

INTERNATIONAL LAW ASSOCIATION

Study Group on Cybersecurity, Terrorism, and International Law

OVERVIEW OF INTERNATIONAL LEGAL ISSUES AND CYBER TERRORISM

Prepared by David P. Fidler, Chair

CONTENTS

I. Introduction: The Study Group, Its Objectives, and this Overview	1
II. An Analytical Framework.....	2
<i>A. Terrorism and International Law</i>	<i>2</i>
<i>B. Cyber Terrorism and International Law</i>	<i>3</i>
III. International Law and Responding to Cyber Terrorism	4
<i>A. The Anti-Terrorism Treaties and Cyber Terrorism.....</i>	<i>4</i>
<i>B. Beyond the Anti-Terrorism Treaties: The Draft Comprehensive Convention on Terrorism, Security Council Mandates, and the Crime of Terrorism in Customary International Law</i>	<i>7</i>
1. <u>The Draft Comprehensive Convention on Terrorism</u>	<u>7</u>
2. <u>Counter-Terrorism Activities Mandated by the Security Council.....</u>	<u>7</u>
3. <u>Customary International Law and the Crime of Terrorism</u>	<u>8</u>
<i>C. Beyond International Law on Terrorism: International Law on Cyber Crime, Extradition Treaties, and Mutual Legal Assistance Treaties.....</i>	<i>8</i>
1. <u>Council of Europe’s Convention on Cybercrime and Cyber Terrorism</u>	<u>8</u>
2. <u>Extradition Treaties, Mutual Legal Assistance Treaties, and Cyber Terrorism</u>	<u>9</u>
<i>D. Extraterritorial Jurisdiction, International Law, and Cyber Terrorism.....</i>	<i>9</i>
<i>E. Summary on International Law and Responding to Cyber Terrorism</i>	<i>10</i>
IV. International Law and Protecting against Cyber Terrorism	11
<i>A. Protecting against Terrorism and Cyber Terrorism</i>	<i>11</i>

<i>B. International Law, Critical Infrastructure Protection, and Cyber Terrorism</i>	<i>12</i>
<i>C. International Law, Securing Dangerous Materials from Terrorists, and Cyber Terrorism.....</i>	<i>14</i>
<i>D. International Law, Damage Mitigation and Recovery, and Cyber Terrorism</i>	<i>15</i>
<i>E. International Law, “Situational Awareness,” and Cyber Terrorism.....</i>	<i>16</i>
<i>F. Summary on International Law and Protecting against Cyber Terrorism</i>	<i>16</i>
V. International Law and Preventing Cyber Terrorism	16
<i>A. International Law and Preventing Terrorism</i>	<i>16</i>
<i>B. International Law, Intelligence Activities, and Preventing Cyber Terrorism.....</i>	<i>17</i>
<i>C. International Law, Pre-Emptive Strikes, and Preventing Cyber Terrorism</i>	<i>18</i>
<i>D. International Law, Prohibiting Terrorist Financing, Stopping Flows of Recruits, and Preventing Cyber Terrorism</i>	<i>18</i>
<i>E. International Law, Root Causes, and Preventing Cyber Terrorism</i>	<i>19</i>
<i>F. Summary on International Law and Preventing Cyber Terrorism</i>	<i>19</i>
VI. The Overview, the Study Group’s Objectives, and Next Steps	19
<i>A. The Overview and the Study Group’s Objectives</i>	<i>19</i>
<i>B. The Overview and the Study Group’s Next Steps</i>	<i>21</i>

OVERVIEW OF INTERNATIONAL LEGAL ISSUES AND CYBER TERRORISM

Prepared by David P. Fidler, Chair

I. Introduction: The Study Group, Its Objectives, and this Overview

1. The International Law Association (ILA) established the Study Group on Cybersecurity, Terrorism, and International Law (Study Group) to examine international legal issues related to cyber terrorism. Cybersecurity policy documents frequently identify cyber terrorism as a threat, even though, to date, experts do not believe terrorists have successfully used cyber weapons or attacks, as opposed to using the Internet to communicate and achieve other goals. However, governments fear terrorists will eventually use malicious cyber activities to attack, for example, cyber-enabled critical infrastructure in order to damage economies and terrorize societies. The gap between oft-raised fears about cyber terrorism and the lack of cyber terrorist attacks has contributed to analyses of cyber terrorism remaining general and speculative in nature.

2. International lawyers have participated in debates about cyber terrorism from the time it emerged as a policy topic. For example, a Council of Europe-sponsored study from 2007 analyzed the applicability of existing treaties on terrorism and cyber crime to cyber terrorism.¹ Although helpful, the existing international legal literature on cyber terrorism reflects neither sustained attention nor consensus on how to define or analyze cyber terrorism. Continued warnings about cyber terrorism invite more systematic international legal scrutiny of this perceived national and international security problem. The increase in international legal interest in other aspects of cybersecurity, such as how deployment of cyber weapons might affect international law on the use of force and armed conflict, also highlight the opportunity to engage in scrutiny of cyber terrorism under international law.

3. 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 will explore international legal issues associated with potential terrorist use of cyber attacks to advance their political and ideological agendas. The Study Group excluded from the scope of its efforts terrorist use of the Internet and cyberspace for other purposes, including communications, propaganda, recruitment, and fundraising.² Nor will the Study Group examine how governments use cyber technologies in general counter terrorism activities, such as conducting surveillance of electronic communications. These topics are important for international law, and the Study Group might, in its final report, recommend that the ILA explore these issues.

4. Four main objectives will guide the Study Group's work:

- Examine the potential threat of cyber terrorism, including how technological trends and innovations might affect the threat;

¹ Council of Europe Counter-Terrorism Task Force, *Cyberterrorism—The Use of the Internet for Terrorist Purposes* (Strasbourg: Council of Europe Publishing, 2007), pp. 94-95.

² However, some international law concerning terrorist financing and flows of foreign fighters to terrorist groups are relevant to thinking about cyber terrorism, as discussed later in this document.

- Develop a definition of “cyber terrorism” to guide its analysis based on relevant international law and state practice on how governments have addressed cyber terrorism;
- 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.

5. In working to achieve these objectives, the Study Group will consider how states and international organizations have used international law to respond, protect against, and prevention terrorism generally. The response, protection, and prevention objectives connect to specific counter-terrorism strategies. The use of international law against terrorism provides a template for the Study Group to use in analyzing international legal issues potentially related to cyber terrorism. This overview uses this template to organize international legal issues according to the central objectives of policies against terrorism. The template also requires the Study Group to identify whether, and to what extent, cyber terrorism might represent a different kind of problem from other forms of terrorism. This requirement connects to the objective of assessing cyber terrorism in light of the technological aspects of this threat.

6. This overview does not identify and analyze every international legal issue, but it attempts to advance the Study Group’s examination of this topic. Nor does it exhaustively examine the issues it includes or provide citations for information and/or assertions it contains. As such, it is preliminary in terms of analysis and research, but the objective is to catalyze input on what we need to accomplish in light of our objectives in a format that might support the Study Group’s analysis, findings, and recommendations. If the Study Group finds this framework sufficiently robust for identifying and analyzing the international law relevant to cyber terrorism, it can inform the Study Group’s final report.

II. An Analytical Framework

A. Terrorism and International Law

7. The absence of terrorist attacks using malicious cyber activities helps explain why, to date, states and international organizations have not developed specific international instruments or rules on cyber terrorism. The evolution of international law on terrorism predominantly reflects reactions to various terrorist acts. This pattern developed before the terrorist attacks on the United States on September 11, 2001, as evidenced by the crafting of treaties focused on different terrorist activities—a process that began in the 1960s. Reactions to the 9/11 attacks continued this pattern as countries and international organizations responded with, among other things, international legal arguments and initiatives.

8. Post-9/11 counter-terrorism policies have emphasized three strategic objectives:
- *Respond* effectively 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, which includes capabilities for rapid recovery from attacks; and

- *Prevent* terrorist attacks through intelligence, information sharing, cutting off financial support and other resources, and pre-emptive covert or military action against imminent or emerging terrorist threats.

9. Although analytical distinct as categories of policy activity, these objectives overlap in practice because actions in each category contribute to the other goals. For example, criminal investigation and prosecution of terrorists support the objectives of protection and prevention. Securing nuclear, chemical, or biological materials from falling into terrorist hands protects against and prevents terrorism involving these materials. After 9/11, governments constructed policy against terrorism with all these overlapping goals as strategic priorities.

10. Although each category forms part of counter-terrorism policy, strategies after 9/11 began to stress 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 specific terrorist offenses and strengthening law enforcement cooperation dominated international law on terrorism. For example, non-proliferation treaties, such as the Biological Weapons Convention, became relevant to counter-terrorism even though these agreements did not address terrorism. The need for robust intelligence in order to prevent terrorist attacks implicated international human rights law more seriously, particularly the rights to freedom of expression and privacy. Intelligence-driven awareness of terrorist activities fed into arguments that pre-emptive force against terrorists was justified under international law.

11. Heightened attention on terrorism permeated through many international organizations, which produced initiatives taken under the instruments governing these organizations. The United Nations (UN) Security Council issued decisions requiring UN member states to fulfill counter-terrorism obligations, and it created a Counter-Terrorism Committee to advance the counter-terrorism agenda. Other multilateral and regional organizations also generated treaty law, such as new anti-terrorism agreements, and soft-law initiatives designed to improve cooperation against terrorism.

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

B. Cyber Terrorism and International Law

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

14. 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 malicious

cyber activities by terrorists could fall within the scope of existing anti-terrorism treaties. Efforts to prevent cyber terrorism through strengthened surveillance of electronic communications or preventive “active defense” measures will confront the international legal controversies experienced in counter-terrorism policy and associated with expanded intelligence activities and pre-emptive self-defense.

15. Third, states and/or international organizations 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 new international law should be developed to support policy against cyber terrorism.

16. Although examining how counter-terrorism efforts use international law provides helpful guidance, cyber terrorism has features not easily mapped against other types of terrorism. For example, international law created to keep nuclear, chemical, or biological materials from terrorists does not apply to cyber technologies. Skepticism that states can restrict terrorist access to the means and methods of cyber attack suggests that cyber as a “dual use” technology presents challenges different from those associated with nuclear, chemical, or biological materials. Indeed, how the technological attributes of cyber might affect policy and international legal options is a question cutting across the Study Group’s efforts.

III. International Law and Responding to Cyber Terrorism

A. The Anti-Terrorism Treaties and Cyber Terrorism

17. As noted above, counter-terrorism policy frequently used international law grounded in criminal law and law enforcement cooperation to support responses to terrorism. Many anti-terrorism 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, mandate the parties take jurisdiction over the offenses, and establish law enforcement assistance obligations connected to the offenses. Through this approach, states harmonized substantive, jurisdictional, and procedural aspects of their national criminal laws and established processes for 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 failure to adopt a comprehensive treaty on terrorism (see below).

18. For the Study Group, the anti-terrorism treaties are important for a number of reasons. First, acts of cyber terrorism might fall within the scope of some agreements, making those instruments relevant for identifying international law applicable to cyber terrorism. How well or poorly the anti-terrorism treaties cover potential acts of cyber terrorism might reveal gaps in this area of international law. Second, the criminal law approach used in the anti-terrorism treaties raises questions about whether development of international law on cyber terrorism should emphasize this strategy.

Table 1. Leading Treaties on Terrorism

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
1988	Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf
1988	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

Source: 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

19. The offenses defined in a number of anti-terrorism treaties could potentially cover malicious cyber activities. The dependence of governmental and economic activities on cyber technologies makes cyber terrorism against sectors and areas addressed in these treaties possible. A cyber attack could fall within the scope of some of these treaties 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” (Convention on Offences and Certain Other Acts Committed on Board Aircraft, Article 1);
- Involves an on-board, in-flight seizure or exercise of control of the aircraft (Convention for the Suppression of Unlawful Seizure of Aircraft, Article 1);
- Destroys, damages, or interferes with air navigation facilities such that the safety of aircraft in flight is endangered (Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Article 1);
- 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” (Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Article 2.1(b));
- Destroys or seriously damages facilities of an airport serving international civil aviation or disrupts the services of the airport (Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Article II);

- Destroys or seriously damages maritime navigational facilities or seriously interferes with their operation in a manner likely to endanger safe navigation of ships (Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Article 3.1(e));
- Places on a fixed platform located on the continental shelf a device likely to endanger the safety of the platform (Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Article 2.1(d));
- 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” (International Convention for the Suppression of Terrorist Bombings, Article 2.1); or
- Damages “a nuclear facility in a manner which releases or risks the release of radioactive material” (International Convention for the Suppression of Acts of Nuclear Terrorism, Article 2.1(b)).

20. Reading these agreements in light of threat of cyber terrorism demonstrates that international law is not devoid of treaty law governments could apply in responding to certain acts of cyber terrorism. The subject matter of some treaties includes sectors often mentioned in discussions of cyber terrorism, such as transportation services, government facilities, nuclear plants, and infrastructure providing public services. However, states did not adopt these agreements with cyber terrorism in mind—in fact, only three treaties listed in Table 1 were concluded after the Internet became a global communications platform in the mid-1990s.

21. For example, the International Convention for the Suppression of Terrorist Bombings (2005) has the broadest scope of the anti-terrorism treaties because its offenses cover numerous sectors rather than just one area (e.g., air or maritime transport) or target (e.g., internationally protected persons or nuclear facilities). This Convention’s defined offense includes the delivery, placement, discharge, or detonation of “an explosive or other lethal device” (Article 2.1). The Convention defines “explosive or lethal device” 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” (Article 1.3).

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

B. Beyond the Anti-Terrorism Treaties: The Draft Comprehensive Convention on Terrorism, Security Council Mandates, and the Crime of Terrorism in Customary International Law

23. The lack of a specific cyber terrorism treaty invites consideration of existing or proposed international law on terrorism broader in scope than the anti-terrorism treaties states could apply in responding to cyber terrorism. The possibilities involve an unfinished treaty, activities undertaken pursuant to Security Council resolutions, and the proposition that customary international law recognizes a crime of terrorism.

1. The Draft Comprehensive Convention on Terrorism

24. UN member states have been negotiating a comprehensive treaty on terrorism since the mid-1990s but have not concluded an agreement. 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. (Article 2)

25. This offense would cover cyber attacks—“by any means”—against a range of targets (e.g., government facilities, transportation systems, infrastructure, and private property) causing different consequences, 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 specific anti-terrorism treaties. However, completion of this treaty is neither imminent nor foreseeable because problems that have blocked progress for nearly twenty years have not been resolved.

2. Counter-Terrorism Activities Mandated by the Security Council

26. The Security Council has adopted resolutions imposing binding counter-terrorism obligations on UN member states. To facilitate implementation of these obligations, 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. None of the Security Council’s resolutions are specific to cyber terrorism, and the Counter-Terrorism Committee has not focused on cyber terrorism. However, the resolutions’

mandates and the Committee's jurisdiction are broad enough to include cyber terrorism. The Committee could become a prominent place to address cyber terrorism within the counter-terrorism cooperation mandated by the Security Council. For example, the Committee could oversee harmonization of national criminal laws concerning cyber terrorism in the same manner it provides guidance on other aspects of counter-terrorism policy and law.

3. Customary International Law and the Crime of Terrorism

27. In 2011, the Special Tribunal for Lebanon held customary international law recognizes an international crime of 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. This formulation accommodates cyber terrorism, which would involve criminal acts (gaining unauthorized access to computer systems) with transnational elements (using the Internet) undertaken to spread fear or coerce behavior. Its potential relevance to responding to cyber terrorism has been recognized.

28. The utility of this customary definition is, however, uncertain. The Special Tribunal's holding has been controversial, indicating that some skepticism exists about the definition's status in customary international law. The ruling does not resolve the impasse over the definition of terrorism that contributes to the failure to complete the Comprehensive Convention on Terrorism. Nor is it clear that states use or rely on the Special Tribunal's customary crime of terrorism in activities and cooperation on counter-terrorism, particularly in filling gaps the anti-terrorism treaties create. Relying on such a controversial customary crime might not be the most effective international legal strategy for responding to cyber terrorism.

C. Beyond International Law on Terrorism: International Law on Cyber Crime, Extradition Treaties, and Mutual Legal Assistance Treaties

1. Council of Europe's Convention on Cybercrime and Cyber Terrorism

29. Responses to cyber terrorism can look beyond international law specific to terrorism to consider treaties focused on criminal law and law enforcement cooperation. The Council of Europe's Convention on Cybercrime is frequently identified as potentially useful with respect to cyber terrorism. Cyber terrorism would involve commission of offenses this treaty defines and requires states parties to criminalize in their laws and fight through law enforcement cooperation. Other treaties with provisions on cyber crime, such as the African Convention on Cybersecurity and Personal Data Protection adopted in June 2014, could have similar relevance for responses to cyber terrorism.

30. However, under treaties on cyber crime, states parties would treat cyber terrorism as ordinary crime because the treaties do 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 such acts as different from other criminal behavior. Why states would deviate from this pattern with cyber terrorism is not clear. In addition, only 43 states

have ratified the Convention on Cybercrime (compared to an average of 168 parties for the anti-terrorism treaties in Table 1),³ which limits its ability to support responses to cyber terrorism.

2. Extradition Treaties, Mutual Legal Assistance Treaties, and Cyber Terrorism

31. States responding to cyber terrorism could use bilateral treaties designed to facilitate cooperation on criminal and law enforcement matters. A government could seek extradition of persons suspected of committing cyber terrorism through extradition agreements or request help investigating cyber terrorism through mutual legal assistance treaties (MLATs). Extradition treaties might support extradition for the crime of cyber terrorism if the requesting and requested states have criminalized this crime in similar ways—a prospect harmonization of national criminal laws on cyber terrorism would enhance. Otherwise, extradition could be based on established cyber crimes, such as causing damage to computer systems through unauthorized access, or non-cyber crimes recognized by the requesting and requested state.

32. MLATs facilitate law enforcement cooperation, but typically are not specific to any type of crime. They could be used, where applicable, in investigating alleged acts of cyber terrorism. However, MLATs have proved difficult to use effectively in connection with cyber crimes, as evidenced by calls for MLATs to be modernized to be more helpful against cyber-crime.

D. Extraterritorial Jurisdiction, International Law, and Cyber Terrorism

33. In addressing terrorism, states have prescribed national criminal law to terrorist acts occurring outside their territories that are directed against their governments, populations, economy, or nationals. States base extraterritorial jurisdiction on terrorism on treaty commitments (e.g., anti-terrorism treaties) or customary international law on prescriptive jurisdiction. 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 nationals located in foreign countries (passive personality principle); or (3) causing significant effects to persons or activities in their territories (effects principle).

34. Application of customary rules on extraterritorial jurisdiction to cyber terrorism is unlikely to raise novel issues simply because the context is cyber. Questions might arise concerning what effects support a charge of cyber terrorism as opposed to cyber or other types of crime, but courts have addressed in non-cyber contexts whether the domestic effects of extraterritorial acts are significant enough to warrant extraterritorial application of national law. Perhaps more importantly, 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 intimate or coerce a government).

³ Convention on Cybercrime, Status (as of October 7, 2014), <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>.

E. Summary on International Law and Responding to Cyber Terrorism

35. Responses to cyber terrorism can draw on a great deal of existing international law, including anti-terrorism, cyber crime, extradition, and mutual legal assistance treaties, and customary rules on the extraterritorial jurisdiction. Completing the Comprehensive Convention on Terrorism would provide another international legal way for responding to cyber terrorism, but the prospects for this treaty are not good. Claims that customary international law recognizes an international crime of terrorism remain controversial, which complicates using this crime in thinking about how to respond to cyber terrorism.

36. Using anti-terrorism or cyber crime treaties does not require crafting a specific definition of cyber terrorism because states will evaluate acts according to offenses defined in those instruments. “Dual criminality” requirements in extradition treaties, combined with the lack of international harmonization on the crime of cyber terrorism, might deter extradition requests based on alleged acts of cyber terrorism and encourage requests grounded in cyber crime or general criminal laws. Applying domestic criminal law in an extraterritorial manner under customary international law is another strategy for responding to cyber terrorism. Overall, using existing treaties and/or customary international law on jurisdiction would allow states to avoid difficulties they would encounter in negotiating a common definition of cyber terrorism.

37. However, relying on existing international law to respond to cyber terrorism would deviate from the pattern states followed as terrorism evolved. The development of treaties on particular forms of terrorism dominates the history of international law on this issue, suggesting that states might prefer to adopt a treaty purpose-built for cyber terrorism. The template for a “Convention on the Suppression of Cyber Terrorism” is well established in anti-terrorism treaties and crime-centric agreements, such as the Convention on Cybercrime.

38. Although states created treaties in response to various terrorist attacks, governments have adopted treaties to facilitate responses to types of terrorism that have not happened. The International Convention for the Suppression of Terrorist Bombings (1997) covers acts of terrorism that release or disseminate biological agents—something that had not occurred when the treaty was adopted. The International Convention on the Suppression of Acts of Nuclear Terrorism (2005) contains offenses not based on actual nuclear terrorism. These examples demonstrate that states could adopt a cyber terrorism treaty before acts of cyber terrorism occur.

39. Whether states should pursue this course is a harder question. Although a Convention on the Suppression of Cyber Terrorism would reflect how states traditionally addressed new types of terrorism, whether a treaty on cyber terrorism modeled on existing anti-terrorism agreements would be effective is not clear. Among other things, this strategy does little to protect against or prevent cyber terrorism. As events after 9/11 demonstrate, policymakers began to emphasize protection against and prevention of terrorism more than reliance on criminal law approaches.

40. Worries about law enforcement strategies exist with cyber crime as well, whether the international law in question is the Convention on Cybercrime, extradition treaties, or MLATs. These concerns include the ratification status of the Convention on Cybercrime, difficulties the cyber context creates for identifying perpetrators with the clarity and timeliness needed to make

extradition and mutual legal assistance treaties effective (the “attribution problem”), and problems making MLATs work in the timeframes required for investigating cyber crimes.

41. Why applying the traditional criminal law approach to cyber terrorism would avoid these challenges, difficulties, and problems is not clear. The diversity of the ways in which states define cyber terrorism in national law suggests that reaching a common definition through a treaty-based or soft-law effort would be politically difficult and diplomatically time-consuming. The definitional challenge would also confront cyber-specific questions, such as whether the criminal offense should cover disabling functionality in addition to damaging property or data, and cyber-specific phenomena, such as “hacktivism,” which many consider more akin to civil disobedience than terrorism. In addition, terrorists sophisticated enough to launch cyber attacks would, in all likelihood, exploit the attribution problem to frustrate criminal law mechanisms.

42. As with terrorism generally, problems with responding to terrorist acts through criminal law strategies supported by international law do not mean these strategies should be abandoned. However, as the post-9/11 era witnessed, states supplemented the traditional approach to terrorism with an emphasis on strategies to protect against and prevent terrorist activities. This overview now considers how international law relates to protection and prevention strategies.

IV. International Law and Protecting against Cyber Terrorism

A. Protecting against Terrorism and Cyber Terrorism

43. The application of criminal law might deter some terrorist activities and, in this way, protect societies from terrorism. However, policymakers developed measures to protect against terrorism in ways that do not rely on the criminal law’s potential deterrent effect. These measures “harden the target” by making it more difficult for terrorist acts to succeed through (1) protecting potential targets against terrorist attacks; (2) securing dangerous materials from terrorist access; and (3) making targets more resilient through capabilities to mitigate the impact of an attack and recover quickly from it. The protection strategy assumes deterrence will fail and terrorists will try to attack. In this context, policymakers need interventions not based in the criminal law, and these interventions raise their own national and international legal issues.

44. For terrorism and cyber terrorism, defending critical infrastructure is at the center of protection strategies. Even before 9/11, U.S. policymakers identified the need to protect critical infrastructure from physical and cyber attacks by terrorists, and the 9/11 attacks intensified this emphasis. Policy documents that discuss cyber terrorism often frame this threat in terms of the vulnerability of critical infrastructure, especially critical infrastructure owned and operated by the private sector. The strategy is to strengthen cyber defenses against malevolent infiltrations regardless of their source. This “all hazards” approach protects against not only cyber terrorism but also cyber crime and cyber espionage because improving cyber defenses “hardens the target” against different threats.

45. Beyond protecting critical infrastructure, policymakers have tried to secure plastic explosives and biological, chemical, and nuclear materials from getting into terrorists’ hands. Through treaties, states criminalized acts of terrorism utilizing biological, chemical, and

radiological materials, but improving the physical security of these items seeks to protect these “dual use” technologies from terrorist acquisition. Achieving this objective also protects against access to these materials by criminals or foreign governments.

46. In terms of resilience, counter-terrorism policy stresses the importance for the public and private sectors to mitigate the consequences of terrorist attacks and recover rapidly. 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.

47. The protection strategy does not require identifying whether an attack’s source is a criminal, intelligence agency, or terrorist. Unlike responses based in the criminal law, protection measures do not need definitions of the actions and intentions of different perpetrators. Protection strategies move away from the reactive criminal law approach. Stronger defenses and resilience capabilities can create deterrent effects, connecting this strategy with the goal of preventing terrorism. Protection reflects a proactive “all hazards” approach to multiple threats.

B. International Law, Critical Infrastructure Protection, and Cyber Terrorism

48. The criminal law approach in counter-terrorism policy has generated a great deal of international law. The strategy of protecting critical infrastructure from terrorist attacks involves international cooperation, but it has not produced much international law. Efforts to protect against terrorism are often domestically focused because governments can take action without international cooperation, especially improving the physical security of critical infrastructure within their respective territories.

49. National policies do, however, identify international cooperation on critical infrastructure protection (CIP), including cyber aspects, as important. Bilateral relations sometimes include CIP activities. Regional organizations, such as the European Union (EU) and the Organization of American States, facilitate CIP cooperation. Security organizations, including NATO and the Shanghai Cooperation Organization, pay attention to CIP. Multilateral organizations, such as the UN, stress the need for better CIP. However, with limited exceptions, cooperation on CIP has largely proceeded without the need for, or the creation of, new international law.

50. Generally, international cooperation on CIP in the cyber context focuses on building domestic capacities to defend against cyber threats. Beefing up defenses involves identifying effective cybersecurity policies and practices (e.g., creating computer incident or emergency response teams), sharing information on threats, providing assistance when requested, and devoting diplomatic attention to this challenge. This pattern echoes cooperation and international law on the security and safety of infrastructure facilities and dangerous materials, transboundary pollution, and industrial accidents, which emphasize securing operations, sharing information, providing assistance, and regularly cooperating to enhance protection capabilities.

51. Existing treaties have proved flexible enough to allow cybersecurity to become an agenda item. International organizations and treaty regimes relevant to critical infrastructure sectors, such as nuclear energy and air transport, have started to consider cybersecurity within their

mandates and mechanisms. The International Atomic Energy Agency (IAEA) developed a Computer and Information Security Programme overseen by its Office of Nuclear Security, and IAEA included cybersecurity in its *Nuclear Security Plan 2014-2017*. The states parties to the Convention on Nuclear Safety (1994) identified cybersecurity as a cross-cutting issue. The International Civil Aviation Organization tasked its Threat and Risk Working Group with addressing cybersecurity in civil aviation, including cyber threats to air traffic management systems. However, cybersecurity threats in the maritime sector have not been on the International Maritime Organization's agenda.⁴

52. Specific international 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. The European Commission has proposed a directive that would require member states to establish a minimum level of national capabilities for network and data security. Members of the Shanghai Cooperation Organization cooperate on "[e]nsuring information security of critical structures of the Parties." When it enters into force, the new African Union Convention on Cybersecurity and Personal Data Protection will require each party to adopt a national cybersecurity policy that includes protecting "essential information infrastructure." Certain proposals to create international law to protect against cybersecurity threats, such as an obligation to provide assistance to victims of cyber attacks or a prohibition against attacks on the Internet's root servers, have not gained diplomatic traction.

53. As the proposal for prohibiting attacks against the Internet's root servers suggests, the scope of CIP extends to critical *cyber* infrastructure, rather than just critical infrastructure dependent on cyber technologies. For example, submarine communication cables move vast amounts of digital communications around the world. Cyber attacks by terrorists could target such cables, raising questions about how cybersecurity for submarine cables is provided and can be improved. International law on submarine cables did not develop with cyber terrorism in mind, and, even outside the context of terrorism, questions have been raised about the adequacy of this law concerning the protection of such cables. Concerning other critical cyber infrastructure, the International Telecommunication Regulations (ITRs), as revised in 2012 by the International Telecommunication Union (ITU), require states parties to work to ensure the security of international telecommunication networks. However, controversy over this and other provisions led many ITU member states to oppose the revised ITRs, which limits prospects for using this body of international law to advance protection of critical cyber infrastructure.

54. The integration of cybersecurity into international policies and legal regimes designed to protect critical infrastructure of all kinds demonstrates that strengthening this process is important for defending against cyber terrorism. Here, international law has a number of functions. First, it provides general rules and supports institutional mechanisms that allow states to focus on cybersecurity and CIP within broader cooperative programs. Second, through these programs, states can produce soft law on cyber CIP that informs not only domestic activities but

⁴ Marsh, *The Risk of Cyber-Attack to the Maritime Sector* (July 2014), <http://nederland.marsh.com/Portals/54/Documents/Marine%20Cyber%20Paper%20-%20Aug%202014.pdf> (stating that the International Maritime Organization confirmed in June 2014 "that the cyber threat had not been brought forward for discussion by a member [state] and consequently, was not on its work program at this time.")

also the work of other international organizations or treaty regimes facing cybersecurity problems. Third, it provides a way to analyze whether common practices by states, such as cybersecurity “due diligence,” reflect emerging customary international law. Fourth, states might determine that binding obligations for cyber CIP are needed and use treaty law to achieve harmonization of stronger cyber defenses.

C. International Law, Securing Dangerous Materials from Terrorists, and Cyber Terrorism

55. States have used international law to ensure that certain dangerous materials do not fall into terrorist hands. This law includes treaties on the protection of nuclear materials during transport and the marking of plastic explosives. 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 binding obligations on UN member states to prevent terrorists from getting access to nuclear, biological, and chemical materials.

56. How relevant these uses of international law are for protecting against cyber terrorism is not clear. Given the nature of cyber technologies, identifying the cyber equivalents of plastic explosives or nuclear, chemical, or biological materials is difficult, if not misguided. Some attention has been paid to the potential need to regulate the 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. However, a zero-day vulnerability is essentially information about a bug in a software program, and such information is also potentially valuable not only to terrorists and criminals but also to software makers, cybersecurity researchers, law enforcement officials, and intelligence agencies.

57. Beyond zero-days, contemplating how states would use international law to secure dangerous malware from terrorist acquisition proves daunting. The danger really 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. Efforts to protect against terrorist use of nuclear, chemical, and biological materials have included efforts to educate scientists on safe, secure, and legal research or provide employment for scientists to reduce the possibility that terrorists would buy their expertise. These ideas also do not translate well to the cyber context.

58. Taking the nature of cyber technologies into account might recommend a different approach to “securing materials.” This approach would emphasize reducing cybersecurity vulnerabilities upstream in hardware and software research, development, and production and cybersecurity risks downstream created by how 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 cyber technologies and their uses, which would require changes in how hardware and software technologies are developed and how people use these technologies. However, problems experienced with trying to improve the “culture of security” within the communities that make and use software illustrate the difficulties this approach would face, without even including collective action problems global application of it would produce.

D. International Law, Damage Mitigation and Recovery, and Cyber Terrorism

59. As noted above, protection strategies also aim to strengthen a government's and society's abilities to mitigate the damage from a terrorist attack and recover quickly from it. Such resilience comes from capabilities that permit rapid identification of an attack and effective control of its consequences. Policymakers have stressed resilience and recovery across all types of terrorism, but especially with respect to terrorism involving biological, chemical, or radiological materials.

60. States have used international law to support these objectives. Member states of the World Health Organization (WHO) revised the International Health Regulations (IHR) in 2005 in order to strengthen national and international capabilities to identify and manage serious disease events regardless of their source. 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 create the ability in each state for mitigation of health and social consequences and rapid return to normality. Treaties on transboundary pollution and transboundary industrial or nuclear accidents also have provisions that attempt to strengthen states parties' abilities to control the effects from such pollution and accidents, whatever the cause.

61. Cybersecurity experts have identified the need for cyber systems to be resilient when adversely affected by unauthorized intrusions, no matter the source. This theme has been particularly prominent concerning the cyber aspects of critical infrastructure protection. The increasing attention international organizations with responsibilities in critical infrastructure sectors are paying to cybersecurity includes the need for post-incident resilience and recovery capabilities at the national level, supported by international assistance when needed.

62. Whether international law can and should play a heightened role in this protection strategy remains open for debate. The "all hazards" approach to resilience and recovery is relevant to defending against potential acts of cyber terrorism, but moving in this direction is not dependent on cyber terrorism becoming an actual, as opposed to an anticipated, problem. However, as the Ebola epidemic in West Africa revealed, far too many WHO member states failed to build and maintain the public health capabilities required by the IHR. International legal obligations for mitigating the consequences of serious disease events have not translated into on-the-ground capabilities, an outcome which raises questions about the effectiveness of an international legal strategy not supported by any plan or financial resources. The success treaty regimes on transboundary air and water pollution and industrial accidents have had often flows from the strength of bilateral or regional relations among states confronted with these problems. Although regional organizations are active in this policy space, cybersecurity threats do not exhibit the geographical proximity that characterizes robust cooperation on transboundary harms.

E. International Law, “Situational Awareness,” and Cyber Terrorism

63. A cross-cutting requirement of the “all hazards” protection strategy is “situational awareness” created through collecting and sharing information about what threats and vulnerabilities exist. In the IHR, sharing information about disease events forms the centerpiece of WHO’s global surveillance system. Scaled-up surveillance raises questions about individual privacy that the IHR addresses. However, achieving situational awareness through heightened governmental cyber surveillance and information sharing creates more intense privacy concerns, as seen in controversies about surveillance and information sharing that erupted during the U.S. Congress’ attempts to adopt cybersecurity legislation.

64. These concerns touch international law’s recognition of the human right to privacy. Even before the disclosures made by Edward Snowden, this right confronted difficulties created by, among other things, the convergence of cybersecurity threats governments had to address and individual and social dependence on cyber technologies. Deepening cooperation against cyber terrorism, whether or not international law plays a role, has to address the implications for human rights created by the need for greater situational awareness in cyber protection strategies.

F. Summary on International Law and Protecting against Cyber Terrorism

65. International law has a smaller “footprint” with respect to protecting against cyber terrorism than it does with responding to such terrorism through criminal and law enforcement measures. The attention paid to critical infrastructure protection in terrorism policies has generated international cooperation, including on the cyber aspects of such protection, but this cooperation has not produced much international law on CIP generally or its cyber components specifically. International law on keeping dangerous materials out of the hands of terrorists and building resilience and recovery capabilities within states does not translate well to the cyber context. The need for situational awareness in the “all hazards” protection strategy exists for cyber terrorism, but this need potentially creates more friction between this strategy and international human rights law than it does for terrorism generally.

66. Although apparently uneven, the attention international organizations and treaty regimes related to critical infrastructure sectors are increasingly paying to cybersecurity might represent a promising way to advance international legal contributions to protecting against cyber terrorism. Evaluating this possibility requires more research about what relevant multilateral and regional organizations and treaty regimes are doing and evaluating potential strategies to cross-fertilize efforts to strengthen cyber defenses across appropriate diplomatic venues.

V. International Law and Preventing Cyber Terrorism

A. International Law and Preventing Terrorism

67. A distinguishing feature of terrorism policy after 9/11 has been a shift by governments, especially the United States, to prevent terrorist attacks. Although response and protection approaches can contribute to this goal, prevention strategies look beyond measures that rely on the criminal law or defensive “harden-the-target” efforts. From the prevention perspective,

criminal law approaches are too often reactive steps occurring after terrorists strike. Protecting against terrorism is important for prevention in some situations, but the protection path remains predominantly passive. By contrast, prevention measures actively seek to find, frustrate, and stop terrorist plots before attacks happen.

68. In general terms, efforts to prevent terrorist attacks have involved (1) expanded intelligence activities designed to identify terrorists and their planning; (2) cutting off financial support and flows of recruits to terrorist groups; (3) covert or overt actions, including the use of force, against individuals and/or groups suspected of planning terrorist attacks; and (4) interventions to address root causes of terrorism. More robust surveillance by governments and pre-emptive military strikes against terrorists produced controversies in international law. States have used international law in trying to suppress terrorist financing. In September 2014, the Security Council required UN member states to end the flow of foreign fighters to terrorist groups as another measure designed to prevent terrorism. For many reasons, attempts to deal with the root causes of terrorism remain largely political measures rather than sources of international legal obligations on terrorism prevention.

B. International Law, Intelligence Activities, and Preventing Cyber Terrorism

69. Preventing terrorism requires gathering and sharing information relevant to identifying potential terrorist activities. The incentive to prevent terrorism led to expanded surveillance and information sharing powers for intelligence and law enforcement agencies in many countries after 9/11. Well before Snowden's disclosures about the National Security Agency (NSA), international human rights advocates expressed concern about the encroachment of counter-terrorism intelligence activities by many governments on the rights to freedom of expression, freedom of assembly, and privacy. What Snowden revealed exacerbated tensions between expansive government surveillance powers and the enjoyment of civil and political rights recognized by international law. Although the NSA conducted electronic surveillance for reasons beyond counter-terrorism, the objective of preventing terrorism has been, and remains, a core rationale for activities by the NSA and the intelligence agencies of other countries.

70. The goal of preventing cyber terrorism does not escape the international legal controversies concerning expanded collection and sharing of intelligence information for counter-terrorism purposes. Although perhaps hard to imagine, trying to prevent *cyber* terrorism through intelligence activities might produce incentives for more intrusive surveillance. Put another way, timeframes for preventing cyber terrorism might be shorter than for preventing kinetic terrorism because the former might generate a smaller intelligence and/or operational "footprint" than the latter. Whether these speculations make any sense, it is hard to believe that pressure to engage in extensive intelligence gathering and sharing will be less for cyber terrorism than more traditional forms of terrorism when prevention is the objective.

71. Pre- and post-Snowden debates about government surveillance and the "right to privacy in the digital age" show few signs of settling down into any sustainable consensus. The emergence of the Islamic State as a dangerous terrorist group that uses the Internet for propaganda and recruiting has put counter-terrorism back at the top of the international political agenda, leading to the re-emergence of arguments stressing how critical intelligence activities are

to preventing terrorist attacks. Implementing the Security Council's resolution on ending the flow of foreign fighters to terrorist groups, such as the Islamic State, will require serious intelligence collection and sharing—both within and among countries—to identify individuals who might be preparing to join foreign terrorist groups.

C. International Law, Pre-Emptive Strikes, and Preventing Cyber Terrorism

72. Efforts to prevent terrorism have included governments using force against terrorists to disrupt imminent or emerging threats of terrorist attacks. The international legal controversies associated with pre-emptive strikes against terrorists include their compatibility with international law on the use of force, international humanitarian law, and international human rights law. Inserting cyber terrorism into this mix does nothing to change the disagreements fueling these controversies. Actionable intelligence that a terrorist group is planning cyber attacks could produce pre-emptive strikes in the same manner the plotting of traditional terrorist actions do.

73. Countries that engage in pre-emptive strikes are unlikely to forgo using force simply because terrorists plan to attack with cyber as opposed to kinetic technologies. Those who believe pre-emptive strikes violate international law are not likely to be more or less opposed if the debate includes prevention of cyber terrorism. Nor does bringing cyber terrorism into this controversy increase the likelihood states will engage in more pre-emptive strikes with cyber means—so-called “active cyber defense”—instead of conventional munitions. Terrorists already so extensively use the Internet for communications, recruiting, propaganda, and fundraising that states supporting pre-emptive strikes have ample reason for using cyber weapons to disrupt cyber-based terrorist planning, preparations, and plots. Cyber strikes against terrorist computers and networks would not, in all probability, constitute a use of force of greater lethality and destructiveness than kinetic operations, place heightened stress on principles of international humanitarian law, or result in extrajudicial killings.

D. International Law, Prohibiting Terrorist Financing, Stopping Flows of Recruits, and Preventing Cyber Terrorism

74. As noted above, states use international law to prohibit the financing of terrorist groups as part of preventing terrorism. This law includes the International Convention on the Suppression of Terrorist Financing (1999) and post-9/11 binding decisions of the Security Council, especially Resolution 1373 (2001). Given that terrorists are unlikely to limit themselves to malicious cyber activities in pursuing their goals, the international law on terrorist financing applies to efforts to provide funds for any terrorist group seeking to develop and use cyber weapons. This reality lessens the need to worry that the international law on terrorist financing does not specifically address or mention cyber terrorism.

75. Security Council Resolution 1373 requires UN member states to criminalize any person's participation in, planning, preparing, or supporting terrorism, which would cover providing cyber-specific capabilities (e.g., zero-day vulnerabilities; malware) or services (e.g., software coding; Internet services) to terrorists. Similarly, the Security Council mandate that UN member

states prevent the flow of individuals to terrorist groups is sufficiently broad that it applies to any person seeking to join a terrorist organization in order to provide cyber-specific skills.

E. International Law, Root Causes, and Preventing Cyber Terrorism

76. Although preventing terrorism is often linked with the need to address the root causes of terrorism, what these root causes are remains subject to debate given the diverse political contexts in which terrorism arises and the disparate motivations individuals have for turning to terrorism. Adding cyber terrorism to the conversation does not clarify this debate. International law applicable to preventing terrorism does not include obligations on states to address the root causes of terrorism. International law relevant to these root causes, such as international human rights law, does not necessarily take on heightened importance or become more effective because states want to prevent cyber terrorism.

F. Summary on International Law and Preventing Cyber Terrorism

77. Strategies for preventing terrorism have generated sustained consensus and intense controversy in international law. The international legal rules developed to prevent and suppress terrorist financing, other forms of support for terrorist activities, and the flow of foreigners to terrorist groups have emerged largely from multilateral processes without significant opposition. These rules apply to preventing cyber terrorism as well as more traditional forms of terrorism, which suggests further development of international law in these areas specifically for cyber terrorism might not be worthwhile.

78. However, controversies populate international law's application to the exercise of government surveillance and information sharing powers and the use of pre-emptive strikes as terrorism prevention strategies. Bringing cyber terrorism into this context provides no obvious way to bridge disagreements that exist. The return of counter-terrorism as an international political priority because of the Islamic State's rise provides momentum for extensive intelligence activities and pre-emptive uses of force against terrorist leaders and groups. This momentum does not decide the international legal controversies in favor of those who back forward-leaning prevention strategies, but neither does it create common ground that could support getting beyond the impasse that characterizes international legal discourse on these prevention issues.

VI. The Overview, the Study Group's Objectives, and Next Steps

A. The Overview and the Study Group's Objectives

79. As this overview shows, the respond, protect, and prevent triad in counter-terrorism policy provides a template for mapping the international legal issues potentially relevant to cyber terrorism. This framework helps organize international law so its applicability to, or importance for, cyber terrorism can be thoroughly assessed. This approach can, with further work, contribute to the Study Group's objective of producing and analyzing an inventory of international law relevant to cyber terrorism. This overview does not, and was not intended to, contain such an

inventory, but its structure and content can accommodate a more comprehensive identification of international law in a manner that makes sense from policy and legal perspectives.

80. Using the respond, protect, and prevent triad also sheds light on the Study Group's objective of developing a definition of cyber terrorism. Applying much of the relevant international law under the response and prevention approaches does not require a detailed definition of cyber terrorism. The "all hazards" approach of the protection strategy also does not need an elaborate definition because it does not depend on identifying the source of a threat or attack. Precision and clarity in defining cyber terrorism would matter most in attempts to harmonize a criminal offense of cyber terrorism through (1) a new anti-terrorism treaty on the suppression of cyber terrorism; or (2) soft-law efforts to strengthen national criminal laws and use of extradition and mutual legal assistance treaties.

81. This overview raises issues relevant to the Study Group's objective of assessing whether pro-active international legal action concerning cyber terrorism would be worthwhile or feasible. Such actions could support response, protection, and/or prevention strategies against cyber terrorism. Recommendations could include maximizing the utility of existing international law by ensuring its applicability to cyber terrorism is clear. This direction could involve various activities, such as states parties to relevant anti-terrorism treaties declaring that defined offenses include acts undertaken through cyber means and methods. Similarly, the Counter-Terrorism Committee could make sure UN member states understand that binding counter-terrorism obligations the Security Council has imposed apply to the cyber realm.

82. Recommendations might also encourage multilateral and regional organizations with responsibilities for critical infrastructure, including critical cyber infrastructure, to heighten the attention they pay to cybersecurity. This approach would include fostering dialogue among such organizations in order to share information and best practices across sectors. The Study Group could also support existing proposals, such as upgrading MLATs to accommodate the demands of investigating cyber crimes. The Study Group may decide to support making new international law, whether in the form of a Convention on the Suppression of Cyber Terrorism, a binding resolution from the Security Council on cyber terrorism, or a treaty focused on protecting critical infrastructure from cyber threats.

83. However, this overview does not contribute much to the Study Group's examination of the threat of cyber terrorism, including how technological trends and innovations might affect this threat. Apart from identifying areas where international legal approaches against terrorism do not transfer well to the cyber context, this overview does not advance the Study Group's ability to understand technological aspects of cyber terrorism. More work is needed to evaluate whether technological perspectives on cyber terrorism inform response, protection, and prevention strategies or support different approaches to cyber terrorism.

B. The Overview and the Study Group's Next Steps

84. Input from Study Group members is requested based on his or her reading of this overview, including on:

- Whether structuring analysis of the international law relevant to cyber terrorism under the respond, protect, and prevent framework is adequate for the Study Group's task (keeping in mind the Study Group must have some analytical structure in order to address comprehensively the international law important to addressing cyber terrorism);
- What substantive areas of international law or international legal issues are not mentioned in the overview that the Study Group should examine;
- What aspects of the international law included in the overview are missing, incomplete, misleading, or wrong;
- Where the Study Group's analysis requires broader and/or deeper consideration of international legal issues identified in the overview (e.g., approaches taken, and instruments adopted, by regional organizations);
- How existing approaches to cyber terrorism taken by countries represented by members of the Study Group differ, if at all, from the framework used in the overview and the areas and issues of international law it discussed;
- Whether you have, at this stage, inclinations about general or specific recommendations the Study Group should consider;
- Whether you have interests in particular international legal areas and issues on which you would like to focus as the Study Group moves forward (e.g., response strategies and use of criminal law; international human rights concerns with government surveillance; regional efforts to address cybersecurity challenges); and
- What other issues, ideas, and concerns you want to communicate.

85. Based on this overview and the input received, the chair and co-rapporteurs will produce a detailed outline to guide needed research and form a preliminary structure of the Study Group's final report. The outline will include a specific research agenda containing issues, questions, and areas that require more attention. The chair and the co-rapporteurs will circulate the outline and agenda for Study Group input, but they will, as that input process is underway, proceed with research and analysis on issues the Study Group will have to address in its final report. The chair, for example, has two research assistants working on questions related to anti-terrorism and cyber crime treaties and cybersecurity efforts of international organizations with responsibilities in critical infrastructure sectors (e.g., nuclear energy, civil aviation, and maritime transport).

86. With these next steps in mind, the chair would like to have input from Study Group members, as described above, **on or before November 14, 2014**. Receiving input by this deadline will permit the chair and co-rapporteurs to complete the detailed outline and research agenda for circulation by the end of 2014 (assuming the chair does not, again, egregiously disrupt the schedule by mismanaging his time). Study Group members should feel free to contact the chair or co-rapporteurs at any time during this process.
