7-2013

Mind the Gap: Explaining Problems with International Law Where Cybersecurity and Critical Infrastructure Protection Meet

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

Mind the Gap: Explaining Problems with International Law Where Cybersecurity and Critical Infrastructure Protection Meet

by David P. Fidler, James Louis Calamaras Professor of Law,
Indiana University Maurer School of Law

Critical infrastructure protection (CIP) policy emphasizes the importance of protecting such infrastructure from vulnerabilities associated with information and communication technologies (ICTs) and recognizing that networked ICTs (and the network architecture) constitute critical infrastructure. Similarly, cybersecurity policy identifies CIP as an objective. The CIP-focused and cybersecurity approaches have stressed the need for international cooperation, including the value of developing international legal rules. However, after over a decade of experience, a gap persists between the much-proclaimed need for more effective international law in this area and the international law that exists.

Three factors explain the gap's persistence. First, cooperation on CIP and its cyber features developed within existing diplomatic mechanisms without requiring new international law. Second, patterns in cybersecurity policy affect what states seek to achieve and how they use international law. Third, international politics on cybersecurity increasingly reflect geo-political competition—a context that has never proved conducive to international law. These factors create obstacles for developing international law on the cyber aspects of CIP, meaning that the existing gap might go from persistent to permanent.

International Cooperation on Critical Cyber Infrastructure

Efforts to bolster CIP, including its cyber aspects, include international cooperation. National CIP strategies identify such cooperation as critical; bilateral relations often involve CIP elements; regional organizations, such as the European Union and Organization of American States, facilitate collaboration on CIP; security organizations, such as NATO and the Shanghai Cooperation Organization, work on CIP; and multilateral institutions, such as the UN, stress the importance of cooperation to achieve better CIP. With some exceptions, this cooperation has proceeded without the need for, or the production of, new international legal rules or

(Continued on Page 3)

* Image courtesy of scottchan/FreeDigitalPhotos.net.

(Continued from Page 2)

instruments specific to the protection of critical cyber infrastructure.

Generally, this cooperation focuses on building domestic capacities to identify and respond to cyber threats, sharing information on threats and effective cybersecurity practices, providing assistance when requested, and devoting regular diplomatic attention to this challenge. Existing diplomatic or treaty-based mechanisms have proved flexible enough to allow cybersecurity and its CIP elements to become part of the agenda. Although most cooperative efforts have not generated new international law specific to the protection of critical cyber infrastructure, they echo international law on transboundary pollution and industrial accidents, which includes responsibilities to prevent and mitigate threats, consult and share information, provide assistance, and engage in periodic diplomacy to improve cooperation.

Specific international rules and mechanisms that have emerged are limited in scope or substance. For example, the EU requires members to identify "European critical infrastructure" in the energy and transport sectors, provide information about such designations, and mandate that operators have security plans.[1] Members of the Shanghai Cooperation Organization agreed to cooperate on "[e]nsuring information security of critical structures of the Parties."[2] A draft African Union treaty requires parties to adopt a national cybersecurity policy that includes protecting "essential information infrastructure."[3]

To date, state practice reveals a preference for using existing mechanisms for cooperation on CIP and its cyber components rather than establishing new legal regimes. Proposals to create-cyber specific international law, such as an obligation to provide assistance to victims of cyber attacks or prohibitions against attacks on the Internet's root servers, have not gained diplomatic traction. Whether this preference remains dominant will depend, in part, on how cybersecurity policy changes and what impact those changes have on prospects for using international law.

Patterns in Cybersecurity Policy and Their International Legal Implications

Although cybersecurity policy is complex, three patterns have emerged. First, policymakers have used a "cyber threat" approach in which they classify an incident into existing categories—crime, terrorism, espionage, and armed conflict—and then apply the policies and legal rules associated with each category. International law exists for each category, but states have so far only developed specific international law for cyber crime (e.g., Council of Europe Convention on Cybercrime). For terrorism, espionage, and armed conflict, pre-cyber international law is applied to cyber incidents (e.g., the law of armed conflict).

However, experts debate the efficacy of this approach, with critics observing that international law on crime, terrorism, espionage, and armed conflict cannot handle cyber threats adequately. Although it is the most prominent cyber crime instrument, the Convention on Cybercrime's effectiveness has been challenged, especially because of its limited number of state parties (39 as of June 2013). Further, international law does not seriously constrain espionage, which creates a permissive context that adversely affects CIP. Despite recent efforts to clarify how the law of armed conflict applies to cyber warfare,[4] its utility for CIP during armed conflict remains unclear.

The second pattern in cybersecurity policy is the "cyber defense" approach, which focuses on defending against cyber threats regardless of their type or origin.

(Continued on Page 4)

---

[1] Council Directive 2008/114/EC 345/75-345/76, Dec. 8, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

[2] Agreement on Cooperation in the Field of International Information Security, 2008, Art. 3.

[3] Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, Jan. 1, 2011. Art. III-1-4, http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf.

[4] International Group of Experts, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381.

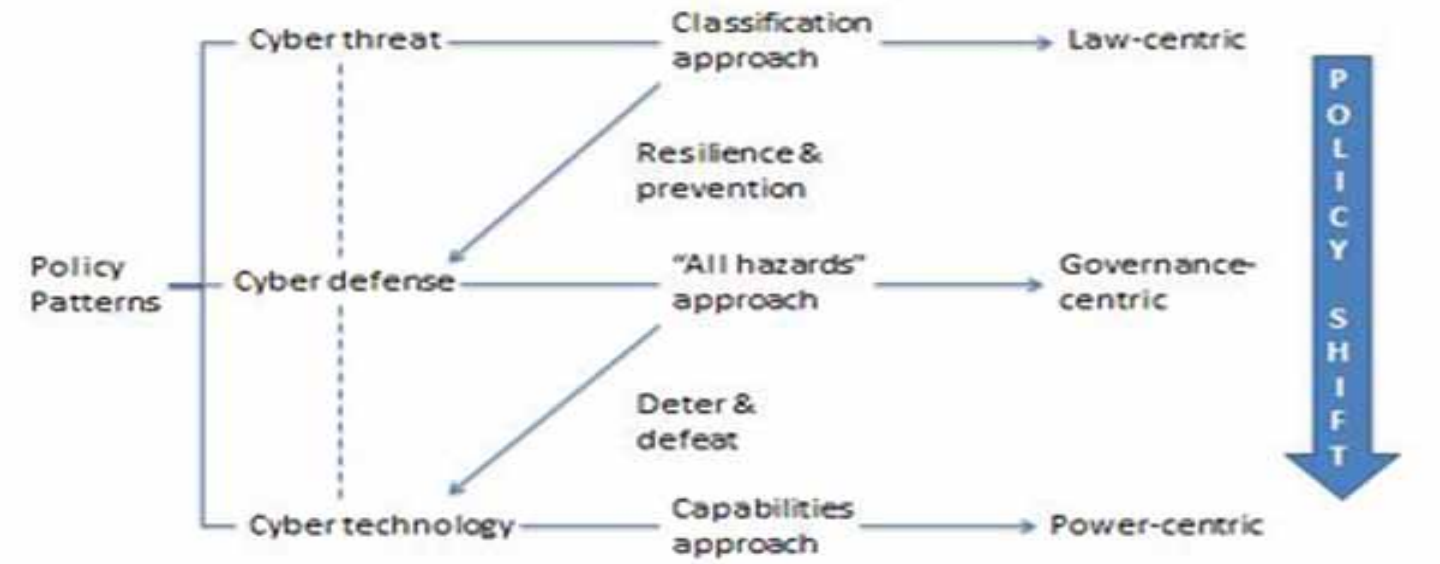
(Continued from Page 3)

This approach adopts an "all hazards" strategy that does not require slotting cyber intrusions into existing policy and legal categories. The motivation behind emphasizing cyber defense relates to concerns that the cyber-threat approach is too reactive, faces technical and legal attribution problems, and fails to achieve prevention, deterrence, or resilience.

Stressing cyber defense produces different legal issues, including the impact of "active defenses" on the principles of sovereignty and non-intervention, the effect of heightened electronic surveillance and information sharing on civil liberties, the problem of regulating critical infrastructure operated by the private sector, and ideological disagreements about Internet governance. While the cyber-threat approach applies existing law (*lex lata*) to cyber incidents, the cyber-defense approach more directly raises questions about what law should be (*lex ferenda*), which stimulate larger considerations about governance on which consensus does not exist (e.g., how should cybersecurity and privacy be balanced?; should Internet governance be more intergovernmental or multi-stakeholder in nature?; and should it emphasize sovereignty or "Internet freedom"?). The lack of consensus limits what states can achieve through international law when cyber defense is the focus.

The third pattern involves emphasis on developing "full spectrum" cyber capabilities—the technological ability to defend against, deter, and—if needed—defeat cyber threats. This "cyber technology" approach holds that focusing on defensive measures is inadequate because, in cyberspace, the offense always has the advantage. Cybersecurity requires technological capabilities that permit not only robust defense but also offensive operations. This pattern is prominent in U.S. policy, as evidenced by actual and contemplated offensive cyber attacks against states and terrorist websites, development of "full spectrum" cyber capabilities by the military and intelligence community, and establishment of "rules of engagement" for offensive operations. Experts believe many countries, ranging from China to Iran, are scaling up their intelligence

(Continued on Page 5)



(Continued from Page 4)

and military cyber capabilities. However, this pattern creates problems for collective action. For example, though keen on cyber defense, NATO members, to date, have resisted discussing the Alliance developing offensive cyber capabilities or engaging in offensive cyber operations.

The cyber-technology approach connects more with material power than application of *lex lata* or development of *lex ferenda*. Technological prowess, rather than law, determines how well critical cyber infrastructure is protected from cyber attack. The cyber-technology approach moves policy closer to managing cybersecurity through balance-of-power politics, including making credible the threat to use cyber capabilities to deter serious attacks on critical infrastructure. In other contexts, international law has not fared well when balance-of-power politics characterized the dynamics of international relations.

Geo-Politics, Cybersecurity, and Critical Infrastructure Protection

In addition to these patterns, cybersecurity policy has shifted in emphasis. Although each pattern remains part of cybersecurity, the patterns overlap in ways that reveal a restless search for more effective strategies. In the CIP context, policymakers have not been content to rely on international legal instruments on cyber crime but have moved to bolster cyber defenses against the range of cyber threats that exist against critical infrastructure. Experts perceive that more powerful countries, including China, Russia, and the United States, are not basing strategies on defensive measures alone but are developing "full spectrum" capabilities to defend against, deter, and defeat serious cyber attacks.

This shift flows from not only the evolution of thinking about cyber threats but also the rise of cybersecurity as a strategic problem in competition among the great powers, especially between the United States and China. Recent events illustrated how raw cybersecurity issues have become in Sino-American relations, with the United States accusing China of cyber theft of U.S. companies' trade secrets, and China accusing the United States of cyber attacks against Chinese targets (accusations assisted by Edward Snowdon's revelations about secret U.S. cyber activities). Although both countries have discussed these problems at a summit and created a working group to address cyber issues, the prospects for new international agreements from this process are, in the current climate of deep mistrust, not good.

Geo-political tensions do not preclude great powers from cooperating, as illustrated by new U.S.-Russia cybersecurity initiatives announced in June 2013, which include confidence-building measures (e.g., information sharing) and a "cyber hot line." However, whether these kinds of initiatives will change the trajectory of cybersecurity in great power politics is doubtful. Confidence-building measures might permit countries to cooperate better on, for example, cyber crime, but such measures do not address strategic tensions related to the threats cyber espionage and military cyber capabilities present to critical infrastructure. And tensions continue to mount, as illustrated by CIP concerns about the security of global ICT supply chains and the licit and illicit markets for "zero day" software exploits. The distrust among the great powers on these strategic and emerging issues represents an obstacle to development of more cyber-specific rules of international law that might benefit CIP.

The gap between calls for additional international law on cybersecurity and critical cyber infrastructure, but existing international law will persist despite cooperation on CIP and its cyber aspects having taken root around the world. Although existing rules and mechanisms facilitate cooperation, policy shifts in cybersecurity are creating a more difficult environment for international law with respect to applying these rules and developing more cyber-specific norms. Given this reality, progress in international cooperation on CIP will depend less on new international law than on maximizing the potential like-minded states can wring from existing regimes, diplomatic venues, and technological capabilities. ❖