DIFFERENT LEGAL CONSTRUCTS FOR STATE RESPONSIBILITY

Maeve Dion [152]

Abstract

For most countries, effective national cyber security will require international cooperation in both the preparation for and mitigation of cyber incidents. Currently, interactions among international cyber incident responders are based on technical, operational, diplomatic, and political relationships, not legal relationships. Most existing international legal frameworks were established for incidents and crimes unrelated to the cyber context; they therefore may be inapplicable or inefficient to properly address and deter cyber incidents that threaten national or international security. National and international cyber security may be improved by establishing a legal framework for accountability, and by holding each country responsible for ensuring minimum levels of security and incident response capabilities and for taking reasonable efforts to mitigate cyber incidents conducted through its information infrastructures. However, before any new constructs or new laws are created, existing legal frameworks should be assessed to determine their appropriateness for managing global and international cyber threats.

BACKGROUND

With society's ever-increasing reliance on the global information infrastructure, cyber security has become a significant aspect of national and international security. Governments, economies, and societies rely on the telecommunications and computer systems that make up this internationally-connected information infrastructure. Such dependence creates vulnerabilities when the information infrastructure becomes a target or field of conflict. Wrongdoers may send a flood of electronic messages to a targeted computer system, causing the system to fail or slow to a crawl due to the heavy communications traffic. Attackers may target a utility company's industrial control systems,[153] causing damage not only to the

152 Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, Arlington, Virginia, U.S.A.

153 Electronic systems that control industrial processes (e.g., for water and wastewater, electric power, oil and natural gas, etc.).

utility company but also to its customers who lose service.

In the past several decades, governments have therefore broadened their traditional definitions of national security to incorporate protection of critical infrastructures, and particularly the computer systems of those critical infrastructures. For example, The Netherlands determined that "[c]ritical infrastructure refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage." In the United States, critical infrastructure includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." In Australia, "[c]ritical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."[154]

Because telecommunications and information systems are connected globally, however, critical infrastructure protection may not be achieved from merely a national approach; it also requires international strategy and coordination. For example, due to the structure of the Internet, a local cyber incident may originate from computers on another continent. The increasingly interconnected computer systems create the potential for a local event to cascade across geographical and sovereign borders. National security incidents in critical infrastructure computer systems may therefore have significant international components, requiring cooperation in efforts of prevention, mitigation, prosecution, and deterrence.

The need for an international effort has been voiced by various international organizations and governments. In 2009 the Council of Europe established an ad hoc advisory group to address legal constructs for state responsibility regarding protection of critical Internet resources and cross-border flow of Internet traffic.[155] The European Commission in 2009 issued a new communication on Protecting

154 These definitions, and others, are found in: Kathryn Gordon & Maeve Dion, *Protection of "Critical Infrastructure" and Role of Investment Policies Relating to National Security* (Organisation for Economic Co-Operation and Development, 2008) (background document to the OECD Secretariat in support of the OECD Roundtables on Freedom of Investment, National Security and 'Strategic' Industries, Paris, France), http://www.oecd.org/dataoecd/2/41/40700392.pdf, p. 4 (Table 1: National Definitions of Critical Infrastructure).

155 Ad hoc Advisory Group on Cross-border Internet. http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/default_en.asp.

Europe from Large Scale Cyber-Attacks and Disruptions, which emphasized the importance of international cooperation for cyber security, and included action items to help member states evolve from a purely national approach.[156] In mid-2008, the Organisation for Economic Co-Operation and Development (OECD) recommended that member countries conduct a systematic review of their laws and regulations relevant to critical information infrastructures, and asses the need for updates, new laws, or new enforcement / implementation regimes; develop a national cyber security strategy that incorporates all the requisite government jurisdictions and private sector operations; and coordinate with other member states and non-OECD countries to take into account interdependency vulnerabilities of the global information infrastructure.[157]

November 2009 saw the launch of Australia's first Cyber Security Strategy, which includes among its priorities: international engagement and effective legal and law enforcement frameworks. Along with the June 2009 update of its National Security Strategy, the United Kingdom released its first U.K. Cyber Security Strategy, for which one key priority was international coordination for the development of international law. The United States' 2009 Cyberspace Policy Review identified multi-jurisdictional legal analyses and international cooperation as two of the most urgent policy action-items.

In addition to international cooperation, cyber security requires a multidisciplinary focus that integrates technical, organizational, political, and legal solutions. Comprehensive legal and policy analyses must guide and support the organizational and technical solutions to security challenges. Although most government policymakers are not experts in technology or telecommunications, it is important that policies and laws are written with a firm understanding of the technology and business realities that sustain the critical infrastructures.

COMMON PERSPECTIVES

National and international recognition of cyber vulnerabilities have resulted in legal research on a variety of related topics. For example:

- Existing literature includes treatises on the cyber component of national

156 Available at http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf.
157 *See OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]*, at http://www.oecd.org/dataoecd/1/13/40825404.pdf.

security,[158] cyber crimes and torts,[159] and law enforcement techniques and forensics.[160] Experts have written texts on cyber crime activities within organized and transnational criminal networks,[161] as well as case studies of actual computer crimes.[162] There has been a degree of international agreement on cyber crime efforts,[163] with some calls for additional international activities such as the creation of new treaties.[164]

- Attention has been given to civil liberty protections,[165] societal issues,[166] and regulation and other business concerns.[167]
- The military community was one of the first to look at policy and legal impacts of the burgeoning information infrastructure, thus developing a relatively rich research portfolio on cyber warfare.[168] Currently there is a nascent effort to create an international manual on cyber warfare, along the lines of the San Remo Manual on International Law Applicable to Armed Conflicts at Sea and the more recent Commentary and Manual on International Law Applicable

158 *E.g.,* Susan W. Brenner, Cyberthreats: The Emerging Fault Lines of the Nation State (Oxford University Press 2009); Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (The National Academies Press 2003); Cybersecurity and Homeland Security (Nova Science Publishers 2006).

159 *E.g.,* Jonathan D. Hart, Internet Law: A Field Guide, Sixth Edition (BNA Books 2008); Michael Rustad, Internet Law in a Nutshell (West 2009); Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger 2010).

160 *E.g.,* Bill Nelson, Amelia Phillips, & Christopher Steuart, Guide to Computer Forensics and Investigations, 4th Edition (Course Technology 2009); Anthony Reyes et al., Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors (Syngress 2007).

161 *E.g.,* Seymour E. Goodman & Abraham D. Sofaer, The Transnational Dimension of Cyber Crime and Terrorism (Hoover Press 2001).

162 *E.g.,* Byron Acohido & Jon Swartz, Zero Day Threat (Union Square Press 2008).

163 *E.g.,* the Council of Europe Convention on Cybercrime.

164 *E.g.,* AFP, "UN chief calls for treaty to prevent cyber war," The Australian (Feb. 1, 2010) (discussing comments by International Telcommunications Union secretary general Hamadoun Toure during a World Economic Forum) at http://www.theaustralian.com.au/australian-it/the-hub/un-chief-calls-for-treaty-to-prevent-cyber-war/story-fn4mm2dt-1225825397532.

165 *E.g.,* Human Rights and the Internet (Palgrave Macmillan 2000); Global Employee Privacy & Data Security Law (BNA Books 2009).

166 *E.g.,* Athina Karatzogianni, The Politics of Cyberconflict (Routledge 2006).

167 *E.g.,* W. Russell Neuman, Lee W. McKnight & Richard Jay Solomon, The Gordian Knot: Political Gridlock on the Information Highway (The MIT Press 1999).

168 *E.g.,* Richard W. Aldrich, "The International Implications of Information Warfare," Airpower Journal, pp. 99-110 (Fall 1996); U.S. Department of Defense Office of General Counsel, "An Assessment of International Legal Issues in Information Operations" (May 1999); Walter Gary Sharp, Sr., CyberSpace and the Use of Force (Aegis Research Corp. 1999); David J. DiCenso, "IW Cyberlaw: The Legal Issues of Information Warfare," Airpower Journal, pp. 85-101 (Summer 1999); Thomas C. Wingfield, The Law of Information Conflict (Aegis Research Corp. 2000); Greg Rattray, Strategic Warfare in Cyberspace (The MIT Press 2001); Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *Jus in Bello*," International Review of the Red Cross, Vol. 84, No. 846, pp.365-98 (June 2002); Cyberwar, Netwar and the Revolution in Military Affairs (Palgrave Macmillan 2006); Pia Palojarvi, A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict (Erik Castren Institute of International Law and Human Rights 2009).

to Air and Missile Warfare.

NOT WAR OR CRIME, BUT STILL A THREAT

Despite the relatively large bodies of work on cyber crime and warfare, only recently have legal researchers begun to recognize a legal "grey area" where an international cyber incident falls below the definitional thresholds of international humanitarian law and yet exceeds the traditional definitions, organizational structure, and deterrent effects of criminal law.[169] This is an area of national security concern, particularly regarding incidents in the computer systems of critical infrastructures. An example of such an incident would be "patriotic" efforts by individuals of Country A who are protesting actions by the government of Country B. These individuals may hack into the governmental or critical infrastructure computer systems of Country B. Alternatively, the protesting individuals may coordinate to flood Country B's government, financial, and media computer systems with so much electronic traffic that the systems fail or slow down so much as to be unusable.[170] Sabotage by protestors is not a new concept, but the situation is complicated by the digital ability to perpetrate sabotage from a distance, possibly anonymously,[171] and with the threat of cascading effects through the interconnected critical infrastructure computer systems.

If the cyber acts have been identified as crimes in a national penal code, the likely legal tools at Country B's disposal are traditional criminal law enforcement efforts and possibly a mutual legal assistance agreement with Country A. Of course, depending on the nature of their relationship, Country A may be reluctant to provide political or law enforcement assistance to Country B. An additional complicating factor is that due to the structure and nature of the Internet, the Country A protestors' malicious activity may be conducted via telecommunications systems beyond the immediate conflict (e.g., not just in Countries A and B, but also Countries X, Y, and Z). If Country B is prepared, it may have a Computer Emergency Readiness Team ('CERT'), and if it is lucky, Countries X, Y, and Z are friendly and have already established cooperative relationships between their CERTs and Country B. (It is important to note that Country B may be neither prepared nor lucky, since countries vary in their capabilities for cyber incident response, law enforcement, and intra- and inter-governmental coordination that may be required.)

169 *See* Eneken Tikk, Kadri Kaska & Liis Vihul, International Cyber Incidents: Legal Considerations (Cooperative Cyber Defence Centre of Excellence, 2010).
170 Called Distributed Denial of Services ('DDoS') attacks.
171 Due to the lack of high confidence in technically attributing an attack to a specific person, as well as a lack of high confidence (or international comfort) in identifying sponsorship of an attack to a specific nation.

The interactions among international cyber protectors and incident responders are mostly based on technical, diplomatic, and political relationships. There is no common, international law that requires other countries to help Country B, and thus there is no liability for failure to help. If the cyber incidents can be defined as armed conflict and can be attributed to specific country, then Country B may initiate actions under international humanitarian law. It should be noted that while traditional conflicts have included cyber components, to date no standalone cyber incidents (unattached to physical conflict) have been deemed armed conflicts, nor have any been sufficiently attributed to the sponsorship of specific countries. Other than the warfare paradigm, the international community appears to have no commonly-accepted framework for managing cyber threats or incidents that impact national security. Further, there is no international agreement that mandates each country have a minimum cyber incident response capability so that cooperation can be provided. There is no single organization that coordinates multinational cyber incident response efforts.

In 2009 an American Bar Association report noted that "the single greatest difficulty encountered thus far in the development of a legal response [to the national security cyber threat] lies in the transnational nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace."[172] Other legal and technical experts may disagree on the need for such legal structures. It is therefore important to investigate this issue in depth, analyzing and comparing various international legal approaches, and incorporating insight and critique by operational experts who understand the technology and business realities.

When faced with global threats or with international threats to a certain geographical region, nations have developed a variety of legal frameworks for cooperation, guidance, and accountability. International legal frameworks help manage global threats such as pandemics and the proliferation of nuclear weapons. Similarly, legal structures address international or regional threats like maritime piracy and environmental pollution. International humanitarian law and human rights law hold nations and individuals accountable for certain internationally wrongful acts. Before creating new constructs and laws, existing legal frameworks should be assessed to determine their applicability to global and international cyber threats. The following tables provide examples of two comparisons which may be investigated.

172 Paul Rosenzweig, Workshop Rapporteur, *National Security Threats in Cyberspace*, Post-Workshop Report, American Bar Association Standing Committee on Law and National Security & The National Strategy Forum (Sept. 2009), http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf.

TABLE ONE

GLOBAL ALERT AND RESPONSE	CYBER COMPARISON
Concerns about the spread of cholera and other epidemics in the mid-to-late 1800s led to international movements that have evolved into the United Nations World Health Organization ('WHO'). Today the WHO establishes norms and standards, provides technical support to improve the health infrastructure within member states, delineates policy guidelines based on scientific and technical evidence, and coordinates international watch and warning and response efforts to minimize the spread of infectious diseases. The WHO maintains a Global Outbreak Alert and Response Network to share intelligence and manage response to incidents. Incident management may include tracking the incident's origins and critical decisions of responders; providing logistics support and access to necessary equipment and supplies; coordinating international response teams; and organizing lines of communication and standardizing public messaging. The WHO's International Health Regulations ('IHR') were first established in 1969. The IHR are legally binding on almost 200 countries. In the most recent redraft of 2005, the IHR require minimum levels of national public health capabilities, mandate incident reporting by member states, and are applicable not only to disease outbreaks but to any serious public health emergency no matter the cause (e.g., chemical leaks or spills and nuclear melt-downs).	Many countries, private businesses, and organizations have watch and warning capabilities for cyber security. Companies such as those who run the Internet backbone have operations centers that constantly monitor global communications traffic. These companies communicate with each other as necessary to manage incidents affecting their networks. Depending on the severity or complexity of an incident, they may also communicate with national or organizational Computer Emergency Readiness Teams ('CERT'). Some governments require private sector reporting of cyber incidents, but other countries instead pursue "public-private partnerships" (cooperative agreements for information sharing and response coordination). For those countries that mandate incident reporting, the laws vary in both definition and scope; countries differ in defining what type of incident must be reported, and the reporting mandate may only apply to certain industries such as telecommunications companies. There is no international, commonly-enforced standard for incident reporting. There is no global organization that mandates minimum levels of national cyber incident response capabilities. While there is no cyber equivalent to the IHR, the closest analogy to the WHO may be the Forum of Incident Response and Security Teams ('FIRST'), whose members include government incident response teams as well as experts from industry and academia. However, as a voluntary, fee-for-membership organization not originating from within an organization such as the United Nations, FIRST is significantly different from the WHO.

TABLE TWO

STATE RESPONSIBILITY	CYBER COMPARISON
Non-state actors are a growing threat to national security. State responsibility for internationally wrongful acts committed by non-state actors is an evolving area of law. In *Nicaragua v. United States*, the International Court of Justice found that in order for a state to be responsible for human rights violations perpetrated by non-state actors, the state must have had "effective control" of the perpetrators. Under this standard, a nation may finance, train, equip, and organize the non-state actors, and yet still not meet the "effective control" test. The Appeals Court of the International Criminal Court for the Former Yugoslavia in the *Tadic* case presented a different standard. The court held, inter alia, that when the non-state actors were not organized militarily, state responsibility for the non-state actors' humanitarian violations existed when the state had "overall control" of the non-state actors. Such "overall control" may be shown by the state's financing, training, or equipping of the perpetrators and by coordinating or planning their actions. Another international law guideline developed after the terrorist attacks against the United States in September 2001. The United States held Afghanistan responsible for merely harboring and supporting al Qaeda – far below the standard of "effective control" or even "overall control." The United Nations Security Council, NATO, and the Organization of American States sanctioned this approach; numerous international law experts also supported this position.	In recent years, of the major international cyber incidents that were made public, most were conducted by non-state actors. Because of the anonymous nature of the Internet, it is difficult to obtain high levels of confidence in attribution of an act to an individual or group, or to show that a nation state sponsored a cyber attack conducted by non-state actors. Even if such proof is discovered, the standards of "effective control," "overall control," or "harboring and supporting" may not be applicable to cyber incidents. The state responsibility standards adhere to internationally wrongful acts which traditionally include genocide, violations of law applicable to armed conflicts, and crimes against humanity. These wrongful acts do not easily correlate to acts performed during cyber incidents which significantly damage a national economy or other critical infrastructure asset. Once "cyber incident-related" activities are identified as internationally wrongful acts, then the state responsibility standards may be analogized.

These examples are not meant as ideals of what is needed in the cyber realm; rather, they are examples of approaches and perspectives that may be investigated. Policymakers can learn much, not only from the processes and development of these international constructs, but also from the years of critique on how to improve such frameworks.

Cyber law literature is currently weighted with cyber war and traditional criminal law analyses. However, paradigms of criminal law and international law (state-on-state

aggression, armed conflicts) may not provide enough perspective regarding state responsibility for cyber incidents. To properly mitigate and manage national and international cyber security threats, additional perspectives and constructs may be needed. The goal of this presentation and whitepaper is to encourage analysts to look beyond the perspectives of warfare and crime, and to suggest that before new constructs or new laws are created, existing legal frameworks should be assessed to determine their appropriateness for managing global and international cyber threats.