Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection

David P. Fidler
Indiana University Maurer School of Law, dfidler@indiana.edu

Follow this and additional works at: https://www.repository.law.indiana.edu/facpub

Part of the Computer Law Commons, and the International Law Commons

Recommended Citation
https://www.repository.law.indiana.edu/facpub/2452

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.
In November 2014, Admiral Michael Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency (NSA), highlighted how extensively critical infrastructure protection (CIP) and cybersecurity are intertwined. In congressional testimony, Rogers observed that a number of states and non-state actors can shut down U.S. critical infrastructure through cyber means, with more nations seeking this capability. "I fully expect that during my time as the commander," Rogers asserted, "we are going to be tasked to help defend critical infrastructure within the United States because it is under attack by some foreign nation or some individual or group." "We have got to develop," Rogers argued, "a set of norms or principles for behaviors in this space."

Rogers’ call for norms to counter cyber threats to critical infrastructure challenges the adequacy of existing norms, including those in international law. This challenge is serious because where cybersecurity and CIP converge is not devoid of international law. In fact, a web of norms based in international law applies to cyber threats to criti-
Critical Infrastructure’s Cybersecurity Problem and International Law. Protecting critical infrastructure gained prominence in the 1990s in response to terrorism and increasing linkages between critical infrastructure and cyber technologies. In 1998, President Clinton established the goal that the United States should be able to protect its critical infrastructure from physical and cyber attacks by 2003. Subsequently, critical infrastructure’s reliance on the Internet deepened to the point, as Admiral Rogers testified, that cyber-dependent control systems “are foundational to almost every networked aspect of our life, from our water to our power to our financial segment to the aviation industry.”

U.S. experiences underscore why cybersecurity has become an important and difficult CIP issue. The Stuxnet operation against Iran and Snowden’s disclosures about NSA capabilities revealed that the United States can penetrate, monitor, manipulate, and damage foreign cyber-connected critical infrastructure. However, the United States has failed to protect its cyber-dependent critical infrastructure.

States should be able to protect its critical infrastructure from physical and cyber attacks by 2003. Subsequently, critical infrastructure’s reliance on the Internet deepened to the point, as Admiral Rogers testified, that cyber-dependent control systems “are foundational to almost every networked aspect of our life, from our water to our power to our financial segment to the aviation industry.”

[The United States’] disequilibrium between offensive and defensive cyber capabilities is a dilemma for critical infrastructure protection around the world.

This disequilibrium between offensive and defensive cyber capabilities is a dilemma for CIP around the world. Although policymakers recognize CIP should include international cooperation, international law has not featured prominently in policy discussions. First, much of a country’s critical infrastructure is located within its territory (e.g., municipal water systems), and governments can protect it...
International law outlaws all but one of the cyber threats to critical infrastructure that give policymakers heartburn.
and analyzing calls for new norms.

Legacy Rules and Cyber Crime Treaties: Existing International Law and Cyber Threats to Critical Infrastructure. Cyber threats to critical infrastructure arise from criminals, terrorists, and the intelligence agencies and militaries of states. With one exception, international law makes cyber activities by state or non-state actors that undermine CIP illegal. Most of the relevant norms come from pre-cyber international law, which are applied to cybersecurity problems. Many constitute fundamental principles, including the prohibitions on intervention, use of force, and attacks on civilian targets in armed conflict. The exception is espionage because international law does not prohibit or regulate it.

International Law, Critical Infrastructure Protection, and Cyber Threats from Non-State Actors. States have developed international law for cyber crime. The leading treaty, the Council of Europe’s Convention on Cybercrime (COE Convention), harmonizes national laws and facilitates law enforcement cooperation on cyber crimes. The African Union’s Convention on Cyber Security and Personal Data Protection (AU Convention) includes the same objectives. Although these treaties do not include crimes specific to critical infrastructure, their offenses apply to using unauthorized access to computers operating critical infrastructure to steal information, disrupt operations, extort money, or cause damage. In cases involving states not party to cyber crime treaties, governments can use general-purpose extradition agreements and mutual legal assistance treaties (MLATs) to address cyber crime involving critical infrastructure.

Terrorist efforts to access, disrupt, or damage computers operating critical infrastructure would fall within the international law on cyber crime. In addition, the International Convention for the Suppression of Terrorist Bombings (Terrorist Bombings Convention), which 168 countries have ratified, can be interpreted to cover terrorist cyber attacks against critical infrastructure. It requires parties to criminalize acts undertaken with the intent to cause death, serious bodily injury, or extensive property destruction to an “infrastructure facility” through a weapon or device “designed, or has the capability, to cause death, serious bodily injury or substantial material damage.” These provisions can encompass malicious software targeting critical infrastructure. States adopted this treaty in 1997 when concerns about terrorism against critical infrastructure became prominent, including worries about cyber vulnerabilities. In short, international law contains a widely accepted norm against terrorism perpetrated
against critical infrastructure through various means, including cyber.

**Cyber Threats to Critical Infrastructure from Military and Intelligence Activities.**

National security officials worry that foreign governments pose cyber threats to critical infrastructure. Recall Admiral Rogers’ prediction that, during his time in office, U.S. Cyber Command and NSA will have to respond to a serious cyber attack on U.S. critical infrastructure, potentially launched by a foreign country. In this context, international law has many norms, whether such an attack occurs in peace or war. During peacetime, international law prohibits the use of force by states, and the attack Rogers fears might violate this rule. Even if the attack did not constitute an illegal use of force, it would violate the obligations to settle disputes peacefully and not to intervene in the domestic affairs of another state. To avoid violating these norms, the foreign country would need to justify its cyber attack, perhaps arguing that it was using force in self-defense in response to an armed attack by the United States.

During armed conflict, the laws of war would apply to cyber attacks on critical infrastructure. Depending on the circumstances, a cyber attack on civilian critical infrastructure could violate the prohibitions on attacking civilian targets, using indiscriminate means and methods of attack, and engaging in attacks that cause disproportionate civilian damage. These rules would not apply if the critical infrastructure was a legitimate military target (e.g., a “dual-use” target), or the cyber operations did not constitute “attacks” under the law of armed conflict, namely acts intended, or reasonably like to cause, injury, death, damage, or destruction.

In his testimony, Admiral Rogers expressed concern that foreign governments are conducting cyber reconnaissance on U.S. critical infrastructure. However, international law does not prohibit foreign governments from spying on U.S. critical infrastructure. This situation is not unusual because, as noted above, international law does not seriously regulate espionage.

Intelligence agencies have exploited every new communications technology, and cyber technologies have been no different. U.S. complaints about Chinese cyber espionage have not gained international legal traction, even before Snowden revealed U.S. cyber espionage capabilities. International law’s permissiveness does not mean spying is harmless. It can create significant costs, disrupt national security strategies, and destabilize relations between nations. However, states have been unwilling to control espionage through international law—an outlook cyber threats to critical infrastructure have not changed.

**A Cyber-Defense Norm: International Law and Strengthening Cybersecurity**

[12] Georgetown Journal of International Affairs
in Critical Infrastructure. The web of norms also involves states using international legal mechanisms and instruments to strengthen cybersecurity within critical infrastructure in two ways. First, states work to strengthen CIP against cyber threats within existing international legal frameworks. These efforts, by and large, do not produce new international law but use established processes to achieve better cyber defenses for critical infrastructure. Second, countries create international legal obligations to protect critical infrastructure from cyber threats. These practices reveal emergence of an international norm on strengthening cyber defenses for critical infrastructure.

The practices also reveal a different approach to CIP. The legacy rules and international law on cyber crime discussed above slot a cyber threat into a category (e.g., terrorism, armed conflict) in order to identify what rules apply. By contrast, the approach informing the cyber-defense norm is an "all hazards" strategy to protect critical infrastructure from the range of cyber threats. This strategy does not focus on whether a cyber intrusion constitutes crime or espionage, but whether networks are protected against infiltrations from any source.

Strengthening Critical Infrastructure's Cyber Defenses Through Existing Cooperative Mechanisms. As cyber threats to CIP became more important, states started to use existing multilateral, regional, and bilateral mechanisms to cooperate on this problem. These efforts typically have not produced new international law but have elevated cybersecurity threats to critical infrastructure in established processes and institutions. For example, the UN's governmental group of experts analyzing international security implications of information technologies identified the need for increased cooperation on cyber threats to critical infrastructure.\textsuperscript{15} ASEAN,\textsuperscript{16} EU,\textsuperscript{17} OAS,\textsuperscript{18} OECD,\textsuperscript{19} NATO,\textsuperscript{20} and U.S.-Canada cooperation\textsuperscript{21} have undertaken activities on this issue. Generally, these efforts seek to strengthen cyber defenses for critical infrastructure, improve information sharing on threats and cybersecurity practices, and facilitate assistance to other countries. International organizations overseeing critical infrastructure sectors are also addressing cybersecurity. The International Atomic Energy Agency (IAEA)\textsuperscript{22} and the International Civil Aviation Organization (ICAO)\textsuperscript{23} are increasing their members' awareness of, and efforts to protect against, cyber threats to nuclear energy and civil aviation.

The IAEA's and ICAO's efforts provide a model for other international organizations or regimes responsible for critical infrastructure sectors to increase CIP activities against cyber threats. To the extent not already underway, activities within other legal
frameworks touching on critical infrastructure, such as treaties on managing shared watercourses or control of industrial accidents, can implement the “soft law” norm of strengthening cyber defenses for critical infrastructure, thus implementing it more widely where cyber-dependent critical infrastructure control systems operate.

**Strengthening Critical Infrastructure’s Cyber Defenses Through New International Law.** Some states have gone beyond cooperation through established mechanisms to adopt international legal obligations specific to protecting critical infrastructure from cyber threats. An EU directive requires EU members to designate “European Critical Infrastructure” in the energy and transport sectors and mandate that operators have security plans covering risks, including cyber threats. Members of the Shanghai Cooperation Organization (SCO) agreed in a treaty to cooperate on ensuring information security within critical infrastructures. The AU Convention requires parties to take cybersecurity actions to protect critical infrastructure. The use of binding requirements distinguishes this part of the web of norms from non-binding activities undertaken within existing legal frameworks.

States could craft more specific international law to bolster cyber defenses for critical infrastructure in a number of ways. Governments could negotiate a “Convention for the Suppression of Acts of Cyber Terrorism” that, among other things, addresses the threat of terrorist cyber activities against critical infrastructure. Following the AU Convention, parties to the COE Convention could amend the treaty to require additional sanctions for cyber crimes committed against critical infrastructure. Reflecting on the Tallinn Manual on the International Law Applicable to Cyber Warfare, governments and non-governmental experts could collaborate in clarifying how international law applies to cyber operations against critical infrastructure in armed conflict and cyber threats against critical infrastructure in peacetime.

**Problems with the Web of Norms.**

Problems with legacy rules and cyber-crime treaties: Although pre-cyber norms apply, many did not function well before cybersecurity came along. The effectiveness of the prohibitions on intervention in the domestic affairs of other states and on the use of force has long been controversial. Adding cyber to the mix has not produced stability. For example, whether various cyber operations, including Stuxnet, violated the use-of-force prohibition has been debated without consensus arising. The possibilities cyber technologies offer intelligence agencies and militaries increase incentives to keep certain legal waters muddied, raising concerns about the effectiveness of legacy rules in the cyber age.

In terms of espionage and armed conflict, the legacy rules apply in
ways that make use of cyber technologies attractive. The Internet has been "God’s gift to spies,"38 and, despite the problems associated with cyber espionage, states generally have no appetite to restrict this practice through international law. The United States favors an international norm against economic espionage,39 but it has not been successful in advancing it—and Snowden’s disclosures have made this objective harder. The law of armed conflict applies in ways that make cyber
gal cyber acts to specific actors often proves technically difficult, a problem compounded by legal principles for determining state responsibility or imposing criminal sanctions on individuals that set high evidentiary thresholds. Thus, the attribution problem often weakens the effectiveness of legacy rules and treaties on cyber crime when applied to protect critical infrastructure from cyber threats.

Finally, in terms of cyber-crime threats to critical infrastructure, exist-
The possibilities cyber technologies offer intelligence agencies and militaries increase incentives to keep certain legal waters muddied, raising concerns about the effectiveness of legacy rules in the cyber age.

weapons, operations, and attacks attractive politically, militarily, and ethically. Being able to disrupt critical infrastructure deemed a "dual use" target with cyber means, rather than destroying it with kinetic violence, offers capabilities advanced militaries want. So, rather than discouraging interest in cyber, the laws of war heighten it.40

Many legacy rules and the law in cyber-crime treaties also struggle with the attribution problem. For example, to apply the prohibition on the use of force or criminal offenses in anti-terrorism and cyber-crime treaties, the rules require identification of the perpetrator. Attributing illegal treaties are not, to date, widely accepted. Only 46 countries have ratified the COE Convention, despite the treaty being open for any state to join for over a decade.41 The AU Convention, adopted in June 2014, has not entered into force, and only AU members can ratify it. These facts mean many states rely on extradition treaties and MLATs to address cyber crime against critical infrastructure, but these instruments have not proved sufficiently effective against cyber crime for many reasons, including the attribution problem.42

Problems with the "allhazards" cyber-defense norm: Using international law to strengthen
cyber defenses in critical infrastructure is not politically controversial, and the "all hazards" approach avoids the attribution problem. However, whether using existing international legal mechanisms or creating new international law can significantly improve cyber defenses for critical infrastructure is a harder question. Non-binding activities in various international organizations, such as IAEA and ICAO, are too recent and uneven to invite either enthusiasm or cynicism. In terms of new international law, the AU Convention has no track record because it is not in force. Whether the SCO treaty has contributed to better cybersecurity in critical infrastructure of SCO members is not apparent. The EU observed that, while opinions differed on whether cybersecurity had improved, its directive "encouraged policies for the protection of national critical infrastructure . . . [and] resulted in concrete actions such as the creation of specific national bodies to deal with CIP policies." More substantively, whether the cyber-defense norm contributes enough to protecting critical infrastructure from cyber threats, especially "advanced persistent threats" from states or criminal organizations, is not clear. Concerns about cyber-defense measures have fed debates about the need for "active defense" strategies, which include, among other approaches, victims "hacking back" against suspected perpetrators. The controversies surrounding active defense mean that no active-defense norm is likely—but skepticism about cyber defenses is not dissipating, as will be addressed below.

Problems with calls for new norms:
Admiral Rogers is not alone in wanting new norms. For years, the Obama administration emphasized the need for "norms of responsible behavior in cyberspace," and, in 2015, the U.S. government has advanced principles it believes "can contribute substantially to conflict prevention and stability in time of peace." U.S. technology companies, such as Microsoft, have developed ideas for norms. However, these calls for new norms confront the damage Snowden did to the United States in international cyber affairs. For example, U.S. arguments that cyber espionage targeting the private sector (including operators of critical infrastructure) constitutes "economic warfare" have been, in the post-Snowden period, dead on arrival internationally. Another problem with the desire for new norms is a lack of clarity about what norms people have in mind and how they differ from what the existing web of norms contains. For example, the U.S.-proposed norms prohibiting a state from damaging or interfering with critical infrastructure or computer emergency response capabilities in another state apply to actions that are illegal under international law. Pushing for cyber-specific corollaries to existing rules is not objectionable, but the upside is limited given that international law
already outlaws the behavior in question. However, some corollaries might re-open controversies in international law. For example, trying to shield national computer emergency response capabilities from cyber operations during armed conflict might highlight disagreements about “dual use” targets, including friction related to positions of countries, such as the United States, that define such targets broadly. Finally, proposals for new norms have to explain how they would fare better than the old ones. Advocacy for cyber-specific corollaries to existing general principles often fails to illuminate why state or non-state actor compliance would improve. Admiral Rogers expressed his concern that a foreign country or non-state group will, in the near future, launch a major cyber attack on U.S. critical infrastructure—an attack that would violate international law. Why Rogers thinks that foreign countries or non-state groups—apparently willing to defy international law—would comply with, or be deterred by, new norms is perplexing. The answer to this riddle might be that norms are not, in fact, the answer to the problem Rogers posited.

**From Norms to Power: The Dawn of Cyber Deterrence.**

In congressional testimony in March 2015, Admiral Rogers focused on the need for the United States to develop, threaten, and use offensive cyber capabilities to deter foreign cyber threats. Rogers argued that strategies focused on cyber defenses are not protecting U.S. computer networks or deterring foreign state and non-state actors from infiltrating them. According to Rogers, the answer is to use offensive cyber capabilities to increase deterrence. In early April 2015, President Obama signed an executive order authorizing sanctions on individuals outside the United States who engage in malicious cyber activities that constitute a threat to U.S. national security, foreign policy, economic health, or financial stability. The executive order included within such threats cyber activities that harm or compromise entities operating critical infrastructure. The executive order seeks to deter individuals, by threat of targeted sanctions, from engaging in malicious cyber activities against U.S. computer networks, especially those used to operate critical infrastructure. In mid-April 2015, the U.S. Department of Defense released its new cyber strategy, and news reports and experts noted the strategy’s emphasis on offensive capabilities and deterrence. These developments reflect heightened emphasis by the U.S. government on deterrence achieved through offensive cyber capabilities and operations or financial and travel sanctions against perpetrators. This shift is not incompatible with an interest in norms, but it reflects less confidence that existing or new norms will, for the foreseeable future, improve cybersecurity for critical infrastructure. Instead, the United States wants to deter cyber threats to...
Heightened emphasis by the U.S. government on deterrence ... reflects less confidence that existing or new norms will, for the foreseeable future, improve cybersecurity for critical infrastructure.

critical infrastructure by exercising material power to threaten and, if necessary, impose punishment. As Admiral Rogers acknowledged, cyber deterrence will not be like previous experiences with deterrence, especially in the nuclear context. What cyber deterrence means, and how it affects the web of norms relevant to protecting critical infrastructure, is about to unfold.
NOTES


2 Hearing of the Select Committee, ibid.

3 Hearing of the Select Committee, ibid.


5 Hearing of the Select Committee, ibid.


10 The North American Electric Reliability Corporation (NERC), a non-profit entity, develops and oversees standards designed to assure the reliability of electrical power generation in North America. However, these standards are not rules of international law but represent industry-driven principles overseen by government agencies. North American Electric Reliability Corporation, accessed May 29, 2015, http://www.nerc.com/Pages/default.aspx.


17 International Convention for the Suppression of Terrorist Bombings, Article 2(4). "Infrastructure facility" is defined as "any publicly or privately owned facility providing on distributing services for the benefit of the public, such as water, sewage, energy, fuel or communications." Ibid., Article 1(2).

18 International Convention for the Suppression of Terrorist Bombings, Article 6(3).


20 Charter of the United Nations, Articles 2(3) and 2(9).


23 Hearing of the Select Committee, ibid.


46 Kerry, “An Open and Secure Internet,” ibid.
48 In the Select Committee’s hearing, members of the Committee and Admiral Rogers discussed whether the large-scale commission of cyber crime and cyber espionage represents economic warfare.
49 Hearing of the Select Committee, ibid.
51 Executive Order, Blocking the Property of Persons Engaging in Significant Malicious Cyber-Enabled Activities, April 1, 2015
55 Hearing of the Select Committee, ibid.