2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Developing Collaborative and Cohesive Cybersecurity Legal Principles

Jeff Kosseff[1]
Assistant Professor of Cybersecurity Law
United States Naval Academy
Annapolis, MD, United States

Abstract: Legal discussions about combatting global cyber threats often focus on international cybercrime arrangements or the application of the law of war to cyberspace. While these discussions are vital, policy-makers and scholars have not devoted adequate attention to creating a global legal framework to bolster the defenses of public and private infrastructure. Due to the interconnected nature of cyberspace and the cross-border impacts of attacks, inadequate security in one country could harm another.

To build cyber strategies that rely in part on defense and deterrence by denial, governments should also focus both on the security of their systems and those of the private sector. Industry has been the target of some of the most destructive cyberattacks worldwide. Guiding international principles for a cyber security legal framework would help nations to build effective laws that reduce the likelihood of successful attacks, and increase resilience after attacks occur. Moreover, international collaboration on cybersecurity laws provides multinational companies with a more coherent legal framework. A patchwork of hundreds of different international security requirements is not only burdensome for companies, but it increases the potential for vulnerabilities, particularly if the company operates in countries with less stringent cybersecurity requirements.

This paper sets out the need for nations to discuss common legal principles for promoting and regulating cybersecurity, similar to the privacy principles articulated

1 Assistant Professor of Cybersecurity Law, United States Naval Academy, Annapolis, MD. J.D., Georgetown University Law Center. M.P.P., B.A., University of Michigan. Thanks to LCDR Joseph Hatfield and Professor Martin Libicki for helpful feedback. The views expressed in this paper are only those of the author, and do not represent the U.S. Naval Academy, Department of the Navy, Department of Defense, or any other party.

in the Organization for Economic Cooperation and Development's Fair Information Practices in 1980. As a starting point for discussion, this paper suggests four goals of common international principles for cybersecurity law: (1) modernization of cybersecurity laws; (2) uniformity of legal requirements; (3) coordination of cooperative incentives and coercive regulations; and (4) supply chain security. Although cybersecurity laws will always vary, international coordination could improve their efficacy by providing some degree of consistency. A dialogue also could help policy-makers learn from other nations' cybersecurity successes and failures.

Keywords: *cybersecurity; cooperation; principles; cybercrime; data security*

1. INTRODUCTION

Over the past decade, there has been great progress on international cooperation to combat cybercrime and build on norms to deter and deny states that leverage the asymmetric nature of cyber operations. All of these discussions are vital and must continue on the international stage. However, international legal discussions also must address cybersecurity law.

At the outset, this Paper defines "cybersecurity law," as the term is often used interchangeably to describe regulation of the private sector's computer systems and networks, federal programs that assist the private sector, cybercrime statutes and the legal norms of cyberwar. For the purposes of this paper, I broadly define cybersecurity law as domestic laws that seek to promote the confidentiality, integrity and availability of public and private computer systems, networks and information.[2] This expansive definition applies equally to governmental regulations and public-private partnerships and to incentives that have the ultimate goal of improving cybersecurity.

Improving the cybersecurity of public and private systems has two primary national security benefits. First, hardened defenses help to reduce or eliminate harm caused by an aggressor. Second, cybersecurity is an important part of a framework to deter attacks, provided that the aggressor is aware of the strong defenses. While deterrence by punishment is an important component of a cyber strategy, so too is deterrence by denial. Cyber deterrence requires nations to ensure that their laws provide adequate assistance and incentives for cybersecurity of both government and private infrastructure. Too often, the security of the private sector is missing from the greater discussion of national cybersecurity.[3] Governments worldwide have recognized the

2 *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985 (2018).

3 *See* Kristen E. Eichensehr, *Public-Private Cybersecurity,* 95 TEX. L. REV. 467, 536 (2017) ("As the operation of government-like power becomes more diffuse and more complicated, the actions of private sector actors can implicate the public law values that traditionally apply to governmental actions, and governmental actions may come into increasing tension with public law values.").

need for private companies to protect their data and cyber infrastructure. The private sector controls vast amounts of infrastructure that are vulnerable to cyberattacks, making the private sector's cybersecurity important not only to nations' economies, but also to their national security.[4]

The interconnected nature of cyber threats – in which an attack in one country could cause harmful spill-over effects in another country – provides policy-makers with a compelling reason to improve cybersecurity laws globally. To do so, nations should collaborate and articulate core principles for cybersecurity, just as the Organization for Economic Cooperation and Development (OECD) did for privacy law nearly four decades ago when it developed its Fair Information Practices.

This paper then draws on examples of successful cybersecurity laws and partnerships worldwide to outline some goals of a global cybersecurity legal framework:

- Modernization of cybersecurity laws to address current threats;
- Uniformity of legal and regulatory requirements;
- Coordination of cooperative cybersecurity programs and regulatory obligations; and
- Supply chain security.

Cybersecurity often involves an alignment of public-sector and private-sector interests. Accordingly, cybersecurity law should move from the outdated, purely punitive model of privacy law to a collaborative and cooperative framework. I refer to this model as "collaborative cybersecurity law," a mixture of incentives, public-private partnerships, and tailored regulations that is designed to improve cybersecurity as a whole.

For this paper, collaborative cybersecurity law has two equally important applications. First, the public and private sectors should collaborate to determine the most effective legal frameworks to build defenses and resilience. Second, governments should collaborate at the local, state/province, and national levels to ensure that their requirements and incentives are aligned to the common goal of protecting global cyber infrastructure. Cyberspace does not have clearly defined geographic or public/private boundaries. Nor should the defense of cyberspace.

I do not suggest the creation of a single set of cybersecurity laws to apply across all nations; such a task would be a fool's errand, as countries have a wide range of tort, constitutional, and administrative laws that would prevent a single law across all jurisdictions. Jurisdictions such as the United States tend to favor cybersecurity laws

4 *See* Roger Hurwitz, *The Play of States: Norms and Security in Cyberspace*, 36 AMERICAN FOREIGN POLICY INTERESTS 322 (2014) ("Our discussion suggests that efforts to establish a state-led comprehensive regime for cyberspace will not succeed, notwithstanding the illusion that it could provide a more stable order and block fragmentation of the Internet.").

that promote free expression over other interests, while jurisdictions such as those in Europe tend to favor privacy protection. Rather than attempt a uniform set of laws, countries should develop a set of shared core cybersecurity values to apply as they develop laws to address cybersecurity threats via laws, regulations, and government programs.

In short, this paper argues that nations must broaden their conception of the international cybersecurity dialogue. While the ongoing discussions regarding cyberwarfare norms are essential, it is only one piece of the much larger solution to improving the security of cyberspace. Nations must also develop a cohesive strategy to secure both public and private cyber information and infrastructure through regulations and incentives.

2. THE GLOBAL IMPACT OF INADEQUATE CYBERSECURITY

Cyber threats are not always confined to geographic borders. Many of the most damaging and persistent cyberattacks have targeted systems and data in multiple countries. The attacks target not only military systems or civilian government computers, but often also home systems that are operated by the private sector. With the private sector controlling critical infrastructure such as logistics, telecommunications, and financial systems globally, the cybersecurity of both the public *and* private sector is crucial to adequate defense.

The pervasive global nature of cyber threats can be seen in botnets, which use infected computers to amass power to launch devastating attacks. As botnets infect more computers, they cause more damage, such as forcing websites offline and interrupting critical services.[5] The Internet of Things era has exponentially increased the number of devices connected to the Internet. Botnets have commandeered these devices, in part due to the inadequate security measures on many IoT devices.[6]

For instance, in October 2016, the Mirai botnet, consisting of hundreds of thousands of infected devices, knocked some of the most popular websites in the world offline by targeting Dyn, a domain name system management service.[7]

Botnets demonstrate the international impact of inadequate cybersecurity. Consider, for example, a webcam that is manufactured in Germany with inadequate password protections. If a consumer in the United States uses that webcam, it could be used in a

5 *See* Elisa Bertino & Nayeem *Islam, Botnets and Internet of Things Security*, 50:2 COMPUTER 76-79 (Feb. 2017).

6 *See* Bernard Marr, *Botnets: The Dangerous Side Effects of The Internet of Things*, FORBES (Mar. 7, 2017).

7 Lorenzo Franceschi-Bicchierai, *Blame the Internet of Things for Destroying the Internet Today*, MOTHERBOARD (Oct. 21, 2016).

botnet that shuts down a website in New Zealand. New Zealand alone cannot address the botnet problem by regulating the security of Internet of Things devices.

Likewise, the WannaCry ransomworm demonstrates the interconnected nature of cyber threats. WannaCry was initially found on European businesses' computers on the early morning of May 12, 2017. The files on infected computers were encrypted, and the computer operators received a demand for bitcoin in exchange for the encryption key, though paying the ransom did not always guarantee decryption of the files. The ransomworm rapidly spread. In all, WannaCry infected more than 200,000 computers around the world.[8]

WannaCry was so malicious and pervasive because it spread using EternalBlue, an exploit that allows malware to spread in Windows operating systems. Hackers allegedly stole EternalBlue from the U.S. National Security Agency.[9] The U.S. and UK authorities have attributed WannaCry to North Korea.[10]

According to the European Union Agency for Network and Information Security, once a computer was infected with WannaCry, it would scan public Internet Protocol addresses for other external networks to infect.[11] Rather than merely spreading across a company's internal network, WannaCry used its infected computers to find and target other vulnerable networks.[12]

WannaCry and Mirai demonstrate the globally interconnected nature of harms associated with cyberattacks. The attacks demonstrate that an attack that initially focuses on one geographic region can have immediate and damaging spill-over effects into other countries. Therefore, it is in a nation's interests to secure not only the computers within its geographic boundaries, but the systems and networks across the globe.

3. THE NEED FOR LEGAL PRINCIPLES TO IMPROVE GLOBAL CYBERSECURITY

Enhanced cybersecurity of a nation's infrastructure plays two critical roles in cyber strategy. First, it reduces or eliminates the risk of harm from an attempted attack by bolstering defenses. Second, the known existence of the attack may deter the attacks from ever occurring.

8 Sam Jones, Timeline: *How the WannaCry Cyber Attack Spread*, FINANCIAL TIMES (May 14, 2017).
9 *Ibid*.
10 David E. Sanger, *U.S. Accuses North Korea of Mounting WannaCry Cyberattack*, N.Y. TIMES (Dec. 18, 2017).
11 European Union Agency for Network and Information Security, *WannaCry Ransomware Outburst* (May 15, 2017); Adam McNeil, *How Did the WannaCry Ransomware Spread?* MALWAREBYTES (May 19, 2017).
12 *See* Abishek Singh, *WannaCry Ransomware Analysis: Lateral Movement Propagation*, ACALVIO (May 16, 2017).

Deterrence strategy has two components: deterrence by punishment and deterrence by denial.[13] Deterrence by denial consists of strategies that both resist attacks and help recovery from attacks once they have occurred (known as "resilience.").[14] For effective cyber deterrence by denial, the private sector must both secure its own system and networks and develop secure products throughout the supply chain. As Dorothy Denning summarized in 2016:

> Cybersecurity aids deterrence primarily through the principle of denial. It stops attacks before they can achieve their goals. This includes beefing up login security, encrypting data and communications, fighting viruses and other malware, and keeping software updated to patch weaknesses when they're found.
>
> But even more important is developing products that have few if any security vulnerabilities when they are shipped and installed. The Mirai botnet, capable of generating massive data floods that overload internet servers, takes over devices that have gaping security holes, including default passwords hardcoded into firmware that users can't change. While some companies such as Microsoft invest heavily in product security, others, including many Internet-of-Things vendors, do not.[15]

Nations can promote such cybersecurity measures by enacting effective regulations and creating public-private partnerships. Defending against attacks helps to mitigate the overall harm.[16] However, a single nation's laws are likely to be insufficient to adequately shore up its cybersecurity. The cyber vulnerabilities in Country A may lead to negative consequences in Country B, and Country B has limited ability, acting alone, to impose consequences for inadequate cybersecurity in Country A. That is where an international dialogue on cybersecurity is vital.

Even to the extent that some cyberattacks are strictly local, an international dialogue about cybersecurity laws can allow nations to share lessons about their experiences with government programs, regulations, and laws. Unlike other areas of law that have centuries of empirical evidence to support or reject their adoption, cybersecurity law needs to address the rapidly evolving threat landscape. If, for instance, requiring a particular safeguard is effective, nations could share these experiences in determining best practices.

13 *See* A. Wess Mitchell, *The Case for Deterrence by Denial*, THE AMERICAN INTEREST (Aug. 12, 2015).
14 *See* Annegret Bendiek and Tobias Metzger, *Deterrence Theory in the Cyber Century*, in LECTURE NOTES IN INFORMATICS (LNI), GESELLSCHAFT FÜR INFORMATIK, BONN 2015.
15 Dorothy Denning, *Cybersecurity's Next Phase: Cyber Deterrence*, SCI. AMERICAN (Dec. 2016).
16 *See* Martin Libicki, Cyberdeterrence and Cyberwar 176 (2009).

In both the areas of cybercriminal law[17] and cyberwarfare,[18] international experts and policy-makers have at least attempted to find areas of broad agreement. However, criminal laws and warfare norms and guidelines often address *responses* to cyberattacks (i.e., criminal prosecutions or military action). While these are absolutely vital to a comprehensive cybersecurity framework, they are only part of the solution. Laws and regulations also should seek to bolster defenses to prevent attacks from succeeding in the first place.

The Council of Europe's Convention on Cybercrime (the Budapest Convention) sets minimum requirements for computer crime statutes in participating nations and provides for mutual assistance in investigating and prosecuting cybercrimes. This cooperation and harmonization is necessary because of the global nature of cybercrimes, and the criminal is often located in a different country from the target.[19] By harmonizing cybercrime laws, the Budapest Convention reduces the likelihood of some countries becoming "safe havens" for cybercriminals.[20] However, the Budapest Convention has been criticized for being unsuccessful and overall not helping to crack down on cybercrime.[21] It has not been adopted outside of a majority of Council of Europe members and the United States. When Russia, North Korea, Iran, China, and other non-members often are the sources of cyber-attacks, the Budapest Convention provides the target countries with little recourse. Moreover, criminal law alone is not always sufficient to prevent attacks in cyberspace due to the challenges of attributing attacks with certainty.[22] While the Budapest Convention plays an important role in harmonizing at least some cybercrime laws in some countries, it is not a panacea.[23]

In some respects, there are even more benefits to coming to a consensus on international cybersecurity law than in criminal law. The Budapest Convention is of limited utility because many of the most pernicious attacks are perpetrated from nations that are not parties to the Convention; laws that effectively promote the cybersecurity of public and private systems and networks, however, provide incremental worldwide benefits, even if they have not been adopted by the handful of nations that are the sources of the attacks. Consider, for example, a cybersecurity regulatory framework that bolsters resistance and reduces the spread of botnets by 75 percent in countries that have adopted its safeguards. If half of the nations were to adopt the framework, the overall

17 ETS 185 – Budapest Convention on Cybercrime, 23.XI.2001.

18 *See* TALLINN MANUAL 2.0 ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) (hereinafter, *"Tallinn Manual"*).

19 *See*, e.g., Jonathan Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, 40 MONASH L.R. 699, 700 ("Although many offences are transnational in nature – for instance trafficking in humans, weapons and drugs, money laundering and terrorism – cybercrime presents unique challenges due to the inherently transnational nature of the underlying technology.").

20 *Id*. at 700.

21 *See, e.g*., Jack Goldsmith, *Cybersecurity Treaties, A Skeptical View*, in FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW (Feb. 2011).

22 Lily Hay Newman, *Hacker Lexicon: What is the Attribution Problem?* WIRED (Dec. 24, 2016).

23 *See* Kim-Kwang Raymond Choo, *The Cyber Threat Landscape: Challenges and Future Research Directions*, COMPUTERS & SECURITY 30:8 (Nov. 2011).

strength of a botnet likely would weaken because it would not be as successful in propagating.

Similarly, the growing body of scholarship that applies *jus ad bellum* and *jus in bello* to cyberwarfare is absolutely essential to our understanding of acceptable responses to cyberattacks and it helps to inform deterrence strategies. Understanding the application of *jus ad bellum* to cyberspace is essential in informing a deterrence by punishment strategy. The two editions of the *Tallinn Manual* have provided a forum for an International Group of Experts on the law of war to articulate both commonalities and differences in views about how their field applies in cyberspace.[24] Although the *Tallinn Manual* does not represent the official views of a single organization or state,[25] it is one of the greatest steps in articulating commonalities and differences in international cyber law.[26]

Likewise, from 2016-17, the United Nations Group of Government Experts attempted to reach an agreement on norms of cyber issues such as international humanitarian law and the right of self-defense. However, those discussions failed to lead to a consensus, as some participants had very different views on the fundamental international norms.[27] Indeed, such consensus will be difficult or impossible for norms related to *jus ad bellum* and *jus in bello*. But such issues should not be the only focus of international discussions. Global norms for *domestic* cybersecurity issues could play an equally vital role in securing cyberspace.

The cybersecurity of a nation's infrastructure may play a significant role in its response to a cyberattack, as the success or failure of cyberdefense often determines whether a cyber act constitutes an unlawful use of force.[28] Consider, for instance, a cyberattack by Iran on a portion of the U.S. power grid that is operated by a private company. If the utility has installed sufficient safeguards, the attack may be nothing more than a nuisance that causes little damage. If, however, the attack succeeds, it could cause significant economic loss, and perhaps even personal injury. Those two outcomes would warrant very different responses under international warfare norms. Just as

24 *See, e.g.*, Kristen Eichensehr, *Review of* The Tallinn Manual on the International Law Applicable to Cyber Warfare, 108 A. J. INT'L L. 585, 586 (2014) ("While the rules on which the IGE agreed are very useful in advancing thought and debate about international law regarding cyberwar, more valuable still are the instances in which the *Tallinn Manual* frankly acknowledges disagreement within the IGE.").

25 *See* TALLINN MANUAL at 2 ("Ultimately, *Tallinn Manual 2.0* must be understood only as an expression of the two International Groups of Experts as to the state of the law.").

26 *See* Gary Korn, *Tallinn Manual 2.0, Advancing the Conversation*, JUSTSECURITY (Feb. 15, 2017) ("[T]he advisory nature of Tallinn 2.0 should not detract from its immense value to legal practitioners and their clients in both the public and private sector as a quality compendium of the general framework of international rules and principles most pertinent to cyber operations.").

27 *See* Remarks of Michele G. Markoff, Deputy Coordinator for Cyber Issues, U.S. Department of State (June 23, 2017) ("It is unfortunate that the reluctance of a few participants to seriously engage on the mandate on international legal issues has prevented the Group from reaching consensus on a report that would further the goal of common understandings among UN Member States on these important issues.").

28 *See* Priyanka R. Dev, *'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 TEX. INT'L L. J. 379 (2015).

the international legal community has attempted to develop common ground as to the application of the law of war to cyber, so too should the community develop principles that guide the protection of cyber infrastructure.

Efforts to develop transnational common ground on cybercrime law and cyberwarfare norms will not solve all of the complex international legal problems associated with threats, though they are necessary components of the overall approach to cybersecurity. Moreover, both efforts provide roadmaps for international dialogues about cybersecurity laws that deter by denial. The Budapest Convention and the *Tallinn Manual* demonstrate that it is possible for nations with different values to at least agree on some core principles for cyberspace. Both the Budapest Convention's formal attempts at proscribing specific cybercrime laws and the *Tallinn Manual'*s attempts to narrate common, nonbinding interpretations are essential as nations confront growing cyber threats.

Although there is not currently a universal set of cybersecurity principles outside of the cybercrime and cyberwarfare contexts, an analogue exists in the privacy arena and demonstrates the utility of setting forth a core set of shared legal values for technology law. In 1980, the OECD, an economic development organization consisting of 35 nations, published the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the centerpiece of which was the OECD Fair Information Practices.[29]

Drawing on robust discussions among participating countries, OECD developed the following eight general principles for information privacy: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability.[30] The Guidelines have been revised only once, in 2013. Each of the eight principles provides a broad framework under which nations could choose how to best regulate privacy. For instance, the collection limitation principles state that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject".[31]

Broad principles such as this allow for some standardization across nations; yet they also provide countries with the flexibility to adhere to these principles within their existing legal systems and policy preferences.[32] The OECD Guidelines have helped

29 *See* Pam Dixon, *A Brief Introduction to Fair Information Practices*, World Privacy Forum, available at https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

30 OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA.

31 *Ibid*.

32 *Id*. at 48, Original Explanatory Memorandum to the OECD Privacy Guidelines ("On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation.").

to shape the contours of privacy laws around the world, even beyond the 34 OECD member nations.[33]

The OECD Guidelines are privacy-focused, though the document's Security Safeguards Principle states that personal data "should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data". The supplemental memorandum for the 2013 revisions suggests that these safeguards include data security breach notification requirements. Although this principle touches on a cybersecurity issue, it focuses on personal information security and does not adequately address the full range of cybersecurity threats, as discussed in the next section. Privacy and cybersecurity are often lumped into the same category of law and share some common issues, but they each present different challenges and should be individually addressed.[34] While the protection of personal information certainly is part of cybersecurity, other threats, such as the theft of trade secrets or attacks on cyber-physical systems, are not adequately addressed by privacy law.[35] Cybersecurity law should promote not only the privacy of personal data, but also the protection of systems and data from attacks that could interrupt economies or threaten national security.

This is not to suggest that the OECD framework has perfectly aligned the privacy laws and regulations of all member nations. Far from it. The European Union views privacy as a fundamental human right, and therefore its privacy laws, including the new General Data Protection Regulation, are often far more stringent than those of other jurisdictions. However, the OECD Principles, at the very least, give participating nations a basis on which to find some commonalities and a general framework for discussing and debating privacy issues.

4. GOALS FOR INTERNATIONAL CYBERSECURITY LEGAL PRINCIPLES

Because nations have had few robust and meaningful discussions about how to promote and regulate cybersecurity via legal frameworks, it would be impossible to propose a comprehensive set of principles to guide governments globally.

33 *See, e.g.*, Monika Kuschewsky, *What Does the Revision of the OECD Privacy Guidelines Mean for Businesses*, AB EXTRA (Oct. 22, 2013) ("Today, its basic privacy principles are essentially reflected in all relevant general data protection frameworks worldwide.").

34 *See, e.g.*, Bob Siegel, *What is the Difference Between Privacy and Security?*, CSO (May 26, 2016) ("A security program protects all the informational assets that an organization collects and maintains. A privacy program focuses on the personal information an organization collects and maintains.").

35 The OECD in 2002 adopted its Guidelines for the Security of Information Systems and Networks, which sets out nine general principles for information security. Although these Guidelines are useful, they do not address the problem that this paper seeks to address. The guidelines apply equally to government entities, businesses, and individual users, and focus more on ethical information security norms rather than guidelines for laws. They do not provide the same level of general principles for laws that OECD's privacy principles do. The guidelines are focused on the security of information, and do not address the comprehensive threats to cybersecurity that nations currently face.

This part sets out the goals of global cybersecurity legal standards and a few areas to begin discussions among nations as they determine how best to address cybersecurity challenges via laws and regulations. To be clear, I do not suggest that this should serve as the list of international cybersecurity principles. Such a framework would require significant multilateral discussion and assessments of both the cybersecurity threats and the legal capabilities and constraints to address those threats. Rather, these four goals are broad topic areas that serve as a starting point for an international discussion about common principles.

A. Modernizing Laws to Address Current Cybersecurity Threats

The laws in many nations do not adequately address some of the newer cybersecurity threats, as the laws are outgrowths of pre-Internet legal fields such as privacy torts and criminal law. International norms could help guide nations as they adjust their laws to the current threat landscape.

One of the core concepts in the cybersecurity field is the CIA Triad: confidentiality, integrity, and availability of data, systems, and networks.[36] Confidentiality protects information from unauthorized access.[37] Integrity ensures that the information is accurate and systems function as intended.[38] Availability guarantees uninterrupted access to information and systems.[39] An effective cybersecurity program will advance all three goals.

Unfortunately, cybersecurity law is often conflated with data security and privacy laws that have been on the books for many years or decades. This results in a focus on the confidentiality of personal information, which is the primary security-related concern of privacy law. Without a doubt, that is an important concern, but it overlooks the confidentiality of other critical but non-personal information, such as corporate trade secrets or classified government information. For instance, many jurisdictions require companies to notify individuals and regulators about disclosure of certain categories of personal information, and data security requirements often apply to particularly sensitive types of personal information such as medical records.

Privacy law cares little about integrity or availability, nor do any data security laws that are largely an outgrowth of privacy laws. Data security regulations, for example, often address the unauthorized access to or acquisition of data. These laws typically do little to address attacks on availability (such as ransomware) or attacks on integrity (such as website defacement or modifications to database systems that cause physical impacts, such as explosions in gas lines).[40]

36 *See* U.S. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 199.
37 *Id*. at 2.
38 *Ibid*.
39 *Ibid*.
40 *See, e.g*., Derek E. Bambauer, *Schrodinger's Cybersecurity*, 48 U.C. DAVIS L. REV. 791 (2015).

Laws should, of course, continue to protect confidentiality. Protecting confidentiality and privacy is not mutually exclusive with protecting integrity and availability. Indeed, many of the concerns regarding interference in the 2016 American election boil down to breaches of confidentiality: the hacks of John Podesta's email account and the Democratic National Committee's servers. However, confidentiality should not be the exclusive focus, particularly in the age of cyber-physical systems and the Internet of Things, when everyday devices are increasingly connected to the Internet and could be vulnerable to attacks. A modern cybersecurity framework must address these threats as well as data breaches.

In addition to promoting all three prongs of the CIA triad, cybersecurity laws should be forward-looking and should minimize harm from future cyberattacks. Ideally, such laws would require companies and governments to bolster defenses to a point where the attacks do not succeed. However, it is highly unlikely that any legal system would entirely prevent all attacks. For that reason, a modern cybersecurity legal framework should also strive to improve resilience – the ability of a company or government to quickly recover after an attack has occurred.[41]

B. Uniformity of Regulations

Regulation of the private sector plays a key role in securing cyber infrastructure. Companies that have some of the most critical cyber infrastructure operate in many countries. Those companies, therefore, are subject to hundreds of legal regimes at the local, state/province, and national levels. To the greatest extent possible, cybersecurity regulations should be standardized across governments to improve the ease and likelihood of compliance. International norms could help to guide that uniformity.

For instance, companies are subject to dozens of data breach notification laws at the state/province and national levels, all varying in terms of the specific requirements that they impose as to what types of personal data trigger the notification requirements and the forms that the notices must take.[42] The breach notice laws apply based on the residency of the individuals whose data was breached. Thus, a company that has customers throughout the world must comply with all of these requirements in the days following a breach. Such compliance can be time-consuming, and can divert attention from efforts to remedy the harms caused by the breach and prevent further intrusions.[43]

Policy-makers at the international level could help strive toward such uniformity by adopting standards that could be the basis of private sector requirements, and jurisdictions should aim for uniformity among the regulations of state, provincial,

41 *See* Fredrik Hult & Giri Silvanesan, *What Good Cyber Resilience Looks Like*, J. OF BUS. CONTINUITY & EMERGENCY PLANNING 112 (2013-14).

42 *See* World Law Group, GLOBAL GUIDE TO DATA BREACH NOTIFICATIONS (2016).

43 *See* Brett V. Newman, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 U. ILL. J.L. TECH & POL'Y 437, 442 (2015).

and local governments. The European Union's GDPR, for example, aims to improve uniformity among European Union members by imposing a single comprehensive set of requirements for privacy and security practices when dealing with European residents' personal information.[44]

Complete global uniformity of cybersecurity laws is impossible, as countries will differ in their legal constraints and values regarding issues such as privacy, expression, and security. For instance, in Europe, privacy is a fundamental human right, while the United States is more likely to balance privacy with other interests such as free expression.[45] However, even some movements toward similar cybersecurity regulations would be useful in providing companies with more effective pathways to comply with the global patchwork of laws.

C. Coordination of Coercive and Cooperative Laws

Cybersecurity laws should contain a mixture of punitive regulations and incentives to promote private sector security. Regulations will always play an important part in bolstering companies' cybersecurity. However, cybersecurity differs from other regulated areas in that the government's goals are often generally aligned with the goals of a company. A rational chief executive does not want their company to experience a denial of service attack or data breach, nor does a rational government official.

For that reason, there is great room for collaboration between the public and private sectors. Such collaboration should form part of a broader strategy for bolstering the cybersecurity of public and private infrastructure.

For instance, governments across the world are increasingly improving and expanding their cyber threat information sharing programs, which allow the private and public sectors to exchange information and collaborate to reduce the spread and damage of cyberattacks. In the European Union, the 2016 NIS Directive requires member states to establish Computer Security Incident Response Teams that monitor, share, and collect information about cyber threats and "establish cooperation relationships with the private sector".[46] Likewise, in late 2015, the U.S. Congress passed the Cybersecurity Information Sharing Act, which provides companies with limited legal immunity for sharing cyber threat information and defensive measures with other companies and the federal government's threat information sharing program. The statute has been called "the first major piece of cybersecurity legislation enacted into

44 *See* Terry Greer-King, *GDPR is Coming: 5 Things to Be Aware Of*, Cisco UK & Ireland Blog (Feb. 23, 2017) ("[E]ach country currently has their own ways of coming up with legislation to control data rights. GDPR is going to drive some uniformity, and make it easier to legislate.").

45 *See* Mark Scott & Natasha Singer, *How Europe Protects Your Online Data Differently Than the U.S.*, N.Y. TIMES (Jan. 31, 2016).

46 Annex I to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive").

law that seeks to directly address the relationship between the private and public sectors".[47] An international dialogue on such efforts could establish best practice for such threat-sharing efforts and might also lead to more effective means of exchanging critical threat information internationally.

Cybersecurity education also requires collaborative efforts from both the public and private sectors. It includes general awareness campaigns to reduce the success of phishing and other social engineering attacks, as well as more advanced collegiate and graduate school training to build a cybersecurity workforce. For instance, the Israeli National Cyber Bureau has developed a plan both to build cybersecurity awareness among the general public,[48] and the EU's NIS Directive requires each member state to adopt a strategy that addresses "education, awareness-raising and training programs relating to the national strategy on the security of network and information systems".[49]

Governments could also provide financial incentives, such as tax credits and research and development funding, to encourage potential targets to invest large sums of money and staffing to bolster their cybersecurity. Because many high-profile targets are multi-national corporations, international coordination on incentives such as tax credits would be particularly useful in developing a global strategy.

International norms to improve cybersecurity education are particularly useful with a global information technology workforce. Nations could determine any particular skill shortages within cybersecurity and align educational programs accordingly. Moreover, international principles could help to guide and improve cybersecurity awareness campaigns to reduce the likelihood of cybersecurity attacks succeeding due to human error.

D. Secure Throughout the Supply Chain

Just as cybersecurity threats arise due to the global interconnection of networks and systems, they also often arise because products and services rely on a number of components developed around the world and inadequate security of a component can make an entire product or service vulnerable. Countries have individually begun addressing the supply chain in a thoughtful manner. For instance, in 2008, the United States began its Comprehensive National Cybersecurity Initiative, which recognized the need for "partnership with industry to develop and adopt supply chain and risk management standards and best practices".[50] However, the Initiative recognized that supply chain cybersecurity is not merely a problem that arises from U.S. companies:

47 Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S.C. L. REV. 585, 586 (2016).

48 *See* Daniel Benoliel, *Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J.L. & TECH 435, 446 (2015).

49 NIS Directive at Art. 7(1)(d).

50 COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, *available at* https://obamawhitehouse.archives.gov/node/233086.

"Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services."[51]

International standards for supply chain cybersecurity would be particularly useful, as products may rely on technology that is manufactured in many nations. A substantive dialogue between governments and industry could develop best practices for supply chain cybersecurity, which could be used as the basis for national or regional cybersecurity laws. Such standardization could improve the overall security of products and services while increasing the ease of compliance.

5. CONCLUSION

This paper argues that nations should broaden their cyber discussion beyond cyberwarfare and attempt to improve the patchwork of domestic laws that seek to improve the cybersecurity of public and private infrastructure and information. Nations cannot address cybersecurity threats merely by developing domestic legal rules that fail to account for the laws and programs in other nations. An international framework for cybersecurity would help nations to align their regulations and public-private partnerships to address threats that often know no borders. Effective cybersecurity laws require collaboration between governments worldwide and between the public and private sectors. Although nations will continue to carve out their own paths, a productive international dialogue would help policy-makers to find some common ground on effective cybersecurity laws and programs.

51 *Ibid*.