff Earle and Jamie Schram, "'We are Coming': ISIS Hacks Defense Department," *New York Post*, Jan. 12, 2015, http://nypost.com/2015/01/12/we-are-coming-isis-hacks-defense-department-twitter-account/.

[35] Angelique Chrisafis and Samuel Gibbs, "French Media Groups to Hold Emergency Meeting after ISIS Cyber-Attack," *The Guardian*, Apr. 9, 2015, http://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers.

[36] John Lichfield, "TV5Monde Hack: 'Jihadist Cyber Attack on French TV State Could Have Russian Link," *The Independent*, June 10, 2015, http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html.

[37] *See, e.g.,* Emma Graham-Harrison, "Could ISIS's 'Cyber Caliphate' Unleash a Deadly Attack on Key Targets?" *The Guardian*, Apr. 12, 2015, http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.

[38] For analysis of terrorist uses of the Internet not involving cyber attacks, see UN Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (New York: United Nations, 2012).

[39] *See, e.g* Statement by the President of the Security Council, UN Doc. S/PRST/2016/6, May 11, 2016 (reporting that the Security Council requests the Counter-Terrorism Committee to develop a comprehensive international framework to counter the ways in which terrorist groups motivate and recruit individuals to commit terrorist acts); *Report by the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat,* UN Doc. S/2016/501, May 31, 2016, ¶¶ 37-43 (reporting on ISIL's use of ICTs and efforts to counter it).

2.1.2 Terminology in Analyzing Cyber Terrorism

27. The manner in which the relationship between cyberspace and terrorism is discussed reflects different meanings given to concepts, such as "cyber terrorism" and "cyber attack." Terminological diversity arises in other areas of cybersecurity, as seen in perspectives on what "cyber war" and "cyber deterrence" mean.[40] International law adds to these challenges. For example, treaty definitions of terrorist offenses determine whether a kinetic or cyber incident qualifies as terrorism. Similarly, international law uses concepts that shape how such incidents are assessed, inclduing "use of force" and "armed attack" in the rules on using force and "attack" in the law of armed conflict.

28. Similarly, other terms, such as the Internet and cyberspace, have no commonly agreed definitions despite their frequent use in analyzing cybersecurity and cyber terrorism. For its purposes, the Study Group used the following terms as described below:

- Information and communication technologies (ICTs): Technologies used to transmit and receive digital information, including (but not limited to) computers, smartphones, and software programs.
- Internet: The global network that uses standardized protocols to facilitate communication and information exchange among individual and interconnected ICTs.
- Cyberspace: The domain or environment of communication and information exchange created by connecting ICTs through the Internet.

29. The lack of agreed definitions of key terms, and the importance of clarity in legal analysis, informed the Study Group's development of a working definition of "cyber terrorism," which Chapter 3 of the report covers. This definition guided the Study Group's evaluation of cyber incidents under international law relevant to terrorism. While useful, the Study Group's definition of cyber terrorism does not represent international law, nor does it eliminate definitional controversies in this area of cybersecurity.

2.2 Internet Governance and Cyber Terrorism

30. Analyzing international legal issues associated with cyber terrorism does not happen in a vacuum. Policy and legal approaches to cyber terrorism arise against, among other things, the backdrop of "Internet governance."[41] Controversies about the scope and substance of Internet governance[42] and competition between multi-stakeholder and

[40] NATO Cooperative Cyber Defence Centre of Excellence "Cyber Definitions," https://ccdcoe.org/cyber-definitions.html (noting "[t]here are no common definitions for Cyber terms—they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements").

[41] *See* Global Commission on Internet Governance, *One Internet* (London: Chatham House, 2016).

[42] States have expressed different perspectives on what "Internet governance" means. These differences appeared in the Working Group on Internet Governance (WGIG) established in 2003 by the UN Secretary-General as part of the World Summit on the Information Society process. In its 2005 report, the WGIG noted "there is not yet a shared view of Internet governance" because, during the Internet's evolution, "very different points of view emerged about the scope and mechanisms of Internet governance." *Report of the*

intergovernmental approaches to Internet governance,[43] affect political discussions in many cyber-related contexts, ranging from human rights to espionage.[44] The politics of these controversies can undermine prospects for addressing cyber problems effectively.

31. In the context of cyber terrorism, initiatives to address perceived gaps in international law have to be mindful of the Internet governance problem. First, disagreements about Internet governance could prevent consensus on international legal steps to combat cyber terrorism. Second, actions, such as defining cyber terrorism in a treaty, could agitate controversies over Internet governance, especially those related to how cybersecurity, or "information security," affects the protection of human rights.

32. Although the Study Group did not delve into the Internet governance debate, it did not ignore the debate's impact on its analysis of options for action. Where appropriate, this report notes where Internet governance controversies might complicate international legal activities the Study Group thinks worthwhile to pursue.[45]

2.3 Technology and Cyber Terrorism

33. The Study Group's objectives include understanding how technological trends might affect the threat of cyber terrorism. This task reflects the need for similar understanding in areas of terrorism associated with "dual use" technologies.[46] Policy on terrorism conducted with weapons of mass destruction (WMD) involves tracking how biological, chemical, and nuclear technologies evolve and what changes mean for the potential of WMD terrorism.[47]

34. The leading concern, especially with respect to biological and chemical terrorism, is that technological developments might make WMD terrorism more likely by lowering

---

Working Group on Internet Governance (2005), ¶ 8. The working definition produced by the WGIG defines Internet governance as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." *Ibid.,* ¶ 10.

[43] Generally, the multi-stakeholder approach to Internet governance favors governance through the participation of all stakeholders, including governments, the private sector, and non-governmental organizations. The intergovernmental approach supports governmental control over Internet governance.

[44]. On international law and Internet governance, *see generally* David P. Fidler, "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations," *American Society of International Law Insights*, Feb. 7, 2013, http://asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision.

[45] *See, e.g.,* Section 5.2.4 (Controversy over Revising the International Telecommunication Regulations) *infra.*

[46] *See generally Governance of Dual-Use Technologies: Theory and Practice* (Elisa D. Harris, ed.) (Cambridge, Mass.: American Academy of Arts & Sciences, 2016) [hereinafter *Governance of Dual-Use Technologies*].

[47] *See, e.g.,* Gigi Kwik Gronvall, *Mitigating the Risks of Synthetic Biology* (Council on Foreign Relations Center for Preventive Action Discussion Paper, Feb. 2015), http://www.cfr.org/health/mitigating-risks-synthetic-biology/p36097.

obstacles to obtaining and exploiting the requisite materials and know-how.[48] The "dual use" nature of these technologies complicates policymaking because technological advances can create benefits for societies. Taking advantage of these benefits while minimizing the possibility of terrorist abuse has proved difficult. The controversies among the scientific, public health, and national security communities about "gain of function" research on pathogens provide an example of this conundrum.[49]

35. Like WMD terrorism, cyber terrorism is presently linked with specific technologies as the means of inflicting damage and spreading terror.[50] Fears about cyber terrorism include the possibility that technological developments will increase the capabilities and motivations of terrorists to launch cyber attacks.[51] Networked ICTs, and their global dissemination, heightens prospects that non-state actors, including criminals and terrorists, can develop powerful capabilities. The scale and sophistication of cyber crime globally provide evidence supporting this concern.

36. The Study Group found little reason to believe technological innovation affecting the use of cyberspace will slow down. Cybersecurity experts identify emerging vulnerabilities in technological developments being widely embraced, including cloud computing, mobile devices, self-driving vehicles, the "Internet of Things," and the "Internet of Everything."[52] The growing dependence of governments, economies, and societies on these technologies increases incentives for more innovation. Whether the next wave of innovation incorporates better cybersecurity in the design of software and hardware remains to be seen, but moves in this direction might agitate the "offense v. defense" dynamic already influencing technological developments in this context.

37. Technological innovation can also create problems for policy and legal measures addressing cyber terrorism. For example, the increasing use of cloud computing complicates jurisdictional issues central to the exercise of governmental authority.[53] In one case, Microsoft challenged a search warrant from the U.S. government ordering disclosure of information stored on a Microsoft server in Ireland.[54] Microsoft argued that

---

[48] *See, e.g.,* Elisa D. Harris, "Dual-Use Threats: The Case of Biological Technology," in *Governance of Dual-Use Technologies*, 60-111.
[49] National Science Advisory Board for Biosecurity*, Framework for Conducting Risk and Benefit Assessments of Gain-of-Function Research: Recommendations of the National Science Advisory Board for* Biosecurity (May 2016).
[50] On the dual-use nature of ICTs, see Herb Lin, "Governance of Information Technology and Cyber Weapons," in *Governance of Dual-Use Technologies*, 112-57.
[51] Joseph Nye, "e-Power to Rise Up the Security Agenda," *NATO Review* (2012), http://www.nato.int/docu/Review/2012/2012-security-predictions/e-Power-cybersecurity/EN/index.htm.
[52] *See* Georgia Institute of Technology, *Emerging Cyber Threats Report 2016*, http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.
[53] Michael Chertoff and Paul Rosenzweig, *A Primer on Globally Harmonizing Internet Jurisdiction and Regulations* (Global Commission on Internet Governance Paper Series No. 10, Mar. 2015).
[54] *In re Warrant to Search Certain Email Accounts Controlled & Maintained by Microsoft Corp.*, 15 F.Supp.3d 466 (S.D.N.Y 2014) (holding Microsoft must comply with the search warrant), *reversed by* U.S. Court of Appeals for the Second Circuit, Docket No. 14-2985, July 14, 2016, http://digitalconstitution.com/wp-content/uploads/2016/07/Decision-opinion.pdf (holding applicable U.S.

the U.S. government has no jurisdiction to order disclosure of information held outside the United States. A cyber terrorist attack on data stored in the cloud could generate competing jurisdictional claims from states for which there are no easy solutions, and jurisdictional conflicts could delay effective responses to cyber terrorism.

38. Innovation will not necessarily lead to greater terrorist interest in certain technologies. Predictions about biotechnology advances generating biological terrorism have not, to date, proved prescient. Although criminals harness ICTs, terrorists have not yet demonstrated similar interest or acumen despite government warnings about threats from cyber terrorism because networked ICTs and the related know-how are globally disseminated. Factors beyond access to technical capabilities and skills inform terrorist actions. Drawing conclusions about probabilities in terrorist behavior from technological possibilities alone might be counterproductive.

39. Uncertainties about how technological developments might affect the likelihood of cyber terrorism complicate efforts to advance a pro-active agenda. Proposals to prevent or protect against possible crises carry less weight than the urgency actual emergencies produce. This pattern is pervasive in counter-terrorism and cybersecurity. International law on terrorism has arisen overwhelmingly through reactions to terrorist incidents. Reactive policymaking also characterizes cybersecurity, with governments scrambling to react, for example, to increasing cyber crime and cyber espionage.

40. In addition, the ways in which technological trends could affect policy and legal thinking are not straightforward. For example, continued technological developments could help or hinder traditional law enforcement approaches to cyber terrorism by making attribution easier or harder.[55] Further, the ease with which terrorists can adapt technologies developed for peaceful uses means that protecting against and preventing cyber terrorism require advanced capabilities terrorists could also "reverse engineer" for malevolent purposes. This dynamic could feed technological competition between the "good guys" and "bad guys" that already threatens measures supporting the protection and prevention objectives.

41. As in other contexts involving technological innovation, applying and developing international law in response to cyber terrorism requires addressing not only existing dangers but also future threats. This challenge will place a premium on crafting flexible, technologically neutral approaches.

2.4 International Law and Cyber Terrorism

42. The international law relevant to cyber terrorism is, at present, mainly composed of "legacy rules"—rules of existing international law adopted to address certain problems that are not cyber-specific but can be applied against cyber terrorism. Some of these

---

law "does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers").

[55] On the attribution problem, see Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* (2015); 38: 4-37.

rules, such as the international law on the use of force, are designed to apply generally rather than to acts involving specific technologies. In addition, many legacy rules are the most relevant principles because states have not developed much international law specific to cyber terrorism.

43. The same pattern also appears in cybersecurity. States have not, to date, developed many treaties targeting cybersecurity problems. The main area where treaty law has developed is cyber crime.[56] For cyber terrorism, cyber espionage, and military use of cyber capabilities, the applicable international law consists of legacy rules based on treaties, customary international law, or general principles of international law.[57]

44. The Study Group sought to assess the adequacy of legacy rules and the advisability of changing these rules or developing entirely new international law specifically to address cyber terrorism.[58] In particular, the report discusses whether a treaty addressing cyber terrorism should be pursued. The feasibility of developing treaty law on cyber terrorism faces obstacles, including general challenges in crafting multilateral treaties; difficulties in defining terrorism experienced in other treaty negotiations; lack of agreement on what cybersecurity means; controversies over Internet governance; and geopolitical competition among countries.

45. Whether customary international law specific to cyber terrorism can develop is just as difficult to assess. International law on terrorism is predominantly treaty-based, and claims that customary international law includes a crime of international terrorism have proved controversial.[59] It is not apparent how efforts against cyber terrorism can avoid the problems seen with custom in the fight against other forms of terrorism.

46. What state practice exists on cyber incidents underscores the difficulties custom formation faces. In response to the Cyber Caliphate's claimed operation against CENTCOM,[60] the U.S. government did not characterize the incident as cyber terrorism even though it considers the Islamic State—the group controlling the Cyber Caliphate—a

[56] *See* Convention on Cybercrime, Nov. 23, 2001, entered into force July 1, 2004, Council of Europe Treaty Series No. 185 [hereinafter COE Convention on Cybercrime]. *See also* Agreement on Cooperation Among States Members of the Commonwealth of Independent States in Combating Offenses Relating to Computer Information, June 1, 2001, entered into force Mar. 14, 2002; Arab Convention on Combating Information Technology Offenses, Dec. 21, 2010, entered into force 2014.

[57] On general principles of international law and cyberspace, see Katharina Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013) [hereinafter *Peacetime Regime for State Activities in Cyberspace*], 135-88.

[58] The prevalence of legacy rules raises the question whether challenges associated with cybersecurity, including cyber terrorism, require changes to pre-cyber rules of international law. On this issue regarding international law and the use of force in connection with cyber terrorism, see Section 4.5 (The Use of Force in Self-Defense, Sanctions, and Responding to Cyber Terrorism) *infra.*

[59] *See* Section 4.3.2 (Customary International Law and the Crime of International Terrorism) *infra.*

[60] Earle and Schram, "'We are Coming': ISIS Hacks Defense Department."

terrorist group. CENTCOM described the incident as "cyber vandalism," because, among other things, the impact was a nuisance rather than disruptive or damaging.[61]

47. Assuming the Cyber Caliphate was responsible, CENTCOM's reaction indicates that the relationship between ICTs and terrorism differs from that between WMD technologies and terrorism. The United States would have considered an attempted use of a biological, chemical, or radiological agent by persons affiliated with the Islamic State against the U.S. military a terrorist offense in U.S. law[62] and international law,[63] no matter how little the attempt actually affected U.S. military operations.

48. The French government initially responded to the cyber incident targeting TV5Monde by opening a terrorism investigation.[64] French officials described the incident as an attack against critical infrastructure and the freedoms of information and expression.[65] TV5Monde regained control of its operations, but its director-general stated the network's "systems had been severely damaged."[66] This framing faded when, later, French officials suspected Russian hackers, not the Islamic State, were responsible. This shift underscored the attribution challenge faced in all areas of cybersecurity.

49. In the French incident, the ways in which the cyber operation might violate international law relevant to terrorism are not clear. Existing anti-terrorism treaties are awkward to apply to cyber incidents.[67] Although the TV5Monde episode involved what the French considered critical infrastructure, it was not a terrorist offense, for example, within the anti-terrorist treaty with the broadest scope, the International Convention for the Suppression of Terrorist Bombings.[68] The incident also does not fit within any other existing anti-terrorism treaties. Instead, the most relevant treaty law for this incident is contained in treaties on cyber crime.[69]

50. The treaty-centric nature of international law on terrorism and controversies about the purported customary crime of international terrorism create problems for interpreting the cyber operations against CENTCOM and TV5Monde as violations of customary

---

[61] U.S. Department of Defense, "CENTCOM Acknowledges Social Media Sites 'Compromised,'" Jan. 12, 2015, http://www.defense.gov/news/newsarticle.aspx?id=123956&source=GovDelivery. Although not a case of cyber terrorism, the U.S. government also called the cyber attack on Sony Pictures, allegedly conducted by North Korea, "cyber vandalism." Eric Bradner, "Obama: North Korea's Hack Not War, But Cybervandalism," CNN.com, Dec. 24, 2014, http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/.

[62] 18 U.S.C. § 2332b(g)(5) (acts of terrorism transcending national boundaries, definition of the "federal crime of terrorism").

[63] International Convention for the Suppression of Terrorist Bombings, Dec. 15, 1997, entered into force May 23, 2001, 2149 UNTS 256 [hereinafter Terrorist Bombings Convention].

[64] Chrisafis and Gibbs, "French Media Groups to Hold Emergency Meeting after ISIS Cyber-Attack."

[65] *Ibid.*

[66] *Ibid.*

[67] *See* Section 4.2 (Anti-Terrorism Treaties) *infra.*

[68] *See* Sections 3.2 (Considerations in Defining Cyber Terrorism) and 4.2 (Anti-Terrorism Treaties) *infra* for analysis of this treaty in the context of cyber terrorism.

[69] *See* Section 4.4 (Treaties on Cyber Crime, Transnational Organized Crime, Extradition, and Mutual Legal Assistance and Extraterritorial Application of Criminal Law) *infra.*

international law. The paucity of state practice cautions against reading too much or too little into these incidents, but they illustrate that state practice will develop features that international lawyers have to assess carefully in addressing cyber terrorism.

2.5 State-Sponsored Terrorism, Weak States, and Cyber Terrorism

2.5.1 State-Sponsored Terrorism and Cyber Terrorism

51. Acts of terrorism are sometimes sponsored or supported by states, including through provision of safe havens, funds, weapons, and false identity documents. States have sponsored or supported terrorist acts for various reasons, including using terrorist groups to conduct "proxy war" or asymmetrical conflict against adversary states.

52. State-sponsored terrorism clearly violates international law. In Resolution 1373 (2001), the Security Council imposed obligations on UN member states to "[r]efrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists[.]"[70] State-sponsored terrorism can also violate international law, as when a state-supported terrorist attack violates anti-terrorism treaties, the principle of non-intervention, or the prohibition on the use of force.

53. State sponsorship or support for potential acts of cyber terrorism is an issue because states have been accused of using non-state actors, such as "patriotic hackers," to conduct cyber operations against other countries.[71] Controversies about attributing terrorist acts to states under international law arose before cyber terrorism became an issue. Whether conventional or cyber terrorism, problems emerge in applying the principles of state responsibility—can the terrorist act be attributed to a state? Attribution is critical. The application of other rules of international law—such as the prohibition on the use of force by states[72] and the use of force in self-defense in response to an armed attack by a state[73]—depends on the act in question being the act of a state.

54. In the cyber context, international law on state responsibility creates a double attribution burden.[74] First, the perpetrator has to be identified, and ICTs and the Internet provide ways for attackers to obscure the source of attacks.[75] Second, if the perpetrator is not an agent of a state, then there has to be evidence that a state ordered or had effective

---

[70] Security Council, Resolution 1373 (2001).
[71] *See generally* Christian Czosseck, "State Actors and Their Proxies in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, 1-30.
[72] *See, e.g.,* Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 33-40.
[73] *See, e.g.,* Nicholas Tsagourias, "Cyber Attacks, Self-Defence, and the Problem of Attribution," *Journal of Conflict & Security Law* (2013); 17: 229-44.
[74] On state responsibility and cyberspace, see Constantine Antonopoulos, "State Responsibility in Cyberspace," in *Research Handbook on International Law and Cyberspace*, 55-71.
[75] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford University Press, 2014), 73.

control or direction over the attack.[76] This double attribution problem makes ICTs potentially attractive for state-sponsored terrorism.[77]

55. The prohibition on state support of terrorism in Security Council Resolution 1373 (2001) applies to cyber terrorism, as defined by the Study Group, given how its definition aligns with definitions of terrorist offenses in many treaties.[78] It is hard to imagine the Security Council would not consider a cyber attack by a non-state actor ordered, controlled, or directed by a state that caused death, injury, or serious property damage and undertaken to spread fear or compel behavior to be a prohibited act of state-sponsored terrorism.

56. The difficulties cyber poses for applying the principles of state responsibility connect to controversial debates about attribution criteria in the international law prohibiting the use of force and regulating the use of force in self-defense.[79] Governments and experts have argued that a state subject to an armed attack by terrorists located in another state can use force against that state if it tolerated the terrorist activities or was unwilling to prevent terrorist attacks coming from its territory.[80] These arguments assert international law on the use of force in self-defense has attribution criteria for state responsibility different from other areas of international law.[81]

---

[76] International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, UN General Assembly Resolution 56/83, Dec. 12, 2001, annex [hereinafter ILC Principles of State Responsibility], Article 8. *See also GGE Report* (2015), ¶ 28(f) (stating "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State").

[77] Harold Hongju Koh, Legal Advisor, U.S. Department of State, *International Law in Cyberspace, Remarks to USCYBERCOM Inter-Agency Legal Conference*, Sept. 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (observing "cyberspace significantly increases an actor's ability to engage in attacks with 'plausible deniability,' by acting through proxies").

[78] *GGE Report* (2013), ¶ 23 (stating "States must not use proxies to commit internationally wrongful acts"); *GGE Report* (2015), ¶ 28(e) (stating "States must not use proxies to commit internationally wrongful acts using ICTs").

[79] On the prohibition on the use of force, see Mary Ellen O'Connell, "The Prohibition of the Use of Force," in *Research Handbook on International Conflict and Security Law* (Nigel D. White and Christian Henderson, eds.) (Cheltenham: Edward Elgar Publishing, 2012), 89-119. On the right to use force in self-defense in cyberspace, see Carlo Focarelli, "Self-Defence in Cyberspace," in *Research Handbook on International Law and Cyberspace*, 255-83.

[80] *See, e.g.,* Daniel Bethlehem, "Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attacks by Nonstate Actors," *American Journal of International Law* (2012); 106(4): 770-77, 76 (arguing international law permits states to use force in self-defense against actual or imminent armed attacks by non-state actors in the territory of another state without that state's consent "in circumstances in which there is a reasonable and objective basis for concluding that the third state is colluding with the non-state actor or is otherwise unwilling to effectively restrain the armed activities of non-state actor such as to leave the state that has a necessity to act in self-defense with no other reasonably available effective means to address an imminent or actual armed attack"). For discussion in the context of cyber, see Tsagourias, "Cyber Attacks, Self-Defence, and the Problem of Attribution."

[81] The ILC's Draft Articles on the Responsibility of States for Internationally Wrongful Acts recognizes that "special rules of international law" could emerge to govern when a state is responsible for internationally wrongful acts. *See* ILC Principles of State Responsibility, Article 55.

57. These ideas have generated controversy and do not necessarily represent international law. In restating the law on state responsibility, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*) observed that the threshold for responsibility is "stringent" in that "[t]he State needs to have issued specific instructions or directed or controlled a particular operation to engage State responsibility."[82]

58. Thus, an important issue concerning state-sponsored cyber terrorism in the future will be the double attribution problem created by the nature of ICTs and the international law on state responsibility.[83] The only ways to alleviate this problem are for cyber-incident attribution to become more technically feasible and accurate and/or change the legal threshold for engaging state responsibility in cyberspace under international law.[84]

2.5.2 Weak States and Cyber Terrorism

59. The problem of weak states involves the potential that terrorists exploit the inability of governments to control effectively what happens inside their territories. In the post-9/11 context, weak states and ungoverned spaces have been prominent concerns because of the fear Al-Qaeda or other groups would use them as bases of operations.[85] Whether the link between weak states and terrorism was or is strong has been challenged.[86] Terrorists have operated in weak states (e.g., Iraq, Nigeria) and in states that failed to address the terrorist threat (e.g., Pakistan).

60. The purported link between weak states and terrorism is also problematical concerning cyber terrorism. Policy documents discussing cyber terrorism do not frequently identify weak states or ungoverned parts of states as a concern, certainly not compared with problems associated with the "dark web" and "deep web"—different types of ungoverned space—where terrorists could acquire malware and expertise.[87]

---

[82] *Tallinn Manual*, 33. *See also* Roscini, *Cyber Operations and the Use of Force in International Law*, 34 (arguing the ILC Principles of State Responsibility constitute the applicable rules of customary international law).
[83] *See* Section 4.5.1 (The Use of Force in Self-Defense and Responding to Terrorism) *infra* for discussion of the use of force in self-defense in response to terrorist attacks not attributable to a state.
[84] David P. Fidler, "*Inter Arma Silent Leges Redux?* Law of Armed Conflict and Cyberconflict," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Derek Reveron, ed.) (Washington, D.C.: Georgetown University Press, 2012), 71-87, 77.
[85] *See, e.g.,* Robert D. Lamb, *Ungoverned Areas and Threats from Safe Havens: Final Report of the Ungoverned Areas Project* (Washington, D.C.: Office of the Under Secretary of Defense for Policy, 2008).
[86] Stewart Patrick, "The Brutal Truth: Failed States are Mainly a Threat to Their Own Inhabitants," *Foreign Policy*, June 20, 2011, http://foreignpolicy.com/2011/06/20/the-brutal-truth/.
[87] The "dark web" refers to "websites that are publicly visible, yet hide the IP addresses of the servers that run them" making it "very difficult to figure out where they're hosted—or by whom." The "deep web" is "the collection of all sites on the web that aren't reachable by a search engine." Andy Greenberg, "Hacker Lexicon: What is the Dark Web?," *Wired*, Nov. 19, 2014, http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

3

DEFINING "CYBER TERRORISM"

61. An important Study Group objective was developing a definition of cyber terrorism to guide its work. The Study Group was aware that fulfilling this objective would be difficult because (1) states have yet to reach consensus on a definition of terrorism in international law; and (2) definitions of cyber terrorism in national laws and policies and secondary literature exhibit diversity.[88] However, the Study Group needed a working definition of cyber terrorism to establish the scope of its work and identify what policy and legal issues arise within that scope.

62. The importance of a definition of cyber terrorism differs depending on the policy strategy under consideration. Applying a law enforcement strategy requires a precise, transparent definition of the crime of cyber terrorism in order to sustain investigation and prosecution and avoid infringing on activities protected by human rights. However, protecting against cyber terrorism through an "all hazards" strategy focused on cyber defenses does not need a detailed, clear definition because the strategy aims to defend against cyber threats regardless of their source or purpose. The strategy of preventing cyber terrorism needs a definition, but the prevention focus means issues critical to law enforcement, such as the requisite intent and severity of damage, require less precision.

3.1 Defining "Terrorism" and International Law

63. As already noted, what constitutes terrorism has been controversial in international politics and law.[89] States have never agreed on a definition of terrorism, and the manner in which countries identify terrorism in domestic policy and law is not uniform.[90] These controversies reflect that states expand or contract what qualifies as terrorism according to their understanding of threats they face and their interests.

64. The international community's difficulties in reaching agreement on a definition of terrorism are reflected in the failure of negotiations on a Comprehensive Convention on International Terrorism, which have lasted nearly twenty years.[91] Different perspectives on terrorism also appear in how cyber terrorism is variously defined,[92] with

---

[88] *See, e.g.,* Keiran Hardy and George Williams, "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism," in *Cyberterrorism: Understanding, Assessment, and Response* (Thomas M. Chen, Lee Jarvis, and Stuart MacDonald, eds.) (New York: Springer, 2014), Chapter 2 (analyzing differences in national laws on terrorism concerning cyber attacks in Australia, Canada, New Zealand, and United Kingdom). *See also* Kristen E. Eichensehr, "The Cyber-Law of Nations," *Georgetown Law Journal* (2015); 103: 317-80, 358 fn. 228 (noting that a proposal for a cyber terrorism treaty "provides no reason to think that the definitional and other difficulties that have plagued international efforts to achieve agreement with regard to non-cyber terrorism would be any less problematic in the cyber context").
[89] *See* Ben Saul, *Defining Terrorism in International Law* (Oxford: Oxford University Press, 2006).
[90] Ivanov, "Combating Cyberterrorism under International Law."
[91] The UN General Assembly started negotiations on this treaty in December 1996. *See* UN General Assembly, Resolution 51/210, Dec. 16, 1996, UN Doc. A/RES/51/210, Jan. 16, 1997.
[92] *See* Annex (Examples of Definitions of Cyber Terrorism) *infra.*

broad or narrow definitions linked with disagreements about larger issues, such as the legitimacy of speech and other activities by political dissidents. Focusing on cyber terrorism does not resolve deadlocks that have prevented the Comprehensive Convention on International Terrorism from being adopted. Differences over how to define "cyber terrorism" also emerge from proposals for international action, such as the call Chinese President Xi Jinping made in December 2015 for a "cyberspace anti-terrorism treaty."[93]

65. However, different political perspectives on terrorism have not stopped states from developing international law on terrorism, and this law contains definitional patterns. The anti-terrorism treaties have avoided the problem of defining terrorism by delineating specific offenses, such as aircraft hijacking and hostage taking, and imposing obligations to harmonize criminal law and facilitate law enforcement cooperation on these offenses. This approach reveals sufficient commonalities to permit extraction of key features of terrorist offenses, including the types of actions, consequences, and intent required to commit them.

66. These commonalities inform (1) parts of the draft Comprehensive Convention on International Terrorism that are not controversial;[94] and (2) the claim that customary international law includes a crime of international terrorism.[95] In addition, international humanitarian law for international and non-international armed conflict prohibits acts or threats of violence the primary purpose of which is to spread terror in civilian populations,[96] and international criminal tribunals have prosecuted individuals for war crimes for violating this prohibition.[97]

67. The Study Group's task does not require resolving the scope and substance problems described above. Rather, it needed to define a particular type of terrorism, which makes patterns in treaties with specific terrorist offenses important. Instruments that define terrorist offenses involving use of specific technologies are particularly helpful, such as (1) the International Convention for the Suppression of Terrorist Bombings (Terrorist Bombings Convention), which covers bombings that release

---

[93] Duncan Hewitt, "China's President Xi Says Internet Must be Governed by Order, Stresses Cyber Sovereignty," *International Business Times*, Dec. 16, 2015, http://www.ibtimes.com/chinas-president-xi-says-internet-must-be-governed-order-stresses-cyber-sovereignty-2227533. Bilateral U.S.-China cooperation on cyber issues includes terrorist activities in cyberspace, a potentially difficult area given "China and the United States have divergent interpretations of what constitutes terrorism." Franz-Stefan Grady, "China-US Talks on Cybercime: What are the Outcomes?," *The Diplomat*, June 16, 2016, http://thediplomat.com/2016/06/china-us-talks-on-cybercrime-what-are-the-outcomes/.

[94] For the latest draft, see UN General Assembly, *Letter Dated 3 August 2005 from the Chairman of the Sixth Committee to the President of the General Assembly*, UN Doc. A/59/894, App. II, Aug. 12, 2005.

[95] Special Tribunal for Lebanon (Appeals Chamber), *Interlocutory Decision on the Applicable Law*, STL-11-01/I, Feb. 16, 2011 [hereinafter Special Tribunal for Lebanon Decision], ¶ 85.

[96] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, entered into force Dec. 7, 1978, 1125 UNTS 3 [hereinafter Additional Protocol I], Article 51(2); and Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, entered into force Dec. 7, 1978, 1125 UNTS 604 [hereinafter Additional Protocol II], Article 13(2).

[97] *See* Section 4.6 (International Humanitarian Law and Responding to Cyber Terrorism during Armed Conflict) *infra* for discussion of the case law.

biological, chemical, or radiological agents; and (2) the International Convention for the Suppression of Acts of Nuclear Terrorism (Nuclear Terrorism Convention).[98]

68. In thinking about existing treaty approaches to defining terrorist offenses, the Study Group evaluated the advantages and disadvantages of following them in developing a working definition of cyber terrorism. On the one hand, states have used international law to identify, define, and establish cooperation for addressing acts associated with terrorism. Adopting prevailing strategies would align the Study Group's definition of cyber terrorism with existing treaty law and state practice. On the other hand, following instruments not specific to the cyber context might produce a definition that does not capture what is different about ICTs and how terrorists might use them.

69. Support for aligning a definition of cyber terrorism with how existing anti-terrorism treaties define terrorist offenses comes from domestic law. Some countries incorporate unlawful uses of ICTs into existing criminal terrorist offenses, rather than creating a specific crime of cyber terrorism. For example:

- The United Kingdom defines terrorism to include an action "designed seriously to interfere with or seriously disrupt an electronic system" the use or threat of which "is designed to influence the government or an international governmental organization or to intimidate the public or a section of the public" and "is made for the purpose of advancing a political, religious, racial or ideological cause."[99]
- The United States includes in the definition of the "federal crime of terrorism" offenses causing death, serious bodily injury, or the risk of serious bodily injury through damage or destruction of property that involve violations of the Computer Fraud and Abuse Act "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct."[100]
- Under its new counter-terrorism law, Israel will evaluate cyber incidents under the law's criteria for what constitutes a "terrorist act," namely commission of a criminal offense with political, religious, or ideological motives intended to incite public fear or coerce a government to commit or abstain from an act.[101]

70. The Study Group decided to track existing approaches to defining terrorist offenses in international law in its working definition of cyber terrorism.[102] As noted above, defining terrorism in international law has been, and remains, fraught with controversy. The Study Group concluded that the most prudent approach involved

---

[98] International Convention for the Suppression of Acts of Nuclear Terrorism, Apr. 13, 2005, entered into force July 7, 2007, 2445 UNTS 89 [hereinafter Nuclear Terrorism Convention].
[99] Terrorism Act of 2000 (as amended), Section 1(1)-(2).
[100] 18 U.S.C. § 2332b(g)(5)
[101] State of Israel Ministry of Justice, The Counter-Terrorism Law 5775-2015, http://www.justice.gov.il/Units/InternationalAgreements/HumanRightsAndForeignRelations/Faq/CounterTerrorismLaw5775-2015_BackgroundDescriptionJune2016.pdf.
[102] For other approaches to defining cyber terrorism, see Mohammad Iqbal, "Defining Cyberterrorism," *Journal of Computer & Information Law* (2004); 22: 397-408; Jeffrey T. Biller, "Cyber-Terrorism: Finding a Common Starting Point," *Journal of Law, Technology & the Internet* (2013); 4(2): 275-351; Shirayaev, "Cybterterrorism in the Context of Contemporary International Law," 139-92.

developing a definition of cyber terrorism that did not deviate from how states have created and implemented international law on terrorism.

3.2 Considerations in Defining Cyber Terrorism

71. A review of international law on terrorism indicates that the task of defining cyber terrorism has to consider four issues—what acts and effects are covered; what damage threshold (if any) such acts must cross; what intent must inform the acts; and what actors are relevant. The anti-terrorism treaties are not uniform in how they handle these issues in defining their respective offenses, so no standard template emerges from these instruments to apply in defining cyber terrorism. In addition, the little state practice relevant to cyber terrorism that exists informed the Study Group's definition.

3.2.1 Acts

72. Anti-terrorism treaties frequently require in their offenses that predicate acts be unlawful and intentional. For example, under the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), a person does not commit an offence without acting unlawfully and intentionally.[103] This requirement makes sense for cyber terrorism as well, given the scale and intensity of ICT and Internet use around the world. To avoid defining cyber terrorism in an overly broad manner, the Study Group's definition requires predicate acts be unlawfully and intentionally committed.

73. The Study Group limited its focus to acts of terrorism committed through ICTs and the Internet and excluded terrorist use of these technologies for other purposes, such as spreading propaganda and raising funds. This exclusion means its definition of cyber terrorism has to reflect this technology-driven choice. Thus, the Study Group reviewed the Terrorist Bombings Convention and the Nuclear Terrorism Convention for insights on how states have defined terrorist offenses linked to particular technologies.

74. The Terrorist Bombings Convention applies to use of an "explosive or incendiary device," which includes a weapon or device designed to, or that can, disseminate toxic chemicals, biological agents or toxins or similar substances, or radiation or radioactive material.[104] The Nuclear Terrorism Convention applies to possession or use of radioactive material, a device designed to disperse radioactive material or emit radiation, and using or causing damage to a nuclear facility in a way that releases radioactive material.[105] Both treaties cover acts involving direct use of specific technologies, but only the Nuclear Terrorism Convention includes the acts of possessing a particular technology and of damaging a facility housing that technology.

75. While using ICTs to attack a target should fall within a definition of cyber terrorism, whether the definition should cover possession of specified tools (e.g.,

[103] Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Sept. 23, 1971, entered into force Jan. 26, 1973, 974 UNTS 177, Article 1(1).
[104] Terrorist Bombings Convention, Article 1(3).
[105] Nuclear Terrorism Convention, Articles 1-2.

malware) or physical attacks on cyber infrastructure is a more difficult question. Including the possession of a specific cyber technology poses questions about the feasibility of defining this act in a sufficiently clear manner.[106] Such inclusion runs the risk of producing an overly broad definition that might chill legitimate cyber defense activities. However, a definition could mitigate these concerns in how it handles the damage threshold and specific intent elements.

76. In terms of kinetic attacks on cyber infrastructure, most discussions of cyber terrorism do not have these types of attacks in mind, which contrasts with the Nuclear Terrorism Convention's inclusion of physical attacks on nuclear facilities. In addition, international law provides some, albeit not comprehensive, coverage of kinetic attacks on cyber infrastructure, which perhaps lessens the need to include them in a definition of cyber terrorism. A kinetic attack on cyber infrastructure could fall within the Terrorist Bombings Convention, which applies to the use of explosive devices against infrastructure facilities, including those supporting communications.[107] However, cyber infrastructure can be damaged without an explosive device (e.g., cutting fiber optic cables), in which case the Terrorist Bombings Convention would not apply.

77. In terms of using ICTs to attack targets, the nature of these technologies means that such an act would involve the source, vector, and immediate target of the attack being ICT-enabled or ICT-dependent. For example, a terrorist develops or acquires malware, transmits the malware through the Internet from his computer, and, by means of the malware, infiltrates and damages a target's computer system or network. The example does not exhaust all possibilities, but it captures the main features of using ICTs to engage in terrorism.[108]

3.2.2 Damage

78. Anti-terrorism treaties sometimes require that offenses involve acts that cause, could cause, or were intended to cause specific types or levels of damage. The Terrorist Bombings Convention defines "explosive or other lethal device" as a device "designed, or has the capability, to cause death, serious bodily injury or substantial material damage."[109] The Nuclear Terrorism Convention defines "radioactive material" and "device" to include the potential for such material and devices to "cause death, serious bodily injury or substantial damage to property or to the environment."[110]

79. These provisions raise the question whether a definition of cyber terrorism should have a damage threshold. Two considerations were important to the Study Group's

[106] *See* Section 5.5 (Securing Dangerous Materials, International Law, and Cyber Terrorism) and Section 5.6 (Export Controls and Protecting against Cyber Terrorism) *infra.*
[107] Terrorist Bombings Convention, Articles 1-2.
[108] For example, a terrorist could use ICTs to attack critical infrastructure without utilizing the Internet by inserting malware into computers through USB drives. Hybrid terrorist acts could involve both kinetic and cyber attacks, but, even with such acts, it remains important legally to define what constitutes cyber terrorism as a distinct form of terrorism.
[109] Terrorist Bombings Convention, Article 1.
[110] Nuclear Terrorism Convention, Articles 1-2.

conclusion that a definition should include them. First, a definition that does not require the consequences of a cyber operation to cross some seriousness or damage threshold might be too broad because it will include acts with minor consequences, such as temporary disruptions to Internet access. Activities of "hacktivists" or of those associated with civil disobedience or protest in cyberspace often cause minor, temporary effects. Including such activities within a definition of cyber terrorism would provoke opposition as an attack on freedom of expression and the function civil disobedience plays in democratic and authoritarian regimes. Hacktivism and cyber civil disobedience are not unregulated because states can apply national and international law on cyber crime to these activities.

80. Second, state practice in cyber incidents contains some indications that a definition of cyber terrorism should include a damage threshold. State responses to the disruption of Estonia's cyber systems in 2007 did not characterize what happened as terrorism, perhaps because the consequences were not serious enough to merit this moniker. The U.S. government described the Cyber Caliphate's claimed attacks on CENTCOM as cyber vandalism because they caused only minor and temporary consequences. Concerning DDoS attacks on banks and the hacking of a dam's computer system, the U.S. government did not allege violations of federal criminal law on terrorism in indicting persons working for Iranian private computer security companies,[111] possibly because these incidents did not produce the kinds of consequences found in the elements of terrorist offenses in U.S. criminal law.[112] By contrast, in initially describing the hacking of TV5Monde as terrorism, French authorities claimed the attack caused serious damage to computer networks. Thus, in defining cyber terrorism setting a damage threshold would help the definition avoid including cyber incidents that are mildly disruptive rather than seriously damaging.

81. In the cyber context, different types of damage should be kept in mind that could produce significant adverse consequences for governments, enterprises, and people reliant on digital data, software, and ICT-dependent facilities and services:

- Damage to data, such as deleting or degrading data stored on computers;
- Damage to computer-operated machines or equipment;
- Damage to government-provided or privately operated public services (e.g., communications, transportation, electricity, water, sanitation, and health) dependent on functioning ICT systems.[113]

[111] United States v. Ahmad Fathi *et al*., Indictment, U.S. District Court, Southern District of New York, 16 Crim 48 (2016). The alleged violations all involved cyber crime offenses under the Computer Fraud and Abuse Act, 18 USC § 1030 *et seq*.

[112] For example, the offense of terrorism transcending national boundaries requires conduct that "(A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or (B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States[.]" 18 USC § 2332b(a)(1).

[113] Although the *Tallinn Manual* did not analyze cyber terrorism, its examination of what consequences from cyber operations qualify as a "use of force" and "armed attack" in international law on the use of

82. The types of damage identified in anti-terrorism treaties involve death, injury, or significant damage to property, the economy, government facilities or functions, or the environment. Each type of damage described above does not, by itself, cross the damage thresholds found in international law on terrorism. This pattern means that states are unlikely to conclude that damage to data, computer-operated machines, or cyber-dependent services crosses the threshold into terrorism without such damage causing death, injury, or significant property, economic, or environmental harm.

83. Terrorists could disseminate false information online in order to terrorize people or cause economic damage. None of the anti-terrorism treaties includes in their offenses the spreading of false information (e.g., about an attack on civil aviation or a nuclear facility) with the intent to cause economic harm or sow terror in a population, even though possibilities for doing so have existed before and after the Internet became a global communications platform. Defining cyber terrorism to include spreading of false information would depart from the ways in which states have defined terrorist offenses in international law. Departing from the status quo would have to be justified by the potential that online communications have for the deliberate spreading of false information to create rapid and widespread adverse consequences in a society.

3.2.3 Specific Intent

84. Definitions of terrorism often require that perpetrators act with specific intent. The Terrorist Bombings Convention requires use of an explosive or other lethal device with the intent to cause (1) death or serious bodily injury; or (2) extensive destruction of a place, facility, or system where the destruction is likely to result in major economic loss.[114] The Nuclear Terrorism Convention requires use of radioactive material or device be done with the intent to (1) cause death, serious bodily injury, or substantial damage to property or the environment; or (2) compel a natural or legal person, international organization, or state to do, or refrain from doing, an act.[115]

85. Another type of specific intent involves the intent to spread fear or terror in a civilian population. The International Criminal Tribunal for the Former Yugoslavia held that the war crime associated with violating Article 51(2) of Additional Protocol I or Article 13(2) of Additional Protocol II requires the perpetrator to commit attacks or threats of attacks with the primary purpose of spreading terror among civilians.[116]

86. In addition to the common use of specific intent in defining terrorist offenses, the context of cyber terrorism supports including specific intent elements in a definition.

---

force and "attack" in international humanitarian law illustrates the complexity of evaluating damage thresholds in cyber contexts. *See Tallinn Manual*, 45-52, 54-61, and 106-10.

[114] Terrorist Bombings Convention, Article 2(1).

[115] Nuclear Terrorism Convention, Article 2(1).

[116] International Criminal Tribunal for the Former Yugoslavia (Appeals Chamber), *Prosecutor v. Galić*, Case No. IT-98-29-A, [Judgment], Nov. 30, 2006, ¶ 104; *Prosecutor v. Dragomir Milošević*, Case No. IT-98-29/1-A, Judgment, Nov. 12, 2009, ¶ 37; *Prosecutor v. Radovan Karadžić*, Case No. IT-95-5/18-T, Judgment, Mar. 24, 2016, ¶¶ 464-466.

Such elements help ensure that acts of cyber civil disobedience are not treated as terrorism because they are not typically undertaken to hurt people or destroy property, coerce a person or entity to act in a certain way, or sow fear in a population.

3.2.4 Actors

87. States have designed existing anti-terrorism treaties to apply to the behavior of non-state actors. In many contexts, this focus is not a problem because states are much less likely to engage in the prohibited behavior, such as aircraft hijacking. However, in some circumstances, anti-terrorism treaties exclude the activities of state actors, such as armed forces. The Terrorist Bombings Convention does not apply to the activities of armed forces during an armed conflict or in the exercise of official duties governed by other rules of international law.[117] Similarly, the Nuclear Terrorism Convention does not address the legality of the use or threat of use of nuclear weapons by states.[118]

88. Such exclusions are not, however, always achieved in negotiations. Efforts on the Comprehensive Convention on International Terrorism have failed for nearly two decades in part because of disagreements about including or excluding from the treaty actions undertaken by state actors, including military forces.[119]

89. ICTs and the Internet are useful for law enforcement, intelligence, and military purposes, which creates challenges for reaching agreement on defining cyber terrorism. Some governments will want to exclude law enforcement, intelligence, and military uses of ICTs from any definition—or the application of any definition—of cyber terrorism. Other governments concerned about cyber espionage and offensive cyber weapons might prefer to include intelligence and military activities in the definition or its application.

3.3 The Study Group's Working Definition of Cyber Terrorism

90. After reviewing these considerations, the Study Group developed the following working definition of cyber terrorism:

> "Cyber terrorism" involves acts intentionally committed by any person who uses information and communication technologies unlawfully in ways that cause, or are intended to cause, death or serious bodily injury to persons, substantial damage to public or private property, the economy, or the environment, or serious disruption of public services and that are undertaken with the intent to spread fear in civilian populations or to compel a government, a civilian population, or an international organization to take or abstain from specific acts or courses of action.

91. This definition does not include, or apply to, law enforcement, intelligence, and military activities involving use of ICTs undertaken by states. Other rules of international law apply to law enforcement use of ICTs, such as conducting surveillance in criminal

[117] Terrorist Bombing Convention, Article 19.
[118] Nuclear Terrorism Convention, Article 4(4).
[119] *See* Section 4.2.5 (Draft Comprehensive Convention on International Terrorism) *infra.*

investigations, and these rules include international human rights law. States have long preferred not to regulate espionage through international law, which means linking a definition of cyber terrorism with intelligence activities would be unacceptable.[120] International humanitarian law prohibits belligerents, including government military forces, from engaging in acts of terrorism.[121]

92. The Study Group's working definition is intended to guide its analysis rather than provide a definition on which criminal proceedings could be based. Just as the Terrorist Bombings Convention contains a detailed definition of "explosive or other lethal device,"[122] an elaborate definition of "information and communication technologies" could be constructed by, for example, identifying these technologies and the means (e.g., malware) and methods (e.g., hacking) used to access, manipulate, and damage ICTs and things dependent on them.

93. The Study Group's definition requires that the use of ICTs cause death, injury, or damage to property, the economy, or the environment. The definition does not include within its scope the spreading of false information online with the intent to cause economic damage or terrorize the civilian population. This choice reflects the Study Group's preference for aligning its working definition with the manner in which states have defined terrorist offenses in international law. The Study Group was also concerned about the potential that governments could abuse "spreading false information" in a definition of cyber terrorism for purposes having nothing to do with addressing terrorism.

94. The Study Group believes its definition appropriately incorporates features commonly found in definitions of terrorist offenses in international law. The definition ties the predicate acts to the unlawful and intentional use of ICTs, which centers the definition on cyber means and methods without restricting this element in ways that cannot respond to technological change. It requires the use of ICTs to cause identified consequences, which means the definition does not apply to (1) general terrorist uses of the Internet, such as recruitment and fundraising; or (2) use of the Internet to engage in expression and association.

95. The definition incorporates a damage threshold by requiring consequences beyond minor and temporary impacts, namely death, serious injury, and substantial property or environmental damage. This damage element means that theft of information stored in computer systems is not cyber terrorism, even if the perpetrator uses the stolen information to coerce a person, government, or organization. The definition captures

---

[120] The problems associated with cyber espionage are, however, causing international lawyers to re-examine the relationship between espionage and international law. *See, e.g.,* Russell Buchan, "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace*, 168-89; Ashley S. Deeks, "Confronting and Adapting: Intelligence Agencies and International Law," *Virginia Law Review* (2016); 102(3): 599-685.

[121] *See* Section 4.6 (International Humanitarian Law and Responding to Cyber Terrorism during Armed Conflict) *infra.* Section 4.6's discussion is not intended to bring state actions within the Study Group's working definition of cyber terrorism. The Study Group's approach follows the anti-terrorism treaties, which exclude state actions, including military operations in armed conflict, from their defined offenses.

[122] Terrorist Bombings Convention, Article 1(3).

direct ICT-specific damage, such as destruction of software or stored data, and indirect damage, such as death, injuries, or damage to property or the economy caused by disruption of ICT-dependent services. The definition includes the type of specific intent requirement often found in terrorist offenses in national and international law.

96. The Study Group's working definition is politically credible because most states would, in all likelihood, consider the acts described to be terrorism, even if some countries define cyber terrorism more broadly. The definition avoids controversies that have plagued attempts to define terrorism, such as problems related to state-sponsored terrorism and the relationship between terrorism and military activities during armed conflict.

4

INTERNATIONAL LAW AND RESPONDING TO CYBER TERRORISM

4.1 Responding to Terrorism and International Law

97. States have developed more international law on responding to terrorism than on protecting against or preventing it. Thus, the Study Group focused first on the international law on responding to terrorism and its relevance for cyber terrorism. Most of the international law on responding to terrorism reflects a law enforcement strategy. Outside the law enforcement context, responses to terrorism involve international law on the use of force and the provision of assistance to victim states after terrorist attacks. The Study Group analyzed how these bodies of international law relate to cyber terrorism. With the exception of two treaties not yet in force,[123] none of this international law was specifically adopted to address cyber terrorism. This part analyzes whether existing international law is adequate for guiding responses to cyber terrorism or whether developing new law directly focused on cyber terrorism is necessary and feasible.

4.2 Anti-Terrorism Treaties

4.2.1 Cyber Terrorism and Offenses Created by Anti-Terrorism Treaties

98. States use international law to apply criminal law and law enforcement cooperation to support responses to terrorism. Many multilateral treaties adopted since the 1960s fall into this category (Table 1). In general, these treaties define specific offenses, require states parties to criminalize the offenses in national law, take jurisdiction over the offenses, and establish law enforcement assistance obligations connected to the offenses. Through this approach, states have harmonized substantive, jurisdictional, and procedural aspects of their national criminal laws and strengthened law enforcement cooperation on the defined crimes. The creation of multiple treaties addressing various offenses flows from states' reactions to different terrorist attacks and the failure to adopt a comprehensive treaty on terrorism.

99. The anti-terrorism treaties are important for analyzing cyber terrorism. First, dependence on ICTs makes cyber terrorism against areas addressed in some treaties already in force possible (e.g., terrorists cyber attacks against civil aviation). Thus, acts of cyber terrorism might readily fall within the scope of some agreements.[124] How well or poorly the anti-terrorism treaties cover cyber terrorism might reveal gaps in international law. Second, the criminal law approach in these treaties raises questions about whether development of international law on cyber terrorism should emphasize this strategy.

---

[123] *See* Section 4.2.3 (Multilateral Anti-Terrorism Treaties Not in Force) *infra*.

[124] This idea was utilized in the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (Article 3(1)(f)) proposed in 2000 by the Hoover Institution, Consortium for Research on Information Security and Policy, and the Center for International Security and Cooperation at Stanford University, http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf.

Table 1. Multilateral Treaties on Terrorism in Force[125]

Year Adopted	Treaty
1963	Convention on Offences and Certain Other Acts Committed on Board Aircraft
1970	Convention for the Suppression of Unlawful Seizure of Aircraft
1971	Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation
1973	Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents
1979	International Convention against the Taking of Hostages
1988	Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
	Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf
	Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation
1997	International Convention for the Suppression of Terrorist Bombings
1999	International Convention for the Suppression of the Financing of Terrorism
2005	International Convention for the Suppression of Acts of Nuclear Terrorism

100. A cyber attack could fall within the scope of specific multilateral treaties in Table 1 if, for example, it:

- Jeopardizes "the safety of [an] aircraft or of the persons or property therein or . . . jeopardize[s] good order and discipline on board";[126]
- Involves an on-board, in-flight seizure or exercise of control of the aircraft;[127]
- Destroys, damages, or interferes with air navigation facilities such that the safety of aircraft in flight is endangered;[128]

[125] UN Treaty Collection, *Text and Status of the United Nations Conventions on Terrorism*, https://treaties.un.org/Pages/DB.aspx?path=DB/studies/page2_en.xml.

[126] Convention on Offences and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, entered into force Dec. 4, 1969, 704 UNTS 219, Article 1. *See also* Section 4.2.3 (Multilateral Anti-Terrorism Treaties Not in Force) *infra.*

[127] Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, entered into force Apr. 14, 1971, 860 UNTS 105, Article 1. *See* Stefan A. Kaiser and Oliver Aretz, "Legal Protection of Civil and Military Aviation against Cyber Interference," in *Peacetime Regime for State Activities in Cyberspace,* 319-48, 331 (noting a person on board an aircraft could access "the aircraft's internal systems and tak[e] over control," which "could be seen as an attack on board an aircraft"). *See also* Section 4.2.3 (Multilateral Anti-Terrorism Treaties Not in Force) *infra.*

[128] Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, entered into force Jan. 26, 1973, 974 UNTS 177, Article 1. *See* Kaiser and Aretz, "Legal Protection of Civil and Military Aviation against Cyber Interference," 332 (noting the offense in this convention "leaves enough room to include . . . cyber attacks or interferences"). *See also* Section 4.2.3 (Multilateral Anti-Terrorism Treaties Not in Force) *infra.*

- Amounts to "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";[129]
- Destroys or seriously damages facilities of an airport serving international civil aviation or disrupts the services of the airport;[130]
- Destroys or seriously damages maritime navigational facilities or seriously interferes with their operation in a manner likely to endanger safe navigation of ships;[131]
- Places on a fixed platform located on the continental shelf a device likely to endanger the safety of the platform;[132]
- Causes death, serious bodily injury, or extensive property destruction to a place of public use, government facility, public transportation system, or infrastructure facility through means of a "lethal device";[133] or
- Damages "a nuclear facility in a manner which releases or risks the release of radioactive material".[134]

101. Reading these agreements in light of threat of cyber terrorism demonstrates that international law is not devoid of treaty law that governments could apply to certain acts of cyber terrorism. The subject matter of some treaties includes sectors mentioned in discussions about cyber terrorism, such as transportation services, government facilities, nuclear plants, and infrastructure providing public services.

4.2.2 The Terrorist Bombings Convention, Terrorist Financing Convention, and Nuclear Terrorism Convention

102. The only three anti-terrorism treaties in force adopted after the Internet emerged—the Terrorist Bombings Convention, the Nuclear Terrorism Convention, and the International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention)[135]—deserve additional attention in order to understand whether they can be interpreted to apply to cyber terrorism. The Terrorist Bombings Convention has the broadest scope of the anti-terrorism treaties. Its offenses cover numerous sectors rather than just one sector (e.g., air transport) or target (e.g., nuclear facilities). However, it does not mention ICTs in connection with terrorist bombings.

---

[129] Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, entered into force Feb. 20, 1977, 1035 UNTS 167, Article 2.1(b).
[130] Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, entered into force Aug. 6, 1989, 1589 UNTS 474, Article II. *See also* Section 4.2.3 (Multilateral Anti-Terrorism Treaties Not in Force) *infra*.
[131] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, entered into force Mar. 1, 1992, 1678 UNTS 201, Article 3.1(e).
[132] Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, entered into force Mar. 1, 1992, 1678 UNTS 304, Article 2.1(d).
[133] Terrorist Bombings Convention, Article 2.1.
[134] Nuclear Terrorism Convention, Article 2.1(b).
[135] International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, entered into force Apr. 10, 2002, 2178 UNTS 197 [hereinafter Terrorism Financing Convention].

103. The Terrorist Bombings Convention's offense includes delivery, placement, discharge, or detonation of "an explosive or other lethal device,"[136] defined as:

- "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
- "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 similar substances or radiation or radioactive material."[137]

104. Certain cyber weapons, and specific uses of such weapons, could be an "explosive or other lethal device," but—given the range of possible cyber weapons, attacks, and targets—the Terrorist Bombings Convention has limited application when cyber terrorism is comprehensively considered. A cyber attack would fall outside the treaty if it did not involve (1) "explosive or incendiary" means or consequences; or (2) release or dissemination of toxic chemicals, biological agents, or radioactive materials.

105. The Terrorist Financing Convention seeks to prevent and suppress the financing of terrorism. It does not specifically include cyber terrorism but could be interpreted as applicable to the financing of cyber terrorism. A person commits an offense under the Terrorist Financing Convention if:

> that person by any means, directly or indirectly, unlawfully and willfully, 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 [i.e., the anti-terrorism treaties]; 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.[138]

106. For the Terrorist Financing Convention to apply cyber terrorism, the acts in question would have to fall within an offense established by one of the multilateral anti-terrorism treaties listed in its annex (see generally Table 1 above) or be intended to cause death or serious injury to civilians with the intent to intimidate a population or compel governmental or intergovernmental behavior. This treaty would not apply to acts of cyber

[136] Terrorist Bombings Convention, Article 2.1.
[137] *Ibid*., Article 3.1.
[138] Terrorism Financing Convention, Article 2(1).

terrorism falling outside the anti-terrorism treaties listed in its annex and intended to cause destruction of, or serious damage to, property.

107. The Nuclear Terrorism Convention does not mention cyber attacks. Its offenses include damaging a nuclear facility (e.g., a civilian nuclear reactor) in a manner that risks releasing radioactive material with the intent to cause death, injury, property or environmental damage, or to compel the behavior of a person, government, or international organization.[139] Launching a cyber attack on a nuclear power station could fall within the scope of this offense.

108. Before the 2012 Nuclear Security Summit, the Executive Secretariat of the International Working Group (which supports the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction) issued a paper on "Cyber Security for Nuclear Power Plants." This paper recommended that the international community should review applicable treaties and other measures for their adequacy in terms of cyber threats to nuclear facilities. It argued that "a cyber attack on a nuclear power plant with the intention of substantial radiation releases should be considered an act of terrorism" prohibited by the Nuclear Terrorism Convention.[140]

4.2.3 Multilateral Anti-Terrorism Treaties Not in Force

109. Two multilateral anti-terrorism treaties adopted in 2010 have not entered into force but are important in the relationship between anti-terrorism treaties and cyber terrorism. First, the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) provides that "[a]ny person commits an offense if that person unlawfully and intentionally . . . 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."[141] The ratification package distributed to countries states the Beijing Convention makes "cyber attacks on air navigation facilities" a criminal offense.[142]

110. Second, the Protocol Supplemental to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) provides that a person "commits an offence if that person unlawfully and intentionally seizes or exercises control of an

[139] Nuclear Terrorism Convention, Article 2(1).
[140] Maurizio Martellini, Thomas Shea, and Sandro Gaycken, *Cyber Security for Nuclear Power Plants* (Jan. 2012), http://www.state.gov/t/isn/183589.htm. *See also* Jack Carawell, "Cyber Threats to Nuclear Power Plants in the Second Nuclear Age," *Cyber Security Review* (Summer 2016), 27-32.
[141] Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, ICAO Doc. 9960, not in force [hereinafter Beijing Convention], Article 1(1)(d). The Beijing Convention seeks to modernize and consolidate (1) Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, entered into force Jan. 26, 1973, 974 UNTS 177; and (2) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, entered into force Aug. 6, 1989, 1589 UNTS 474.
[142] Administrative Package for Ratification of or Accession to the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention, 2010), http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf.

aircraft in service . . . by any technological means."[143] This offense is "intended to catch potential cyber attacks where offenders could gain control and seize the aircraft through computer equipment or other technological means from remote locations but without the use of force at all."[144]

111. The Beijing Convention and Protocol are important for a number of reasons.[145] The countries negotiating these agreements intended for them to apply to cyber terrorism, making these treaties the first multilateral anti-terrorism treaties to do so.[146] However, defining offenses in these new agreements to include cyber terrorism might raise questions about interpreting provisions in the earlier treaties as covering cyber terrorism.

112. The Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971) makes destroying, damaging, or interfering with air navigation facilities in ways that endanger the safety of aircraft in flight an offense. The Beijing Convention seeks to modernize the 1971 convention by, among other things, including cyber attacks on air navigation facilities in this offense. Similarly, the Convention for the Suppression of Unlawful Seizure of Aircraft (1970) includes as an offense the on-board, in-flight seizure or exercise of control of an aircraft. The Beijing Protocol supplements the 1970 convention by adding "any technological means" to the offense of seizing or exercising control of an aircraft.

113. Do the Beijing Convention's and Beijing Protocol's inclusion of cyber attacks as part of modernizing earlier anti-terrorism treaties on civil aviation mean those earlier treaties should not be read in ways that include cyber attacks? On the one hand, the cyber provisions of the new agreements contain something not directly addressed in the existing treaties. The cyber provisions, then, contain substance the older agreements do not. On the other hand, application of treaty interpretation principles can produce the conclusion that the text, object, and purpose of the older agreements cover cyber attacks. The Study Group concluded that the Beijing Convention and Protocol do not preclude interpreting the earlier treaties on civil aviation as applicable to cyber attacks.

---

[143] Protocol Supplemental to the Convention for the Suppression of Unlawful Seizure of Aircraft, Sept. 10, 2010, ICAO Doc. 9959, not in force. [hereinafter Beijing Protocol], Article II. The Beijing Protocol supplements the Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, entered into force Apr. 14, 1971, 860 UNTS 105.

[144] Alejandro Piera and Michael Gill, "Will the New ICAO-Beijing Instruments Build a Chinese Wall for International Aviation Security?" *Vanderbilt Journal of Transnational Law* (2014); 47:145-237, 191.

[145] The Beijing Convention and Protocol both need 22 parties before they enter into force, and, as of this writing, the Beijing Convention has 14 parties, and the Beijing Protocol has 15 parties. International Civil Aviation Organization, *Current Lists of Parties to Multilateral Air Law Treaties*, http://www.icao.int/secretariat/legal/Lists/Current%20lists%20of%20parties/AllItems.aspx.

[146] The possible vulnerability of civil aviation to cyber terrorism arose in connection with U.S. federal government allegations in a search warrant that a cybersecurity researcher had hacked into a civilian aircraft's navigation system and caused the plane to fly sideways. *See* Kim Zetter, "Feds Say that Banned Researcher Commandeered a Plane," *Wired,* May 15, 2015, http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

4.2.4 Regional Anti-Terrorism Treaties

114. States have also adopted treaties through regional organizations to address terrorism (Table 2). Although they are not identical, regional anti-terrorism treaties generally use the law enforcement approach that dominates the multilateral treaties. Regional agreements often incorporate the offenses found in the multilateral anti-terrorism treaties and require or encourage parties to ratify these instruments.[147]

Table 2. Regional Terrorism Treaties[148]

Year Adopted	Treaty
1971	Organization of American States Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance
1977	European Convention on the Suppression of Terrorism
1987	South Asian Association for Regional Cooperation (SAARC) Regional Convention on Suppression of Terrorism
1998	Arab Convention on the Suppression of Terrorism
1999	Treaty on Cooperation among the States Members of the Commonwealth of Independent States in Combatting Terrorism
	Convention of the Organization of the Islamic Conference on Combating International Terrorism
	Organization of African Unity Convention on the Prevention and Combating of Terrorism
2001	Shanghai Convention against Terrorism, Separatism, and Extremism
2002	Inter-American Convention against Terrorism
2004	Convention of the Cooperation Council for the Arab States of the Gulf on Combating Terrorism
2005	Council of Europe Convention on the Prevention of Terrorism
2007	Association of Southeast Asian Nations (ASEAN) Convention on Counter-Terrorism

115. The only regional agreement that mentions cyber terrorism is the ASEAN Convention on Counter Terrorism.[149] Under areas of cooperation, the ASEAN Convention provides that states parties "may . . . include appropriate measures, among others, to: . . . [s]trengthen capability and readiness to deal with chemical, biological, radiological, nuclear (CBRN) terrorism, cyber terrorism and any new forms of terrorism[.]"[150] This provision does not require states parties to cooperate on cyber terrorism. The ASEAN Convention does not expressly include cyber terrorism as an

[147] *See, e.g.,* Inter-American Convention Against Terrorism, June 3, 2002, entered into force July 10, 2003, http://www.oas.org/juridico/english/treaties/a-66.html, Articles 2 and 3.
[148] UN, *International Instruments Related to the Prevention and Suppression of International Terrorism* (New York: UN, 2008).
[149] ASEAN Convention on Counter Terrorism, Jan. 13, 2007, entered into force May 11, 2011, http://www.asean.org/news/item/asean-convention-on-counter-terrorism.
[150] *Ibid.,* Article VI(1)(j).

offense because it incorporates the offenses in multilateral anti-terrorism agreements,[151] nor does it define "cyber terrorism."

116. For the ASEAN Convention and other regional anti-terrorism treaties that link to the offenses in multilateral agreements, their utility as regional instruments against cyber terrorism depends on whether parties to the multilateral treaties interpret and implement them as applicable to cyber terrorism as discussed above. Alternatively, parties to regional agreements could amend them to include cyber terrorism specifically within their scope, in the same way parties to the multilateral treaties did with the Beijing Convention and Protocol and could do with other multilateral anti-terrorism agreements.

4.2.5 Draft Comprehensive Convention on International Terrorism

117. UN member states have been negotiating a comprehensive treaty on international terrorism since the mid-1990s without success. Although consensus has been reached on many issues, negotiations have deadlocked over (1) distinguishing terrorism from violence undertaken pursuant to the right of self-determination by peoples under colonial, alien, or foreign domination or occupation; and (2) the desire of some UN member states to include "state terrorism" within the treaty.[152]

118. The current draft defines its offense as follows:

> 1. 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.[153]

119. This offense would cover cyber attacks—"by any means"—against a range of targets (e.g., government facilities, transportation systems, infrastructure facilities, and

[151] *Ibid.*, Article II.
[152] UN, "Speakers Urge Differences be Resolved in Draft Comprehensive Convention on International Terrorism, as Sixth Committee Begins Session," Press Release, Oct. 7, 2014, http://www.un.org/press/en/2014/gal3475.doc.htm.
[153] UN General Assembly, Letter Dated 3 August 2005 from the Chairman of the Sixth Committee to the President of the General Assembly, UN Doc. A/59/894, Appendix II, Aug. 12, 2005, Article 2.

private property) causing different consequences, ranging from death to property damage likely to result in major economic loss. Although the draft convention was not proposed to address cyber terrorism, its scope fits the multi-faceted threat of cyber terrorism better than the sector-specific anti-terrorism treaties. The potential for the Comprehensive Convention on International Terrorism to cover cyber terrorism has been recognized.[154]

120. However, completion of this treaty is neither imminent nor foreseeable because problems that have blocked progress for twenty years have not been resolved. Introducing cyber terrorism will not break the stalemate because the problems behind the deadlock have nothing to do with the use of ICTs by states or terrorists.

4.2.6 Potential Steps Concerning the Anti-Terrorism Treaties and Cyber Terrorism

121. The Study Group's review of existing anti-terrorism treaties produces three steps states could take. First, where defined offenses can be committed through ICTs, the states parties could declare or recognize the treaties' application to cyber attacks. A state party could unilaterally, or as part of a group of parties, declare it believes an anti-terrorism treaty applies to cyber terrorism. States parties could also use formal treaty processes, such as conferences of states parties, to recognize the application of treaties to cyber terrorism. However undertaken, this step could clarify when cyber terrorism falls within relevant treaties and could constitute subsequent practice to the extent the recognition or declaration establishes the state parties' agreement regarding what the treaties cover.[155]

122. Second, parties particularly concerned about cyber terrorism can implement their obligations under relevant anti-terrorism treaties in ways that include cyber attacks. This approach could include amending implementing legislation or issuing declaratory statements about the applicability of the treaties to acts of cyber terrorism. Such "bottom up" actions could potentially stimulate states parties to address the issue collectively.

123. Third, states could adopt a treaty specifically on cyber terrorism. The existing anti-terrorism treaties are not purpose-built for cyber terrorism, and the coverage produced by applying some treaties remains limited. To apply fully the approach found in the anti-terrorism treaties to cyber terrorism would require a treaty focused on this particular form of terrorism.

4.3 Beyond the Anti-Terrorism Treaties

124. The patchwork applicability of anti-terrorism treaties to cyber terrorism invites consideration of other international law on terrorism states could apply. The possibilities involve Security Council resolutions and customary international law.

---

[154] UN, "Legal Committee Urges Conclusion of Draft Comprehensive Convention on International Terrorism," Press Release, Oct. 8, 2012, http://www.un.org/press/en/2012/gal3433.doc.htm (describing representative of Thailand urging the conclusion of the Comprehensive Convention on International Terrorism because of, among other reasons, the "growing threat of cyber-terrorism").

[155] Vienna Convention on the Law of Treaties, May 23, 1969, entered into force Jan. 27, 1980, 1155 UNTS 332, Article 31(3)(b).

4.3.1 Security Council Counter-Terrorism Mandates

125. The Security Council has imposed binding obligations on UN member states to adopt specific counter-terrorism policies.[156] Other Security Council resolutions encouraged (rather than required) UN member states to take actions against terrorism.[157] To facilitate implementation of its counter-terrorism resolutions, the Security Council established the Counter-Terrorism Committee, which monitors country-level progress, provides technical assistance, identifies best practices, and constitutes a forum for cooperation on counter-terrorism.[158]

126. None of the Security Council's counter-terrorism resolutions are specific to cyber terrorism. The Counter-Terrorism Committee has not focused on cyber terrorism as defined by the Study Group. In reporting actions taken pursuant to Security Council resolutions, UN member states have reported information or concerns about terrorist use of the Internet to communicate, recruit, and raise funds.[159] The only mention of cyber attacks in a report on implementation of Resolution 1373 (2001) involved concerns expressed by the North Atlantic Treaty Organization (NATO) with such attacks, but the reference was not specific to terrorists' potential use of cyber attacks.[160] Similarly, the UN Global Counter-Terrorism Strategy adopted in 2006 does not address terrorists using ICTs to attack government or civilian targets.[161]

127. However, the Security Council's resolutions and the Counter-Terrorism Committee's jurisdiction are broad enough to include cyber terrorism. The Committee could address cyber terrorism more systematically under its mandate from the Security Council. For example, the Committee could encourage harmonization of national criminal laws concerning cyber terrorism in the same manner it provides guidance on

---

[156] UN Security Council, Resolution 1373 (2001) (imposing obligations on UN member states to prevent and suppress various acts related to terrorism); Resolution 1540 (2004), Apr. 28, 2004 (obligating UN member states to prevent nuclear, chemical, and biological weapons from being obtained or used by non-state actors); and Resolution 2178 (2014) (requiring UN member states to prevent and suppress the cross-border flow of individuals seeking to engage in terrorism).

[157] *See, e.g.,* UN Security Council, Resolution 1624 (2005), Sept. 14, 2005 (calling on UN member states to take actions to prevent incitement of terrorism).

[158] UN Security Council, *Counter-Terrorism Committee*, http://www.un.org/en/sc/ctc/.

[159] *See, e.g.,* Counter-Terrorism Committee, *Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States* (Sept. 2011), 7, 73, and 77; UN Security Council, *Global Survey of Implementation by Member States of Security Council Resolution 1624 (2005)*, UN Doc. S/2012/16, Jan. 9, 2012 (mentioning risks associated with incitement to terrorism exacerbated by Internet communications).

[160] Counter-Terrorism Committee, *Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States*, 64.

[161] UN General Assembly, Resolution 60/288 on the United Nations Global Counter-Terrorism Strategy, UN Doc. A/RES/60/288, Sept. 20, 2006. This Strategy includes encouraging UN member states to explore ways and means to (1) coordinate international and regional efforts "to counter terrorism in all its forms and manifestations on the Internet; and (2) "[u]se the Internet as a tool for countering the spread of terrorism[.]" *Ibid*., ¶ 12.

other aspects of counter-terrorism policy and law. The Committee could also include cyber terrorism as a topic for the global research network it launched in February 2015.[162]

128. Alternatively, the Security Council could act directly on cyber terrorism. It could (1) clarify that the scope of its counter-terrorism resolutions includes cyber terrorism; (2) supplement its counter-terrorism resolutions with new ones that encompass cyber terrorism;[163] and/or (3) facilitate collective action through, for example, establishing a mechanism under the Counter-Terrorism Committee for UN member states to share information on actual or suspected cyber terrorist attacks and on effective policies and practices for responding to, protecting against, and preventing such attacks.

4.3.2 Customary International Law and the Crime of International Terrorism

129. In 2011, the Special Tribunal for Lebanon held customary international law recognizes a crime of international terrorism with three elements: (1) a criminal act that (2) involves a transnational element (3) done with the intent to spread fear among the population (generally involving creation of public danger) or directly or indirectly to coerce a national or international authority to take, or refrain from taking, some action.[164] This formulation accommodates cyber terrorism, which would involve criminal acts (unauthorized access to computer systems) with transnational elements (using the Internet or other transnational computer networks) undertaken to spread fear or coerce behavior. Its potential relevance to responding to cyber terrorism has been recognized.[165]

130. The correctness and utility of this definition are, however, uncertain. The Special Tribunal's holding is controversial, indicating that skepticism exists about the crime's status in customary international law.[166] The ruling has not resolved the impasse over finalizing the Comprehensive Convention on International Terrorism. Nor is it clear states use or rely on the Special Tribunal's crime of international terrorism, particularly in filling gaps the anti-terrorism treaties create. Relying on such a controversial ruling is not the most effective strategy for responding to cyber terrorism.

---

[162] UN Counter-Terrorism Committee, Counter-Terrorism Committee Launches Global Research Network, Feb. 20, 2015, http://www.un.org/press/en/2014/gal3475.doc.htm.
[163] "Cyber Security for Nuclear Power Plants" (recommending the Security Council "should determine whether existing Resolutions 1373 and 1540 should be amended to address nuclear cyber terrorism").
[164] Special Tribunal for Lebanon Decision, ¶ 85.
[165] Michael P. Scharf, "Special Tribunal for Lebanon Issues Landmark Ruling on Definition of Terrorism and Modes of Participation," *American Society of International Law Insights*, Mar. 4, 2011, http://www.asil.org/sites/default/files/insight110304.pdf.
[166] *See, e.g.,* Ben Saul, "Legislating from a Radical Hague: The United Nations Tribunal for Lebanon Invents an International Crime of Transnational Terrorism," *Leiden Journal of International Law* (2011); 24(3): 677-700.

4.4 Treaties on Cyber Crime, Transnational Organized Crime, Extradition, and Mutual Legal Assistance and Extraterritorial Application of Criminal Law

4.4.1 Cyber Crime Treaties and Cyber Terrorism

131. In addition to anti-terrorism treaties, responses to cyber terrorism can be based in international law on criminal law and law enforcement cooperation. The Council of Europe's Convention on Cybercrime (COE Convention) is useful with respect to cyber terrorism.[167] Cyber terrorism would involve commission of offenses this treaty defines and requires states parties to criminalize and combat. Other treaties with provisions on cyber crime, such as the African Union's Convention on Cyber Security and Personal Data Protection (2014) (AU Convention),[168] have similar relevance.

132. The COE Convention would treat cyber terrorism as ordinary cyber crime. It does not contain offenses delineating terrorism as a different kind of criminal activity. In national and international law, states have created special criminal law for terrorist acts in order to mark them as different from other criminal behavior. Why states would deviate from this pattern and rely on cyber crime laws if cyber terrorism emerges is not clear. States parties to the COE Convention adopted a protocol on xenophobia and racism,[169] which offers a procedural model for a cyber terrorism protocol.

133. As of the end of July 2016, 49 states have ratified the COE Convention, compared to an average of 168 parties for the anti-terrorism treaties listed in Table 1.[170] The additional protocol has 24 states parties.[171] Acceptance of the COE Convention is poor by countries in Asia, the Middle East, and Africa, and important states, such as China, India, and Russia, have not joined. Limited ratification means the COE Convention is not a global instrument as the multilateral anti-terrorism treaties are, which reduces its potential effectiveness against cyber terrorism.[172]

---

[167] Council of Europe Committee of Experts on Terrorism (CODEXTER), *Opinion for the Committee of Ministers on Cyberterrorism and the Use of Internet for Terrorist Purposes* (2008), http://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf.

[168] African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, not in force, EX.CL/846 (XXV) [hereinafter AU Convention].

[169] Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Jan. 1, 2003, entered into force Mar. 1, 2006, Council of Europe Treaty Series No. 189.

[170] Council of Europe, *Convention on Cybercrime Status* (as of July 31, 2016), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=20/02/2015&CL=ENG.

[171] Council of Europe, *Additional Protocol to the Convention on Cybercrime Status* (as of July 31, 2016), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG.

[172] The same problem limits the utility of other regional agreements that contain provisions on cyber crime. *See, e.g.,* Commonwealth of Independent States Agreement on Cooperation in Combating Offenses Related to Computer Information (2001); Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009); and the Arab Convention on Combating Information Technology Offences (2010).

134. In adopting the AU Convention, AU member states rejected the COE Convention in their efforts against cyber crime.[173] The AU Convention does not include an offense specific to cyber terrorism. As with the COE Convention, the AU Convention's provisions on cyber crime could apply to cyber terrorism. The AU Convention only mentions terrorism in requiring states parties to consider the use of ICTs as aggravating circumstances in the commission of offenses, including terrorism.[174] This provision would apply to the use of ICTs in committing terrorist offenses under national criminal codes, such as using the Internet to plan and execute a kinetic attack.

135. The AU Convention is the most recently adopted treaty that addresses cyber crime, and, during the time it was negotiated, the threat of cyber terrorism was prominent in policy debates. Yet, AU member states did not include in the AU Convention any provisions specific to cyber terrorism. Why they did not do so perhaps relates to the sense that, at the present time, cyber terrorism is not a pressing problem for African states, unlike cyber crime specifically and cybersecurity generally. Unlike the COE Convention, the AU Convention is only intended to be a regional agreement.[175] When, and even whether, the AU Convention enters into force remains uncertain.[176]

4.4.2 Transnational Organized Crime and Cyber Terrorism

136. Another option for addressing cyber terrorism is the UN Convention against Transnational Organized Crime (TOC Convention).[177] Generally, the TOC Convention requires states parties to establish as criminal offenses, and engage in law enforcement cooperation concerning, the commission of serious crimes that have a transnational element and involve participation in an organized criminal group.[178]

137. The TOC Convention does not define or list specific crimes (including cyber crime) in order to make sure the treaty can address "new types of crime that emerge constantly as global, regional and local conditions change over time."[179] The states parties to the TOC Convention have identified cyber crime as an emerging crime of concern,[180] which indicates they believe the treaty applies to this threat. The TOC

[173] *See generally* Mailyn Fidler, "Cyber Diplomacy with Africa: Lessons from the African Cybersecurity Convention," *Council on Foreign Relations Net Politics,* July 7, 2016, http://blogs.cfr.org/cyber/2016/07/07/cyber-diplomacy-with-africa-lessons-from-the-african-cybersecurity-convention/.
[174] AU Convention, Article 30(1)(b).
[175] *Ibid.*, Article 35.
[176] *Ibid.*, Article 36. The AU Convention contains provisions that are relevant to other strategies against cyber terrorism, and the report mentions this treaty in Part 5 (International Law and Protecting Against Cyber Terrorism) *infra*.
[177] UN Convention against Transnational Organized Crime, Nov. 15, 2000, entered into force Sept. 29, 2003, 2225 UNTS 209 [hereinafter TOC Convention].
[178] *Ibid.*, Article 2 (defining "organized criminal group" and "serious crime"), Article 3 (scope of application), and Article 5 (criminalization of participation in an organized criminal group).
[179] UN Office on Drugs and Crime, *Organized Crime*, http://www.unodc.org/unodc/en/organized-crime/index.html.
[180] UN Office on Drugs and Crime, *Emerging Crimes*, http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html.

Convention has 187 states parties,[181] which gives this agreement more geographic scope than regional cyber crime instruments.

138. Whether the TOC Convention represents a good choice in terms of responding to cyber terrorism is questionable. Generally, cyber crime has increased significantly during the time the TOC Convention has been in force, which suggests the treaty does not deter organized cyber crime groups. Nor is it clear how much states parties use the TOC Convention to respond to cyber crime. A study of cybercrime by the UN Office on Drugs and Crimes indicated that states use bilateral extradition and mutual legal assistance agreements to address cyber crime more than regional or multilateral treaties.[182] The states parties have focused on other crimes through protocols on human trafficking, smuggling migrants, and illicit firearms manufacturing and trafficking.[183]

4.4.3 Extradition and Mutual Legal Assistance Treaties and Cyber Terrorism

139. States responding to cyber terrorism could use treaties designed to facilitate general law enforcement cooperation. A government could seek extradition of persons suspected of cyber terrorism through extradition agreements, which are usually bilateral. Such treaties might support extradition for the crime of cyber terrorism if the requesting and requested states have criminalized this crime in ways to satisfy the principle of double criminality—a strategy harmonization of national criminal laws on cyber terrorism would enhance. Lack of such harmonization means "dual criminality" requirements in extradition treaties would require basing extradition requests in cyber crime statutes or general criminal laws where harmonization might be present.

140. However, states have experienced problems using extradition treaties to fight terrorism. For example, the United States and United Kingdom amended their extradition treaty to overcome friction created by UK extradition requests for persons alleged to be involved in terrorism in Northern Ireland.[184] The fix in these kinds of disputes has been to make terrorist acts extraditable offenses under extradition treaties and exclude them from the "political offense" exception such treaties routinely include.

141. Variations in state attitudes about some activities, such as hacktivism, could generate similar problems under extradition treaties. Alternatively, extradition could be based on cyber crimes, such as causing damage to computers through unauthorized access, or non-cyber crimes recognized by the requesting and requested states.

142. States could request help investigating cyber terrorism through mutual legal assistance treaties (MLATs), which are also often bilateral. MLATs facilitate law

[181] UN Treaty Collection, *UN Convention against Transnational Organized Crime: Status of Ratification* (as of July 31, 2016), https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en.
[182] UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Feb. 2013), 201.
[183] UN Office on Drugs and Crime, *Signatories to the United Nations Convention on Transnational Organized Crime and Its Protocols*, http://www.unodc.org/unodc/en/treaties/CTOC/signatures.html.
[184] *See, e.g.,* Daniel Byman, *Deadly Connections: States that Sponsor Terrorism* (Cambridge: Cambridge University Press, 2005), 249-51.

enforcement cooperation, but typically are not specific to any type of crime. They could be used, where applicable, in investigating alleged cyber terrorism. However, MLATs have proved difficult to use given the "internationalization" of digital evidence and the increase in cyber crimes. MLATs have become notorious for operating in cumbersome and time-consuming ways, such that MLAT-related "delays can be aggravating or problematic in traditional criminal investigations, [but] they are likely to be devastating in cybercrime investigations."[185] These problems have led to calls for MLATs to be modernized to be more helpful against cyber crime.[186]

4.4.4 Extraterritorial Jurisdiction, International Law, and Cyber Terrorism

143. States have prescribed national criminal law to terrorist acts occurring outside their territories directed against their governments, populations, economy, or nationals. States base such extraterritorial jurisdiction against terrorism on treaty commitments (e.g., anti-terrorism treaties) or customary international law on prescriptive jurisdiction.[187] In the absence of treaty rules, states adopting criminal law on cyber terrorism could apply it to extraterritorial acts (1) perpetrated by their nationals (nationality principle); (2) targeting their nationals in foreign countries (passive personality principle); or (3) causing significant effects to persons or activities in their territories (effects principle).

144. Application of customary rules on extraterritorial jurisdiction to cyber terrorism is unlikely to raise novel issues. Questions might arise concerning what level of effects supports a charge of cyber terrorism as opposed to cyber or other types of crime, but national courts have addressed in non-cyber contexts whether the alleged domestic effects of extraterritorial acts are significant enough to warrant extraterritorial application of national law. In addition, a factor distinguishing cyber terrorism from cyber crime is intent rather than effects because, typically, terrorist crimes include specific intent requirements (e.g., acts done with the intent to coerce a government). The exercise of extraterritorial criminal jurisdiction by states demonstrates that specific intent poses no barriers to such jurisdiction.

---

[185] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara: Praeger, 2010), 143.

[186] *See, e.g.,* Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age* (Global Network Initiative, Jan. 2015), http://csis.org/files/attachments/GNI%20MLAT%20Report.pdf. For one proposal on expediting cross-border data requests, see Jennifer Daskal and Andrew K. Woods, "Cross-Border Data Requests: A Proposed Framework," *Lawfare,* Nov. 24, 2015, https://lawfareblog.com/cross-border-data-requests-proposed-framework. The United States and the United Kingdom have started talks to improve law enforcement cooperation on digital data. Ellen Nakashima and Andrea Peterson, "The British Want to Come to America—With Wiretap Orders and Search Warrants," *Washington Post,* Feb. 4, 2016, https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

[187] *See, e.g.,* Terrorist Bombings Convention, Article 6 (on jurisdiction); *Foreign Relations Law of the United States* (Minneapolis: West Publishing, 3rd ed., 1987), § 403.

4.4.5 Summary on Cyber Crime, Transnational Organized Crime, Extradition, and Mutual Legal Assistance Treaties and Extraterritorial Application of Criminal Law

145. States could apply treaty law specific to cyber crime, such as the COE Convention, and more general-purpose law enforcement instruments—extradition and mutual legal assistance treaties—to cyber terrorism. These approaches would not require negotiation of a common definition of cyber terrorism because states would apply existing criminal offenses and law enforcement cooperation mechanisms in these agreements. However, existing treaties on cyber crime are not widely ratified, which limits their potential against cyber terrorism. Although widely ratified, the TOC Convention does not appear to have had much, if any, impact on organized cyber crime. Using extradition treaties and MLATs to respond to cyber terrorism would confront the same problems countries experience in using them against cyber crime.

146. Customary international law on the extraterritorial application of domestic criminal law provides another path for responding to cyber terrorism. This approach can be frustrated by, among other things, problems that arise between countries about criminal laws that apply extraterritorially. Further, even if a state's exercise of prescriptive jurisdiction beyond its borders creates no controversies, the state would still need other countries to extradite suspects and/or engage in law enforcement cooperation in order to apply its national criminal law effectively.

147. Finally, relying on cyber crime conventions, the TOC Convention, extradition agreements, and MLATs would mean treating terrorism as ordinary criminal activities. Although this approach poses no conceptual or practical legal problems, states typically distinguish terrorism from other forms of crime, as demonstrated by the international law on terrorism. This pattern suggests states might not be content to rely on international law on cyber crime, organized crime, or general-purpose extradition and mutual legal assistance treaties if terrorists begin to engage in cyber attacks to advance their agendas.

4.5 The Use of Force in Self-Defense, Sanctions, and Responding to Cyber Terrorism

4.5.1 The Use of Force in Self-Defense and Responding to Terrorism

148. Traditionally, the prohibition on the use of force in international law was directed at states, and a state's right to use force in self-defense was triggered by an armed attack by another state, or an attack attributable to another state under international law on state responsibility.[188] Over time, terrorism affected this body of international law, initially through state-sponsored terrorism.[189] Even though state-sponsored terrorism

[188] UN Charter, Articles 2(4) and 51.
[189] Mary Ellen O'Connell, "Lawful Self-Defense to Terrorism," *University of Pittsburgh Law Review* (2001-2002); 63: 889-904; Walter Gary Sharp, Jr., "The Use of Armed Force Against Terrorism: American Hegemony or Impotence?" *Chicago Journal of International Law* (2000); 1(1): 37-47.

created problems, such as attributing terrorist violence to a state under principles of state responsibility, the paradigm remained one state's use of force against another state.[190]

149. The bigger change happened after major terrorist attacks in the 2000s when several states supported the proposition that, under international law, terrorist violence not necessarily attributable to a state could trigger the victim state's right to use force in self-defense in the territory of another state without its consent.[191] This proposition generated criticism,[192] indicating that whether it forms part of international law is controversial. Recent uses of military force against the Islamic State in reaction to its terrorist violence have again focused attention on the issue.[193]

150. Terrorism in the first decade of the twenty-first century also generated other questions. At what point does terrorist violence become an armed attack activating a state's right to respond with force in self-defense? What kind of attribution is required to justify the use of force against terrorists? Before the victim state can resort to force, what is required from the state where the armed attack by terrorists originated or from the state of the perpetrators' nationality? How do the requirements of necessity and proportionality apply to the use of force in self-defense in response to terrorist attacks? At what point does the right to use force in self-defense against a terrorist group end?

151. In terms of the armed-attack threshold, where to draw this line concerning terrorist violence was problematic well before cyber terrorism became a policy and legal concern.[194] The 9/11 terrorist attacks led NATO to declare that the United States had been victim of an armed attack, triggering the collective self-defense obligations of alliance members.[195] However, terrorism on this scale rarely occurs. Traditional arguments that "armed attack" constitutes a high threshold are in tension with state practice that interprets varying levels of terrorist violence as armed attacks.[196] In grappling with terrorism, many governments want to preserve military options, which

---

[190] *See* Section 2.5 (State-Sponsored Terrorism, Weak States, and Cyber Terrorism) *supra*.
[191] *See, e.g.,* Bethlehem, "Principles Relevant to the Scope of State's Right of Self-Defense," 776 (arguing international law does not require state consent "in circumstances in which there is a reasonable and objective basis for concluding that the third state is unable to effectively restrain the armed activities of the nonstate actor such as to leave the state that has a necessity to act in self-defense with no other reasonably available effective means to address an imminent or actual armed attack"). *See generally* Advisory Council on International Affairs, *Counterterrorism from an International Perspective* (Advisory Report No. 49, Sept. 2006), 24-25; Tams, "The Use of Force Against Terrorists," 359-97.
[192] *See, e.g.,* Mary Ellen O'Connell, "Dangerous Departures," *American Journal of International Law* (2013); 107: 380-86.
[193] Marc Weller, "Striking ISIL: Aspects of the Law on the Use of Force," *American Society of International Law Insights*, Mar. 11, 2015, http://www.asil.org/insights/volume/19/issue/5/striking-isil-aspects-law-use-force.
[194] *See, e.g.,* Mary Ellen O'Connell, "Evidence of Terror," *Journal of Conflict & Security Law* (2002); 7(1): 19-36.
[195] NATO's invocation of Article 5 of the Washington Treaty after 9/11 represents the first and, to date, the only time NATO has declared an alliance member has been the victim of an armed attack.
[196] Steven R. Ratner, *Self-Defense Against Terrorists: The Meaning of Armed Attack* (University of Michigan Law School Public Law and Legal Theory Working Paper No. 270, May 2012); O'Connell, "The Prohibition on the Use of Force," 89-119.

informs preferences for flexibility in determining when terrorist acts trigger the right to use force in self-defense.

152. Controversies also arose about the victim state using force in another state to respond to terrorist violence without the other state being responsible for the violence under international law. International lawyers have debated the legality of the victim state's use of force in self-defense when the other state has proved unable or unwilling to address the terrorist threat within its territory.[197] This controversy includes whether a state's unwillingness or inability to address the threat in its territory permits the victim state to use force against that state (in addition to using force against terrorists) under the right to use force in self-defense.[198]

4.5.2 Cyber Terrorism and the Use of Force in Self-Defense

153. Turning to cyber terrorism, problems do not arise from hypotheticals that are easy cases. A cyber-9/11 scenario involving significant death and destruction would be an armed attack. Such terrorist attacks happen infrequently, and—given the capabilities, resources, and planning required for a digital 9/11 attack—they might be equally rare with cyber terrorism.[199] Cyber attacks by terrorists that produce temporary disruptions or limited damage, such as those the Cyber Caliphate claimed to have conducted against CENTCOM, do not cross the terrorism threshold, let alone the armed-attack threshold.[200]

154. Controversies would likely emerge with cyber terrorist attacks that fall between these ends of the consequence spectrum, which is where controversies have arisen in international law with conventional terrorism. Would a Stuxnet-like attack causing limited physical damage conducted by terrorists be an armed attack permitting the victim state to use force in response?[201] Would a cyber terrorist attack that disabled critical infrastructure, without causing permanent damage, cross the threshold? Would a state consider a cyber terrorist attack that damaged digital data, thus causing economic losses, an armed attack?

---

[197] *See, e.g.,* Bethlehem, "Principles Relevant to the Scope of State's Right of Self-Defense," 770-77; O'Connell, "Dangerous Departures," 380-86.

[198] *See, e.g.,* International Court of Justice, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda),* I.C.J. Reports 2005 (Merits), ¶¶ 146-47 (discussing whether the unwillingness or inability of a state to address irregular forces in its territory triggers a right of self-defense against that state).

[199] U. S. Department of Defense, *Law of War Manual* (Washington, D.C.: U.S. Department of Defense, 2015), 996 ("operations described as 'cyber attacks' or 'computer network attacks' are not necessarily 'armed attacks' for the purposes of triggering a State's inherent right of self-defense under *jus ad bellum*").

[200] U.S. Department of Defense, "CENTCOM Acknowledges Social Media Sites 'Compromised,'" Jan. 12, 2015, http://www.defense.gov/news/newsarticle.aspx?id=123956&source=GovDelivery. Hybrid attacks involving kinetic and cyber elements would require examining whether their combined effects cross the armed-attack threshold.

[201] For background on Stuxnet and its policy and legal implications, see Dorothy E. Denning, "Stuxnet: What Has Changed?," *Future Internet* (2012); 4: 672-87; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

155. We also do not know how use of ICTs by terrorists might affect international legal analysis of self-defense issues. International law on the use of force is designed to be neutral as to technologies, but state practice might treat the armed-attack threshold differently if terrorists use ICTs rather than conventional weaponry.[202] As noted above, many states prefer a flexible interpretation of the right of self-defense in responding to terrorist violence. However, it is not clear this approach would prevail if terrorists use cyber weapons as opposed to kinetic violence.

156. Although not an act of terrorism, the Stuxnet attack helps illustrate this point. Whether the Stuxnet operation constituted an armed attack has been controversial.[203] If the perpetrators had used kinetic munitions, there is little doubt states would have considered the operation an armed attack. Why, then, is there controversy about a cyber attack that caused kinetic damage to physical infrastructure? Does the controversy suggest the armed-attack threshold might be different when cyber weapons are used? The same questions could arise in applying this threshold should terrorists use cyber weapons.

157. Other episodes provide more evidence of state practice but do not clarify the armed-attack threshold concerning cyber terrorist attacks. The cyber operations directed against Saudi Aramco in 2012[204] and Sony Entertainment in 2014,[205] allegedly conducted by Iran and North Korea respectively, involved destruction of stored data and damage to computers. However, in neither case did the victim state publicly announce it considered the cyber attacks to constitute an armed attack under international law.

158. The cyber context also complicates analysis if acts of cyber terrorism did constitute an armed attack. To use force in self-defense, the perpetrators must be identified and located, and the ability of cyber terrorists to obscure where the attack originated creates problems. What governments or companies (e.g., Internet service providers) must be asked for cooperation in ending the attacks or responding to them before the victim state can use force in self-defense? What if a government, under national law, cannot force an Internet service provider to stop an attack?

159. Given the difficulties with attribution in cyber contexts, when does a state, which is asked for assistance by the victim state, become so uncooperative that the victim state can resort to force in self-defense? What if asking for the cooperation of another state increases the risk of ongoing acts of cyber terrorism? At what point can a victim

---

[202] For discussion of "armed attack" in connection with cyber warfare, see *Tallinn Manual,* 54-61.
[203] *Ibid.*, 58 (noting only some members of the International Group of Experts believed the Stuxnet operation to be an armed attack). *But see* Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law* (2012); 17(2): 187-209.
[204] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0.
[205] Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew into a Firestorm," *New York Times*, Dec. 30, 2014, http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

state dispense with cooperation in order to plead necessity in acting "to safeguard an essential interest against a grave and imminent peril"?[206]

160. The attribution problem, and the cyber context more broadly, might also affect the principles of immediacy, necessity, and proportionality that regulate the use of force in self-defense. Determining who or what is responsible for a cyber attack can take time, which complicates a state's ability to satisfy the immediacy principle.[207] Military responses to terrorist violence have provoked controversies about how the necessity and proportionality principles apply to uses of force taken in self-defense.[208] States that have used military force against terrorists prefer broad readings of the principles of necessity and proportionality, in the same way they prefer flexibility in determining what constitutes an armed attack.

161. Inserting cyber weapons into this context creates more complexity. A kinetic response by a state to a cyber attack by terrorists raises questions about whether such a response is necessary and proportional. State practice is unlikely to restrict responses to cyber attacks to cyber means and methods, but the difference between cyber and kinetic technologies matters in analyzing how the necessity and proportionality principles apply to uses of force in self-defense. The difficulties associated with attribution of cyber attacks loom larger if a state wants to respond with kinetic violence rather than cyber counter-strikes, an issue relevant to the necessity and proportionality principles.

162. States might respond to cyber terrorist attacks through cyber rather than kinetic means, which raises other questions. A state might claim its cyber response does not amount to a use of force, and, as such, does not rely on the right to use force in self-defense.[209] Here, the threshold question involves the use of force by the victim, not an armed attack by the terrorist. States might prefer a high use-of-force threshold to permit robust cyber strikes in response to cyber terrorism, avoiding the need to classify the cyber terrorism as an armed attack or the cyber response as a use of force.

163. Again, the Stuxnet operation provides food for thought because whether it amounted to a use of force in international law has been analyzed.[210] If Stuxnet was not a use of force, it was not an armed attack, meaning it did not trigger Iran's right to use force in self-defense. Likewise, if it was not a use of force, the countries responsible for the operation did not need to justify it under the right to use force in self-defense, but would need to provide a justification under other rules of international law.

---

[206] ILC Principles of State Responsibility, Article 25. *See also* Ivanov, "Combating Cyberterrorism under International Law," 65-67 (discussing the plea of necessity).
[207] On the immediacy principle in the context of cyber warfare, see *Tallinn Manual*, 63-66.
[208] Christian J. Tams and James G. Devaney, "Applying Necessity and Proportionality to Anti-Terrorist Self-Defence," *Israel Law Review* (2012); 45(1): 91-106.
[209] On the use of force in the context of cyber warfare, see *Tallinn Manual*, 42-52.
[210] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?," *Journal of Conflict & Security Law* (2012); 17: 211-27; *Tallinn Manual*, 45 (stating that the Stuxnet operation represents a cyber operation "that amount[s] to a use of force").

164. Cyber attacks by terrorists could also implicate international legal arguments about whether an accumulation of low-level attacks can cross the armed-attack threshold and trigger a state's right to use force in self-defense. Here, the accumulated attacks could involve a combination of kinetic and cyber attacks, or a series of cyber attacks. Generally, a state's use of force in self-defense against another state under the so-called "accumulation of events theory" has been controversial.[211] However, given "the growing awareness that transnational terrorist attacks present states with a serious problem," the accumulation of events theory "is not as widely rejected as it was in the past."[212]

165. In thinking about use of force issues, the Study Group found itself in a conundrum. The paucity of state practice relevant to cyber terrorism turns analysis into speculation about what might happen if terrorists "go cyber" in the future. But, state responses to conventional terrorism have generated controversies linked to state preferences for flexibility in interpreting and applying international law on the use of force. Why states would opt for less flexibility in the context of cyber terrorism is not obvious, especially when cyber terrorism has not yet emerged as a practical problem. In these circumstances, seeking clarity about triggering thresholds, the immediacy, necessity and proportionality principles, and the accumulation of events theory is more likely to re-play existing controversies than persuade states to support clear rules.

4.5.3 Sanctions and Cyber Terrorism

166. States might experience acts of cyber terrorism that do not cross the armed-attack threshold and, thus, do not trigger the right to use force in self-defense.[213] Here, the question becomes what measures states can take to address cyber terrorism not attributable to another state. Before acting, a state victimized by cyber terrorism must seek the cooperation of the state from which the cyber terrorism appeared to emanate, but the same problems associated with attribution, the cooperation required, and timing issues in addressing ongoing acts arise here as well. In addition, how the proportionality requirement for counter-measures applies in responses to cyber terrorism is not clear.[214]

167. Although not a case of cyber terrorism, the U.S. government implemented sanctions against individuals in the North Korean government believed to be responsible for the cyber operation conducted against Sony Entertainment, which the Obama

---

[211] David Kretzmer, "The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*," *European Journal of International Law* (2013); 24(1): 235-82, 244.
[212] *Ibid.*
[213] *See* O'Connell, "Cyber Security without Cyber War," 187-209; Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law* (2014); 54(3): 697-732; Nicholas Tsagourias, "The Law Applicable to Countermeasures against Low-Intensity Cyber Operations," *Baltic Yearbook of International Law* (2014); 14: 105-23.
[214] *See generally* Tobias Feakin, *Developing a Proportionate Response to a Cyber Incident* (Council on Foreign Relations Cyber Brief, Aug. 2015), http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

administration called "cyber vandalism."[215] Shortly thereafter, President Obama issued another executive order imposing sanctions on individuals determined to have engaged in cyber-enabled activities reasonably likely to result in, or contribute to, a significant threat to national security, foreign policy, the economic health, or financial stability of the United States.[216] Such sanctions could be applied to terrorists who engage in cyber operations against the United States, in the same way the U.S. government and other countries apply sanctions against individuals involved in conventional terrorism.

4.6 International Humanitarian Law and Responding to Cyber Terrorism

168. Although most of the international law developed to counter terrorism addresses peacetime contexts, international humanitarian law (IHL) has rules about terrorism committed by states and non-state actors during armed conflicts. Analyzing the international law relevant to responding to terrorism should include IHL as part of understanding how international law might inform responses to cyber terrorism perpetrated by non-state actors.

4.6.1 The Prohibition on Acts or Threats of Violence Committed with the Primary Purpose of Terrorizing Civilians

169. In international and non-international armed conflict, treaty law prohibits "[a]cts or threats of violence the primary purpose of which is to spread terror among the civilian population."[217] This prohibition is considered part of customary IHL.[218] The prohibition would apply to the use of ICTs in armed conflict. The *Tallinn Manual* states that "[c]yber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population, are prohibited,"[219] and the *Manual* provides examples of actions that would violate this prohibition:

- A "cyber attack against a mass transit system that causes death or injury . . . if the primary purpose of the attack is to terrorize the civilian population"; and
- A "threat to use a cyber attack to disable a city's water distribution system to contaminate drinking water and cause death or illness . . . if made with the primary purpose of spreading terror among the civilian population[.]"[220]

---

[215] Executive Order, Imposing Additional Sanctions with Respect to North Korea, Jan. 2, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea.
[216] Executive Order, Blocking the Property of Certain Persons Engaged in Significant Malicious Cyber-Enabled Activities, Apr. 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.
[217] Additional Protocol I, Article 51(2); and Additional Protocol II, Article 13(2). *See also* U.S. Department of Defense, *Law of War Manual*, 657.
[218] International Committee of the Red Cross [ICRC], *Customary International Humanitarian Law, Rule 2: Violence Aimed at Spreading Terror Among the Civilian Population*, https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule2; *Tallinn Manual*, 122.
[219] *Tallinn Manual*, 122.
[220] *Ibid.*, 123.

170. Although this prohibition covers ICTs, complexities arise with its application in cyber contexts. The rule prohibits "acts or threats of violence." Like the meaning of "attack" in IHL,[221] this phrase means the cyber action must produce or threaten actual or foreseeable death or injury to persons and/or damage or destruction to property, rather than depriving people access to, or use of, ICTs. Certain cyber operations directed against civilians might not qualify as "acts or threats of violence" but still be intended to spread terror among civilians. For cyber operations that fall outside this prohibition, IHL contains other rules.[222] In addition, determining whether a cyber attack was made with the primary purpose of spreading terror among civilians might be difficult given (1) the attribution problem; and (2) potentially broad readings of "dual use" targets that can be attacked under the law of armed conflict.

4.6.2 International Criminal Law and Violation of the Prohibition on Acts or Threats of Violence Intended to Spread Terror Among Civilians

171. Whether a violation of the prohibition on acts or threats of violence primarily intended to terrorize civilians constitutes a crime in IHL is not as clear as the legal status of the prohibition. Neither Additional Protocol I nor Additional Protocol II defines a violation of its prohibition as a grave breach subjecting a perpetrator to criminal liability. The statute establishing the International Criminal Tribunal for the Former Yugoslavia (ICTY) also did not include violations of this prohibition in its list of war crimes.[223]

172. However, the ICTY has prosecuted individuals for committing acts or threats of violence the primary purpose of which was to spread terror among civilians under its jurisdiction for violations of "the laws and customs of war."[224] The ICTY held that the prohibition on acts or threats of violence primarily intended to terrorize civilians was customary international law and, thus, provided the basis for a war crime under its statute.[225] As applied by the ICTY, the elements of this crime require that the offender:

- Engaged in acts or threats of violence against civilians, and the victims suffered grave consequences as a result of such acts or threats of violence;
- Willfully made civilians the object of the acts or threats of violence; and
- Committed the acts or threats of violence with the primary purpose of spreading terror among the civilian population.[226]

173. The statute for the International Criminal Tribunal for Rwanda (ICTR) gave the tribunal jurisdiction over violations of Additional Protocol II, including "acts of

[221] *See ibid.* for discussion of "attack" in IHL in the context of cyber warfare.
[222] *See* Section 4.6.3 (Prohibitions on Measures or Acts of Terrorism) *infra.*
[223] *Report of the Secretary-General Pursuant to Paragraph 2 of Security Council Resolution 808 (1993)*, May 3, 1993, Annex (Statute of the International Tribunal).
[224] *Ibid.*, Article 3.
[225] *Prosecutor v. Stanislav Galić*, ¶¶ 87-90; *Prosecutor v. Radovan Karadžić,* ¶ 458.
[226] *Prosecutor v. Stanislav Galić*, , ¶ 100; *Prosecutor v. Radovan Karadžić,* ¶ 459

terrorism."[227] However, the ICTR did not prosecute anyone for "acts of terrorism" that violated Additional Protocol II.

174. The Rome Statute establishing the International Criminal Court (ICC) does not include acts or threats of violence undertaken with the primary purpose of spreading terror in the civilian population in its definition of the crime against humanity[228] or its list of war crimes.[229] Under the ICC, acts or threats of violence committed with the primary purpose of terrorizing civilians come into play in sentencing individuals found guilty of crimes subject to the ICC's jurisdiction.[230]

175. Like the ICTR Statute, the statute of the Special Court for Sierra Leone (SCSL) gave the court jurisdiction over violations of Additional Protocol II, including "acts of terrorism."[231] The SCSL prosecuted defendants for committing acts of terrorism.[232]

176. Based on state practice approving and operating international criminal tribunals and the jurisprudence of these courts, whether a cyber attack could constitute this war crime might depend on the jurisdiction of the investigating tribunal. International courts established for particular armed conflicts (e.g., former Yugoslavia, Rwanda, and Sierra Leone) treated acts or threats of violence committed to terrorize civilians as war crimes, but the ICC does not. Further, applying the elements of the war crime of terror and the burden of proof associated with imposing criminal sanctions might confront difficulties in the cyber context, including how the attribution problem could adversely affect identifying the offender and analyzing intent.

4.6.3 Prohibitions on Measures or Acts of Terrorism

177. Certain cyber operations during armed conflict might not satisfy all the elements of the prohibition on acts or threats of violence the primary purpose of which is to spread terror in a civilian population, and, thus, might not constitute the war crime of terror. A cyber operation directed against civilian targets might not cross the "attack" threshold in

---

[227] UN Security Council, Resolution 955 (1994), Nov. 8, 1994, Annex (Statute of the International Tribunal for Rwanda), Article 4. This jurisdiction includes violations of Article 13(2) of Additional Protocol II.
[228] Rome Statute of the International Criminal Court, UN Doc. A/CONF.183/9, July 17, 1998, entered into force July 1, 2002 [hereinafter Rome Statute], Article 7. Acts or threats of violence undertaken with the primary purpose of spreading terror in the civilian population could constitute a crime against humanity if such acts constituted a widespread or systematic attack directed against a civilian population and involved "inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health" (Article 7(k)).
[229] *Ibid.*, Article 8. However, Article 10 recognizes that the Rome Statute's definition of crimes subject to the ICC's jurisdiction is not intended to limit or prejudice "existing or developing rules of international law for purposes other than this Statute."
[230] Robert Cryer, Hakan Friman, Darryl Robinson, and Elizabeth Wilmshurst *An Introduction to International Criminal Law and Procedure* (Cambridge: Cambridge University Press, 3rd ed., 2014), 344.
[231] Agreement between the United Nations and the Government of Sierra Leone on the Establishment of a Special Court for Sierra Leone, January 16, 2002, Article 3.
[232] *See, e.g.,* SCSL, *Prosecutor v. Fofana and Kondewa,* Case No. SCSL-04-14-A, Judgment on Appeal, May 28, 2008. These cases involved acts or threats of violence within the meaning of Article 13(2) of Additional Protocol II.

IHL[233] but be primarily intended to spread terror among the civilian population. Or, a cyber operation might be an attack but be undertaken with a variety of motivations rather than with the primary purpose of terrorizing civilians.

178. While these examples do not fall within the prohibition and war crime described above, the operations they describe could violate other treaty prohibitions against acts of terror. For international armed conflict among states, Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War prohibits the use of "all measures of intimidation or of terrorism" against protected persons.[234] Similarly, in non-international armed conflict, Additional Protocol II prohibits "acts of terrorism" by state or non-state actors against "[a]ll persons who do not take a direct part or who have ceased to take part in hostilities" undertaken "at any time and in any place whatsoever."[235]

179. These treaty prohibitions cover actions that do not constitute attacks in IHL because "measures" and "acts" are broader terms than "attacks."[236] Nor do these rules require that the primary purpose of the measures or acts be to spread terror in the civilian population.[237] A measure or act would violate these treaty prohibitions if terrorizing civilians is only one of a number of motivations.

180. Whether these treaty prohibitions are customary international law is an issue. The study of customary IHL by the International Committee of the Red Cross cited sources supporting the claim that custom includes these prohibitions, including the UN Secretary General's statement that prohibitions in Article 4 of Additional Protocol II "have long been considered customary international law."[238] However, with reference to Geneva Convention IV, only a minority of members of the International Group of Experts who produced the *Tallinn Manual* "took the position that the confluence of Article 33, Article 51(2), and State practice has resulted in a customary norm prohibiting any operations, including cyber operations, intended (whether the primary purpose or not) to terrorize the civilian population."[239] The *San Remo Manual on the Law of Non-*

---

[233] U.S. Department of Defense, *Law of War Manual*, 1005 (noting a cyber operation not amounting to an "attack" within the meaning of IHL "may be directed at civilians or civilian objects").
[234] Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, entered into force Oct. 21, 1950, 75 UNTS 287 [hereinafter Geneva Convention IV], Article 33; U.S. Department of Defense, *Law of War Manual*, 657.
[235] Additional Protocol II, Article 4(2)(d).
[236] *See* ICRC, *Commentary on Convention (IV) Relative to the Protection of Civilian Persons in Time of War of 12 August 1949* (Geneva: ICRC, 1958), 225 (connecting such measures and acts with collective penalties); ICRC, *Commentary on Additional Protocol II to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) of 8 June 1977* (Geneva: ICRC, 1987), 1375 (noting Article 4(2)(d) is based on Article 33 of Geneva Convention IV and highlighting the broad scope of the prohibition).
[237] ICRC, *Commentary on Convention (IV)*, 225 (noting measures and acts of terrorism could be intended to prevent hostile acts); ICRC, *Commentary on Additional Protocol II*, 1375 (noting acts directed against installations the effects of which could harm protected persons are prohibited).
[238] ICRC, *Customary International Humanitarian Law, Rule 2: Violence Aimed at Spreading Terror Among the Civilian Population*, https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule2.
[239] *Tallinn Manual*, 124.

International Armed Conflict did not expressly state that the relevant prohibition in Additional Protocol II is customary international law.[240]

181. Whether violations of the prohibitions on measures or acts of terrorism involve criminal responsibility in international law has also been debated. As noted above, the ICTY prosecuted individuals for violations of Additional Protocol I's and Additional Protocol II's prohibition on acts or threats of violence primarily intended to terrorize civilians.[241] The ICTY statute did not expressly grant the ICTY the power to prosecute individuals for violating the prohibitions on measures or acts of terrorism in Geneva Convention IV or Additional Protocol II.[242] However, these prohibitions, if part of customary international law, could fall under the "laws and customs of war," violations over which the ICTY has jurisdiction under its statute.

182. The statutes establishing the ICTR and SCSL granted jurisdiction to prosecute individuals for committing "serious violations" of Article 4 of Additional Protocol II, including "acts of terrorism."[243] ICTR case law held that "serious violations" of Article 4 of Additional Protocol II meant that victims suffered "grave consequences," which echoes the requirement for grave consequences caused by acts or threats of violence the primary purpose of which is to spread terror in the civilian population.[244]

183. However, ICTR jurisprudence does not include cases applying "acts of terrorism" in Article 4 of the court's statute. The SCSL prosecuted individuals for acts or threats of violence the primary purpose of which was to spread terror among civilians,[245] but it had no cases involving acts of terrorism under Article 4 of the Additional Protocol II. Thus, neither the ICTR nor the SCSL cases shed light on treating violations of the prohibition on acts of terrorism in Additional Protocol II as a war crime.

184. Although Geneva Convention IV and Additional Protocol II prohibit "measures" or "acts" of terrorism respectively, the status of these prohibitions in customary international law and international criminal law is not clear. In that regard, they are not as well anchored in international law as the narrower prohibition on threats or acts of violence the primary purpose of which is to spread terror in a civilian population. This weaker status might pose problems concerning cyber terrorism during armed conflict. The demanding thresholds in the "threats or acts of violence" rule might make the broader prohibitions in Geneva Convention IV and Additional Protocol II more relevant given the range of potential uses of ICTs in armed conflict.

---

[240] International Institute of Humanitarian Law, *San Remo Manual on the Law of Non-International Armed Conflict with Commentary* (San Remo: International Institute of Humanitarian Law, 2006), 45.
[241] Additional Protocol I, Article 51(2); Additional Protocol II, Article 13(2).
[242] Geneva Convention, Article 33; Additional Protocol, Article 4(2)(d).
[243] ICTR Statute, Article 4; SCSL Statute, Article 3.
[244] *See* Section 4.6.2 (International Criminal Law and Violation of the Prohibition on Acts or Threats of Violence Intended to Spread Terror Among Civilians) *supra*.
[245] Additional Protocol II, Article 13(2).

4.7 Response Assistance, International Law, and Cyber Terrorism

185. Treaties supporting anti-terrorism efforts and facilitating cooperation on cyber crime include obligations to engage in law enforcement assistance. Responses to terrorist incidents can also involve states offering to provide other help to countries that suffer attacks, such as technical assistance and humanitarian aid. Cyber terrorist attacks could also create the need in victim states for assistance, particularly technical help to contain the damage and recover. Serious episodes, such as Estonia experienced in 2007,[246] have forced nations to address the need to provide assistance to victim states. These observations identify the importance of exploring international law on the provision of technical and humanitarian assistance to countries that might experience cyber terrorism.

186. Generally, the anti-terrorism treaties do not impose obligations on states parties to provide assistance outside the law enforcement context. The Nuclear Terrorism Convention permits a state party in possession of radioactive material, device, or nuclear facility involved in an act of nuclear terrorism to "request the assistance and cooperation of other States Parties," which "are encouraged to provide assistance . . . to the maximum extent possible."[247] The Terrorist Bombings Convention does not even include such non-binding exhortations. Further, state practice demonstrates that governments do not believe they are under a customary obligation to provide technical or humanitarian assistance to victims of terrorist attacks.

187. This situation mirrors other contexts in which states provide technical assistance and humanitarian relief, such as after natural disasters. Generally, states have avoided creating binding duties concerning disaster aid because neither victim countries nor assistance-providing nations have wanted to bind themselves.[248] This reality does not mean assistance fails to flow after disasters. Rather, it reveals reluctance by states to use international law to regulate disaster relief. This reluctance explains why advocates for improved disaster relief re-framed the issue in terms of human rights, including the right of disaster victims to receive humanitarian assistance.[249]

188. In terms of assistance after nuclear or industrial accidents, treaties typically require a state party that receives a request for assistance from another state party to consider the request and decide "whether it is in a position to render the assistance required and indicate the scope and terms of the assistance that might be rendered."[250]

---

[246] On the Estonia incident, see Eneken Tikk, Kadri Kask, and Lils Vihul, *International Cyber Incidents: Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence, 2010), 14-34.
[247] Nuclear Terrorism Convention, Article 18(5).
[248] *See, e.g.,* Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations, June 18, 1998, entered into force Jan. 8, 2005, 2296 UNTS 5 (setting up procedures for discretionary requests and provision of telecommunication resources as part of disaster relief). *See generally* David P. Fidler, "Disaster Relief and Governance after the Indian Ocean Tsunami: What Role for International Law?" *Melbourne Journal of International Law* (2005); 6: 458-73.
[249] *Human Rights and Natural Disasters* (Brookings-Bern Project on Internal Displacement, 2008).
[250] Convention on the Transboundary Effects of Industrial Accidents, Mar. 17, 1992, entered into force Apr. 19, 2000, 2105 UNTS 457, Article 12(1); Convention on Assistance in Case of a Nuclear Accident or Radiological Emergency, Sept. 26, 1986, entered into force Feb. 26, 1987, 1457 UNTS 133, Article 2(3).

This type of obligation does not actually require the requested state to provide assistance, just to consider a request and decide whether to help.

189. The lack of international law requiring states to provide assistance after terrorist attacks, natural disasters, or accidents raises problems for using international law for similar purposes in connection with cyber terrorism. One proposal to use international law to create a duty to help victims of serious cyber attacks illustrates these difficulties.[251] First, this proposal was premised on the difficulty of attributing cyber attacks to specific actors, meaning it was not designed as a strategy for responding to cyber terrorism.[252] In addition to the attribution problem, the political nature of terrorist incidents makes states reluctant to commit in advance to legal obligations to provide assistance, as illustrated by the lack of such duties in anti-terrorism treaties.

190. Second, the duty informing the proposal comes from the law of the sea's requirement that ships respond to emergency distress signals from other vessels.[253] This obligation has not served as the basis for assistance obligations in other areas, indicating that states have little interest in using it for different purposes.[254] These questions help explain why the idea for a duty to assist victims of cyber attacks has advanced as a non-binding responsibility rather than a binding obligation.[255]

191. Given these considerations, a norm on providing assistance to victims of serious cyber incidents might be best pursued by distancing the norm from the strategy of responding to cyber terrorism.[256] This approach would avoid the attribution problem, the politics involved in cases of terrorism, and the lack of international legal precedents on the provision of assistance in the anti-terrorism context.

192. The Study Group picks up this idea when examining the strategy of protecting against cyber terrorism, which adopts an "all hazards" approach to cyber threats.[257] This strategy does not require categorizing incidents as cyber terrorism in order for action to be taken. A norm supporting the provision of assistance to victims of cyber attacks, regardless of source, is more likely to gain interest than one triggered by terrorist acts.[258]

---

[251] Duncan Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* (2011); 52: 373-432.
[252] *Ibid.,* 378.
[253] *Ibid.,* 409.
[254] The ITU Constitution requires that ITU member states "give absolute priority to all telecommunications concerning safety of life at sea, on land, in the air or in outer space, as well as to the epidemiological telecommunications of exceptional urgency of the World Health Organization." Article 40. However, this obligation is not a duty to provide emergency assistance as the law of sea requires for vessels in distress.
[255] *See, e.g.,* Duncan Hollis and Tim Maurer, "A Red Cross for Cyberspace," *Time*, Feb. 18, 2015, http://time.com/3713226/red-cross-cyberspace/; Christopher Painter, "The Global Conference on Cyberspace: Putting Principles into Practice," *Council on Foreign Relations Net Politics*, Apr. 23, 2015, http://blogs.cfr.org/cyber/2015/04/23/the-global-conference-on-cyberspace-putting-principles-into-practice/.
[256] *See GGE Report* (2015), ¶ 13(h) (identifying norm that "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts").
[257] *See* Part 5 (International Law and Protecting Against Cyber Terrorism) *infra.*
[258] *See, e.g.,* NATO, *Wales Summit Declaration,* Sept. 5, 2014, ¶¶ 72-73 (discussing alliance cooperation on defending against and responding to cyber attacks, threats, and risks generally).

4.8 International Law and Responding to Cyber Terrorism: Summary of Options for International Legal Action

4.8.1 Better Utilization of Existing International Law

193. States parties to anti-terrorism, cyber crime, organized crime, extradition, and mutual legal assistance treaties could, where appropriate, indicate that these agreements apply to acts of cyber terrorism. Using the offenses and procedures in established treaties to cover cyber terrorism avoids having to amend these instruments. The Security Council could take the same approach and clarify that its counter-terrorism resolutions, especially Resolution 1373 (2001), apply to cyber terrorism.

194. In terms of the multilateral anti-terrorism treaties, the most important agreements to target are the civil aviation safety treaties, the maritime navigation safety agreement, the Terrorist Bombings Convention, and the Nuclear Terrorism Convention. Although these widely ratified treaties do not cover all types of cyber terrorist attacks, harnessing them for responses to cyber terrorism could be an important step for states to take. Bringing cyber terrorism into these treaties would permit states parties to use the treaty processes to cooperate more effectively on this terrorist threat.

195. The Security Council could also facilitate collective action on cyber terrorism by instructing the Counter-Terrorism Committee to focus on the issue and develop mechanisms for information sharing among UN member states about actual or possible cyber terrorist attacks and ways to respond to, protect against, and prevent such attacks.

196. States parties to cyber crime treaties and the TOC Convention can make clear that the offenses and procedures these agreements contain apply to cyber terrorism. However, existing cyber crime treaties, such as the COE Convention, are not, at present, widely ratified, especially compared to the anti-terrorism agreements and the TOC Convention. This fact counsels putting emphasis on multilateral instruments, such as the anti-terrorism treaties and the TOC Convention.

197. Using extradition and mutual legal assistance treaties to strengthen international law on responding to cyber terrorism presents more challenges. These treaties are largely bilateral, which means there are many treaties that are not identical. Thus, an effort to ensure these instruments apply to cyber terrorism faces a patchwork of agreements and political interests that would, in all likelihood, produce fragmented results.

198. In terms of customary international law, the rules on extraterritorial application of domestic criminal law permit the exercise of extraterritorial jurisdiction in connection with crimes associated with cyber terrorism. These rules do not prevent problems from arising when such jurisdiction is exercised, such as the need to use extradition or mutual legal assistance treaties to get custody of suspects or investigate suspected criminal activity. The claim that customary international law recognizes an crime of international

terrorism is controversial, which means that embracing it as part of strengthening existing international law on responses to cyber terrorism might not be worthwhile.

199. Whether international law on the use of force and self-defense provides options for strengthening responses to cyber terrorism is controversial. The use of force by states in responding to terrorism has produced debates about the legality of such responses and disagreements about when the "use of force" and "armed attack" thresholds are triggered and how the principles of immediacy, necessity, and proportionality apply to force used in self-defense against terrorists. Those interested in reducing the ability of states to use force in response to terrorism have to contend with the preference many states have to retain the option to use force. This preference requires maintaining ambiguity and flexibility on when and how states can use force in self-defense against terrorists.

200. Bringing cyber terrorism into this contentious space does not resolve these controversies. In fact, the range of consequences a terrorist group could achieve through ICTs creates incentives for states to retain as much discretion as possible in using, or threatening to use, force (including through cyber means) in response to cyber terrorism. Doubts about the effectiveness of responses to cyber terrorism based in law enforcement approaches reinforce the interest states have in preserving the use-of-force option.

201. In terms of armed conflict, existing treaty and customary international law prohibit acts or threats of violence the primary purpose of which is to spread terror in civilian populations. This ban applies to the use of ICTs. Strengthening this prohibition with cyber terrorism in mind could involve ensuring that a violation of this ban constitutes a war crime. Although the ICTY, ICTR, and SCSL treated violations of this prohibition as a war crime, the Rome Statute does not include such violations in its list of war crimes. Given the importance of the Rome Statute and the ICC in international criminal law, this fact presents an obstacle to making violations of the prohibition a war crime regardless of the technologies used.

202. Treaty law for international and non-international armed conflict also bans measures or acts of terrorism against civilians or persons not taking part in hostilities, and this prohibition applies to the use of any technology, including ICTs. However, whether this ban is customary international law is not settled, nor is it clear whether violations of the prohibition constitute a war crime. Strengthening this prohibition with cyber terrorism in mind requires (1) solidifying how the ban in the relevant treaties applies to the use of ICTs during armed conflict; and (2) encouraging states to support making the ban part of customary international law and violations of it a war crime. Shifting state practice in these directions is likely to prove difficult for many reasons, including the perception that cyber terrorism is not a core concern for IHL when it comes to contemporary international and non-international armed conflict.

4.8.2 Creating New International Law

203. A second option involves adopting new international law to strengthen responses to cyber terrorism. States parties to relevant anti-terrorism treaties, cyber crime

agreements, and the TOC Convention could amend these instruments or adopt protocols to incorporate cyber terrorism into the regimes. This approach would require defining the offense of cyber terrorism and adding any special extradition and law enforcement cooperation procedures needed for investigating and prosecuting this offense.

204. Amending treaties or negotiating new protocols is, however, often difficult, especially compared to the option of clarifying that cyber terrorism already falls within existing agreements. Even if negotiations succeed, the number of countries that accept amendments or join protocols is often fewer than the number of states parties to the main agreement. This pattern suggests that amending the COE Convention or the TOC Convention, or adding protocols to these treaties, in order to address cyber terrorism might not prove an effective strategy.

205. A second possibility is to push for conclusion of the negotiations on the Comprehensive Convention on International Terrorism, which, in its current draft form, would apply to cyber terrorism. However, the prospects for finishing these negotiations are not good, and throwing cyber terrorism into the mix as another reason to conclude this treaty will not transform the stalemate into productive diplomacy.

206. States worried about cyber terrorism could take the issue to the Security Council and seek binding decisions. This idea would follow the precedents the Security Council set in Resolutions 1373 (2001), 1540 (2004), and 2178 (2014). The Security Council could declare cyber terrorism a threat to international peace and security and impose obligations on UN member states to criminalize cyber terrorism, cooperate through sharing information and investigating and prosecuting the crime of cyber terrorism, and reporting to the Counter-Terrorism Committee on steps taken to implement these obligations. Such a Security Council decision would, in effect, achieve many objectives a treaty on cyber terrorism would seek (see below). Whether the Security Council would move in this direction in the absence of serious acts of cyber terrorism is uncertain.

207. Another initiative would involve negotiating a treaty specifically on cyber terrorism. Such a treaty could follow the template established in existing anti-terrorism treaties and include obligations to criminalize the offense of cyber terrorism and to engage in law enforcement cooperation. A cyber terrorism treaty could incorporate mutual legal assistance provisions that address challenges associated with collecting technical and other data needed for effective investigation and prosecution.[259] States concluded the Terrorist Bombings Convention and the Nuclear Terrorism Convention before terrorists had engaged in the offenses these conventions criminalize, which provides precedents for pro-active lawmaking on cyber terrorism.

208. Given controversies with Security Council resolutions imposing binding counter-terrorism obligations,[260] many states might prefer to negotiate a treaty rather than

[259] An alternative to a treaty on cyber terrorism would be a multilateral mutual legal assistance agreement specific to criminal activities in cyberspace, including cyber crime and cyber terrorism.
[260] *See, e.g.,* Daniel H. Joyner, *International Law and the Proliferation of Weapons of Mass Destruction* (Oxford: Oxford University Press, 2009) (arguing Security Council Resolution 1540 was an *ultra vires* act).

leaving cyber terrorism for the Security Council to address. In addition, a treaty on cyber terrorism could include provisions that would not only strengthen responses to cyber terrorism but also help protect against and prevent cyber terrorism.[261]

209. Negotiating treaties can take years. Talks for the Nuclear Terrorism Convention began in 1998 and concluded in 2005. However, UN member states started work on the Terrorist Bombings Convention in 1996 and finished by the end of 1997, indicating that not all treaty negotiations on terrorism become protracted. The prospect of lengthy negotiations is not, in itself, a reason to reject pursuing a treaty on cyber terrorism.

210. The current lack of consensus on what constitutes cyber terrorism would likely make negotiations for a treaty complicated. Some states might use the negotiations for scoring points on other cybersecurity issues, such as cyber espionage and military cyber operations undertaken by governments. The negotiations for the draft Comprehensive Convention on International Terrorism have been adversely affected by controversies about state rather than non-state actions, including military operations during armed conflict. Given the nature of ICTs, their utility for governmental purposes, and political and legal disputes about cyber operations conducted by states, reaching consensus on an approach to cyber terrorism that excludes state behavior will be challenging.

211. Whether states should pursue a treaty on cyber terrorism is a harder question. Although international law on terrorism is largely based in law enforcement approaches, the effectiveness of this strategy is not clear. Anti-terrorism treaties have not prevented terrorism from continuing to be a major problem, exemplified by emergence of Al-Qaeda and then the Islamic State. The weaknesses of traditional approaches are what led policymakers after 9/11 and other major terrorists attacks to emphasize preventing and protecting against terrorism rather than reacting to attacks through criminal law.

212. Similarly, doubts about the effectiveness of cyber crime, extradition, and mutual legal assistance treaties and the TOC Convention have been raised in connection with criminal activities in cyberspace, with concerns ranging from the attribution problem to frustrations with making MLATs work in the timeframes required for investigating cyber crimes. It is not clear how applying the law enforcement approach in these agreements to the cyber terrorism challenge would avoid the problems these treaties have experienced.

213. An alternative strategy would involve the UN taking the lead in preparing a model treaty on combating cyber terrorism. The purpose of such an agreement would be to make available to UN member states an instrument for bilateral or regional cooperation on cyber terrorism. This approach would avoid the problems associated with negotiating a multilateral treaty while providing guidance for states that want to strengthen their policies and practices against cyber terrorist threats.

[261] *See* Part 5 (International Law and Protecting against Cyber Terrorism) and Part 6 (International Law and Preventing Cyber Terrorism) *infra.*

5

INTERNATIONAL LAW AND PROTECTING AGAINST CYBER TERRORISM

5.1 Protecting against Terrorism and Cyber Terrorism through an "All Hazards" Approach

214. Law enforcement strategies grounded in criminal law might deter some terrorist activities and, in this way, protect societies from terrorism. However, policymakers have developed measures to protect against terrorism in ways that do not rely on criminal law. These measures "harden the target" by making it more difficult for terrorists to succeed through (1) protecting targets against attacks; (2) securing dangerous materials from terrorist access; and (3) creating resilience through capabilities to mitigate the impact of attacks and recover from them. This strategy assumes deterrence will fail and terrorists will try to attack. In this context, policymakers need interventions not based in criminal law, and these interventions raise their own national and international legal issues.[262]

215. For terrorism and cyber terrorism, critical infrastructure is at the center of protection strategies.[263] Before 9/11, U.S. policymakers identified the need to protect critical infrastructure from physical and cyber attacks by terrorists.[264] The 9/11 attacks intensified this emphasis,[265] which is also important for many countries.[266] Policy documents often frame the cyber terrorism threat in terms of the vulnerability of critical infrastructure.[267] However, in the cyber realm, critical infrastructure is vulnerable to more than terrorists. Policymakers also worry about foreign governments, malicious insiders, and criminals penetrating ICT-enabled critical infrastructure.[268, 269]

---

[262] *See generally* David P. Fidler, "Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection," *Georgetown Journal of International Affairs* (2015); 8-20.

[263] Internationally, consensus does not exist on what constitutes critical infrastructure. The norm against cyber attacks on critical infrastructure supported by the UN Group of Governmental Experts raised the need for shared understandings of what comprises critical infrastructure. *See GGE Report* (2015), ¶¶ 5, 13(f).

[264] Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*, May 22, 1998.

[265] U.S. Office of Homeland Security, *National Strategy for Homeland Security* (July 2002); White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003).

[266] Counter-Terrorism Committee, *CTED Stresses Need to Protect Critical Infrastructures*, Mar. 23, 2015, http://www.un.org/en/sc/ctc/news/2015-03-23_cted_protect_infrastructure.html.

[267] *See, e.g.,* Organization for Security and Co-Operation in Europe, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace* (2013).

[268] A number of cyber incidents involving critical infrastructure have been linked with foreign governments rather than terrorists. Kim Zetter, "Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired,* Jan. 8, 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (analyzing attack by hackers alleged to be in Russia against a German steel mill that disrupted industrial control systems and damaged the mill); Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, Mar. 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (describing the hacking of Ukrainian electrical stations allegedly by Russian-based persons that caused temporary disruption); Joseph Berger, "A Dam, Small and Unsung, is Caught Up in an Iranian Hacking Case," *New York Times,* Mar. 26, 2016, A15 (reporting on U.S. indictment of persons associated with Iran's Revolutionary Guard for hacking banks and a computer system in a New York dam).

[269] Executive Order, Blocking the Property of Persons Engaging in Significant Malicious Cyber-Enabled Activities (2015). This order came after the United States accused North Korea of launching cyber attacks

216. Given the range of cyber threats to critical infrastructure, the strategy is to strengthen defenses against infiltrations regardless of their source.[270] This "all hazards" approach protects against not only cyber terrorism but also cyber crime and espionage because improving cyber defenses "hardens the target" against multiple threats.

217. Beyond critical infrastructure, policymakers have tried to secure dangerous items from getting into the hands of terrorists, including plastic explosives[271] and biological, chemical, and nuclear materials.[272] Through treaties, states have criminalized terrorism utilizing biological, chemical, and radiological materials,[273] and improving the physical security of these items seeks to protect these and related technologies from terrorist acquisition.[274] Achieving this objective also protects against access by criminals and foreign governments. In this way, the protection strategy guards against a range of threats rather than reacting to only one type of threat.

218. Concerning resilience, counter-terrorism policy stresses the importance of mitigating the consequences of terrorist attacks and recovering rapidly from them.[275] These tasks focus on capabilities beyond law enforcement and the criminal justice system, including emergency management, health care, specialized response capacities (e.g., chemical decontamination), and public communications.

219. Building resilience often involves making capabilities adaptable to different incidents, ranging from accidents to terrorist attacks. Here again is the "all hazards" approach that seeks to produce benefits across a spectrum of threats. Together with stronger defenses, resilience can create deterrent effects, connecting this strategy with the goal of preventing terrorism.

220. The objectives of hardening targets and making them resilient in the event of an incident give protection strategies distinct characteristics. The "all hazards" nature of these strategies means governments do not have to slot threats or incidents into categories in order to define courses of action. Put another way, strengthening cybersecurity does not require identifying whether a potential or actual attack's source is a criminal, foreign intelligence agency, or terrorist. Rather, it requires developing ways to reduce vulnerabilities to unauthorized access and mitigate the consequences of infiltrations that

---

against Sony Entertainment, which—under the U.S. list of critical infrastructure sectors—includes "motion picture studios" within the "commercial facilities sector." U.S. Department of Homeland Security, *Commercial Facilities Sector*, http://www.dhs.gov/commercial-facilities-sector.

[270] *See, e.g.,* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0) (Feb. 12, 2014).

[271] Convention on the Marking of Plastic Explosives for the Purpose of Detection, Mar. 1, 1991, entered into force June 21, 1998, 2122 UNTS 359.

[272] UN Security Council, Resolution 1540 (2004).

[273] Terrorist Bombings Convention.

[274] Convention on the Physical Protection of Nuclear Materials, Mar. 3, 1980, entered into force Feb. 8, 1987, 1456 UNTS 124; Arms Control Association, *Nuclear Security Summit at a Glance*, Apr. 2014, http://www.armscontrol.org/factsheets/NuclearSecuritySummit.

[275] *National Strategy for Homeland Security*, 65-66.

occur. Unlike law enforcement responses, protection measures do not need detailed definitions of criminal offenses that identify predicate actions and specific intentions.

221. Protection strategies move away from the reactive criminal law approach and embrace proactive "due diligence" activities intended to reduce the prospects of harmful events and outcomes.[276] Such activities seek to decrease vulnerabilities and increase capabilities to mitigate damage if adverse events occur.[277] These goals bring to mind areas of international law that contain obligations on states to take steps to protect persons or activities inside or beyond their respective territories from specified harms.[278]

222. Inside a state's territory, due-diligence obligations arise in, among other places, foreign direct investment[279] and human rights.[280] Externally, such duties appear in international environmental law, especially the principle that a state must take steps to prevent activities within its jurisdiction from causing damage in the territory of another state.[281] Often, due-diligence actions involve governments regulating the private sector in order to protect persons within or outside their jurisdictions.[282] International law on economic, social, and cultural rights requires states to protect such rights from being undermined by non-state actors, such as corporations.[283] These approaches are relevant for designing strategies to protect against malicious cyber activities.[284]

223. Obligations similar to due diligence also appear in the international law created by the International Telecommunication Union (ITU). The ITU Constitution requires ITU member states to maintain, safeguard, and prevent disruptions of the channels and

---

[276] *See, e.g.,* Duncan French and Tim Stephens, *Due Diligence in International Law* (First Report of ILA Study Group on Due Diligence in International Law, Mar. 7, 2014); Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," 165-70 (on the duty not to harm the rights of other states).
[277] *See, e.g.,* Robert Knake, *Cleaning Up U.S. Cyberspace* (Council on Foreign Relations Cyber Brief, Dec. 2015), http://www.cfr.org/internet-policy/cleaning-up-us-cyberspace/p37333 (noting importance of the government and private sector working "together to improve cyber hygiene, monitor for infections, and take action when notified of infections").
[278] On the relevance of due diligence obligations in international law to cyberspace, see Robin Geiss and Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention," in *Peacetime Regime for State Activities in Cyberspace*, 621-57, 633-57; Karine Bannelier-Christakis, "Cyber Due Diligence: Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *Baltic Yearbook of International Law* (2014); 14: 23-39; Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum*, June 22, 2015, http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.
[279] French and Stephens, *Due Diligence in International Law*, 6-11.
[280] *Ibid*., 14-22.
[281] *Ibid.*, 24-29. *See also* Thilo Marauhn, "Customary Rules of International Environmental Law—Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?," in *Peacetime Regime for State Activities in Cyberspace*, 465-84.
[282] A related, but separate and more difficult, question is whether non-state actors have due-diligence obligations under international law.
[283] French and Stephens, *Due Diligence in International Law,* 18-21.
[284] *GGE Report* (2015), ¶ 13(c) (identifying norm that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs") and ¶ 17(e) (encouraging states to cooperate "to mitigate malicious ICT activity emanating from their territory").

installations that carry international telecommunications.[285] These duties are particularly important for ITU members in fulfilling their obligation to give priority to all telecommunications concerning safety of life at sea, on land, in the air, or in outer space and to the WHO's urgent epidemiological communications.[286] The ITU Constitution also includes obligations for member states in connection with preventing harmful interference with radio services.[287]

224. Protection strategies are important to explore because much remains to be done to improve cyber defenses against all kinds of threats, and private-sector enterprises need to strengthen their cyber defenses.[288] However, unlike approaches grounded in criminal law, protection strategies have not received as much attention in international law. Despite the policy emphasis on protecting critical infrastructure from terrorism and cyber terrorism, states have developed little international law that specifically supports critical infrastructure protection. This smaller footprint raises questions about whether protection strategies offer opportunities for development of international law on cyber terrorism.

5.2 Critical Infrastructure Protection, International Law, and Cyber Terrorism

5.2.1 Existing International Legal Mechanisms and Critical Infrastructure Protection

225. A cyber terrorist attack against critical infrastructure, however defined, would be illegal and criminal under national criminal laws, including those implementing treaties on cyber crime.[289] Depending on the nature of the attack, the critical infrastructure targeted, and the scale of the impact, it could also constitute an armed attack under international law, triggering the right to use force in self-defense,[290] or it might violate international humanitarian law during armed conflict.[291] But, these bodies of international law define responses to an attack. They do not contain obligations to protect critical infrastructure *before* a cyber attack occurs.

226. When we shift from response to protection, the legal landscape changes. The strategy of protecting critical infrastructure from terrorism has not produced much international law. Generally, efforts to protect critical infrastructure are domestically

---

[285] ITU Constitution, in *Collection of the Basic Texts of the International Telecommunication Union* (Geneva: ITU, 2011), Article 38(2)-(5).
[286] *Ibid.,* Article 40.
[287] *Ibid.*, Article 45.
[288] Robert Knake, "Private Sector and Government Collaboration on Cybersecurity: The Home Depot Model," *Council on Foreign Relations Net Politics*, Mar. 31, 2015, http://blogs.cfr.org/cyber/2015/03/31/private-sector-and-government-collaboration-on-cybersecurity-the-home-depot-model/.
[289] *See* Section 4.4 (Treaties on Cyber Crime, Transnational Organized Crime, Extradition, and Mutual Legal Assistance and Extraterritorial Application of Criminal Law) *supra. See also* Fidler, "Whither the Web?," 10 (arguing "international law outlaws all but one [i.e., espionage] of the cyber threats to critical infrastructure that give policymakers heartburn").
[290] *See* Section 4.5 (The Use of Force in Self-Defense, Sanctions, and Responding to Cyber Terrorism) *supra.*
[291] *See* Section 4.6 (International Humanitarian Law and Responding to Cyber Terrorism during Armed Conflict) *supra.*

focused. Governments can usually improve the security of critical infrastructure within their territories without international cooperation and without using international law.[292]

227. However, national policies increasingly identify cooperation on critical infrastructure protection (CIP), including cyber aspects, as important.[293] Internationally, the UN's Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) has identified the need for increased cooperation on cyber threats to critical infrastructure.[294] Regional organizations, such as the Association of South East Asian Nations (ASEAN),[295] European Union (EU),[296] Organization of American States (OAS),[297] Organization for Economic Cooperation and Development (OECD),[298] all facilitate CIP cooperation. Security organizations, including NATO[299] and the Shanghai Cooperation Organization,[300] devote attention to CIP. Bilateral relations include CIP activities.[301]

228. In April 2015, over forty countries launched the Global Forum for Cyber Expertise (GFCE) to cooperate on cyber capacity-building efforts.[302] Within the GFCE, the U.S. government announced cyber capacity-building initiatives, including a partnership with the African Union.[303] Critical infrastructure protection is one area in which the GFCE will encourage capacity-building efforts.[304] In July 2015, the GGE also stressed the importance of international cooperation to help less developed countries build capacity to protect ICT infrastructure and ICT-dependent critical infrastructure.[305]

---

[292] Fidler, "Whither the Web?," 10. Protection of critical infrastructure from future threats does not, for example, fall within international legal obligations related to settling disputes because protection requires prospective collaboration rather than reactive cooperation after events that threaten peace and security.
[293] *Framework for Improving Critical Infrastructure Cybersecurity*, 4.
[294] *GGE Report* (2013), ¶ 26(e); *GGE Report* (2015) ¶ 13(h).
[295] Caitríona H. Heinl, *Regional Cyber Security: Towards a Resilient ASEAN Cyber Security Regime* (RSIS Working Paper No. 263, Sept. 9, 2013), http://www.rsis.edu.sg/wp-content/uploads/rsis-pubs/WP263.pdf.
[296] European Commission, *Critical Infrastructure*, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm.
[297] OAS, *Critical Infrastructure Protection Programs: Cyber Security*, http://www.oas.org/en/sms/cicte/programs_cyber.asp; Inter-American Committee against Terrorism, *Declaration on Protection of Critical Infrastructure from Emerging Threats*, Mar. 20, 2015, OEA/SER.L/X/2/15 & CICTE/doc.1/15, Mar. 23, 2015.
[298] OECD, *Critical Information Infrastructures Protection*, http://www.oecd.org/sti/ieconomy/ciip.htm.
[299] *Critical Infrastructure Protection* (Matthew Edwards ed.) (NATO Science for Peace and Security Series Vol. 116) (Amsterdam: IOS Press, 2014).
[300] Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security, June 16, 2009, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.
[301] *See, e.g.,* Canada-United States Action Plan for Critical Infrastructure (2010), http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf.
[302] Painter, "The Global Conference on Cyberspace: Putting Principles into Practice."
[303] *Ibid.*
[304] *See, e.g.,* Spain's proposal for a GFCE initiative on protection critical information infrastructure. GFCE, *Report of International Kickoff Meeting 2 & 3 November 2015* (Nov. 15, 2015), 10-11.
[305] *GGE Report* (2015), ¶¶ 19-23.

229. With some exceptions, cooperation on CIP has largely proceeded without the need for, or the creation of, new international law.[306] Cooperation on CIP in the cyber context focuses on encouraging states to strengthen domestic capacities. Beefing up defenses involves identifying effective policies (e.g., creating computer incident or emergency response teams), sharing information, providing assistance, and devoting diplomatic attention to this challenge. This pattern echoes cooperation and international law on the security and safety of facilities using nuclear materials,[307] transboundary pollution,[308] and industrial accidents,[309] which emphasize securing operations, sharing information, providing assistance, and cooperation to enhance protection capabilities.

230. Existing treaties not specific to CIP have proved flexible enough to allow cybersecurity for CIP to become an agenda item. International organizations, treaty regimes, and cooperative mechanisms relevant to critical infrastructure sectors, such as nuclear energy, air and maritime transport, submarine communication cables, and communication satellites, have started to consider cybersecurity within their mandates.

231. The International Atomic Energy Agency (IAEA) developed a Computer and Information Security Programme overseen by its Office of Nuclear Security[310] and included cybersecurity in its *Nuclear Security Plan 2014-2017*.[311] The states parties to the Convention on Nuclear Safety identified cybersecurity as a cross cutting issue.[312] The International Civil Aviation Organization (ICAO) has taken action to address cybersecurity, including adding recommendations on cybersecurity to the annex on security in the Convention on International Civil Aviation.[313] The Facilitation and Maritime Safety Committees of the International Maritime Organization (IMO) "have initiated consideration of cyber security matters[.]"[314] The International Cable Protection Committee, which addresses the security of submarine communication cables, has also

[306] Fidler, "Whither the Web?," 13.
[307] Convention on Nuclear Safety, Sept. 20, 1994, entered into force Oct. 24, 1996, 1963 UNTS 293.
[308] Convention on the Law of the Non-Navigational Uses of International Watercourses, May 21, 1997, entered into force Aug. 17, 2014, UN Doc. A/51/869.
[309] Convention on the Transboundary Effects of Industrial Accidents.
[310] Oszvald Glöcker, *IAEA Coordinated Research Project (CRP) on Cybersecurity of Digital I&C Systems in Nuclear Power Plants*, May 26, 2011, http://www.iaea.org/NuclearPower/Downloadable/Meetings/2011/2011-05-24-05-26-TWG-NPPIC/Day-3.Thursday/TWG-CyberSec-O.Glockler-2011.pdf.
[311] IAEA, *Nuclear Security Plan 2014-2017*, GOV/2013/42-GC(57)/19, Aug. 3, 2013, http://www-ns.iaea.org/downloads/security/nuclear-security-plan2014-2017.pdf.
[312] Sixth Review Meeting of the Contracting Parties to the Convention on Nuclear Safety, *Summary Report*, CNS/6RM/2014/11_Final, Apr. 4, 2014, 6.
[313] Convention on International Civil Aviation, Dec. 7, 1944, entered into force Mar. 5, 1947, ICAO Doc. 7300, Annex 17 (Security). For an overview of ICAO's activities on cybersecurity, see Raymond Benjamin, "Meeting a Global Threat with a Global Response: Aviation's Collaborative and Multidisciplinary Actions on Cybersecurity," *Cyber Security Review* (Autumn 2015): 38-40. *See also* Kaiser and Aretz, "Legal Protection of Civil and Military Activities against Cyber Interference," in *Peacetime Regime for State Activities in Cyberspace*, 325-40 (on civil aviation and cyber interference).
[314] IMO, *Maritime Security*, http://www.imo.org/en/MediaCentre/HotTopics/piracy/Pages/default.aspx.

started to consider cybersecurity issues.[315] The need to strengthen international space law to address cybersecurity threats to satellites has been recognized.[316]

232. The Security Council's Counter-Terrorism Committee has addressed CIP in working with UN member states on implementing Security Council resolutions on terrorism. The Committee's Executive Directorate has emphasized "the urgent need for Member States to protect critical infrastructures."[317] The Committee has included CIP in reviewing member states' implementation of Resolution 1373 (2001).[318]

5.2.2 Treaty Law Specific to Critical Infrastructure Protection

233. Specific treaty law for CIP that has emerged is limited in scope or substance. The EU requires member states to identify "European critical infrastructure" in the energy and transport sectors, provide information about designated infrastructure, and mandate that operators have security plans, including for cyber risks.[319] In December 2015, the European Commission adopted the Network and Information Security Directive, the "first EU-wide legislation on cybersecurity," which requires EU member states to improve their cybersecurity capabilities and operators of essential services (such as energy, transport, banking, health, and digital infrastructure) to adopt "appropriate security measures and report incidents to the national authorities."[320]

234. Members of the Shanghai Cooperation Organization agreed to cooperate on "[e]nsuring information security of critical structures[.]"[321] When it enters into force, the African Union's Convention on Cybersecurity and Personal Data Protection will require each party to adopt a national cybersecurity policy that includes protecting cyber

[315] International Cable Protection Committee, *ICPC Achievements*, July 24, 2015, https://www.iscpc.org/about-the-icpc/achievements/ (reporting on ICPC Chairman's participation in the Worldwide Cyber Security Summit in 2013). On international law and the protection of submarine cables, see Wolff Heintzchel von Heinegg, "Protecting Critical Submarine Cable Infrastructure: Legal Status and Protection of Submarine Communication Cables under International Law," in *Peacetime Regime for State Activities in Cyberspace*, 1-30.
[316] *See* Martha Mejia-Kaiser, "Space Law and Unauthorized Cyber Activities," in *Peacetime Regime for State Activities in Cyberspace*, 349-72, 366-71.
[317] Counter-Terrorism Committee, *CTED Stresses Need to Protect Critical Infrastructures*.
[318] *See, e.g.,* Counter-Terrorism Committee, *Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States,* 64 (noting vulnerabilities facing critical infrastructure in the transportation sector of many states).
[319] Council of the European Union, Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection, Dec. 8, 2008, *Official Journal of the European Union,* L/345/75-L/345/81, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. On EU law and cybersecurity, see Ramses A. Wessel, "Towards EU Cybersecurity Law: Regulating a New Policy Field," in *Research Handbook on International Law and Cyberspace*, 403-25.
[320] European Commission, *Commission Welcomes Agreement to Make EU Online Environment More Secure*, Press Release, Dec. 8, 2015, http://europa.eu/rapid/press-release_IP-15-6270_en.htm.
[321] Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security, Article 3.

infrastructure essential for the functioning of critical infrastructure and imposing more severe sanctions for criminal activities directed against such infrastructure.[322]

235. These general and sector-specific obligations involve binding requirements, which distinguishes them from non-binding activities undertaken in many existing treaty regimes. The examples come from diverse geographical groupings of states and countries with different political interests and levels of economic development. This interest in using international law directly to address cybersecurity challenges in protecting critical infrastructure suggests that more could be done with this approach.

5.2.3 New Norms Supporting Critical Infrastructure Protection

236. As part of efforts to strengthen cybersecurity, norms have been proposed that relate to CIP.[323] The U.S. government has expressed concern that U.S. critical infrastructure is vulnerable to malicious cyber activity undertaken by other countries and non-state actors, and the Commander of U.S. Cyber Command and Director of the NSA stressed the need for "norms or principles for behavior in this space."[324]

237. The U.S. government promoted a norm that countries should not knowingly conduct cyber operations in ways that damage critical infrastructure,[325] and the GGE endorsed this norm in 2015.[326] The U.S. government also promoted a norm that prohibits countries from interfering with activities of computer security incident or emergency response teams because these capabilities are critical to protecting critical infrastructure and responding to incidents.[327] The GGE also backed this norm.[328]

238. At present, proposals and support for such norms usually are in the realm of "soft law" because they are not attached to treaty-making processes and are not the basis for claims the norms are customary international law. Some norms, such as the one against countries knowingly damaging critical infrastructure through cyber operations, are cyber-specific corollaries of existing international legal rules, including the principles on sovereignty and non-intervention and the prohibition on the use of force by states, under which such critical infrastructure-damaging operations are already illegal.[329]

---

[322] AU Convention, Article 24.
[323] Interest in cyber norms exists beyond the issue of CIP. *See, e.g., GGE Report* (2015), ¶ 9 (stressing the importance of identifying "voluntary, non-binding norms for responsible State behaviour and to strengthen common understandings to increase stability and security in the global ICT environment").
[324] Hearing of the House Select Intelligence Committee, "Cybersecurity Threats: The Way Forward," Nov. 20, 2014 (Federal News Service Transcript) (testimony of Admiral Michael Rogers), https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf.
[325] Alex Grigsby, "The UN GGE on Cybersecurity: What is the UN's Role?" *Council on Foreign Relations Net Politics*, Apr. 15, 2015, http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/.
[326] *GGE Report* (2015), ¶ 13(f).
[327] Grigsby, "The UN GGE on Cybersecurity."
[328] *GGE Report* (2015), ¶ 13(k).
[329] Fidler, "Whither the Web?," 17. On the principle of sovereignty and cyberspace, see Benedkt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State*

239. Promoting norms against cyber activities conducted by states that international law already prohibits should not be controversial. These norms reflect the application of general international legal rules to cyber-specific contexts. From that perspective, they are not new norms, which raises questions about why they are being promoted as such rather than as efforts to clarify how existing norms apply in cyberspace. Are the proposed norms designed to address the perceived failure of general international legal rules in the cyber context? If so, how are the proposed norms, which are based on the general rules, going to fare better? Further, proposed norms about state behavior do not address non-state actors that might conduct cyber attacks against critical infrastructure.

5.2.4 Controversy over Revising the International Telecommunication Regulations

240. The ITU Constitution contains a general obligation on ITU member states concerning the maintenance and safeguarding of their international telecommunication facilities.[330] This duty supports protecting such facilities as critical infrastructure. However, negotiations on including a provision specific to security in the revised International Telecommunication Regulations (ITRs), a treaty adopted under ITU auspices, produced controversy.[331] Many ITU member states refused to accept the revised ITRs. In announcing the U.S. government's decision to reject the revised ITRs, the lead U.S. negotiator stated the U.S. government believed "the ITRs are not a useful venue for addressing security issues," and the United States "cannot accede to vague commitment that would have significant implications but few practical improvements on security."[332]

241. This controversy was not about treating ICT-dependent telecommunication networks as critical infrastructure. It had to do with disagreements about Internet governance.[333] The United States and other countries opposed any role for the ITU in Internet governance potentially created by the revised ITRs, including the provision on security. Although this controversy does not preclude the ITU from addressing cyber threats to international telecommunication infrastructures, it suggests ITU efforts on cybersecurity might be fraught with problems.

Activities in Cyberspace, 189-216. On the principle of non-intervention and cyberspace, see Terry D. Gill, "Non-Intervention in the Cyber Context," in *Peacetime Regime for State Activities in Cyberspace*, 217-38.

[330] ITU Constitution, Article 38(2)-(5). On international telecommunications law and cyberspace, see Ian Walden, "International Telecommunications Law, the Internet and the Regulation of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, 261-89.

[331] The provision of the revised ITRs in question is Article 5A, which requires ITU member states to "endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public." ITU, *Final Acts of the World Conference on International Telecommunications* (Dubai, Dec. 3-14, 2012), International Telecommunication Regulations, 6.

[332] Ambassador Terry Kramer, *Remarks on the World Conference on International Telecommunications*, Dec. 13, 2012, http://www.state.gov/e/eb/rls/rm/2012/202040.htm.

[333] *See* Section 2.2 (Internet Governance and Cyber Terrorism) *supra.*

5.2.5 Critical Infrastructure Protection, International Law, and the Private Sector

242. The private sector often operates much of a country's critical infrastructure. International legal obligations on states for protecting critical infrastructure from cyber attacks can be identified. However, due-diligence duties directly applicable to private-sector owners and operators of critical infrastructure do not exist in international law. Treaties relevant to critical infrastructure protection typically require states parties to regulate and hold responsible private-sector actors within their respective jurisdictions.[334] The Study Group has seen no evidence that international law contains direct duties for critical infrastructure operators in the private sector, whether the threat is conventional or cyber terrorism. This situation is consistent with other areas of international law in which due diligence has been analyzed.[335]

5.2.6 Critical Infrastructure Protection and International Law: Summary

243. The integration of cybersecurity into international policies and activities designed to protect critical infrastructure demonstrates this process is important for defending against cyber terrorism. Here, international law plays two roles. First, it provides rules and institutional mechanisms that allow states to focus on cybersecurity and CIP within broader cooperative regimes. Through these efforts, states are producing "soft law" on their responsibilities to improve cybersecurity for critical infrastructure. This soft law informs domestic activities and cooperation in intergovernmental organizations and treaties.[336] Second, states use international law to develop binding obligations for cyber CIP and harmonized approaches to stronger cyber defenses.

244. State practice contains some indications of a nascent cyber-defense norm focused on the responsibility states have to improve cybersecurity as part of protecting critical infrastructure.[337] This norm functions like due-diligence norms in other areas of international law. It emphasizes the need for states to take steps—including regulation of the private sector—to protect activities and persons in their territories from harm and build capacities to mitigate adverse effects that might occur, including cross-border harms. As in other due-diligence contexts, these steps are most effectively carried by engaging the public and private sectors—and ensuring collaboration between them.

---

[334] *See, e.g.,* Convention on Nuclear Safety, Article 9 (providing "[e]ach Contracting Party shall ensure that prime responsibility for the safety of a nuclear installation rests with the holder of the relevant license and shall take appropriate steps to ensure that each such license holder meets its responsibility?).
[335] French and Stephens, *Due Diligence in International Law*, 18-19 (noting that, despite attempts to apply human rights obligations directly to corporations, international law does not contain such obligations).
[336] These efforts also relate to the development of "confidence-building measures." *See GGE Report* (2015), ¶ 16(d)(ii) (identifying the value of "mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure").
[337] *Ibid.*, ¶ 13(g) (identifying norm that "States should take appropriate measures to protect their critical infrastructure from ICT threats").

5.3 Resilience, International Law, and Cyber Terrorism

245. Protection strategies aim to strengthen a government's and society's abilities to mitigate the damage from a terrorist attack and recover from it. Resilience comes from capabilities that permit rapid identification of an attack and its scope, effective control of its consequences, and rapid restoration of the *status quo ante*. Policymakers have stressed the need for resilience across all types of terrorism, but especially with respect to terrorism involving biological, chemical, or radiological materials.

246. States have used international law to support these objectives. For example, the World Health Organization (WHO) revised the International Health Regulations (IHR) in order to strengthen national and international capabilities to identify and manage serious disease events regardless of their source.[338] The IHR require WHO member states to participate in a global disease surveillance system and build and maintain national surveillance and response capacities for serious health incidents, whether the threats result from naturally occurring phenomena, accidents, or terrorist attacks. This "all hazards" approach is designed to have each state possess the ability to mitigate the negative health and social consequences and rapidly return to normality.

247. Similarly, treaties on transboundary industrial and nuclear accidents attempt to strengthen states parties' abilities to control effects from accidents, whatever the cause. For example, the Convention on the Transboundary Effects of Industrial Accidents requires states parties to "take appropriate measures to establish and maintain adequate emergency preparedness to respond to industrial accidents."[339]

248. Cybersecurity experts have identified the need for cyber systems to be resilient when affected by unauthorized intrusions, no matter the source.[340] This theme has been prominent concerning the cyber aspects of CIP.[341] The development by states of computer incident or emergency response capabilities reflects the cyber resilience objective. States could use international law to support cyber resilience by, for example, including resilience in activities supporting the cyber-defense norm discussed above.

5.4 Beyond Critical Infrastructure: Due Diligence, International Law, and Protecting against Cyber Terrorism

249. Although critical infrastructure has received the lion's share of attention, terrorists have attacked targets that are not critical infrastructure. The terrorist attacks in Paris against a satirical publication and a supermarket are examples. Cyber attacks against targets that are not critical infrastructure could also happen with cyber terrorism.

---

[338] World Health Organization, *International Health Regulations (2005)* (Geneva: WHO, 2nd ed., 2008).
[339] Convention on the Transboundary Effects of Industrial Accidents, Article 8(1). *See also* Convention on Nuclear Safety, Article 16.
[340] *See, e.g.,* Symantec, *A Manifesto for Cyber Resilience* (2014), http://www.symantec.com/content/en/us/enterprise/other_resources/b-a-manifesto-for-cyber-resilience.pdf.
[341] Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, Feb. 12, 2013.

250. Protecting computer systems and networks beyond critical infrastructure from cyber terrorism is a daunting challenge. The penetration of ICTs in economies, societies, and individual lives means governments cannot protect all non-governmental activities and must collaborate with the private sector to increase cybersecurity. Such collaboration has proved difficult with cyber crime, a problem the private sector increasingly faces. Attempting to advance these efforts by stressing cyber terrorism confronts problems because private-sector entities probably perceive the likelihood of being attacked by cyber terrorists is remote compared to other cybersecurity risks.

251. Unlike the cyber-defense norm related to CIP, little, if any, state practice reflects that governments believe they have a responsibility under international law to protect their economies and societies broadly from malevolent cyber activities. Moving states in this direction might run into problems, including the diverse abilities of governments to fulfill this responsibility, resistance by states to binding duties to develop and maintain capabilities for cyber due diligence,[342] and the fear that more government involvement in private-sector cybersecurity would threaten privacy, civil liberties, and innovation.

5.5 Securing Dangerous Materials, International Law, and Cyber Terrorism

252. States have used international law to ensure that certain dangerous weapons and materials do not fall into terrorist hands. This law includes treaties on the protection of nuclear materials during international transport[343] and the marking of plastic explosives.[344] Non-proliferation treaties concerning nuclear, biological, and chemical weapons are also considered useful in reducing potential terrorist acquisition of these materials. The Security Council has also imposed obligations on UN member states to prevent terrorists from getting access to nuclear, biological, and chemical materials.[345]

253. How relevant this international law is for protecting against cyber terrorism is not clear. Identifying cyber equivalents of plastic explosives or radiological, chemical, and biological materials is difficult, if not misguided. Some attention has been paid to the potential need to regulate buying and selling of so-called "zero day" software vulnerabilities because terrorists could buy and weaponize them in malware designed to attack critical infrastructure or other targets.[346] However—unlike plastic explosives and radiological, chemical, and biological materials—a zero-day vulnerability is simply information about a software flaw. Restricting access to this type of information is

[342] On capacity building, see Camino Kavanagh, "The UN GGE on Cybersecurity: The Important Drudgery of Capacity Building," *Council on Foreign Relations Net Politics*, Apr. 13, 2015, http://blogs.cfr.org/cyber/2015/04/13/the-un-gge-on-cybersecurity-the-important-drudgery-of-capacity-building/.
[343] Convention on the Physical Protection of Nuclear Materials.
[344] Convention on the Marking of Plastic Explosives for the Purpose of Detection.
[345] UN Security Council, Resolution 1540 (2004).
[346] *See, e.g.,* Paul Stockton & Michele Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law & Policy Review* (2013); 32: 101-28; Michele Golabek-Goldman, *A New Strategy for Reducing the Threat of Dangerous Zero-Day Sales to Global Security and the Economy* (Harvard Kennedy School of Government, Mar. 25, 2014); Mailyn Fidler, "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis," *I/S: A Journal of Law and Policy for the Information Society* (2015); 11: 405-83.

difficult because it is valuable not only to terrorists and criminals but also to software makers, cybersecurity researchers, law enforcement officials, and intelligence agencies.

254. Beyond zero-days, it is not clear how states would use international law to secure dangerous malware from terrorists. The danger with malware arises from the expertise to write and disseminate malevolent code rather than from the code itself, which is not directly threatening to life and property as nuclear, chemical, and biological materials are. Further, malware tailored to attack specific computer systems cannot be easily used against other targets. Efforts to protect against terrorist use of nuclear, chemical, and biological materials include educating scientists on safe, secure, and legal research[347] or providing employment to reduce the possibility that terrorists would buy their expertise.[348] These ideas also do not translate well to the cyber context.

255. The nature of ICTs might require a different approach to "securing materials" that would emphasize reducing (1) cybersecurity vulnerabilities in hardware and software in research, development, and production; and (2) cybersecurity risks created by the ways governments, private-sector organizations, and individuals use cyber products and services. The objective would not be zero tolerance for zero-days but improvements in the security of ICTs and their use throughout production processes and supply chains.[349]

256. This objective would require changes in how hardware and software technologies are developed and how people use them. For example, software manufacturers worldwide are not liable for the security of their products, unlike products in other sectors. However, creating a "culture of cybersecurity" through vendor liability and other strategies would face obstacles, including opposition from powerful companies and collective action problems global application of such strategies would produce.[350]

5.6 Export Controls and Protecting against Cyber Terrorism

257. States use export controls on dual-use technologies to prevent terrorists from obtaining them. For example, the U.S. export control system seeks to prevent supporters of international terrorism from getting biological, chemical, and nuclear materials and technologies.[351] International law can require or support such use of export controls.[352]

---

[347] *See, e.g.,* Committee on Education on Dual Use Issues in the Life Sciences, *Challenges and Opportunities for Education about Dual Use Issues in the Life Sciences* (Washington, D.C.: National Academies Press, 2010).
[348] Richard G. Lugar, "Nunn-Lugar: Science Cooperation Essential for Nonproliferation Efforts," *Science & Diplomacy* (2012), http://www.sciencediplomacy.org/files/nunn-lugar.pdf.
[349] *GGE Report* (2015), ¶ 13(i) (identifying norm that "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products").
[350] *See, e.g.,* Christopher Paul and Isaac R. Porche III, "Toward a U.S. Army Cyber Security Culture," *International Journal of Cyber Warfare and Terrorism* (2011); 1(3): 70-80.
[351] U.S. Department of State, *Overview of Export Control System*, http://www.state.gov/strategictrade/overview/.
[352] *See, e.g.,* UN Security Council, Resolution 1540 (2004).

States often attempt to harmonize export controls on dual-use technologies and monitor their distribution through non-binding regimes, such as the Wassenaar Arrangement.[353]

258. The utility of an export-control strategy for protecting against cyber terrorism is questionable. Countries participating in the Wassenaar Arrangement added certain types of intrusion software and Internet Protocol surveillance systems to the export control list,[354] but this action arose from concerns about authoritarian governments using such software and systems to abuse human rights.[355] Further, the U.S. government's attempt to implement these changes encountered opposition from technology companies and cybersecurity researchers. Google argued that proposed U.S. implementing regulations were "dangerously broad and vague," would "have a significant negative impact on the open security research community," and would damage Google's "ability to defend ourselves, our users, and make the web safer."[356] Such opposition led to the United States to decide to seek further negotiations with its Wassenaar partners on the intrusion software and surveillance system controls.[357]

259. Global dissemination and availability of ICTs and know-how, including black markets for tools and exploits, poses challenges for export control strategies. Counter-terrorism officials worry that terrorists have access to the latest encryption technologies—just one indication of how accessible cyber tools and techniques are.[358] In addition, developing attack capabilities requires computer skills as well as software. Nevertheless, interest by states in export controls to restrict dissemination of malware continues to exist.[359]

---

[353] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, http://www.wassenaar.org/ [hereinafter Wassenaar Arrangement].
[354] Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (13) 1, Dec. 4, 2013.
[355] Edin Omanovic, "A Way Forward to Effectively Regulate the Trade in Surveillance Technology," *Privacy International*, Mar. 24, 2014, https://www.privacyinternational.org/?q=node/464.
[356] Neil Martin and Tim Willis, "Google, the Wassenaar Arrangement, and Vulnerability Research," *Google Online Security Blog*, July 20, 2015, https://googleonlinesecurity.blogspot.com/2015/07/google-wassenaar-arrangement-and.html.
[357] Michael Mimoso, "White House Wants to Renegotiate U.S. Implementation of Wassenaar," *Threat Post*, Mar. 1, 2016, https://threatpost.com/white-house-wants-to-renegotiate-u-s-implementation-of-wassenaar/116531/; Tim Starks, "Back to the Drawing Board on Wassenaar," *Politico*, Apr. 11, 2016, http://www.politico.com/tipsheets/morning-cybersecurity/2016/04/back-to-the-drawing-board-on-wassenaar-hoyer-goes-to-bat-for-administration-on-it-plan-defending-military-grocery-stores-213687.
[358] Andrew Parker, Director General of the Security Service, *Terrorism, Technology, and Accountability: Address to the Royal United Services Institute*, Jan. 8, 2015, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html. *See also* Section 6.5.3 (Preventing Cyber Terrorism, Encryption, and International Law) *infra.*
[359] *See, e.g.,* U.S. Department of Defense, *The DoD Cyber Strategy* (Apr. 2015), 27 (noting the U.S. government "has a range of domestic export control regimes for governing dual-use technologies that can be used to prevent proliferation" of destructive malware).

5.7 Situational Awareness, Civil and Political Rights, and Protection Strategies

260. An "all hazards" protection strategy requires "situational awareness" created by searching for, collecting, and sharing information about threats and vulnerabilities.[360] Identifying malware signatures, intrusion tactics, and good defensive practices and sharing them can increase protective measures against threats in the cyber ecosystem. This threat data often does not include personally identifying information and, thus, raises fewer privacy concerns when collected and shared.[361]

261. However, achieving situational awareness to protect against threats, including terrorism, through surveillance and information sharing between the public and private sectors creates concerns about civil and political rights.[362] Privacy controversies about surveillance and information sharing between the government and private sector have arisen repeatedly with attempts to adopt cybersecurity legislation in the United States, Europe, and other countries. The need for situational awareness also touches international law's recognition of the rights of privacy and freedom of opinion and expression.[363]

262. Even before Edward Snowden began his disclosures of NSA surveillance programs in 2013, human rights advocates were worried about government surveillance of cyber communications. In 2011, the UN's Special Rapporteur on the right to freedom of opinion and expression identified government activities targeting Internet use that "are clearly incompatible with States' obligations under international human rights law, and often create a broader 'chilling effect' on the right to freedom of opinion and expression."[364] These concerns focused on authoritarian governments and informed the "Internet freedom" perspective championed by democratic states.

263. Snowden exposed surveillance activities undertaken by democracies, especially the countries that constitute the so-called "Five Eyes." Snowden's leaks made the "right to privacy in the digital age" a significant issue with the adoption of a UN General Assembly resolution,[365] reports from UN human rights officials,[366] and appointment of a

---

[360] *GGE Report* (2015), ¶ 13(j) (identifying norm that "States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure").
[361] *See e.g.,* Jennifer Granick, "The Right Way to Share Information and Improve Cybersecurity," *Just Security*, Mar. 26, 2015, http://justsecurity.org/21498/share-information-improve-cybersecurity/.
[362] On human rights and cyberspace, see Dinah PoKempner, "Cyberspace and State Obligations in the Area of Human Rights," in *Peacetime Regime for State Activities in Cyberspace*, 239-60.
[363] International Covenant on Civil and Political Rights, Dec. 16, 1966, entered into force Mar. 23, 1976, 999 UNTS 171, Article 17 (privacy) and Article 19 (freedom of opinion and expression).
[364] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/17/27, May 16, 2011, ¶ 26.
[365] UN General Assembly, *Resolution 68/167—The Right to Privacy in the Digital Age*, UN Doc. A/RES/68/167, Dec. 18, 2013.
[366] *The Right to Privacy in the Digital Age: Report of the Office of the UN High Commissioner for Human Rights*, UN Doc. A/HRC/27/37, June 30, 2014; *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UN Doc. A/69/397, Sept. 23, 2014.

special rapporteur on the right to privacy.[367] However, these UN activities do not mean states have reached consensus on how cyber surveillance undertaken for national security reasons affects human rights recognized in international law.

264. Efforts to protect against cyber threats, including cyber terrorism, through an "all hazards" approach confront domestic and international political and legal difficulties associated with increasing surveillance and information sharing while respecting civil and political rights. Unfortunately, disagreements are deep not only between democratic and authoritarian countries but also among and within democracies in contexts where governments have growing security interests in surveillance and information sharing. Acknowledging that international human rights law applies to surveillance and information sharing in protection strategies does not resolve the disagreements that exist.

265. One way to avoid these disagreements is to focus "all hazard" protection strategies (as opposed to law enforcement approaches) on collecting and sharing technical information that does not contain personally identifiable information. Whether states could agree on this approach is, however, questionable. The controversy about information sharing has obstructed progress on cybersecurity legislation in a number of countries, even though the option to focus information sharing on technical data not implicating privacy has been on the table for years. Other countries want to use protection strategies under broad notions of terrorism. Even if states agreed to limit information sharing for "all hazards" protection purposes to technical data, the imperative to prevent terrorism involves the same human rights controversies.[368]

5.8 International Law and Protecting against Cyber Terrorism: Summary of Options for International Legal Action

5.8.1 Better Utilization of Existing International Law

266. Existing international law offers ways to strengthen an "all hazards" approach to protecting against cyber threats, including cyber terrorism. Here, the center of gravity is critical infrastructure protection. States parties to various treaties are moving to protect critical infrastructure by strengthening cyber defenses through cooperative processes in the treaties and other mechanisms. Through these activities, a nascent cyber-defense norm might be emerging that reflects responsibilities states have to protect critical infrastructure from cyber threats and cooperate on achieving this protection. This pattern in bilateral, regional, and multilateral regimes should be encouraged and aided by, among other things, identifying best practices and analyzing challenges these efforts create.

267. One treaty regime where advancing cyber-defense activities related to critical infrastructure would face problems is the ITU. The failure of the ITU's negotiations on revising the ITRs flowed, in part, from inclusion within the revised regulations of a provision on security. Given the extent of this controversy, suggesting that ITU member

[367] Human Rights Council, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/28L.27, Mar. 24, 2015.
[368] *See* Section 6.5 (Surveillance, International Human Rights, and Preventing Cyber Terrorism) *infra.*

states work to strengthen strategies to protect critical communication infrastructures from the range of cyber threats might not be received well.

268. International human rights concerns associated with an "all hazards" cyber defense strategy can be mitigated by focusing information sharing on information that does not contain personally identifiable data. However, the prospects for reducing the tensions between this needed component of an "all hazards" cyber-defense approach and international human rights law are not, at present, good.

5.8.2 Creating New International Law

269. Strengthening cyber defenses for critical infrastructure could form part of a treaty addressing cyber terrorism. Even though the "all hazards" approach does not privilege one threat over another, a treaty on cyber terrorism could support stronger, all-around cyber-defense activities. It could harmonize criminal law and law enforcement cooperation and catalyze improvements in cyber defenses for critical infrastructure, including resilience capabilities.

270. Creating new international law to protect against cyber terrorism through export controls or a strategy of "securing dangerous materials" is not a promising option. The export control regime used to address ICTs, the Wassenaar Arrangement, is not a treaty, and its controls are not binding on participating states. Using treaty law to prevent certain ICTs from falling into terrorist hands would not be effective given the nature of these technologies and their global dissemination.

6

INTERNATIONAL LAW AND PREVENTING CYBER TERRORISM

6.1 Preventing Terrorism and International Law

271. A distinguishing feature of policy on terrorism after 9/11 and other major terrorist attacks was a shift by many governments to strategies designed to prevent terrorism. Response and protection approaches contribute to prevention when they deter terrorist violence, but prevention strategies look beyond criminal law and "harden the target" efforts. Prevention of terrorism connects to general principles of international law that contain duties on states to prevent all forms of violence and conflict.[369]

272. From the prevention perspective, criminal law approaches to terrorism largely guide responses after terrorists strike. Protecting against terrorism is important for prevention, but the protection path remains predominantly passive and, thus, vulnerable to persistent terrorist efforts. By contrast, prevention measures actively seek to find, frustrate, and stop terrorist activities before attacks occur.

273. In general terms, efforts to prevent terrorism involve:

- Expanding intelligence activities to identify terrorists and their planning;
- Cutting off financial support and flows of recruits to terrorist groups;
- Reducing incitement for people to engage in terrorism;
- Undertaking covert or overt actions, including the use of military force, against individuals and/or groups suspected of terrorist activities; and
- Addressing the root causes of terrorism.

274. States have used, or appealed to, international law in pursuing terrorism prevention. After 9/11 and other major terrorist attacks, the UN Security Council adopted resolutions requiring or urging UN member states to take actions to prevent terrorism.[370] Regional organizations adopted treaties with terrorism prevention as an objective.[371]

275. Some prevention strategies generated controversies in international law. Expanded surveillance for counter-terrorism purposes raised international human rights issues before Snowden began his disclosures.[372] Concerns have arisen about efforts to prohibit incitement of terrorism infringing on the freedom of expression.[373] Pre-emptive

[369] Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," 172.
[370] *See* Section 6.3 (Security Council Mandates on Terrorism Prevention and Cyber Terrorism) *infra.*
[371] Inter-American Convention against Terrorism; Council of Europe Convention on the Prevention of Terrorism, May 16, 2005, entered into force June 1, 2007, Council of Europe Treaty Series No. 196.
[372] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (2011).
[373] UN Security Council, *Global Survey of the Implementation by Member States of Security Council Resolution 1624 (2005)*.

or preventive uses of military force against terrorist threats justified under the right to use force in self-defense generated debates about the legality of such actions.[374]

276. Terrorism prevention strategies, and the legal instruments and controversies related to them, are in play when thinking about preventing cyber terrorism. Efforts to prevent terrorist acts, such as using military force against terrorists, could make it more difficult for them to develop and use ICTs to attack. International legal obligations on states to prevent terrorism require prevention of acts of cyber terrorism as well. Finally, features of cyber terrorism exacerbate controversies in the relationship between international law and terrorism prevention.

6.2 Defining Terrorism and Preventing Terrorism

277. The strategy of preventing terrorism requires a definition of terrorism to guide prevention activities. Countries have failed to agree on a definition of terrorism,[375] but this problem has not deterred states and the Security Council from creating international legal obligations on terrorism prevention.

278. In terms of what terrorism means, the prevention strategy is generally grounded in the offenses contained in the anti-terrorism treaties. Security Council resolutions on terrorism prevention emphasize the importance of UN member states joining these instruments.[376] Treaties emphasizing terrorism prevention adopted after 9/11 also use the anti-terrorism treaties to define what states parties mean by terrorism.[377]

279. However, problems experienced with terrorism prevention demonstrate that states do not necessarily restrict their understanding of terrorism to the offenses found in the anti-terrorism treaties. UN human rights bodies have raised concerns that some states have vague and broad anti-incitement laws, creating the potential for non-violent political speech and advocacy to be treated as incitement to terrorism—a problem "complicated by differences of view regarding the definition of the term 'terrorism' itself."[378]

280. Analyzing prevention strategies in connection with cyber terrorism reinforces the importance of the Study Group's working definition of cyber terrorism. This definition tracks how states have defined terrorist offenses in the anti-terrorism treaties.[379] This affinity facilitates using terrorism prevention strategies found in international law to think about preventing cyber terrorism. Definitional proximity permits interpreting obligations on states to prevent terrorism to include duties to prevent cyber terrorism.[380]

---

[374] *See, e.g.,* Arend, "International Law and the Preemptive Use of Military Force," 89-103.
[375] See Section 3.1 (Defining "Terrorism" and International Law) *supra.*
[376] UN Security Council, Resolution 1373 (2001), Resolution 1624 (2004), and Resolution 2178 (2014).
[377] Inter-American Convention against Terrorism, Article 2; Council of Europe Convention on the Prevention of Terrorism, Article 1 and Appendix.
[378] UN Security Council, *Global Survey of the Implementation by Member States of Security Council Resolution 1624 (2005)*, ¶ 91.
[379] *See* Section 3.2 (Considerations in Defining Cyber Terrorism) *supra.*
[380] *See* Section 6.3 (Security Council Mandates on Terrorism Prevention and Cyber Terrorism) and Section 6.4 (Terrorism Prevention in Treaty Law and Preventing Cyber Terrorism) *infra.*

281. However, this approach does not eliminate potential definitional problems and questions related to cyber terrorism in the context of prevention. None of the existing anti-terrorism treaties in force expressly applies to cyber terrorism, which requires scrutinizing these treaties to see whether they can be interpreted as applicable to cyber terrorism.[381] With terrorism prevention strategies centered on the offenses found in the anti-terrorism treaties, the importance of being able to apply these treaties to cyber terrorism becomes apparent, as it did with response strategies. Problems with this approach again raise the potential need to adopt a treaty specifically on cyber terrorism.

282. Concerns about terrorism prevention strategies covering more than the offenses in the anti-terrorism treaties are also important in thinking about preventing cyber terrorism. Here, two problems converge in a way that creates controversy. First, human rights advocates worry that many states define and use terrorism prevention as a way to infringe on rights that international law protects, such as freedom of expression.

283. Second, terrorist exploitation of the Internet to communicate, spread propaganda, recruit, and raise funds creates pressure for terrorism prevention policies to target a broad range of activities in cyberspace. This dynamic explains why some definitions of "cyber terrorism" include terrorist use of the Internet for purposes other than damaging property or harming people. The need to address terrorist uses of the Internet places additional stress on tensions between terrorism prevention and respect for human rights in international law.

6.3 Security Council Mandates on Terrorism Prevention and Cyber Terrorism

284. The Security Council has adopted resolutions that required or encouraged UN member states to take actions to prevent terrorism and acts related to terrorism. Resolution 1373 (2001) contains a number of mandates, including preventing the financing of terrorist acts,[382] suppressing recruitment of members for terrorist groups, preventing the movement of terrorists across borders, and taking steps to prevent the commission of terrorist acts (such as providing early warning information to other states). In Resolution 1624 (2005), the Security Council called on UN member states to prohibit incitement to commit terrorist acts, prevent such conduct, and deny safe haven to any persons guilty of incitement. In Resolution 2178 (2014), the Security Council required UN member states to prevent and suppress recruiting, organizing, transporting, and equipping individuals who travel to participate in terrorist acts in other states.

285. None of the Security Council's resolutions relevant to the prevention of terrorism mentions cyber terrorism.[383] The Security Council's Counter-Terrorism

[381] *See* Section 4.2 (Anti-Terrorism Treaties) *supra.*
[382] *See also* Terrorist Financing Convention.
[383] Nor has the Security Council demonstrated much interest in the emergence of cyber threats to international peace and security. Janos Ferencz, "Powers of the Security Council to Make Determinations under Article 39 of the Charter in Case of Cyber Operations," *Opinio Juris*, Aug. 10, 2015, http://opiniojuris.org/2015/08/10/emerging-voices-powers-of-the-security-council-to-make-determinations-under-article-39-of-the-charter-in-case-of-cyber-operations/.

Committee has also not focused on cyber terrorism. Its survey of UN member states' implementation of Resolution 1373 (2001) does not contain information specifically about cyber terrorism.[384] The Committee's survey on the implementation of Resolution 1624 (2005) reflected concerns with use of the Internet to engage in incitement of terrorism but contained nothing about cyber terrorism as defined by the Study Group.[385]

286. Nevertheless, these Security Council resolutions are relevant to prevention of cyber terrorism in two ways. First, the resolutions encompass the offenses in the anti-terrorism treaties. As analyzed earlier,[386] terrorists could commit some of these offenses through using ICTs. In those cases, prevention measures undertaken pursuant to Security Council resolutions should also address cyber means and methods of terrorism.

287. Second, the resolutions do not limit terrorism prevention to the offenses in the anti-terrorism treaties. While this broader scope creates controversy, use of ICTs to cause death, injury, or damage to property with the intent to spread fear or compel behavior constitutes terrorism within the meaning of the resolutions. As defined in this report, cyber terrorism is terrorism of the kind the Security Council has declared a threat to international peace and security.

288. For the Study Group, the Security Council's mandates and calls for preventive actions can readily be interpreted to apply to cyber terrorism and acts related to such terrorism. Resolution 1373 (2001)'s mandates cover efforts to finance, support, or facilitate acts of cyber terrorism. Resolution 2178 (2014)'s requirements on preventing and suppressing terrorist recruitment apply to attempts to recruit persons skilled in ICTs. Resolution 1624 (2005)'s call to prohibit and prevent incitement to commit terrorist acts covers incitement to commit acts of cyber terrorism.

289. Reading Security Council resolutions on terrorism prevention as applicable to cyber terrorism would be helped if UN member states expressly supported this approach. This support could arise through the Counter-Terrorism Committee's work overseeing implementation of Security Council resolutions on terrorism.

6.4 Terrorism Prevention in Treaty Law and Preventing Cyber Terrorism

290. In 2005, the Council of Europe adopted the Convention on the Prevention of Terrorism as part of the post-9/11 emphasis on preventing terrorism. Like the Council of Europe's Convention on Cybercrime, the Convention on the Prevention of Terrorism is important in this area of policy concern.[387] This treaty requires states parties to take

---

[384] Counter-Terrorism Committee, *Global Survey of the Implementation of Security Council Resolution 1373 by Member States* (2011).
[385] Counter-Terrorism Committee, *Global Survey of the Implementation by Member States of Security Council Resolution 1624 (2005)*.
[386] *See* Section 4.2 (Anti-Terrorism Treaties) *supra.*
[387] Council of Europe, *Action against Terrorism: Convention on Prevention of Terrorism (CETS No. 196)*, http://www.coe.int/t/dlapil/codexter/Overview_196_en.asp (noting the Convention was the first treaty to criminalize public provocation to commit terrorism, recruitment for terrorism, and training for terrorism).

appropriate actions to prevent the terrorist offenses found in the anti-terrorism treaties while respecting human rights.[388] It requires states parties to:

- Make public provocation to commit a terrorist offense, recruitment for terrorism, and training for terrorism criminal offenses in national law;[389]
- Take jurisdiction over these offenses;[390]
- Investigate allegations these offenses have been committed;[391] and
- Extradite or prosecute any person alleged to have committed these offenses.[392]

291. Unlike the Security Council resolutions, the scope of the Convention on the Prevention of Terrorism is restricted to the offenses found in the anti-terrorism treaties. The offenses the Convention requires states parties to criminalize—provocation, recruitment, and training—are legally defined to include the offenses in the anti-terrorism treaties. Thus, this treaty does not explicitly cover cyber terrorism.

292. The treaty could apply if, for example, a person attempted to recruit or train a software programmer to use ICTs to commit any offense established in the anti-terrorism treaties, such as unlawful acts against civil aviation or nuclear terrorism. If the UN adopted a treaty on cyber terrorism and it entered into force, the Convention on the Prevention of Terrorism could be amended to include the offenses in it.[393]

293. The Council of Europe adopted a protocol to the Convention on the Prevention of Terrorism in October 2015.[394] This protocol supports the obligations the Security Council imposed in Resolution 2178 (2014) on preventing and suppressing terrorist recruitment. The protocol makes "a number of acts, including taking part in an association or group for the purpose of terrorism, receiving terrorist training, travelling abroad for the purposes of terrorism and financing or organising travel for this purpose, a criminal offence" and "provides for a network of 24-hour-a-day national contact points facilitating the rapid exchange of information."[395]

294. Despite global interest in preventing terrorism, the Convention on the Prevention of Terrorism only has 35 parties a decade after it was adopted, and no non-members of the Council of Europe have ratified it.[396] Given that protocols often have fewer parties than the main treaties, the new protocol might have fewer parties than the

[388] Council of Europe Convention on the Prevention of Terrorism, Articles 1-3 and Appendix.
[389] *Ibid.,* Articles 5-7.
[390] *Ibid.*, Article 14.
[391] *Ibid.*, Article 15.
[392] *Ibid.*, Article 18.
[393] *Ibid.,* Article 28.
[394] Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Oct. 22, 2015, not in force, Council of Europe Treaty Series No. 217.
[395] Council of Europe, *Details of Treaty No. 217*, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217.
[396] Council of Europe, *Convention on the Prevention of Terrorism: Status of Ratification* (as of July 31, 2016), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=196&CM=1&DF=&CL=ENG.

Convention.[397] Such limited participation perhaps counsels against seeing the Convention, or one modeled on it, as helpful for preventing cyber terrorism. Prevention measures of the type included in this treaty could, instead, be built into a treaty designed to address cyber terrorism as a specific form of terrorism.

6.5 Surveillance, International Human Rights, and Preventing Cyber Terrorism

6.5.1 Preventing Terrorism, Surveillance, and International Human Rights Law

295. Human rights inform terrorism prevention because terrorism threatens human rights that governments have international legal obligations to protect.[398] Preventing terrorism requires gathering and sharing information relevant to identifying terrorists and their activities. The incentive to prevent terrorism led to expanded surveillance and information-sharing powers for intelligence and law enforcement agencies in the domestic law of many countries after 9/11 and other major terrorist attacks.

296. The emergence of the Islamic State as a dangerous terrorist group that exploits the Internet in its operations has reinforced how critical surveillance activities are to counter-terrorism. Implementing the Security Council's resolution on ending the flow of foreign fighters to terrorist groups requires serious intelligence collection and sharing—within and among countries—to identify and interdict individuals who might be preparing to join foreign terrorist groups.[399]

297. The move into expanded surveillance by many countries demonstrated their belief that terrorism prevention, among other considerations, is a legitimate reason for undertaking surveillance under international human rights law. The UN High Commissioner for Human Rights acknowledged that surveillance for terrorism prevention was legitimate in evaluating the impact of surveillance on privacy protected by the International Covenant on Civil and Political Rights.[400]

298. However, human rights advocates have expressed concerns about encroachment of counter-terrorism surveillance on the rights to freedom of opinion and expression, freedom of assembly, and privacy protected by international law. Snowden's revelations exacerbated tensions between expansive surveillance powers, counter-terrorism efforts, and human rights.[401] Although the NSA and other agencies conducted surveillance for reasons beyond counter-terrorism, the objective of preventing terrorism has been, and remains, a core rationale for NSA surveillance.

---

[397] As of this writing, the protocol has been ratified by one member state of the Council of Europe. Council of Europe, *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism: Status of Ratification* (as of July 31, 2016), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217/signatures?p_auth=Ulw9Oecg.

[398] *See, e.g.,* Office of the UN High Commissioner for Human Rights, *Human Rights, Terrorism and Counter-Terrorism*, 7.

[399] UN Security Council, Resolution 2178 (2014).

[400] *The Right to Privacy in the Digital Age: Report of the Office of the UN High Commissioner for Human Rights*, ¶ 24.

[401] *See* Section 5.7 (Situational Awareness, Civil and Political Rights, and Protection Strategies) *supra.*

299. Although international human rights law recognizes terrorism prevention as a legitimate reason for surveillance, conducting surveillance for this purpose has to comply with domestic and international law's requirements, including that the surveillance not constitute arbitrary or unlawful interference with privacy.[402] As controversies triggered by Snowden show, how these requirements apply reveals disagreements among states, particularly with respect to mass and/or extraterritorial surveillance activities.

300. Post-Snowden reports by UN human rights officials asserted mass surveillance can constitute arbitrary interference with privacy because it can create discriminatory and disproportionate impacts on privacy relative to the contribution surveillance makes to counter-terrorism.[403] The officials also argued that international human rights law applies to surveillance states undertake outside their territories.[404] As commentators noted, these interpretations do not reflect the ways in which many governments interpret international law or how governments actually engage in domestic or foreign surveillance.[405]

301. Although nothing new, gaps between statements by UN human rights officials and state behavior signal entrenched problems. Before Snowden, UN human rights efforts raised concerns about governments using counter-terrorism to engage in domestic surveillance that violated international human rights law.[406] The attention generated by Snowden does not appear to have had an impact on this problem. Human Rights Watch criticized a new Chinese counter-terrorism law because it would establish "a total digital surveillance architecture subject to no legal or legislative control" that was inconsistent "with international law and the protection of human rights."[407]

302. After Snowden, UN human rights officials identified problems with foreign surveillance conducted for counter-terrorism purposes. These efforts have not, to date, stimulated major changes in the countries Snowden's disclosures highlighted, especially the United States and the United Kingdom. Changes made by the United States, such as according the privacy interests of foreign nationals approximately the same treatment as U.S. persons, did not rely on, or even refer to, international human rights law.[408] More

---

[402] International Covenant on Civil and Political Rights, Article 17.
[403] *The Right to Privacy in the Digital Age: Report of the Office of the UN High Commissioner for Human Rights*, ¶ 25 (asserting "[m]ass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime"); *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶ 12 (arguing "mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether").
[404] *Report of the Office of the UN High Commissioner for Human Rights*, ¶¶ 31-36.
[405] *See, e.g.,* Peter Margulies, "Sweeping Claims and Casual Legal Analysis in the Latest U.N. Mass Surveillance Report," *Lawfare*, Oct. 20, 2014, http://www.lawfareblog.com/2014/10/sweeping-claims-and-casual-legal-analysis-in-the-latest-u-n-mass-surveillance-report/.
[406] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (2011), ¶ 26.
[407] Human Rights Watch, *China—Draft Counterterrorism Law a Recipe for Abuses: Major Overhaul Needed for Law to Conform with International Legal Obligations*, Jan. 20, 2015, http://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses.
[408] Presidential Policy Directive/PPD-28 on Signals Intelligence Activities, Jan. 17, 2014.

recent terrorist attacks, such as those in Paris in November 2015, San Bernardino in December 2015, Brussels in March 2016, and Orlando in June 2016 have produced renewed interest in expanded government surveillance powers for counter-terrorism.[409]

6.5.2 Preventing Cyber Terrorism, Surveillance, and International Human Rights Law

303. The imperative associated with undertaking surveillance for terrorism prevention purposes exists for cyber terrorism. Preventing cyber terrorism produces incentives for intrusive surveillance. First, cyber terrorism is unlikely to exist without some connection to other terrorist activities, which means surveillance for counter-terrorism is part of surveillance for preventing cyber terrorism. Second, timeframes for preventing cyber terrorism might be shorter than for kinetic terrorism because the former might have a smaller, harder-to-identify operational "footprint" than the latter.

304. Thus, efforts to prevent cyber terrorism do not escape the controversies associated with applying international human rights law to surveillance for terrorism prevention. Cyber terrorism does not contain unique elements that provide ways to close the gap between what international human rights law requires (according to UN human rights officials) and how states conduct surveillance for counter-terrorism purposes. Cyber terrorism is likely to be connected with other terrorist activities, so attempting to cabin off cyber terrorism for *sui generis* human rights consideration in the context of terrorism prevention is not credible, nor does it have a basis in international law.

305. Given the present lack of cyber terrorism as defined by the Study Group, the human rights controversies about surveillance for terrorism prevention are, at the moment, abstract. However, a major cyber strike by terrorists would undoubtedly trigger demands for more surveillance to prevent future acts of cyber terrorism. Then, the arguments about how international human rights law applies to heightened surveillance to prevent terrorism would play out again, and probably no more productively than they have in the wake of major conventional terrorist attacks.

6.5.3 Preventing Cyber Terrorism, Encryption, and International Law

306. In 2016, tension between the use of encryption to protect digital communications and counter-terrorism efforts became a major issue. Although intelligence and law enforcement concerns about terrorist use of encryption had already

[409] Andrea Peterson and Brian Fung, "Paris Attacks Should be 'Wake Up Call' for More Digital Surveillance, CIA Director Says," *Washington Post*, Nov. 16, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/11/16/paris-attacks-should-be-wake-up-call-for-more-digital-surveillance-cia-director-says/; Tom McCarthy, "Surveillance Must Increase after Terror Attacks, Say 2016 Candidates," *The Guardian*, Dec. 6, 2015, http://www.theguardian.com/us-news/2015/dec/06/paris-attacks-san-bernardino-shooting-surveillance-hillary-clinton-donald-trump-election; Missy Ryan, "Brussels Attacks Rekindle Privacy vs. Security Debate in Europe," *Washington Post*, Mar. 26, 2016, https://www.washingtonpost.com/world/europe/brussels-attacks-rekindle-privacy-vs-security-debate-in-europe/2016/03/26/60a68558-f2dc-11e5-a2a3-d4e9697917d1_story.html ; Steven T. Dennis, "Republicans Seek Wider FBI Surveillance Power after Orlando," Bloomberg," June 14, 2016, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217/signatures?p_auth=Ulw9Oecg.

emerged, the U.S. government's attempt to force Apple, Inc. to bypass encryption on an iPhone used by one of the perpetrators of the San Bernardino attacks generated controversy.[410] This controversy involved many features, but it reinforced worries that terrorist use of encryption would adversely affect efforts to prevent terrorist attacks.[411] For example, encrypted communications can complicate surveillance of terrorist activities, make cyberspace "go dark" for counter-terrorism efforts, and, thus, undermine the critical role surveillance plays in terrorism prevention. Not everyone agreed with government warnings about the impact of encryption on surveillance of digital communications,[412] but the issue became too prominent to ignore.

307. The encryption controversy has global scope, with countries beyond the United States grappling with the implications of encryption for counter-terrorism.[413] International lawyers also had to address the issue, with the most prominent discussion occurring in international human rights law. For example, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression argued that "[e]ncryption and anonymity . . . provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."[414]

308. Although not focused on cyber terrorism as defined by the Study Group, the encryption controversy is relevant for preventing all forms of terrorist activity, including terrorist exploitation of cyberspace.[415] However, at present, consensus about how to address encryption in counter-terrorism is lacking within and across countries. Linking encryption with the rights of privacy and the freedoms of opinion and expression connects encryption with the existing frictions between surveillance for counter-terrorism and respect for human rights under international law discussed above.

6.6 Use of Military Force, International Law, and Preventing Cyber Terrorism

309. Efforts to prevent terrorism include governments using military force to disrupt imminent attacks (anticipatory self-defense) or emerging threats (preventive or pre-emptive self-defense). The controversies associated with such military strikes against

---

[410] The U.S. government terminated its litigation against Apple when it managed to find a way to access the contents of the iPhone in question with the help of a third party. Kevin Parrish, "FBI Drops Its Fight with Apple over Shooter's Recovered iPhone 5C," *Digital Trends,* Mar. 28, 2016, http://www.digitaltrends.com/mobile/fbi-apple-vacate/.

[411] Tom Risen, "Eyes on Obama as FBI, Congress Blast Encryption: Law Makers Decry Encryption as a Venue for Terrorist Planning," *U.S. News & World Report*, Dec. 10, 2015, http://www.usnews.com/news/articles/2015/12/10/eyes-on-obama-as-fbi-congress-blast-encryption.

[412] *See, e.g,* Berkman Center for Internet & Society, *Don't Panic: Making Progress on the "Going Dark" Debate* (Feb. 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[413] *See, e.g.,* Amar Toor, "French Law Would Fine Apple if It Does Not Hand Over Encrypted Data in Terror Cases," *The Verge*, Mar. 4, 2016, http://www.theverge.com/2016/3/4/11160044/france-apple-encryption-terrorism-law.

[414] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/29/32, May 22, 2015, ¶ 56.

[415] For example, encrypted communications could make it harder for intelligence and law enforcement officials to identify and understand attempts by terrorist groups to use the Internet to radicalize individuals.

terrorists include their compatibility with international law on the use of force and self-defense, the law of armed conflict, and international human rights law on extrajudicial killing.[416] International law permits the use of force against imminent terrorist attacks, but controversy surrounds using force against emerging terrorist threats as preventive self-defense. While international law on the use of force against imminent terrorist attacks or emerging terrorist threats can be readily described, a UN special rapporteur cautioned that "the question of which framework applies, and the interpretation of aspects of the rules, have been the subject of significant debate."[417]

310. Inserting cyber terrorism into this debate requires analyzing two scenarios—the use of kinetic force and the use of cyber force to prevent an imminent attack or emerging threat of cyber terrorism. The use of kinetic force to prevent cyber terrorism would agitate the debate, especially whether (1) the cyber threat justifies the use of lethal force in self-defense; and (2) the use of kinetic force is disproportionate to the cyber threat. If the use of kinetic force cannot be justified under the right of self-defense, then those ordering the use of force could be accused of extrajudicial killing in violation of international human rights law.

311. Applying these bodies of international law would require information about the threat prevented (e.g., was the thwarted attack likely to cause death or injuries?), but, as with conventional terrorism, the state launching the preventive strike is unlikely to make such classified information available. This lack of transparency, combined with skepticism that many cyber threats would warrant use of lethal force to prevent, would make the justifications of anticipatory self-defense or, if accepted as permitted by international law, pre-emptive self-defense harder to sustain.

312. However, countries that believe use of kinetic force to prevent terrorism is legitimate are not likely to renounce this option because terrorists might attack with ICTs. Those who believe preventive kinetic strikes violate international law might be more opposed to such strikes against threats of cyber terrorism. The international legal debate about the preventive use of force against terrorism would continue unabated.

313. The other scenario involves using cyber operations to prevent imminent acts, or an emerging threat, of cyber terrorism.[418] Preventive cyber attacks might not raise questions about the proportionality of force used in self-defense or extrajudicial killing when they do not result in, or could not foreseeably cause, death, injury, or substantial property damage. Being able to avoid the controversies that the use of kinetic force to prevent cyber terrorism would generate provides incentives to develop "active cyber defense" capabilities in order to gather actionable intelligence and launch preventive cyber strikes.

---

[416] *See, e.g., Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions: Study on Targeted Killings*, UN Doc. A/HRC/14/24/Add.6, May 28, 2010.
[417] *Ibid.*, ¶ 36.
[418] Offensive cyber capabilities to undertake such cyber attacks are rapidly developing. In 2016, the United States disclosed that it was conducting offensive cyber attacks against the Islamic State as part of the armed conflict being waged against this group. *See* David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, Apr. 25, 2016, A1.

314. However, these incentives should be kept in perspective. Terrorists already so extensively use the Internet for communications, recruiting, propaganda, and fundraising that states supportive of preventive strikes against terrorists have ample national security reasons for developing capabilities to monitor and disrupt cyber-based terrorist activities.

6.7 Root Causes of Terrorism, International Law, and Preventing Cyber Terrorism

315. Preventing terrorism is often linked with the need to address its root causes. This idea has been prominent in efforts to counter violent extremism.[419] Despite the frequency with which root causes are raised, what these causes are remains subject to debate. The diverse contexts in which terrorism arises and the disparate motivations individuals have for turning to terrorism make the search for root causes complex, difficult, and prone to go well beyond legal instruments. Solutions offered for root causes, such as "improve human rights" or "generate economic opportunities for the disenfranchised," often overlook all the failed efforts to achieve these objectives.

316. International law applicable to preventing terrorism often does not include duties to address the root causes of terrorism.[420] Obligations in international law relevant to root causes, such as international human rights law, do not necessarily take on heightened legal importance or become more effective because states want to prevent terrorism.

317. Thus, a root-causes approach to cyber terrorism is not likely to be productive. Debates about root causes do not disappear when terrorism is preceded by the word "cyber." The Islamic State's use of the Internet and social media underscores how difficult identifying root causes can be when cyber elements come into play. The Islamic State's cyber media operations are sophisticated and global, meaning this terrorist movement attracts cyber-literate adherents from different parts of the world to participate in violent extremism that rejects Western modernity. At the moment, this phenomenon is 'a riddle wrapped in a mystery inside an enigma.'

6.8 International Law and Preventing Cyber Terrorism: Summary of Options for International Legal Action

6.8.1 Better Utilization of Existing International Law

318. Strategies for preventing terrorism have generated consensus and controversy in international law. In terms of consensus, the international legal rules developed to prevent financing of terrorism, other forms of support for terrorist activities, incitement to commit

[419] *See, e.g.,* White House, *Fact Sheet: The White House Summit on Countering Violent Extremism*, Feb. 18, 2015, https://www.whitehouse.gov/the-press-office/2015/02/18/fact-sheet-white-house-summit-countering-violent-extremism; Liang, *Cyber Jihad: Understanding and Countering Islamic State Propaganda.*

[420] *But see* ASEAN Convention on Counter Terrorism, Article VI(2) (providing that "[s]ubject to the consent of the Parties concerned, the Parties shall cooperate to address the root causes of terrorism and conditions conducive to the spread of terrorism to prevent the perpetration of terrorist acts and the propagation of terrorist cells").

terrorism, and the flow of foreigners to terrorist groups emerged from multilateral treaty negotiations and Security Council resolutions. Although not adopted to address cyber terrorism, this international law can be interpreted to apply to cyber terrorism without amending these instruments.

319. The best strategy for utilizing existing international law in this way is to focus on the Security Council resolutions that impose obligations or urge action concerning terrorism prevention, namely Resolutions 1373 (2001), 1624 (2005), and 2178 (2014). The Counter-Terrorism Committee could work with the Security Council to make clear that the resolutions cover cyber terrorism as a threat to international peace and security.[421] In hewing closely to how states have previously defined terrorist offenses, the Study Group's definition of cyber terrorism would support this approach.

320. To make use of the Council of Europe's Convention on the Prevention of Terrorism and its new protocol, the existing anti-terrorism treaties that define the Convention's scope would have to be interpreted to cover cyber terrorism.[422] Otherwise, applying this Convention and its protocol to cyber terrorism would require adoption of a treaty on cyber terrorism.

321. Controversies have arisen with terrorism prevention in connection with intelligence activities' impact on human rights law and the use of force against terrorists justified as anticipatory self-defense or, more problematically, pre-emptive self-defense. Efforts to prevent cyber terrorism will not reduce the interest in surveillance seen in terrorism prevention strategies, and there is nothing about cyber terrorism suggesting that concerns about surveillance based in human rights law will dissipate. Debates about the legality of preventive strikes against imminent or emerging threats of cyber terrorism will only lessen if states conduct them through cyber operations rather than kinetic weapons.

322. In these two contexts, it is difficult to identify credible suggestions for better utilization of existing international law in relation to cyber terrorism. The main controversies involve fundamental political and legal disagreements about what the law means and how it applies when the objective is the prevention of terrorism.

6.8.2 Creating New International Law

323. Here, two courses of action are worth considering. First, the Security Council could adopt a resolution on the prevention of cyber terrorism that creates binding obligations and/or urges UN members to take action. The Security Council adopted the resolutions on terrorism prevention discussed above in response to terrorist activity, including the 9/11 attacks and the rise of the Islamic State. Convincing the Security Council to be pro-active on cyber terrorism without a signature incident would be difficult, but a call for such a resolution could still help bring attention to the issue.

[421] This coverage would also inform reading the Terrorist Financing Convention as applying to the financing of cyber terrorism.
[422] *See* Section 4.2 (Anti-Terrorism Treaties) *supra*.

324. Second, the objective of preventing cyber terrorism could be included in a treaty addressing this form of terrorism. This report previously identified a specific treaty on cyber terrorism as a potential strategy for strengthening responses to cyber terrorism and efforts to protect countries from such terrorism.[423] Such a treaty could include prevention as an objective as well, which would make the instrument comprehensive in terms of policy approaches to cyber terrorism. Preventing cyber terrorism could also be an objective of additional protocols to existing treaties that address terrorism or cyber crime.

[423] *See* Section 4.8 (International Law and Responding to Cyber Terrorism: Summary of Options for International Legal Action) and Section 5.8 (International Law and Protecting against Cyber Terrorism: Summary of Options for International Legal Action) *supra.*

7

CONCLUSIONS

7.1 The Report and the Study Group's Objectives

325. The Study Group had four objectives:

- Examine the potential threat of cyber terrorism;
- Develop a definition of "cyber terrorism";
- Produce and analyze an inventory of international law potentially relevant to cyber terrorism; and
- Assess whether pro-active international legal actions concerning cyber terrorism would be worthwhile and feasible.

326. The Study Group believes it has achieved these objectives, and it summarizes its findings in this concluding part.

7.1.1 Examine the Potential Threat of Cyber Terrorism

327. The Study Group noted the perceived gap between warnings about cyber terrorism and the general and episodic international legal attention paid to this problem. Policy concerns about terrorists attacking with ICTs continued as the Study Group worked on this report, but the ongoing lack of incidents of cyber terrorism (as defined in this report) remains an issue. By contrast, terrorist use of the Internet to communicate, spread propaganda, and recruit members became an even more pressing problem because of the rise of violent extremist groups, such as the Islamic State, and their extensive use of cyberspace for multiple purposes.[424]

328. It remains plausible that terrorist groups will develop the motivation and capabilities to engage in cyber attacks, but, since the Study Group started its work, no "game changing" technological or other development has transformed the plausible into the probable. Cyber incidents associated with terrorist groups, such as the one involving CENTCOM claimed by the Islamic State's Cyber Caliphate, have not revealed technological sophistication indicating a threshold has been crossed. However, some experts believe the Islamic State's use of the Internet, and its purported recruiting of computer experts, portends a potential shift towards cyber attack capabilities.

329. This context creates problems for pro-active international legal action to address cyber terrorism because, in the absence of actual incidents, creating political and diplomatic traction to address a speculative threat is more difficult.

---

[424] *See, e.g.,* Counter-Terrorism Committee, Special Meeting of the Counter-Terrorism Committee and Technical Sessions of the Counter-Terrorism Committee Executive Directorate on Preventing and Combating Abuse of ICT for Terrorist Purposes, Dec. 16-17, 2015, http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html.

7.1.2 Develop a Definition of Cyber Terrorism

330. The Study Group developed a working definition of cyber terrorism to guide its analysis.[425] The Study Group's definition tracks how states and international organizations have defined terrorism in other contexts, particularly in the definition of offenses in anti-terrorism treaties. Having a definition that shares features with existing international law has advantages, such as (1) facilitating strategies to utilize international legal instruments and mechanisms more effectively; (2) centering potential law-making activities on familiar ground; and (3) avoiding political and human rights controversies broader concepts of terrorism create.

7.1.3 Identify and Analyze International Law Potentially Relevant to Cyber Terrorism

331. The report identifies and assesses a significant amount of international law that is potentially relevant to responding to, protecting against, and preventing cyber terrorism. The report is not an exhaustive analysis because the Study Group did not consider in detail, for example, every regional anti-terrorism or cyber crime treaty. However, the review was sufficiently comprehensive to inform the Study Group's thinking about what actions might strengthen international law's contribution to addressing cyber terrorism.

332. The international law examined is not evenly distributed across the response, protect, and prevent strategies. States have developed more international law relevant to responding to terrorism—largely through application of criminal law and law enforcement approaches—than for protecting against and preventing terrorist acts. This heavier "footprint" on the response strategy contrasts with post-9/11 policy emphases on protection against and prevention of terrorism.

7.2 Assessment of Potential Actions to Strengthen International Law on Cyber Terrorism

333. In its analysis of international law relevant to cyber terrorism under the response, protection, and prevention strategies, the Study Group summarized potential options for international legal action.[426] The report divided these options into strategies for better utilization of existing international law and for creation of new international law. Here, the Study Group identifies what it believes are the most feasible options for strengthening international law on cyber terrorism.

[425] *See* Section 3.3 (The Study Group's Working Definition of Cyber Terrorism) *supra*.
[426] *See* Section 4.8 (International Law and Responding to Cyber Terrorism: Summary of Options for International Legal Action), Section 5.8 (International Law and Protecting against Cyber Terrorism: Summary of Options for International Legal Action) and Section 6.8 (International Law and Preventing Cyber Terrorism: Summary of Options for International Legal Action) *supra.*

7.2.1 Better Utilization of Existing International Law

334. Across the response, protection, and prevention strategies, the report identified possibilities for applying existing international legal rules, instruments, and mechanisms to cyber terrorism. The best approaches involve states (1) interpreting offenses contained in certain anti-terrorism treaties as applicable to cyber terrorism; (2) reading Security Council resolutions on terrorism to cover cyber terrorism; and (3) using processes established in treaties or Security Council resolutions (e.g., the Counter-Terrorism Committee) to bolster protection of critical infrastructure and societies in general against cyber attacks. Potentially the most promising of these options is for states parties to exploit existing treaty regimes related to improve critical infrastructure protection against cyber attacks. This approach is being adopted in multilateral regimes on nuclear energy, civil aviation, and maritime transport and could be expanded and accelerated.

335. Even though these approaches do not create new international law, they would require states to incorporate cyber terrorism within the scope of different treaties and Security Council resolutions. States would need sufficient incentives to undertake such efforts, and the lack of cyber terrorist incidents weakens this strategy's political pull. Uneven political interest could produce only patchwork progress on these options.

7.2.2 Creating New International Law

336. The Study Group identified a number of possibilities for creating new international law. Parties to existing treaties potentially relevant to cyber terrorism could amend the agreements, or adopt protocols to them, to bring this issue formally into these regimes. The Beijing Convention and Protocol adopted by ICAO reflect this strategy, but it could be used with other anti-terrorism treaties, including the Terrorist Bombings Convention and the Nuclear Terrorism Convention. Similarly, parties to the Council of Europe's Convention on Cyber Crime, Convention on the Prevention of Terrorism, or similar regional agreements could adopt cyber-terrorism protocols. The UN could draft model treaties on cyber terrorism that states could use to strengthen bilateral or regional cooperation against cyber terrorism.

337. However, working across different treaty regimes would, in all likelihood, produce fragmented results that do not coherently or consistently raise the profile of cyber terrorism in international law. A more unified, systematic strategy would involve (1) negotiating a treaty on cyber terrorism that included provisions on responding to, protecting against, and preventing acts of such terrorism; and/or (2) the Security Council's adoption of a resolution requiring UN member states to address cyber terrorism response, protection, and prevention in the same way the Security Council has done for terrorism generally and terrorism linked to biological, chemical, and nuclear materials.

7.3 Recommendations for the International Law Association

338. In submitting this report, the Study Group has completed its task for the ILA. Based on its work, the Study Group makes the following recommendations to the ILA:

- Amend the Study Group's mandate and extend the timeline for its work to the end of 2018, create a new study group, or establish an ILA committee on terrorism and cyberspace to prepare for the consideration of states, international organizations, and non-state experts:

    1) A multilateral convention on responses to, protection against, and prevention of cyber terrorism;
    2) A model treaty for bilateral or regional purposes on improving cooperation on combatting cyber terrorism;
    3) A model protocol for existing anti-terrorism and cyber crime treaties that specifically addresses cyber terrorism; and/or
    4) A resolution by the Security Council on cyber terrorism.

    Through such activities, the ILA could develop documents that states, international organizations, and non-governmental experts might find useful in thinking about the role and functions of international law in addressing the intersections between ICTs and terrorism. This type of activity is within the scope of ILA's work because ILA bodies have produced draft conventions and instruments that influenced the progressive development of international law.[427]

- Amend the Study Group's mandate, create a new study group or groups, or establish an ILA committee on terrorism and cyberspace to examine:

    1) International law and the use of the Internet and ICTs by terrorist groups for communications, propaganda, raising funds, and recruitment;
    2) The relationship between international law and Internet governance in connection with terrorist use of the Internet; and
    3) The threshold for engaging state responsibility under international law specifically in connection with cyber attacks by state and non-state actors.

* * *

[427] *See, e.g.,* the drafting by the ILA Committee on Cultural Heritage of the Buenos Aires Draft Convention on the Protection of Underwater Cultural Heritage, "which served as the model for the UNESCO Convention of the same name, now in force[.]" ILA, *Cultural Heritage Law*, http://www.ila-hq.org/en/committees/index.cfm/cid/13.

ANNEX

DEFINITIONS OF "CYBER TERRORISM"

This Annex contains various definitions of "cyber terrorism," and one of "information terrorism," from dictionaries, experts, and governmental and intergovernmental sources.

Dictionary Definitions:

- *Merriam Webster Dictionary*: "Terrorist activities intended to damage or disrupt vital computer systems."
- *Oxford English Dictionary*: "The politically motivated use of computers and information technology to cause severe disruption or widespread fear."

Expert Definitions:

- Mark M. Pollitt (1998): Cyber terrorism involves "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[428]
- Dorothy Denning (2000): "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples."[429]
- Gabriel Weimann (2005): "Cyberterrorism is the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)."[430]
- William L. Tafoya (2011): Cyber terrorism involves "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information."[431]

[428] Mark M. Pollitt, "Cyberterrorism—Fact or Fancy?'" *Computer Fraud & Security* (1998); 2 (February): 8-10.
[429] Dorothy E. Denning, Testimony before the Special Oversight Panel on Terrorism of the Committee on Armed Services, U.S. House of Representatives, May 23, 2000, http://fas.org/irp/congress/2000_hr/00-05-23denning.htm.
[430] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?," *Studies in Conflict & Terrorism* (2005); 28:129-49.
[431] William L. Tafoya, "Cyber Terror," *FBI Law Enforcement Bulletin* (Nov. 2011), https://leb.fbi.gov/2011/november/cyber-terror.

Governmental and Intergovernmental Definitions:

- U.S. National Infrastructure Protection Center (2001): Cyber terrorism is "a criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a political, social or ideological agenda."[432]

- Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (2008):

  > 2. Information terrorism.
  >
  > This threat emanates from terrorist organizations and individuals involved in terrorist activities acting unlawfully through information resources against regarding them. It is characterized by the use of information networks by terrorist organizations to carry out terrorist activities and recruit new supporters; destructive impact on information resources leading to disruption of public order; control or blocking of mass media channels; use of the Internet or other information networks for terrorist propaganda, creating an atmosphere of fear and panic in the society, as well as other negative impacts on the information resources.[433]

- NATO (2008): Cyber terrorism is "a cyber attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal."[434]
- South Africa (2011): Cyber terrorism "means use of internet based attacks in terrorist activities by individuals and groups, including acts of deliberate large scale disruptions of computer networks, especially computers attached to the internet, by the means of tools such as computer viruses."[435]
- Austria (2013): "Cyber terrorism is defined as a politically motivated crime of state and / or non-state actors against computers, networks and the information stored therein. Its aim is to provoke a severe or long-term disruption of public life or to cause serious damage to economic activity with the intention of severely intimidating the population, of forcing public authorities or an international organisation to carry out, tolerate or omit an act or of profoundly unsettling or destroying the political, constitutional, economic or social foundations of a state

[432] U.S. National Infrastructure Protection Center, "Cyberterrorism: An Evolving Concept," *NIPC Highlights*, http://www.nipc.gov/publications/highlights/2001/highlight-01-06.htm.
[433] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Annex 2.
[434] NATO, *Cyber Defence Concept* MC0571 (2008).
[435] NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Terrorism*, https://ccdcoe.org/cyber-definitions.html.

or an international organisation. These acts constitute organised cyber sabotage (attacks) caused by political-fundamentalist groups or individual perpetrators; they are directed against states, organisations or enterprises."[436]

Cyber Terrorism Offenses in National Criminal Law:

- India's Information Technology Act, Section 66F:

(1) Whoever, —

(A) with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant [e.g., malware] and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that is is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified in section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Who commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.[437]

- Pakistan's Prevention of Electronic Crimes Ordinance:

17. Cyber terrorism.—

[436] *Ibid.*
[437] India, Information Technology Act, Section 66F, http://cis-india.org/internet-governance/resources/section-66f-of-the-i-t-act-2000.

(1) Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be accessed a computer or computer network or electronic system or electronic device or by any available means, and thereby knowingly engages in or attempts to engage in a terroristic act commits the offence of cyber terrorism.

Explanation l.—For the purposes of this section the expression "terroristic intent" means to act with the purpose to alarm, frighten, disrupt, harm, damage, or carry out an act of violence against any segment of the population, the Government or entity associated therewith.

Explanation 2.—For the purposes of this section the expression "terroristic act" includes, but is not limited to,—

(a) altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness, or death to any segment of the population;

(b) transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity;

(c) aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the commission of such act of violence is actually completed; or

(d) stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any form of chemical, biological or nuclear weapon, or any other weapon of mass destruction.

(2) Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life, and with fine and in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten-million rupees, or with both.[438]

[438] Pakistan, Prevention of Electronic Crimes Ordinance, https://www.unodc.org/res/cld/document/pak/2009/prevention_of_electronic_crimes_ordinance_html/2014_Pakistan_ordinance_on_electronic_crimes_2009.pdf.

BIBLIOGRAPHY

Treaties (in chronological order)

Convention on International Civil Aviation, Dec. 7, 1944, entered into force Mar. 5, 1947, ICAO Doc. 7300.

Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, entered into force Oct. 21, 1950, 75 UNTS 287.

Convention on Offences and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, entered into force Dec. 4, 1969, 704 UNTS 219.

International Covenant on Civil and Political Rights, Dec. 16, 1966, entered into force Mar. 23, 1976, 999 UNTS 171.

Vienna Convention on the Law of Treaties, May 23, 1969, entered into force Jan. 27, 1980, 1155 UNTS 332.

Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, entered into force Apr. 14, 1971, 860 UNTS 105.

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Sept. 23, 1971, entered into force Jan. 26, 1973, 974 UNTS 177.

Organization of American States Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance, Feb. 2, 1971, OAS Treaty Series No. 37.

Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, Dec. 14, 1973, entered into force Feb. 20, 1977, 1035 UNTS 167.

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, entered into force Mar. 26, 1975, 1015 UNTS 164.

European Convention on the Suppression of Terrorism, Jan. 27, 1977, entered into force Aug. 4, 1978, Council of Europe Treaty Series No. 90.

Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, entered into force Feb. 20, 1977, 1035 UNTS 167.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, entered into force Dec. 7, 1978, 1125 UNTS 3.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, entered into force Dec. 7, 1978, 1125 UNTS 604.

International Convention against the Taking of Hostages, Dec. 17, 1979, entered into force June 3, 1983, 1316 UNTS 205.

Convention on the Physical Protection of Nuclear Materials, Mar. 3, 1980, entered into force Feb. 8, 1987, 1456 UNTS 124.

Convention on Assistance in Case of a Nuclear Accident or Radiological Emergency, Sept. 26, 1986, entered into force Feb. 26, 1987.

South Asian Association for Regional Cooperation (SAARC) Regional Convention on Suppression of Terrorism, Nov. 4, 1987, entered into force Aug. 22, 1988, http://saarc-sec.org/areaofcooperation/detail.php?activity_id=21.

Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, entered into force Aug. 6, 1989, 1589 UNTS 474.

Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, entered into force Mar. 1, 1992, 1678 UNTS 201.

Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, entered into force Mar. 1, 1992, 1678 UNTS 304.

Convention on the Marking of Plastic Explosives for the Purpose of Detection, Mar. 1, 1991, entered into force June 21, 1998, 2122 UNTS 359.

Convention on the Transboundary Effects of Industrial Accidents, Mar. 17, 1992, entered into force Apr. 19, 2000, 2105 UNTS 457, Article 12(1);, 1457 UNTS 133

Convention on Nuclear Safety, Sept. 20, 1994, entered into force Oct. 24, 1996, 1963 UNTS 293.

Convention on the Law of the Non-Navigational Uses of International Watercourses, May 21, 1997, entered into force Aug. 17, 2014, UN Doc. A/51/869.

International Convention for the Suppression of Terrorist Bombings, Dec. 15, 1997, entered into force May 23, 2001, 2149 UNTS 256.

Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations, June 18, 1998, entered into force Jan. 8, 2005, 2296 UNTS 5.

Rome Statute of the International Criminal Court, July 17, 1998, entered into force July 1, 2002, UN Doc. A/CONF.183/9.

Arab Convention on the Suppression of Terrorism, Apr. 22, 1998, http://www.refworld.org/docid/3de5e4984.html.

Treaty on Cooperation among the States Members of the Commonwealth of Independent States in Combating Terrorism, June 4, 1999, http://www.refworld.org/docid/47fdfb290.html.

Convention of the Organization of the Islamic Conference on Combating International Terrorism, July 1, 1999, http://www.oic-oci.org/english/convenion/terrorism_convention.htm.

Organization of African Unity Convention on the Prevention and Combating of Terrorism, July 1, 1999, entered into force Dec. 6, 2002, http://www.au.int/en/treaties/oau-convention-prevention-and-combating-terrorism.

International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, entered into force Apr. 10, 2002, 2178 UNTS 197.

UN Convention against Transnational Organized Crime, Nov. 15, 2000, entered into force Sept. 29, 2003, 2225 UNTS 209.

Commonwealth of Independent States (CIS) Agreement on Cooperation in Combatting Offenses Related to Computer Information, June 1, 2001, http://itlaw.wikia.com/wiki/Agreement_on_Cooperation_Among_the_States_Members_of_the_Commonwealth_of_Independent_States_in_Combating_Offences_Relating_to_Computer_Information.

Shanghai Convention against Terrorism, Separatism, and Extremism, June 15, 2001, entered into force Mar. 29, 2003, http://www.refworld.org/docid/49f5d9f92.html.

Agreement on Cooperation Among States Members of the Commonwealth of Independent States in Combating Offenses Relating to Computer Information, June 1, 2001, entered into force Mar. 14, 2002.

Convention on Cybercrime, Nov. 23, 2001, entered into force July 1, 2004, Council of Europe Treaty Series No. 185.

Agreement between the United Nations and the Government of Sierra Leone on the Establishment of a Special Court for Sierra Leone, January 16, 2002, https://www.icrc.org/ihl.nsf/b0d5f4c1f4b8102041256739003e6366/65cb6be7caca532cc1256c1d0027f549?OpenDocument.

Inter-American Convention Against Terrorism, June 3, 2002, entered into force July 10, 2003, http://www.oas.org/juridico/english/treaties/a-66.html.

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Jan. 1, 2003, entered into force Mar. 1, 2006, Council of Europe Treaty Series No. 189.

Convention of the Cooperation Council for the Arab States of the Gulf on Combating Terrorism, 2004, https://www.unodc.org/tldb/en/regional_instruments.html.

International Convention for the Suppression of Acts of Nuclear Terrorism, Apr. 13, 2005, entered into force July 7, 2007, 2445 UNTS 89.

Council of Europe Convention on the Prevention of Terrorism, May 16, 2005, entered into force June 1, 2007, Council of Europe Treaty Series No. 196.

ASEAN Convention on Counter Terrorism, Jan. 13, 2007, entered into force May 11, 2011, http://www.asean.org/news/item/asean-convention-on-counter-terrorism.

Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security, June 19, 2009, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, ICAO Doc. 9960, not in force.

Protocol Supplemental to the Convention for the Suppression of Unlawful Seizure of Aircraft, Sept. 10, 2010, ICAO Doc. 9959, not in force.

Arab Convention on Combating Information Technology Offences, Dec. 21, 2010, entered into force 2014, http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences.

ITU Constitution, in *Collection of the Basic Texts of the International Telecommunication Union* (Geneva: ITU, 2011), 3-56.

African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, not in force, EX.CL/846 (XXV).

Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Oct. 22, 2015, not in force, Council of Europe Treaty Series No. 217.

Cases (in chronological order)

International Court of Justice. *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda),* I.C.J. Reports 2005 (Merits).

International Criminal Tribunal for the Former Yugoslavia (Appeals Chamber). *Prosecutor v. Galić*, Case No. IT-98-29-A, 30 Nov. 30, 2006.

Special Court for Sierra Leone. *Prosecutor v. Fofana and Kondewa,* Case No. SCSL-04-14-A, Judgment on Appeal, May 28, 2008.

International Criminal Tribunal for the Former Yugoslavia . *Prosecutor v. Dragomir Milošević*, Case No. IT-98-29/1-A, Judgement, Nov. 12, 2009.

Special Tribunal for Lebanon (Appeals Chamber). *Interlocutory Decision on the Applicable Law*, STL-11-01/I, Feb. 16, 2011.

In re Warrant to Search Certain Email Accounts Controlled & Maintained by Microsoft Corp., 15 F.Supp.3d 466 (S.D.N.Y 2014).

International Criminal Tribunal for the Former Yugoslavia. *Prosecutor v. Radovan Karadžić*, Case No. IT-95-5/18-T, Judgment, Mar. 24, 2016.

In re Warrant to Search Certain Email Accounts Controlled & Maintained by Microsoft Corp., U.S. Court of Appeals for the Second Circuit, Docket No. 14-2985, July 14, 2016, http://digitalconstitution.com/wp-content/uploads/2016/07/Decision-opinion.pdf.

Governmental and Intergovernmental Documents and Publications

18 U.S.C. § 2332b(a)(1) and (g)(5) (acts of terrorism transcending national boundaries; definition of the "federal crime of terrorism") (United States).

Canada-United States Action Plan for Critical Infrastructure (2010), http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf.

Computer Fraud and Abuse Act, 18 USC § 1030 *et seq* (United States).

Council of Europe. *Action against Terrorism: Convention on Prevention of Terrorism (CETS No. 196)*, http://www.coe.int/t/dlapil/codexter/Overview_196_en.asp.

_____. *Additional Protocol to the Convention on Cybercrime Status* (as of June 24, 2016), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG.

_____. *Additional Protocol to the Convention on the Prevention of Terrorism: Status of Ratification* (as of June 24, 2016), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217/signatures?p_auth=Ulw9Oecg.

_____. *Convention on Cybercrime Status* (as of June 24, 2016), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=20/02/2015&CL=ENG.

_____. *Convention on the Prevention of Terrorism: Status of Ratification* (as of June 24, 2016), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=196&CM=1&DF=&CL=ENG.

Council of Europe Committee of Experts on Terrorism (CODEXTER). *Opinion for the Committee of Ministers on Cyberterrorism and the Use of Internet for Terrorist Purposes,* 2008, http://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf.

Council of Europe Counter-Terrorism Task Force. *Cyberterrorism—The Use of the Internet for Terrorist Purposes* (Strasbourg: Council of Europe Publishing, 2007).

Council of the European Union. Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection, Dec. 8, 2008, *Official Journal of the European Union,* L/345/75-L/345/81, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

Denning, Dorothy E. Testimony before the Special Oversight Panel on Terrorism of the Committee on Armed Services, U.S. House of Representatives, May 23, 2000, http://fas.org/irp/congress/2000_hr/00-05-23denning.htm.

European Commission. *Commission Welcomes Agreement to Make EU Online Environment More Secure*, Press Release, Dec. 8, 2015, http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

_____. *Critical Infrastructure*, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm.

Executive Order. Imposing Additional Sanctions with Respect to North Korea, Jan. 2, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea.

Executive Order. Blocking the Property of Certain Persons Engaged in Significant Malicious Cyber-Enabled Activities, Apr. 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

Global Forum for Cyber Expertise. *Report of International Kickoff Meeting 2 & 3 November 2015* (Nov. 15, 2015).

Glöcker, Oszvald. *IAEA Coordinated Research Project (CRP) on Cybersecurity of Digital I&C Systems in Nuclear Power Plants*, May 26, 2011, http://www.iaea.org/NuclearPower/Downloadable/Meetings/2011/2011-05-24-05-26-TWG-NPPIC/Day-3.Thursday/TWG-CyberSec-O.Glockler-2011.pdf.

Koh, Harold Hongju (Legal Advisor, U.S. Department of State). *International Law in Cyberspace, Remarks to USCYBERCOM Inter-Agency Legal Conference*, Sept. 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm.

Hearing of the House Select Intelligence Committee. "Cybersecurity Threats: The Way Forward," Nov. 20, 2014 (Federal News Service Transcript), https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf.

Human Rights Council. *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/28L.27, Mar. 24, 2015.

India. Information Technology Act, Section 66F, http://cis-india.org/internet-governance/resources/section-66f-of-the-i-t-act-2000.

Inter-American Committee against Terrorism. *Declaration on Protection of Critical Infrastructure from Emerging Threats*, Mar. 20, 2015, OEA/SER.L/X/2/15 & CICTE/doc.1/15, Mar. 23, 2015.

International Atomic Energy Agency. *Nuclear Security Plan 2014-2017*, GOV/2013/42-GC(57)/19, Aug. 3, 2013, http://www-ns.iaea.org/downloads/security/nuclear-security-plan2014-2017.pdf.

International Cable Protection Committee. *ICPC Achievements*, July 24, 2015, https://www.iscpc.org/about-the-icpc/achievements/.

International Civil Aviation Organization. *Current Lists of Parties to Multilateral Air Law Treaties*,

http://www.icao.int/secretariat/legal/Lists/Current%20lists%20of%20parties/AllItems.aspx.

_____. Administrative Package for Ratification of or Accession to the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention, 2010), http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf.

International Law Commission. *Responsibility of States for Internationally Wrongful Acts*, UN General Assembly Resolution 56/83, Dec. 12, 2001, annex.

International Maritime Organization. *Maritime Security*, http://www.imo.org/en/MediaCentre/HotTopics/piracy/Pages/default.aspx.

International Telecommunication Union. *Final Acts of the World Conference on International Telecommunications* (Dubai, Dec. 3-14, 2012).

Kramer, Terry (U.S. Ambassador). *Remarks on the World Conference on International Telecommunications*, Dec. 13, 2012, http://www.state.gov/e/eb/rls/rm/2012/202040.htm.

Lamb, Robert D. *Ungoverned Areas and Threats from Safe Havens: Final Report of the Ungoverned Areas Project* (Washington, D.C.: Office of the Under Secretary of Defense for Policy, 2008).

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0) (Feb. 12, 2014).

National Science Advisory Board for Biosecurity*, Framework for Conducting Risk and Benefit Assessments of Gain-of-Function Research: Recommendations of the National Science Advisory Board for* Biosecurity (May 2016).

NATO. *Cyber Defence Concept* MC0571 (2008).

_____. *Wales Summit Declaration,* Sept. 5, 2014.

NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Terrorism*, https://ccdcoe.org/cyber-definitions.html.

Office of the UN High Commissioner for Human Rights. *Human Rights, Terrorism, and Counter-Terrorism*, Fact Sheet No. 32, 2008, http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf.

Organization of American States. *Critical Infrastructure Protection Programs: Cyber Security*, http://www.oas.org/en/sms/cicte/programs_cyber.asp.

Organization for Economic Cooperation and Development. *Critical Information Infrastructures Protection*, http://www.oecd.org/sti/ieconomy/ciip.htm.

Organization for Security and Co-Operation in Europe, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace* (2013).

_____. *OSCE Anti-Terrorism Reference* (Feb. 2015), http://www.osce.org/secretariat/99765.

Pakistan. Prevention of Electronic Crimes Ordinance, https://www.unodc.org/res/cld/document/pak/2009/prevention_of_electronic_crimes_ordinance_html/2014_Pakistan_ordinance_on_electronic_crimes_2009.pdf

Parker, Andrew (Director General of the Security Service). *Terrorism, Technology, and Accountability: Address to the Royal United Services Institute*, Jan. 8, 2015, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html.

Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*, May 22, 1998.

Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, Feb. 12, 2013.

Presidential Policy Directive/PPD-28 on Signals Intelligence Activities, Jan. 17, 2014.

Report by the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat, UN Doc. S/2016/501, May 31, 2016.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98*, June 24, 2013.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, July 22, 2015.

Report of the Secretary-General Pursuant to Paragraph 2 of Security Council Resolution 808 (1993), May 3, 1993, Annex (Statute of the International Tribunal).

Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions: Study on Targeted Killings, UN Doc. A/HRC/14/24/Add.6, May 28, 2010.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc. A/69/397, Sept. 23, 2014.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/17/27, May 16, 2011.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/29/32, May 22, 2015.

Report of the Working Group on Internet Governance (2005).

The Right to Privacy in the Digital Age: Report of the Office of the UN High Commissioner for Human Rights, UN Doc. A/HRC/27/37, June 30, 2014.

Sixth Review Meeting of the Contracting Parties to the Convention on Nuclear Safety, *Summary Report*, CNS/6RM/2014/11_Final, Apr. 4, 2014.

State of Israel Ministry of Justice. The Counter-Terrorism Law 5775-2015, http://www.justice.gov.il/Units/InternationalAgreements/HumanRightsAndForeignRelations/Faq/CounterTerrorismLaw5775-2015_BackgroundDescriptionJune2016.pdf

Statement by the President of the Security Council, UN Doc. S/PRST/2016/6, May 11, 2016.

Terrorism Act of 2000 (as amended) (United Kingdom).

United Nations. *International Instruments Related to the Prevention and Suppression of International Terrorism* (New York: UN, 2008).

_____. "Legal Committee Urges Conclusion of Draft Comprehensive Convention on International Terrorism," Press Release, Oct. 8, 2012, http://www.un.org/press/en/2012/gal3433.doc.htm.

_____. "Speakers Urge Differences be Resolved in Draft Comprehensive Convention on International Terrorism, as Sixth Committee Begins Session," Press Release, Oct. 7, 2014, http://www.un.org/press/en/2014/gal3475.doc.htm.

_____. *UN Action to Counter Terrorism: International Legal Instruments*, http://www.un.org/en/terrorism/instruments.shtml.

UN General Assembly. *Letter Dated 3 August 2005 from the Chairman of the Sixth Committee to the President of the General Assembly*, UN Doc. A/59/894, Appendix II, Aug. 12, 2005.

_____. *Letter Dated 3 August 2005 from the Chairman of the Sixth Committee to the President of the General Assembly*, UN Doc. A/59/894, App. II, Aug. 12, 2005.

UN General Assembly. *Resolution 51/210*, Dec. 16, 1996, UN Doc. A/RES/51/210, Jan. 16, 1997.

_____. *Resolution 60/288 on the United Nations Global Counter-Terrorism Strategy*, UN Doc. A/RES/60/288, Sept. 20, 2006.

_____. *Resolution 68/167—The Right to Privacy in the Digital Age*, UN Doc. A/RES/68/167, Dec. 18, 2013.

UN Office on Drugs and Crime. *Comprehensive Study on Cybercrime* (Feb. 2013),

_____. *Emerging Crimes*, http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html.

_____. *Organized Crime*, http://www.unodc.org/unodc/en/organized-crime/index.html.

_____. *(Inter-) Regional Action Against Terrorism* (2015), https://www.unodc.org/tldb/en/regional_instruments.html.

_____. *Signatories to the United Nations Convention on Transnational Organized Crime and Its Protocols*, http://www.unodc.org/unodc/en/treaties/CTOC/signatures.html.

_____. *The Use of the Internet for Terrorist Purposes* (New York: United Nations, 2012).

UN Security Council. *Global Survey of Implementation by Member States of Security Council Resolution 1624 (2005)*, UN Doc. S/2012/16, Jan. 9, 2012.

_____. Resolution 955 (1994), Nov. 8, 1994.

_____. Resolution 1373 (2001), Sept. 28, 2001.

_____. Resolution 1540 (2004), Apr. 28, 2004.

_____. Resolution 1624 (2005), Sept. 14, 2005.

_____. Resolution 2178 (2014), Sept. 24, 2014.

UN Security Council Counter-Terrorism Committee, http://www.un.org/en/sc/ctc/.

_____. *CTED Stresses Need to Protect Critical Infrastructures*, Mar. 23, 2015, http://www.un.org/en/sc/ctc/news/2015-03-23_cted_protect_infrastructure.html.

_____. *Counter-Terrorism Committee Launches Global Research Network*, Feb. 20, 2015, http://www.un.org/press/en/2014/gal3475.doc.htm.

_____. *Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States* (Sept. 2011).

_____. Special Meeting of the Counter-Terrorism Committee and Technical Sessions of the Counter-Terrorism Committee Executive Directorate on Preventing and Combating Abuse of ICT for Terrorist Purposes, Dec. 16-17, 2015, http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html.

UN Treaty Collection. *Text and Status of the United Nations Conventions on Terrorism*, https://treaties.un.org/Pages/DB.aspx?path=DB/studies/page2_en.xml.

_____. *UN Convention against Transnational Organized Crime: Status of Ratification* (as of June 24, 2016), https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en.

United States v. Ahmad Fathi *et al*., Indictment, U.S. District Court, Southern District of New York, 16 Crim 48 (2016).

U.S. Department of Defense. "CENTCOM Acknowledges Social Media Sites 'Compromised,'" Jan. 12, 2015, http://www.defense.gov/news/newsarticle.aspx?id=123956&source=GovDelivery

_____. *The DoD Cyber Strategy* (Apr. 2015).

_____. *Law of War Manual* (Washington, D.C.: U.S. Department of Defense, 2015).

U.S. Department of Homeland Security. *Commercial Facilities Sector*, http://www.dhs.gov/commercial-facilities-sector.

U.S. Department of State. *Overview of Export Control System*, http://www.state.gov/strategictrade/overview/.

U.S. National Infrastructure Protection Center. "Cyberterrorism: An Evolving Concept," *NIPC Highlights*, http://www.nipc.gov/publications/highlights/2001/highlight-01-06.htm.

U.S. Office of Homeland Security. *National Strategy for Homeland Security* (July 2002).

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, http://www.wassenaar.org/.

Wassenaar Arrangement. *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (13) 1, Dec. 4, 2013.

White House. *Fact Sheet: The White House Summit on Countering Violent Extremism*, Feb. 18, 2015, https://www.whitehouse.gov/the-press-office/2015/02/18/fact-sheet-white-house-summit-countering-violent-extremism.

_____. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003).

_____. *National Strategy to Secure Cyberspace* (Feb. 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

World Health Organization, *International Health Regulations (2005)* (Geneva: WHO, 2nd ed., 2008).

Books and Book Chapters

Antonopoulos, Constantine. "State Responsibility in Cyberspace," in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias and Russell Buchan, eds.) (Cheltenham: Edward Elgar Publishing, 2015), 55-71.

Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara: Praeger, 2010).

Buchan, Russell. "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias and Russell Buchan, eds.) (Cheltenham: Edward Elgar Publishing, 2015), 168-89.

Byman, Daniel. *Deadly Connections: States that Sponsor Terrorism* (Cambridge: Cambridge University Press, 2005).

Critical Infrastructure Protection (Matthew Edwards ed.) (NATO Science for Peace and Security Series Vol. 116) (Amsterdam: IOS Press, 2014).

Cryer, Robert, Hakan Friman, Darryl Robinson, and Elizabeth Wilmshurst. *An Introduction to International Criminal Law and Procedure* (Cambridge: Cambridge University Press, 3rd ed., 2014).

Cyberterrorism: Understanding, Assessment, and Response (Thomas M. Chen, Lee Jarvis, and Stuart MacDonald, eds.) (New York: Springer, 2014).

Czosseck, Christian. "State Actors and Their Proxies in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 1-30.

Committee on Education on Dual Use Issues in the Life Sciences. *Challenges and Opportunities for Education about Dual Use Issues in the Life Sciences* (Washington, D.C.: National Academies Press, 2010).

Fidler, David P. "*Inter Arma Silent Leges Redux?* Law of Armed Conflict and Cyberconflict," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Derek Reveron, ed.)(Washington, D.C.: Georgetown University Press, 2012), 71-87.

Focarelli, Carlo. "Self-Defence in Cyberspace," in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias and Russell Buchan, eds.) (Cheltenham: Edward Elgar Publishing, 2015), 255-83.

Foreign Relations Law of the United States (Minneapolis: West Publishing, 3rd ed., 1987).

Geiss, Robin and Henning Lahmann. "Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 621-57.

Gill, Terry D. "Non-Intervention in the Cyber Context," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 217-38.

Governance of Dual-Use Technologies: Theory and Practice (Elisa D. Harris, ed.) (Cambridge, Mass.: American Academy of Arts & Sciences, 2016).

Hardy, Keiran and George Williams. "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism," in *Cyberterrorism: Understanding, Assessment, and Response* (Thomas M. Chen, Lee Jarvis, and Stuart MacDonald, eds.) (New York: Springer, 2014), Chapter 2.

Harris, Elisa D. "Dual-Use Threats: The Case of Biological Technology," in *Governance of Dual-Use Technologies: Theory and Practice* (Elisa D. Harris, ed.) (Cambridge, Mass.: American Academy of Arts & Sciences, 2016), 60-111.

Human Rights and Natural Disasters (Brookings-Bern Project on Internal Displacement, 2008).

International Group of Experts. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

International Institute of Humanitarian Law. *San Remo Manual on the Law of Non-International Armed Conflict with Commentary* (San Remo: International Institute of Humanitarian Law, 2006).

Joyner, Daniel H. *International Law and the Proliferation of Weapons of Mass Destruction* (Oxford: Oxford University Press, 2009).

Kaiser, Stefan A. and Oliver Aretz. "Legal Protection of Civil and Military Aviation against Cyber Interference," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 319-48.

Lin, Herb. "Governance of Information Technology and Cyber Weapons," in *Governance of Dual-Use Technologies: Theory and Practice* (Elisa D. Harris, ed.) (Cambridge, Mass.: American Academy of Arts & Sciences, 2016), 112-57.

Marauhn, Thilo. "Customary Rules of International Environmental Law—Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 465-84.

Mejia-Kaiser, Martha. "Space Law and Unauthorized Cyber Activities," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 349-72.

O'Connell, Mary Ellen. "The Prohibition of the Use of Force," in *Research Handbook on International Conflict and Security Law* (Nigel D. White and Christian Henderson, eds.) (Cheltenham: Edward Elgar Publishing, 2012), 89-119.

Pirker, Benedkt."Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 189-216.

PoKempner, Dinah. "Cyberspace and State Obligations in the Area of Human Rights," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 239-60.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014).

Saul, Ben. *Defining Terrorism in International Law* (Oxford: Oxford University Press, 2006).

Saul, Ben and Kathleen Heath. "Cyber Terrorism," in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias and Russell Buchan, eds.) (Cheltenham: Edward Elgar Publishing, 2015), 147-67.

Singer, Peter W. and Allan Friedman. *Cybersecurity and Cyberwar* (Oxford: Oxford University Press, 2014).

Walden, Ian. "International Telecommunications Law, the Internet and the Regulation of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 261-89.

Weimann, Gabriel. "Cyberterrorism: The Sum of All Fears?," *Studies in Conflict & Terrorism* (2005); 28:129-49.

Wessel, Ramses A. "Towards EU Cybersecurity Law: Regulating a New Policy Field," in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias and Russell Buchan, eds.) (Cheltenham: Edward Elgar Publishing, 2015), 403-25.

von Heinegg, Wolff Heintzchel. "Protecting Critical Submarine Cable Infrastructure: Legal Status and Protection of Submarine Communication Cables under International Law," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 1-30.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

Ziolkowski, Katharina. "General Principles of International Law as Applicable in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy* (Katharina Ziolkowski, ed.) (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 135-88.

Articles, News Stories, and Other Secondary Sources

Advisory Council on International Affairs. *Counterterrorism from an International Perspective* (Advisory Report No. 49, Sept. 2006), 24-25.

Arend, Anthony Clark. "International Law and the Preemptive Use of Military Force," *Washington Quarterly* (2003), 26(2): 89-103.

Arms Control Association. *Nuclear Security Summit at a Glance*, Apr. 2014, http://www.armscontrol.org/factsheets/NuclearSecuritySummit

Awan, Imran. "Debating the Term Cyber-Terrorism: Issues and Problems," *Internet Journal of Criminology* (2014), http://www.internetjournalofcriminology.com/awan_debating_the_term_cyber-terrorism_ijc_jan_2014.pdf.

Bannelier-Christakis, Karine. "Cyber Due Diligence: Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *Baltic Yearbook of International Law* (2014); 14: 23-39.

Behn, Sharon. "Could IS Turn Next to Cyber War?," *Voice of America*, Dec. 18, 2015, http://m.voanews.com/a/islamic-state-cyber-war/3109289.html.

Benjamin, Raymond. "Meeting a Global Threat with a Global Response: Aviation's Collaborative and Multidisciplinary Actions on Cybersecurity," *Cyber Security Review* (Autumn 2015): 38-40.

Bethlehem, Daniel. "Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attacks by Nonstate Actors," *American Journal of International Law* (2012); 106(4): 770-77.

Berger, Joseph. "A Dam, Small and Unsung, is Caught Up in an Iranian Hacking Case," *New York Times,* Mar. 26, 2016, A15.

Berger, J. M. and Jonathan Morgan. *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter* (Brookings Project on U.S. Relations with the Islamic World Analysis Paper No. 20, Mar. 2015), http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

Berkman Center for Internet & Society. *Don't Panic: Making Progress on the "Going Dark" Debate* (Feb. 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Biller, Jeffrey T. "Cyber-Terrorism: Finding a Common Starting Point," *Journal of Law, Technology & the Internet* (2013); 4(2): 275-351.

BioWeapons Prevention Project. "How do Countering Bioterrorism and the BWC Relate to Each Other?," Dec. 6, 2011, http://www.bwpp.org/documents/revcon/BWPP2010%202011-RevConProject-Conclusion-Bioterrorism.pdf.

Bradner, Eric. "Obama: North Korea's Hack Not War, But Cybervandalism," CNN.com, Dec. 24, 2014, http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/.

Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?," *Journal of Conflict and Security Law* (2012); 17: 211-27.

Carawell, Jack. "Cyber Threats to Nuclear Power Plants in the Second Nuclear Age," *Cyber Security Review* (Summer 2016), 27-32.

Chertoff, Michael and Paul Rosenzweig. *A Primer on Globally Harmonizing Internet Jurisdiction and Regulations* (Global Commission on Internet Governance Paper Series No. 10, Mar. 2015).

Chrisafis, Angelique and Samuel Gibbs. "French Media Groups to Hold Emergency Meeting after ISIS Cyber-Attack," *The Guardian*, Apr. 9, 2015, http://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers.

Cieply, Michael and Brooks Barnes. "Sony Cyberattack, First a Nuisance, Swiftly Grew into a Firestorm," *New York Times*, Dec. 30, 2014, http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

Cohen, Aviv. "Cybterterrorism: Are We Legally Ready?" *Journal of International Business & Law* (2010); 9(1): 1-40.

Cohen, Jared. "Digital Counterinsurgency: How to Marginalize the Islamic State Online," *Foreign Affairs* (Nov./Dec. 2015), 52-58.

Daskal, Jennifer and Andrew K. Woods. "Cross-Border Data Requests: A Proposed Framework," *Lawfare,* Nov. 24, 2015, https://lawfareblog.com/cross-border-data-requests-proposed-framework.

Deeks, Ashley S. "Confronting and Adapting: Intelligence Agencies and International Law," *Virginia Law Review* (2016); 102(3): 599-685.

Denning, Dorothy E. "Stuxnet: What Has Changed?," *Future Internet* (2012); 4: 672-87.

Dennis, Steven T. "Republicans Seek Wider FBI Surveillance Power after Orlando," Bloomberg," June 14, 2016, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217/signatures?p_auth=Ulw9Oecg.

Earle, Geoff and Jamie Schram. "'We are Coming': ISIS Hacks Defense Department," *New York Post*, Jan. 12, 2015, http://nypost.com/2015/01/12/we-are-coming-isis-hacks-defense-department-twitter-account/.

Eichensehr, Kristen E. "The Cyber-Law of Nations," *Georgetown Law Journal* (2015); 103: 317-80.

Feakin, Tobias. *Developing a Proportionate Response to a Cyber Incident* (Council on Foreign Relations Cyber Brief, Aug. 2015), http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

Ferencz, Janos. "Powers of the Security Council to Make Determinations under Article 39 of the Charter in Case of Cyber Operations," *Opinio Juris*, Aug. 10, 2015, http://opiniojuris.org/2015/08/10/emerging-voices-powers-of-the-security-council-to-make-determinations-under-article-39-of-the-charter-in-case-of-cyber-operations/.

Fidler, David P. *Countering Islamic State Exploitation of the Internet* (Council of Foreign Relations Cyber Brief, June 2015), http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-internet/p36644.

_____. "Cyber War Crimes: Islamic State Atrocity Videos and the Laws of War," *Computer Law Review International* (2015); 16(6): 161-65.

_____. "Disaster Relief and Governance after the Indian Ocean Tsunami: What Role for International Law?" *Melbourne Journal of International Law* (2005); 6: 458-73.

_____. "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations," *American Society of International Law Insights*, Feb. 7, 2013, http://asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision.

_____. "Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection," *Georgetown Journal of International Affairs* (2015); 8-20.

Fidler, Mailyn. "Cyber Diplomacy with Africa: Lessons from the African Cybersecurity Convention," *Council on Foreign Relations Net Politics,* July 7, 2016, http://blogs.cfr.org/cyber/2016/07/07/cyber-diplomacy-with-africa-lessons-from-the-african-cybersecurity-convention/

_____. "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis," *I/S: A Journal of Law and Policy for the Information Society* (2015); 11: 405-83.

Fleck, Dieter. "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New *Tallinn Manual*," *Journal of Conflict & Security Law* (2013); 18(2): 331-51.

French, Duncan and Tim Stephens. *Due Diligence in International Law* (First Report of ILA Study Group on Due Diligence in International Law, Mar. 7, 2014).

Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law* (2010); 43: 57-118.

Georgia Institute of Technology. *Emerging Cyber Threats Report 2016*, http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.

Golabek-Goldman, Michele. *A New Strategy for Reducing the Threat of Dangerous Zero-Day Sales to Global Security and the Economy* (Harvard Kennedy School of Government, Mar. 25, 2014).

Grady, Franz-Stefan. "China-US Talks on Cybercime: What are the Outcomes?," *The Diplomat*, June 16, 2016, http://thediplomat.com/2016/06/china-us-talks-on-cybercrime-what-are-the-outcomes/.

Graham-Harrison, Emma. "Could ISIS's 'Cyber Caliphate' Unleash a Deadly Attack on Key Targets?" *The Guardian*, Apr. 12, 2015, http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.

Granick, Jennifer. "The Right Way to Share Information and Improve Cybersecurity," *Just Security*, Mar. 26, 2015, http://justsecurity.org/21498/share-information-improve-cybersecurity/.

Greenberg, Andy. "Hacker Lexicon: What is the Dark Web?," *Wired*, Nov. 19, 2014, http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

Grigsby, Alex. "The UN GGE on Cybersecurity: What is the UN's Role?" *Council on Foreign Relations Net Politics*, Apr. 15, 2015, http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/.

Gronvall, Gigi Kwik. *Mitigating the Risks of Synthetic Biology* (Council on Foreign Relations Center for Preventive Action Discussion Paper, Feb. 2015), http://www.cfr.org/health/mitigating-risks-synthetic-biology/p36097.

Harold, Scott Warren, Martin C. Libicki, and Astrid Stuth Cevallos. *Getting to Yes with China in Cyberspace* (Santa Monica: RAND, 2016).

Heinl, Caitríona H. *Regional Cyber Security: Towards a Resilient ASEAN Cyber Security Regime* (RSIS Working Paper No. 263, Sept. 9, 2013), http://www.rsis.edu.sg/wp-content/uploads/rsis-pubs/WP263.pdf.

Hewitt, Duncan. "China's President Xi Says Internet Must be Governed by Order, Stresses Cyber Sovereignty," *International Business Times*, Dec. 16, 2015, http://www.ibtimes.com/chinas-president-xi-says-internet-must-be-governed-order-stresses-cyber-sovereignty-2227533.

Hollis, Duncan B. "An e-SOS for Cyberspace," *Harvard International Law Journal* (2011); 52(2): 373-432.

Hollis, Duncan and Tim Maurer. "A Red Cross for Cyberspace," *Time*, Feb. 18, 2015, http://time.com/3713226/red-cross-cyberspace/.

Hoover Institution, Consortium for Research on Information Security and Policy, and the Center for International Security and Cooperation at Stanford University, http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf.

Human Rights Watch. *China—Draft Counterterrorism Law a Recipe for Abuses: Major Overhaul Needed for Law to Conform with International Legal Obligations*, Jan. 20, 2015, http://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses.

International Committee of the Red Cross. *Commentary on Convention (IV) Relative to the Protection of Civilian Persons in Time of War of 12 August 1949* (Geneva: ICRC, 1958).

_____. *Commentary on Additional Protocol II to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) of 8 June 1977* (Geneva: ICRC, 1987).

_____. *Customary International Humanitarian Law, Rule 2: Violence Aimed at Spreading Terror Among the Civilian Population*, https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule2.

International Law Association. *Cultural Heritage Law*, http://www.ila-hq.org/en/committees/index.cfm/cid/13.

Iqbal, Mohammad. "Defining Cyberterrorism," *Journal of Computer & Information Law* (2004); 22: 397-408.

Ivanov, Eduard. "Combating Cyberterrorism under International Law," *Baltic Yearbook of International Law* (2014): 14: 55-69.

Kavanagh, Camino. "The UN GGE on Cybersecurity: The Important Drudgery of Capacity Building," *Council on Foreign Relations Net Politics*, Apr. 13, 2015, http://blogs.cfr.org/cyber/2015/04/13/the-un-gge-on-cybersecurity-the-important-drudgery-of-capacity-building/.

Knake, Robert. *Cleaning Up U.S. Cyberspace* (Council on Foreign Relations Cyber Brief, Dec. 2015), http://www.cfr.org/internet-policy/cleaning-up-us-cyberspace/p37333.

_____. "Private Sector and Government Collaboration on Cybersecurity: The Home Depot Model," *Council on Foreign Relations Net Politics*, Mar. 31, 2015, http://blogs.cfr.org/cyber/2015/03/31/private-sector-and-government-collaboration-on-cybersecurity-the-home-depot-model/.

Kretzmer, David. "The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*," *European Journal of International Law* (2013); 24(1): 235-82.

Liang, Christina Schori. *Cyber Jihad: Understanding and Countering Islamic State Propaganda* (Geneva Centre for Security Policy Paper 2015/2, Feb. 2015), http://www.gcsp.ch/Emerging-Security-Challenges/Publications/GCSP-Publications/Policy-Papers/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda.

Lichfield, John. "TV5Monde Hack: 'Jihadist Cyber Attack on French TV State Could Have Russian Link," *The Independent*, June 10, 2015, http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html.

Lugar, Richard G. "Nunn-Lugar: Science Cooperation Essential for Nonproliferation Efforts," *Science & Diplomacy* (2012); 1(1): http://www.sciencediplomacy.org/files/nunn-lugar.pdf.

Margulies, Peter. "Sweeping Claims and Casual Legal Analysis in the Latest U.N. Mass Surveillance Report," *Lawfare*, Oct. 20, 2014, http://www.lawfareblog.com/2014/10/sweeping-claims-and-casual-legal-analysis-in-the-latest-u-n-mass-surveillance-report/.

Martellini, Maurizio, Thomas Shea, and Sandro Gaycken. *Cyber Security for Nuclear Power Plants* (Jan. 2012), http://www.state.gov/t/isn/183589.htm.

Martin, Neil and Tim Willis. "Google, the Wassenaar Arrangement, and Vulnerability Research," *Google Online Security Blog*, July 20, 2015, https://googleonlinesecurity.blogspot.com/2015/07/google-wassenaar-arrangement-and.html.

Mimoso, Michael. "White House Wants to Renegotiate U.S. Implementation of Wassenaar," *Threat Post*, Mar. 1, 2016, https://threatpost.com/white-house-wants-to-renegotiate-u-s-implementation-of-wassenaar/116531/.

Nakashima, Ellen and Andrea Peterson. "The British Want to Come to America—With Wiretap Orders and Search Warrants," *Washington Post,* Feb. 4, 2016, https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

NATO Cooperative Cyber Defence Centre of Excellence "Cyber Definitions," https://ccdcoe.org/cyber-definitions.html.

Nye, Joseph. "e-Power to Rise Up the Security Agenda," *NATO Review* (2012), http://www.nato.int/docu/Review/2012/2012-security-predictions/e-Power-cybersecurity/EN/index.htm.

O'Connell, Mary Ellen. "Cyber Security without Cyber War," *Journal of Conflict & Security Law* (2012); 17(2): 187-209.

____. "Dangerous Departures," *American Journal of International Law* (2013); 107: 380-86.

_____. "Evidence of Terror," *Journal of Conflict & Security Law* (2002); 7(1): 19-36.

_____. "Lawful Self-Defense to Terrorism," *University of Pittsburgh Law Review* (2001-2002); 63: 889-904.

Omanovic, Edin. "A Way Forward to Effectively Regulate the Trade in Surveillance Technology," *Privacy International*, Mar. 24, 2014, https://www.privacyinternational.org/?q=node/464.

Painter, Christopher. "The Global Conference on Cyberspace: Putting Principles into Practice," *Council on Foreign Relations Net Politics*, Apr. 23, 2015, http://blogs.cfr.org/cyber/2015/04/23/the-global-conference-on-cyberspace-putting-principles-into-practice/.

Parrish, Kevin. "FBI Drops Its Fight with Apple over Shooter's Recovered iPhone 5C," *Digital Trends,* Mar. 28, 2016, http://www.digitaltrends.com/mobile/fbi-apple-vacate/.

Patrick, Stewart. "The Brutal Truth: Failed States are Mainly a Threat to Their Own Inhabitants," *Foreign Policy*, June 20, 2011, http://foreignpolicy.com/2011/06/20/the-brutal-truth/.

Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0.

Peterson, Andrea and Brian Fung. "Paris Attacks Should be 'Wake Up Call' for More Digital Surveillance, CIA Director Says," *Washington Post*, Nov. 16, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/11/16/paris-attacks-should-be-wake-up-call-for-more-digital-surveillance-cia-director-says/.

Piera, Alejandro and Michael Gill. "Will the New ICAO-Beijing Instruments Build a Chinese Wall for International Aviation Security?" *Vanderbilt Journal of Transnational Law* (2014); 47:145-237.

Paul, Christopher and Isaac R. Porche III. "Toward a U.S. Army Cyber Security Culture," *International Journal of Cyber Warfare and Terrorism* (2011); 1(3): 70-80.

Pollitt, Mark M. "Cyberterrorism—Fact or Fancy?'" *Computer Fraud & Security* (1998); 2 (Feb.): 8-10.

Ratner, Steven R. *Self-Defense Against Terrorists: The Meaning of Armed Attack* (University of Michigan Law School Public Law and Legal Theory Working Paper No. 270, May 2012).

Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks," *Journal of Strategic Studies* (2015); 38: 4-37.

Risen, Tom. "Eyes on Obama as FBI, Congress Blast Encryption: Law Makers Decry Encryption as a Venue for Terrorist Planning," *U.S. News & World Report*, Dec. 10, 2015, http://www.usnews.com/news/articles/2015/12/10/eyes-on-obama-as-fbi-congress-blast-encryption.

Ryan, Missy. "Brussels Attacks Rekindle Privacy vs. Security Debate in Europe," *Washington Post*, Mar. 26, 2016, https://www.washingtonpost.com/world/europe/brussels-attacks-rekindle-privacy-vs-security-debate-in-europe/2016/03/26/60a68558-f2dc-11e5-a2a3-d4e9697917d1_story.html.

Sanger, David E. "U.S. Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, Apr. 25, 2016, A1.

Saul, Ben. "Legislating from a Radical Hague: The United Nations Tribunal for Lebanon Invents an International Crime of Transnational Terrorism," *Leiden Journal of International Law* (2011); 24(3): 677-700.

Scharf, Michael P. "Special Tribunal for Lebanon Issues Landmark Ruling on Definition of Terrorism and Modes of Participation," *American Society of International Law Insights*, Mar. 4, 2011, http://www.asil.org/sites/default/files/insight110304.pdf.

Schmitt, Michael N. "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law* (2014); 54(3): 697-732.

_____. "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum*, June 22, 2015, http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.

Sharp, Walter Gary Jr. "The Use of Armed Force Against Terrorism: American Hegemony or Impotence?" *Chicago Journal of International Law* (2000); 1(1): 37-47.

Shiryaev, Yaroslav. "Cyberterrorism in the Context of Contemporary International Law," *San Diego International Law Journal* (2012); 14: 139-92.

Starks, Tim. "Back to the Drawing Board on Wassenaar," *Politico*, Apr. 11, 2016, http://www.politico.com/tipsheets/morning-cybersecurity/2016/04/back-to-the-drawing-board-on-wassenaar-hoyer-goes-to-bat-for-administration-on-it-plan-defending-military-grocery-stores-213687.

Stockton, Paul and Golabek-Goldman, Michele. "Curbing the Market for Cyber Weapons," *Yale Law & Policy Review* (2013); 32: 101-28.

Symantec. *A Manifesto for Cyber Resilience* (2014), http://www.symantec.com/content/en/us/enterprise/other_resources/b-a-manifesto-for-cyber-resilience.pdf.

Tafoya, William L. "Cyber Terror," *FBI Law Enforcement Bulletin* (Nov. 2011), https://leb.fbi.gov/2011/november/cyber-terror.

Tams, Christian J. "The Use of Force against Terrorists," *European Journal of International Law* (2009); 20(2): 359-97.

Tams, Christian J. and James G. Devaney. "Applying Necessity and Proportionality to Anti-Terrorist Self-Defence," *Israel Law Review* (2012); 45(1): 91-106.

Tikk, Eneken, Kadri Kask, and Lils Vihul. *International Cyber Incidents: Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence, 2010).

Toor, Amar. "French Law Would Fine Apple if It Does Not Hand Over Encrypted Data in Terror Cases," *The Verge*, Mar. 4, 2016,

http://www.theverge.com/2016/3/4/11160044/france-apple-encryption-terrorism-law.

Tsagourias, Nicholas. "Cyber Attacks, Self-Defence, and the Problem of Attribution," *Journal of Conflict & Security Law* (2013); 17: 229-44.

_____. "The Law Applicable to Countermeasures against Low-Intensity Cyber Operations," *Baltic Yearbook of International Law* (2014); 14: 105-23.

Wappes, Jim. "Experts Debate Research Pause, Gain-of-Function Issues," CIDRAP News, Dec. 15, 2014, http://www.cidrap.umn.edu/news-perspective/2014/12/experts-debate-research-pause-gain-function-issues.

Weller, Marc. "Striking ISIL: Aspects of the Law on the Use of Force," *American Society of International Law Insights*, Mar. 11, 2015, http://www.asil.org/insights/volume/19/issue/5/striking-isil-aspects-law-use-force.

Woods, Andrew K. *Data Beyond Borders: Mutual Legal Assistance in the Internet Age* (Global Network Initiative, Jan. 2015), http://csis.org/files/attachments/GNI%20MLAT%20Report.pdf.

Zetter, Kim. "Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired,* Jan. 8, 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

_____. "Feds Say that Banned Researcher Commandeered a Plane," *Wired,* May 15, 2015, http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

_____. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, Mar. 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.