National Security Cyberspace Institute
NSCI

CyberPro

December 2009

Keeping Cyberspace Professionals Informed

THE LAW AND POLICY OF PROTECTING OUR CRITICAL INFORMATION INFRASTRUCTURES

BY MAEVE DION, CENTER FOR INFRASTRUCTURE PROTECTION, GEORGE MASON UNIVERSITY SCHOOL OF LAW

In a recent seminar, a participant asked, "What is the law of critical information infrastructure protection?" The answer is that there is no single field of law, but rather a collection of various areas, which include:

- Security Regulations in certain industries / sectors
- Privacy and Data Protection Law
- Open Government Rules
- Information Sharing Limitations among Government Entities
- Antitrust / Competition Laws
- Private Ordering (Contracts and Tort Law)
- Criminal Law
- Emergency Powers
- National Security and Defense Law
- International Law

The law may be established by statute, regulation, executive order, etc., or it may be determined in case law developed by courts. In every instance, though, these areas of law are based upon a balancing of policy priorities, such as public safety and security, consumer protection, economic competitiveness and the safeguard of civil liberties.

At its heart, this model of lawmaking does not change when the subject involves cyber attacks and security, although some of the weighed factors may be more extreme – for example, the potential breadth of consequences due to interconnections and interdependencies, or the necessity for detailed planning and preparedness because the speed of response limits the time available for contemporaneous deliberation, etc. One factor that is more challenging in cyber incidents is the identification of the wrongdoer within the relevant level of legal proof. Yet even in this case, policymakers are still balancing the same policy priorities.

Thus it is vital that policies for the protection of critical information infrastructures be predicated on sound strategy that is rooted in societal priorities and norms. Solutions must be led by strategies, not by the latest and greatest tools or technologies.

In the development of such strategies, decisions are more political than legal. For example, it is a political decision as to whether our security priorities and resources should focus on the greatest likely threats (most probable) or on the threats of greatest consequence (perhaps not likely, but catastrophic if they happen).

Law can play a part in helping to identify when the sometimes competing policy priorities may overlap or conflict, and in carving out exceptions or solutions. The European Union (E.U.) has a data protection regime that includes restrictions on the use and transfer of personal data; this directive is based on the protection of privacy, a fundamental human right. In recent years, some E.U. member countries have deemed Internet Protocol addresses to be personal data, which could present a security threat by limiting the ability to share important information when responding to a cyber attack. However, member countries also have the ability to make exceptions to the data protection limitations for purposes such as national security and defense, or criminal law investigation and enforcement.

Law is a living thing and can always be refined. Because most of the existing laws were created before the advent of the global information infrastructure, some may not fit our current paradigm in which information can be accessed digitally, from great distances, and perhaps anonymously. Rather than create a whole new set of laws relevant only to cyber incidents, courts and lawmakers can refine existing law to accommodate the new methods of access and communications.

In an example from the United States, the crime of insider trading has traditionally required some sort of breach of fiduciary duty – the wrongdoer must have been an "insider" who improperly used information available to him precisely because he was an insider. Earlier this year, the U.S. Court of Appeals for the Second Circuit changed this traditional requirement, finding that insider trading can be accomplished by an outsider who hacks into a corporate network, gains access via fraudulent misrepresentation, and trades on "insider" information. The court could have retained the traditional standard, leaving prosecution for theft as the only remedy in the hacking situation. However, the wrongdoer was in the Ukraine, and prosecution for theft may not have been easy or cost effective. With insider trading, though, the Security and Exchange Commission can freeze the proceeds of suspected illegal transactions, keeping the potentially ill-gotten gains in this country while the transactions are investigated and tried.

This case has been remanded on the facts, and yet might be appealed to the U.S. Supreme Court; and while the case does not directly speak to cyber threats to national security, it gives an example of how courts can try to refine the law when new technologies create new methods for committing crimes.

More relevant perhaps to this newsletter are some areas of international law that are calling out to be refined in this new age of the global information infrastructure.

In many countries, cyber attacks are listed as a serious national security threat. Each country, though, has different infrastructure vulnerabilities and threats, different governmental authorities and jurisdictions, and different societal / commercial reliance on the information infrastructure. A national security threat in one country may be a nuisance in another. Some countries may not need to consider the U.S. business concerns of tort liabilities. Other countries may have purely governmental-owned communications infrastructures. Because of the variety of these factors, governments therefore have a diverse array of security approaches, levels of preparedness and legal regimes relevant to cyber incidents.

Yet despite all these differences, it is commonly accepted that *national* cyber security requires *international* cooperation and collaboration. It is my contention that international cyber security also requires some norms or structure of national responsibility for quelling cyber conflict that is originating from, or conducted via, that nation's territory.

Some countries have more robust domestic laws and enforcement mechanisms relevant to crimes that target, or are facilitated by, the information infrastructure; other countries are only just beginning this endeavor. There is no common international understanding regarding monitoring, logging/data storage or information sharing to assist in the pursuit of attackers; we have not yet developed norms for international responsibilities, liabilities or sanctions. There is no rule that says governments must protect their domestic computers and information infrastructures from being hijacked into botnets that threaten the national security of another nation. There is no requirement that countries must have their ISPs provide assistance in blocking bad traffic that may be taking down the power grid to another country.

The international law of state responsibility looks at a country's liability for assisting in wrongful acts perpetrated by identified actors (either other countries or non-state actors). Parsing the law requires an initial assessment of (a) what it means to "assist" in (b) an internationally wrongful act that is (c) conducted by either another country or by non-state actors. International law in these areas is far from clear in relation to physical attacks, let alone cyber attacks, but we can use these requirements to roughly frame-out some cyber-related questions for further study:

a) A finding of "state responsibility" has required some level of participation in the planning or coordination of the wrongful acts (not just the facilitation or funding, for example). There needs to be some further scholarship here, regarding cyber incidents, for surely there must be some sort of state responsibility for a country which, while not planning or coordinating the attack, permits its facilitation via the state's territorial infrastructure, without which the attack may not succeed.

b) Traditionally, the wrongful acts have been human rights violations (murder, torture, etc.). Even the potential new crime of aggression (still in draft state), coming out of the International Criminal Court, requires a use of "armed force," a term whose cyber connotations are not universally understood in the international arena. Many countries have already identified cyber attacks as national security threats; these may result in risks to human life, or to the national market / economy. These wrongful acts may not require a traditional "use of armed force." (For more on the application of the Law of Armed Conflict in cyberspace, see NSCI's interview with Col. Charlie Williamson from the June 2009 issue of CyberPro.)

c) In cyber incidents, it is sometimes challenging to identify the specific wrongdoers, and recent cyber incidents have shown how difficult it is to attribute state sponsorship to politically-motivated cyber attacks. For cyber incidents, though, whether the wrongful act was conducted by a country or by non-state actors, a country should be held responsible for allowing the wrongful act to be perpetrated via the information infrastructure within its sovereign territory.

As mentioned, there is a lot of work yet to be done in these areas of law. Many academics and researchers are attempting to find solutions to these problems, including legal solutions, national security policies and frameworks for international coordination.

In closing, I'd like to draw your attention to the new research agenda of the Cyber Conflict Studies Association, available at http://www.cyberconflict.org/Research-agenda. For those with an interest in legal matters, Study Two is the section that addresses law and policy. In the next year, this study will conduct virtual working groups that will develop primers in four areas:

- What U.S. agencies and departments have authorities that are implicated during cyber emergencies / conflict? Are these authorities properly understood? Comprehensive enough for national security? Too complex for operational deployment?

- How is the Posse Comitatus Act (PCA) properly understood in the context of cyber conflict? Given that U.S. law has enabled much cooperation between military and law enforcement, how can PCA be explained to lessen operational confusion and remove unnecessary restrictions to cooperation?

- From the U.S. perspective, what are the impacts of cyberwar, both defensive and offensive capabilities, on government-private sector or civil-military relations?

- From the U.S. perspective, when does cyberwar constitute a use of armed force or act of war? When does cyber conflict justify sanctions or other non-military state coercion? What are the other thresholds for government action?

We welcome your participation in this work (contact information is available on the Web site, or write to maeve@cyberconflict.org). The law and policy of protecting our critical information infrastructures is ever-evolving, and may require new strategies and possibly new legal doctrine. Hopefully this article will help encourage further scholarship on the topics.

About the Author

Maeve Dion is on the research faculty at the Center for Infrastructure Protection, George Mason University School of Law. Her work focuses on legal, policy, economic and educational issues relating to critical infrastructure protection, particularly information infrastructure. Maeve also leads a legal research project for the Cyber Conflict Study Association, and she provides academic legal support to task forces of the President's National Security Telecommunications Advisory Committee. Maeve holds an honors B.A. in political science from Eckerd College, and a J.D. cum laude from George Mason University School of Law.