UNPACKING THE INTERNATIONAL LAW ON CYBERSECURITY DUE DILIGENCE: LESSONS FROM THE PUBLIC AND PRIVATE SECTORS

Scott J. Shackelford, JD, PhD*, Scott Russell, JD**, & Andreas Kuehn***[1]

ABSTRACT

Although there has been a relative abundance of work done on exploring the contours of the law of cyber war, far less attention has been paid to defining a law of cyber peace applicable below the armed attack threshold. Among the most important unanswered questions is what exactly nations' due diligence obligations are to one another and to their respective private sectors. The International Court of Justice ("ICJ") has not yet explicitly considered this topic, though it has ruled in the *Corfu Channel* case that one country's territory should not be "used for acts that unlawfully harm other States." But what steps exactly do nations and companies under their jurisdiction have to take under international law to secure their networks, and what of the rights and responsibilities of transit states? This Article reviews the arguments surrounding the creation of a cybersecurity due diligence norm and argues for a proactive regime that takes into account the common but differentiated responsibilities of public and private sector actors in cyberspace. The analogy is drawn to cybersecurity due diligence in the private sector and the experience of the 2014 National Institute of Standards and Technology ("NIST") Framework to help guide and broaden the discussion.

[1] *Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford
**Post-Graduate Fellow, Center for Applied Cybersecurity Research, Indiana University.
*** Zukerman Cybersecurity Predoctoral Fellow, Center for International Security and Cooperation, Stanford University; PhD Candidate School of Information Studies, Syracuse University. An earlier form of this article was published as *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector*, *in* ETHICS AND POLICIES FOR CYBER WARFARE __ (Mariarosaria Taddeo ed., 2015). We would like to thank Oxford University Press for allowing the republication and expansion of this chapter as an article for the present volume.

TABLE OF CONTENTS

INTRODUCTION

Rarely does a day go by in which some variety of cyber attack is not front-page news. From Sony to JP Morgan, Saudi Aramco to the Ukraine crisis, cybersecurity is increasingly taking center stage in diverse arenas of geopolitics, international economics, security, and law. In mid-2015 alone numerous high-profile incidents came to light involving both the public and private sectors, including the breach of more than twenty-one million current and former federal employee's private information from the U.S. Office of Personnel Management.[2] Yet despite the increasing proliferation of these incidents, the field of international cybersecurity law and policy remains relatively immature. For example, although there has been a relative abundance of work done on exploring the contours of the law of cyber war, far less attention has been paid to defining a law of cyber peace applicable below the armed attack threshold.[3] This is surprising since the vast majority of cyber attacks do not cross this threshold.[4] Among the most important unanswered questions is what exactly are nations' due diligence obligations to secure their networks and to prosecute or extradite cyber attackers. The International Court of Justice ("ICJ") has some guiding jurisprudence on this point, such as *Corfu Channel* case that one country's territory should not be "used for acts that unlawfully harm other States."[5] But analogizing is required, and these cases are not dispositive. A wealth of information is available in the arena of cybersecurity due diligence from both the public and private sectors that has, to date, been largely untapped to help answer the question of what steps nations and companies under their jurisdiction should take to secure their networks, along with clarifying the rights and responsibilities of transit states.

This Article reviews the arguments surrounding the creation of a cybersecurity due diligence norm and argues for a proactive regime that takes into account the common but differentiated responsibilities of various stakeholders in cyberspace. The analogy is

---

[2] *See, e.g.*, Bill Chappell, *Federal Employee Breach Very Likely Included Security Clearance Info*, NPR (June 12, 2015), http://www.npr.org/sections/thetwo-way/2015/06/12/414031155/federal-employee-breach-included-classified-clearance-info.

[3] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICATION TO CYBER WARFARE 17 (Michael N. Schmitt ed., 2013) (discussing when a cyber attack could trigger the right of self-defense).

[4] *See* NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 34, 67 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter NATIONAL ACADEMIES].

[5] Corfu Channel (U.K. v. Albania), 1949 I.C.J. 4, para. 49 (April 9).

drawn to cybersecurity due diligence in the private sector and the experience of the 2014 National Institute of Standards and Technology Cybersecurity Framework ("NIST Framework") to help guide and enrich the discussion.[6] Ultimately we argue that international jurisprudence has an invaluable role to play, but the experience of national regulators and the private sector is also informative in this space especially given the robust and necessary public-private cross-pollination occurring with regards to clarifying and spreading cybersecurity best practices. Yet despite its importance, this is a topic that has received remarkably little attention in the literature to date.[7]

This Article is structured as follows. We begin by reviewing the applicable ICJ jurisprudence and literature on cybersecurity due diligence under international law. We then turn to national case studies to help flesh out a potential cybersecurity due diligence norm focusing on the cyber powers of the United States, Germany, and China. Finally, we review lessons from the private-sector cybersecurity due diligence context focusing on mergers and acquisitions and supply chain management to better understand contemporary risk mitigation realities and conclude with some implications for managers and policymakers.

I. UNPACKING DUE DILIGENCE UNDER INTERNATIONAL LAW

International law has been defined as "the body of legal rules," norms, and standards that applies "between sovereign States" and non-State actors, including international organizations and multinational companies, enjoying legal personality.[8] The primary sources of international law include treaties, general principles of law, and

---

[6] *See* Rachel Ensign, *Cybersecurity Due Diligence Key in M&A Deals*, WALL ST. J. (Apr. 24, 2014), http://blogs.wsj.com/riskandcompliance/2014/04/24/cybersecurity-due-diligence-key-in-ma-deals.

[7] *Cf.* Contemporary Practice of the United States Relating to International Law: International Oceans, Environment, Health, and Aviation Law: White House and Department of Defense Announce Strategies to Promote Cybersecurity, 105 AM. J. INT'L L. 794, 795 (2011) ("Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse."); John M. Prescott, *Responses to Five Questions on National Security Law*, 38 WM. MITCHELL L. REV. 1536, 1541 (2012) (discussing the U.S. International Strategy for Cyberspace); Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance*, 62 AM. U.L. REV. 1273, 1354 (2013) (discussing the due diligence aspect of the 2011 U.S. International Strategy for Cyberspace).

[8] *Definition of International Law*, INT'L LABOR ORG, http://www.actrav.itcilo.org/actrav-english/telearn/global/ilo/law/lablaw.htm (last visited Mar. 25, 2015).

custom, the third of which requires evidence of State practice that nations follow out of a sense of legal obligation.[9] The subsidiary sources of international law include judicial decisions and scholarly writing. Given the recent nature and rapid development of cyber-capabilities, there are comparatively few treaties that specifically address the rights and obligations of States vis-a-vis these cyber-capabilities, with the notable exception of the Budapest Convention discussed below.[10] Absent a robust treaty regime and given the geopolitical difficulties of negotiating new agreements in this area, it is vital to clarify the role of customary international law as it relates to due diligence.

A. An Introduction to Customary International Cybersecurity Law

A vital component of customary international cybersecurity law was articulated by the ICJ case *Nicaragua v. United States*, which involved a dispute over the United States' involvement with the Contra rebellion in Nicaragua.[11] In *Nicaragua*, the ICJ held that customary international obligations would arise from the consistent, widespread practice of States engaging in specific acts or omissions, performed out of a sense of obligation that such acts or omissions were required by international law (*opinio juris*). The combination of State practice and *opinio juris*, performed by a significant number of States and without the express disavowal of a significant number of States, would give rise to international obligations under customary international law. The underlying rationale behind this logic is that this combination reflects a consensus in the international community that the actions taken represent an unspoken international obligation.

Despite *Nicaragua's* clear articulation of the rule, in practice the development of customary international law presents a temporal dilemma, since for a State to engage in actions out of a sense of legal duty, this presupposes the existence of such a duty, and

[9] Statute of the International Court of Justice, art. 38, June 26, 1945, 59 Stat. 1055. http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0.
[10] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[11] Case Concerning the Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 183 (June 27).

therefore the prior existence of the customary international law.[12] To help resolve this dilemma, Professor Frederic Kirgis, in response to *Nicaragua,* argued for what he called a "sliding scale approach."[13] Professor Kirgis argues that State practice and *opinio juris* need to be understood on a spectrum, wherein the requirement for *opinio juris* increases as the evidence of State practice decreases. Rather than impose strict requirements for both State practice and *opinio juris*, the sliding scale approach argues that a strong history of State practice can give rise to international obligations absent *opinio juris*, and that likewise compelling *opinio juris* could give rise to international obligations with little evidence of State practice conforming thereto.[14] This sliding scale approach may prove particularly important in the cybersecurity realm as these novel technologies have arisen too rapidly for evidence of widespread State practice to emerge, yet compelling *opinio juris* may still exist as the basis for international obligations.

Proving *opinio juris*, however, is a difficult task, especially in the cyber context. The temporal dilemma means that pointing to existing rules is oftentimes complicated, so the preferred method is to identify broad principles. The ICJ suggests that these broad principles may be found by looking to treaties, as such accords evidence a widespread agreement among States, and indeed most courts rely on treaties to identify *opinio juris*, often exclusively so.[15] Yet again in the cyber realm, treaties thus far have largely focused on implementing domestic cybercrime laws, and have done relatively little to address cybersecurity standards, leaving such decisions to the private sector and standards bodies such as the NIST Framework, discussed below.[16] The Budapest Convention, the African Union Convention on Cybersecurity and Data Protection, and the various ASEAN working groups on cybercrime all could serve as *opinio juris* that States have an obligation to enact and enforce cybercrime laws within their territories and to cooperate to prosecute and extradite cybercriminals, but these agreements often lack binding

---

[12] Curtis A. Bradley, *The Chronological Paradox, State Preferences, and Opinio Juris,* DUKE L. (June 1, 2013), http://law.duke.edu/cicl/pdf/opiniojuris/panel_1-bradley-the_chronological_paradox,_state_preferences,_and_opinio_juris.pdf.
[13] Frederic L. Kirgis, *Custom on a Sliding Scale,* 81 AM. J. INT'L L. 146, 147 (1987).
[14] *See id*.
[15] Mitu Gulati, *How Do Courts Find International Custom?,* DUKE L. (2013), http://law.duke.edu/cicl/pdf/opiniojuris/panel_6-gulati-how_do_courts_find_international_custom.pdf.
[16] *See infra* Part II(B).

language.[17] Similarly, the Organization of American States has also encouraged member States to join the Budapest Convention and to increase regional cooperation to mitigate cybercrime, whereas a nonbinding U.N. General Assembly Resolution calls on States to "eliminate safe havens" for cybercriminals.[18] While it is unlikely that a non-signatory State would be bound to the specific terms of a treaty to which it did not sign—particularly in the short term—that treaty may still serve to identify broad principles that form *opinio juris*, and thereby can build a foundation for international obligations.

The search for cybersecurity *opinio juris* is further complicated by the multifaceted cyber threat comprising cybercrime, espionage, terrorism, and war. While the classification of State cyber-activities is a well-known problem,[19] the mere fact that these activities are so widespread suggests a lack of *opinio juris* against aggressive State cyber-activity below the armed-attack threshold. This is reinforced by discussions of the international law relating to espionage, which is largely unregulated outside the law of war context.[20] Similarly, domestic cybersecurity practices are highly variable and can involve the surreptitious installation of malware—as alleged of Chinese telecommunications providers and the NSA alike—discussed further below.[21] Given the relative lack of multilateral progress, claiming a widespread consensus for an underlying cybersecurity norm is challenging; a situation that is only marginally helped by investigating related ICJ jurisprudence on the subject.

B. ICJ Jurisprudence as it Relates to Cybersecurity Due Diligence

Although the ICJ has never directly addressed cybersecurity due diligence requirements, the cases discussing due diligence generally can serve as broad guideposts for States from which we may infer cyber-specific applications. It is worth noting that

---

[17] For an extended discussion of these and other applicable treaty regimes, see Chapter 6 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[18] General Assembly resolution 55/63, Combatting the criminal use of information technologies, A/RES/55/63 (22 Jan., 2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf. Accessed 26 March 2015.

[19] For more on this topic, see Chapter 1 of SHACKELFORD, *supra* note 17.

[20] *See* A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 601-602 (2007).

[21] Wolfgang Gruener, *Many New PCs in China Come With Malware Preinstalled,* TOM'S HARDWARE (Sept. 24, 2012), http://www.tomshardware.com/news/microsoft-pc-windows-security-china,17758.html.

these cases all arose prior to the proliferation of cyber attacks, but some of the principles that underlay them may still have some applicability, including *Corfu Channel*, *Trail Smelter*, and *Nicaragua*.[22] Before reviewing these cases it is first important, though, to attempt a definition of "cybersecurity due diligence." In the transactional context, this term has been defined as "the review of the governance, processes and controls that are used to secure information assets."[23] The concept as it is used here builds from this definition and may be understood as the customary national and international obligations of both State and non-State actors to help identify and instill cybersecurity best practices and governance effective mechanisms so as to promote cyber peace through enhancing the security of computers, networks, and ICT infrastructure. Cybersecurity due diligence obligations may exist between States, between non-State actors (e.g., private corporations, end-users), and between State and non-State actors. Applicable instruments include technical standards, legal requirements born from treaty or custom, as well as national policies and private-sector industry norms, discussed below.[24]

1. Corfu Channel

One of the earliest ICJ cases on the issue of international due diligence standards was the 1947 resolution of the Corfu Channel dispute.[25] In this instance, two British warships struck mines and were sunk in the Corfu Channel, an international strait located in Albanian territorial waters. The British brought the case before the ICJ, which focused primarily on the right of innocent passage and on the duty of the Albanian government to warn the British of the mines' existence. Although the Court ruled that there was insufficient evidence to conclude that the Albanian government had placed the mines itself, it did conclude that the Albanian government should have known of the mines' existence, and therefore had a duty to warn the British warships. The ICJ based its decision on "certain general and well-recognized principles," specifically "every

[22] However, it should be noted that other jurisprudence is also on point and is not discussed here due to space constraints, including: *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* – General Assembly, ICJ Reports, 8 July 1996, at 22, para. 29; *Case Concerning Pulp Mills on the River Uruguay* (Argentina v. Uruguay), Judgment, 20 April 2010, para. 193.
[23] Tim Ryan & Leonard Navarro, *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks,* KROLL CALL (Jan. 28, 2015), http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/.
[24] *See infra* Part II.
[25] Corfu Channel Case (United Kingdom v. Albania), 1949 I.C.J. 244 (Dec.15).

State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[26]

This obligation, although articulated in the context of domestic waterways, has carryover into the cybersecurity realm. The most direct cyber-parallel would be a duty to warn other States operating within the subject State's domestic networks of vulnerabilities known to exist on those networks, but this might extend more generally to a duty to warn other States of vulnerabilities detected in that other State's networks.[27] While this principle is unlikely to require the warning State to identify vulnerabilities with particularity, it could require a State to warn other States of the existence of the equivalent of 'cyber mines' (such as logic bombs).[28] The underlying principle of these duties, drawn from Corfu, is that States have a duty to warn other States of known or foreseeable harms, particularly when those harms arise from within the warning State's sovereign territory. However, whether such duties could effectively coexist with the current international standards regarding espionage, discussed above, and the exceptions for national security, discussed below, is not yet apparent.[29] Nor is it obvious how this reasoning will jive with the increasing use of cloud-based computing by companies and governments and the related jurisdictional issues that such use entails.[30]

Of particular note in *Corfu Channel* is that the ICJ articulated different standards of proof for direct State actions and omissions. The standard required to prove a State action was not specifically stated, although the ICJ noted that it required "a degree of certainty not shown here," whereas to prove an omission required "no room for reasonable doubt."[31] Some commentators have noted that the language used for

---

[26] *Id.* at 22.
[27] Eneken Tikk, *Ten Rules of Behavior for Cyber Security*, SURVIVAL, June 2011, at 119.
[28] Logic bombs often appear as malware and are designed to set off a malicious function when certain conditions are met – such as a specific time and date. The full extent of logic bomb infiltration on existing networks is unknown, but there have been logic bombs implanted in U.S. critical national infrastructure. *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 92 (2010).
[29] *See infra* Part I(A); *supra* Part I(D).
[30] *See, e.g.*, *Cloudy Jurisdiction: Addressing the thirst for Cloud Data in Domestic Legal Processes*, EFF (Internet Governance Forum - Baku 2012), https://www.eff.org/document/cloudy-jurisdiction-addressing-thirst-cloud-data-domestic-legal-processes.
[31] Corfu, *supra* note 25, 17-18.

omissions appears to reflect a higher standard than that for direct actions.[32] Nonetheless, omissions are likely to be easier to prove in practice, as the ICJ is more willing to accept circumstantial evidence in these instances, particularly when the opposing party controls the direct evidence.[33] Consequently in *Corfu*, although the British government failed to meet the standard of proof that the Albanian government had placed the mines, it nonetheless was able to satisfy the evidentiary burden to prove that the Albanian government would have known of the mines' existence. This issue is relevant to cyber attacks since even though a given exploit may be launched from within a State's territorial boundaries, attributing it back to that State's government is no easy feat.[34]

The attribution problem may become less burdensome, however, when attempting to prove the State's knowledge of attackers within its territory given Corfu's allowance for "more liberal recourse to inferences of fact and circumstantial evidence" when the evidence is controlled by the opposing State.[35] Although the mere fact that the activity occurred in the State's territory is not evidence of knowledge, activities such as the use of the State's non-commercial critical infrastructure may serve as a rebuttable presumption that the State had knowledge of the attack.[36] Some commentators go even further and assert that States may be held accountable without actual or presumed knowledge if that State failed to enact or enforce appropriate cyber-legislation, citing a failure to satisfy a State's duty to prevent cyber attacks within its own territory.[37] Regardless of the viability of such an expansive view of State responsibility, the principle of *Corfu* is that the ICJ will not absolve States of liability for actions occurring within its territory solely due to a lack of direct attribution to the State.

2. Trail Smelter

[32] Katherine Del Mar, *The International Court of Justice and Standards of Proof, in* THE ICJ AND THE EVOLUTION OF INTERNATIONAL LAW: THE ENDURING IMPACT OF THE CORFU CHANNEL CASE 98, 107 (Karine Bannelier et al. eds., 2012).
[33] Corfu, *supra* note 25, at 18.
[34] Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F.L. REV. 167, 193-195 (2012).
[35] Corfu, *supra* note 25, at 18.
[36] Wolff Heintschel Von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace,* 89 INT'L L. STUD. 123, 137 (2013).
[37] Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 12-13 (2009).

The issue of due diligence was also addressed in the ICJ's *Trail Smelter* dispute, which involved the emission of environmentally hazardous materials across the U.S.-Canadian border, raising the question of what obligations States owe neighboring States. This case thus placed the principle of territorial sovereignty at loggerheads with newer conceptions surrounding effects jurisdiction. Ultimately, *Trail Smelter* held that "no State has the right to use or permit the use of its territory . . . to cause injury by fumes . . . to the territory of another . . . when the case is of serious consequence and the injury is established by clear and convincing evidence."[38] Although directed towards the emission of "fumes," *Trail Smelter* has come to represent the broader "no harm" principle, which requires of States "that activities within their jurisdiction or control respect the environment of other States."[39]

This "no harm" principle, although directed towards environmental harms, enjoys parallels with cybersecurity, and may serve as the foundation for a broader State obligation not to permit domestic activities that result in "serious consequences" internationally. Specifically, the analogy could be drawn such that if noxious activity from one State causes serious repercussions in another, then the offending state has a duty to mitigate the threat. Indeed, as with environmental pollution, overuse can occur in cyberspace, such as when spam messages consume limited bandwidth, which has been called a form of "information pollution," and distributed denial of service attacks that can cause targeted websites to crash through too many requests for site access.[40] However, though recognized by the ICJ, this precedent does not enjoy significant State practice, since recognizing it would likely mean litigation surrounding a potentially vast array of transboundary pollution; a laudable goal to be sure, but an impracticable one for the foreseeable future. Yet *Trail Smelter*'s reference to cases of "serious consequence" ultimately suggests that State practice may exist in maintaining noxious domestic activity below a certain threshold of permissibility, albeit a high one, and therefore could support a broader no harm principle in customary international law applicable to cyber attacks.

---

[38] Trail Smelter Arbitration (U.S. v. Can.), 3 Rep. Int'l Arb Awards (R.I.A.A.) 1905 (1941).
[39] Ralph Bodle, *Climate Law and Geoengineering, in* CLIMATE CHANGE AND THE LAW, IUS GENTIUM: COMPARATIVE PERSPECTIVES ON LAW AND JUSTICE 447, 457 (Erkki Hollo et al. eds., 2012).
[40] Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield,* 3 DUKE L. & TECH. REV. 1, 1 (2010); Roger Hurwitz, *The Prospects for Regulating Cyberspace: A Schematic Analysis on the Basis of Elinor Ostrom*, MIT (Nov. 10, 2009), http://web.mit.edu/ecir/pdf/hurwitz-ostrom.pdf.

3. Nicaragua

Perhaps the least clear, yet potentially most far-reaching international cybersecurity due diligence obligation from the ICJ is the one articulated in *Nicaragua*: that of State sovereignty. In deciding against the United States in that case introduced above, the ICJ articulated the obligation of States not to intervene in the domestic affairs of other States if that intervention related to "the choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[41] This principle of State sovereignty may be read as being in contradiction to the effects jurisdiction basis of the Court's decision in *Trail Smelter*. However, it is an important debate in the cybersecurity context with some States asserting varying degrees of national sovereignty over their domestic intranets even as others espouse the virtues of a "global networked commons."[42] Indeed, several dozen nations now routinely filter traffic, which some say is threatening the dawn of a new age of Internet sovereignty.[43] How multi-stakeholder Internet governance will jive with classic conceptions of State sovereignty over the long run remains unclear, but the potential for domestic cyber policies to have international ramifications has never been greater[44]; a fact that may entail obligations on the cyber powers in particular, some of which are discussed below.[45]

Yet exactly what "cyber non-intervention" entails is unclear. Apart from cyber-operations that amount to a "use of force"[46] or which pass the armed attack threshold triggering the law of armed conflict,[47] there is a wide range of cyber-activity that may impact State sovereignty, and there is no clear delineation of what behavior is internationally acceptable. The *Tallinn Manual*, although directed towards the application of the law of armed conflict to cyber-operations, recognizes that a cyber-

[41] Nicaragua, *supra* note 11, 106-108.
[42] Hillary Rodham Clinton, *Remarks on Internet Freedom*, U.S. Department of State (Jan. 21, 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
[43] James A. Lewis, *Why Privacy and Cyber Security Clash*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 123 (Kristin M. Lord and Travis Sharp, eds., 2011).
[44] *See, e.g.*, Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd*, 379 F.3d 1120 (9th Cir. 2005), *rev'd en banc*, 433 F.3d 1199 (9th Cir. 2006); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 5 (2006).
[45] *See infra* Part II(A).
[46] See TALLINN MANUAL, *supra* note 3, at 42–44.
[47] *Id.* at 54.

operation that falls below a "use of force" can still qualify as an "intervention."[48] An example of this category of cyber-intervention is likely Stuxnet, a sophisticated cyber weapon designed to target Iranian nuclear facilities.[49] Classification of Stuxnet has been a contentious issue, with some arguing it was a "use of force" and others that it constituted an "armed attack," but Stuxnet at a minimum met the requirements of an intervention.[50]

The governing principle for an intervention is that it must be "coercive" towards activity protected by State sovereignty. Therefore, it is not sufficient for an activity to be merely coercive; it must also be coercive towards the State's choice of political, economic, social, or cultural system.[51] While traditional espionage is widely accepted not to be coercive towards any one of these areas, there is more debate over the coerciveness of economic espionage. Since economic espionage involves the theft of valuable trade secrets and intellectual property, now made far easier through the use of cyber technologies,[52] some commentators have suggested that this activity so negatively impacts the economy of the victim State that it may be deemed coercive towards that

---

[48] *Id*. at 44. The UN Charter generally divides conflict into three zones. The first threshold is defined by Article 2(4), which makes the threat or use of force illegal without UN Security Council (UNSC) authorization. There are many examples of acts that states have not treated as breaching Article 2(4)'s prohibition on the use of force, including trade disputes, space-based surveillance, espionage, and economic sanctions. *See* Bruno Simma, *NATO, the UN, and the Use of Force*, 10 EUR. J. INT'L L. 1, 2–3 (1999); NATIONAL ACADEMIES, *supra* note 4, at 242. But even though state practice has shown that such acts do not activate Article 2(4) protections, it is an open question how threats of force may be regulated in cyberspace; for example, "[d]oes introducing vulnerabilities into an adversary's system . . . constitute a threat of force . . . ?" *Id.* at 242, 257 (noting that prohibited threats under Article 2(4) might include "verbal threats, initial troop movements, initial movement of ballistic missiles, [or the] massing of troops on a border . . . ."). The second zone includes the thresholds encompassed in Articles 39 and 42, at which point the UNSC may designate a breach to international peace and security and take action to restore order. *Id*. at 242 (discussing Articles 39 and 42 as the "two exceptions to this prohibition on the use of force."). The final barrier is Article 51, which allows for the "right of individual or collective self-defense" in response to an armed attack. UN Charter, art. 51; NATIONAL ACADEMIES, *supra* note 4, at 243.

[49] *See* Kim Zetter, Aleksandr Matrosov et al., *Stuxnet Under the Microscope*, ESET at 17 (Rev. 1.31, 2011); Steven Cherry, *How Stuxnet is Rewriting the Cyberterrorism Playbook*, IEEE SPECTRUM (Oct. 13, 2010), http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook.

[50] TALLINN MANUAL, *supra* note 3, at 45 (The classification of Stuxnet as an intervention is theoretical, as Iran never formally acknowledged or condemned Stuxnet, although some sources suggested Iran was considering such international legal action.); *see* Shahrooz Shekaraubi, *Iran's Case against Stuxnet*, INT'L POL'Y DIGEST (March 18, 2014) http://www.internationalpolicydigest.org/2014/03/18/irans-case-stuxnet/).

[51] Nicaragua, *supra* note 11, at 108.

[52] The "legal vacuum[]" surrounding cyber espionage can be especially problematic for investigators. Jeremy Kirk, *GhostNet Cyber Espionage Probe Still has Loose Ends*, PC WORLD (June 18, 2009), https://www.pcworld.com/article/166901/article.html. For more background on cyber espionage, see Chapter 1 of SHACKELFORD, *supra* note 17.

State's sovereignty with regard to economic matters, and therefore should be classified as an intervention under international law.[53] Moreover, a cyber-intervention by indirect means may also run afoul of a State's international obligations. For instance, the Arab Spring revolutions of the early 2010s were facilitated in part through the use of social media, particularly Facebook and Twitter.[54] These U.S. firms' policies derived from liberal notions of free speech and assembly, and activists used these platforms to mobilize and organize in a manner that subverted traditional governmental mechanisms for societal control. While certainly not as direct as the provision of arms, as in *Nicaragua*, this nonetheless provided a powerful platform through which activists were able to organize an anti-government movement. And while these events are likely not attributable back to the U.S. government,[55] the United States has supported efforts to circumvent Internet censorship,[56] ensuring access to platforms that other States may not support.

A potentially more difficult case of a cyber-intervention is the anonymity software Tor, which is a software package that was originally developed by the U.S. Navy to facilitate secure and anonymous online communication, and is currently freely available online around the world.[57] Through a process known as "onion routing," Tor makes attempts to monitor or censor network traffic difficult; indeed, Tor's efficacy has led to the NSA referring to it as "the King of high-secure, low-latency Internet anonymity."[58] As such, Tor can facilitate the free speech of individuals living in

---

[53] *See* Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 511-512 (2015). Another example of coercion is briefly discussed in the *Tallinn Manual*, which suggests that actions taken to induce regime change may be viewed as coercive towards a State's choice of political system. TALLINN MANUAL, *supra* note 3, at 45. Going further, we may use the facts in *Nicaragua* to speculate that provisioning rebel groups with cyber-weapons to facilitate rebellion would reasonably be deemed an intervention, particularly if the use of those cyber-weapons by the provisioning State would amount to a use of force.

[54] Pierre Omidyar, *Social Media: Enemy of the State or Power to the People?*, HUFF. POST (Feb. 27, 2014), http://www.huffingtonpost.com/pierre-omidyar/social-media-enemy-of-the_b_4867421.html.

[55] *See* TALLINN MANUAL, *supra* note 3, at 29–36.

[56] *See, e.g.*, James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES (June 12, 2011), http://www.nytimes.com/2011/06/12/world/12internet.html?pagewanted=all&_r=0.

[57] *About Tor*, TOR, https://www.torproject.org/about/overview.html.en (last visited Aug. 4, 2015).

[58] *Tor: 'The King of High-Secure, Low-Latency Anonymity'*, GUARDIAN (Oct. 4, 2013), http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity. However, the technology is far from perfect leading to data breaches that have called into question Tor's continuing utility. *See* Richard Adhikari, *Tor Has Been Breached - What Now?*, TECH. NEWS WORLD (Aug. 1, 2014), http://www.technewsworld.com/story/80834.html?rss=1. The rise of encrypted "https" sites is also

countries that heavily control Internet traffic, including China and its "Great Firewall."[59] While championed by some as a victory for free speech, this service also represents an affront to Chinese State sovereignty. Though the U.S. government is not directly providing Tor to Chinese nationals, the U.S. Navy did develop the software and it was U.S. policy to permit Tor to be freely available. Given that cryptography was on the U.S. Munitions List until 1992 and high-level encryption remains subject to export controls,[60] Tor presents a closer analogy to *Nicaragua* and represents how difficult the notion of non-intervention can be in a digital environment.

Taking the broadest potential interpretation of "intervention" that is at the heart of *Nicaragua*, even the Internet itself implicates State sovereignty. Professor Lawrence Lessig warned of the powerful societal influences that network architecture shapes as part of his famed claim that "code is law."[61] The Internet's architecture reinforces anonymity and free speech, which given the phenomenal growth of the Internet can influence the internal affairs of foreign states.[62] Akin to the German Empire surreptitiously shuttling Vladimir Lenin into Russia to foment revolutionary fervor during the First World War, an open Internet allows for the infiltration of ideologies into States where those ideologies might be considered destabilizing.[63] Considering the ever-expanding importance of the Internet to States, including to those States' political, economic, social, and cultural systems, this raises concerns in some quarters over the outsized role that the U.S. currently occupies in the development of the Internet and online services.[64]

Considering the State practice on intervention, however, there seems to be a growing consensus that international obligations fall not on the offending State to restrain

---

decreasing the need for Tor. *See* HTTPS Everywhere, https://www.eff.org/Https-Everywhere (last visited Aug. 11, 2014).

[59] *A Closer Look at the Great Firewall of China*, TOR BLOG (Oct. 6, 2014), https://blog.torproject.org/blog/closer-look-great-firewall-china.

[60] For a more in depth discussion of encryption export controls, see John R. Shane & Lori E. Scheetz, *Export Controls for Tech Companies: The Basics and the Pitfalls of U.S. Encryption Controls*, 18 J. INTERNET L. 1, 1 (2014).

[61] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

[62] *See* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 148 (2009).

[63] *See* J. Michael Daniel, Robert Holleyman & Alex Niejelow, *China's Undermining an Open Internet,* POLITICO (Feb. 4, 2015) http://www.politico.com/magazine/story/2015/02/china-cybersecurity-114875.html#.Vc3_0hRVhBc.

[64] *See* Thomas Schulz, *Tomorrowland: How Silicon Valley Shapes Our Future*, DER SPIEGEL, (March 4, 2015) http://www.spiegel.de/international/germany/spiegel-cover-story-how-silicon-valley-shapes-our-future-a-1021557.html.

any undue influence, but on the victim State to affirmatively exclude it. In response to the pervasive use of social media by protest groups, numerous countries either blocked Twitter, as with Iran,[65] or specifically requested that Twitter censor certain accounts and tweets within their territory, as with Egypt.[66] In this way, Twitter's code is the law, and States wishing to impose more speech-restricting standards must ask Twitter to affirmatively censor content within their borders, or block it entirely. Likewise, China's response to tools like Tor has not been to seek their removal by the U.S. government, but rather to prevent their download and to restrict their functionality within Chinese networks.[67] These reactions suggest that a de jure (if not de facto) open Internet may well become the international default, and that any State wishing to impose greater restrictions is obliged to take action. This understanding of the Internet is reflected by its architecture: code may become customary international law.

The current status of State practice may also be a reflection of the underlying weakness of the non-intervention principle and of the further erosion of Westphalian sovereignty – the historic system that has long underpinned international relations – in favor of a more effects jurisdiction-based order, as seen in *Trail Smelter*.[68] Although nominally violative of international law, international relations could nonetheless be characterized largely as a battle of low-level interventions, with each State attempting to influence the policies of foreign States. Asserting a hard rule of non-intervention can come off as somewhat idealistic, as some degree of intervention is widely acknowledged in the international community. Indeed the ICJ itself recognized the apparent weakness of the principle in *Nicaragua* stating that, "examples of trespass against this principle are not infrequent."[69] In practice, non-intervention may be more of a diplomatic sparring match, where low-level interventions are met and countered with opposing low-level

---

[65] Ali Sheikholeslami, *Iran Blocks Facebook, Twitter Sites Before Elections*, BLOOMBERG, (May 23, 2009) http://www.bloomberg.com/apps/news?pid=newsarchive&sid=anh.uW3gNZp4.
[66] *Twitter's Censorship Plan Rouses Global Furor*, ASSOC. PRESS, (Jan. 27, 2014) http://www.cbsnews.com/news/twitters-censorship-plan-rouses-global-furor/.
[67] Andrew Jacobs, *China Further Tightens Grip on the Internet*, N.Y. TIMES (Jan. 29, 2015), http://www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html?_r=1&assetType=nyt_now.
[68] *See* Leo Gross, *The Peace of Westphalia, 1648-1948*, 42 AM. J. INT'L L. 20, 20, 26 (1948); CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 222 (1998).
[69] Nicaragua, *supra* note 11, at 106.

interventions. When viewed in this manner, the current international tension surrounding cyber espionage fits well with low-level cyber-operations justifying opposing in kind responses, and as will be discussed with regard to countermeasures. The open question becomes, though, at what level does such a low-intensity conflict rise to something more, as is being debated now in the Obama Administration with regards to the 2015 OPM breach.[70]

4. Countermeasures and the Gabčíkovo–Nagymaros Project

A victim State to a violation of customary international law is empowered to take appropriate "countermeasures" in response.[71] Countermeasures are otherwise unlawful State actions (or omissions) that are legally permitted[72] when used by a victim State in response to unlawful activity to induce the offending State to cease the unlawful activity.[73] While there is a large body of work discussing countermeasures, delineated most completely in the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts,[74] the element attracting the majority of the attention is "proportionality," e.g., that the countermeasures must be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[75] This proportionality requirement empowers States to engage in a wide range of activities, albeit with restrictions for actions implicating international humanitarian law, human rights, or the threat of or use of force.[76] Therefore, a victim State to a violation of international standards of due diligence may be empowered to take appropriate countermeasures against the offending State, so long as those countermeasures are proportional to the violation of due diligence.

Yet what constitutes a "proportional" countermeasure to a violation of due diligence remains unclear. Although proportionality is a well-known requirement in both

---

[70] *See supra* note 2 and accompanying text; *see infra* note 91and accompanying text.
[71] Naulilaa Incident Arbitration, (Port. V. Ger.), 2 R.I.A.A. 1011 (1928).
[72] This distinguishes countermeasures from retorsions, which are "unfriendly, although lawful" State actions. *See* TALLINN MANUAL, *supra* note 3, at 40.
[73] Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law,* 54 VA. J. INT'L L. 697, 700 (2014).
[74] Responsibility of States for Internationally Wrongful Acts, art. 1, G.A. Res. 56/83, Annex, U.N. Doc. A/RES/56/83 (Jan. 28, 2002) [hereinafter Articles on State Responsibility].
[75] *Id.* at art. 51.
[76] *Id.* at art. 50(1)(a,b,c,d).

the law of armed conflict and international humanitarian law, proportionality in the countermeasures context is subject to a distinct body of law,[77] and was specifically addressed in the ICJ case *Hungary v. Slovakia* on the Gabčíkovo–Nagymaros Project.[78] The case involved a dispute over the construction and operation of a dam, wherein Hungary's failure to comply with the terms of the project prompted Slovakia to intentionally divert the Danube, a border river. The ICJ determined that although Hungary had violated international law by failing to comply with the terms of the dam agreement, Slovakia's countermeasures were nonetheless unlawful because they were not proportionate.[79] Despite Hungary's initial violation being grounded in treaty law, not due diligence, Slovakia's actions may nonetheless prove useful as a point of comparison when evaluating responses to violations of due diligence, potentially suggesting that active interference with essential resources (such as throttling Internet traffic)[80] may be viewed as disproportionate to more passive failures to satisfy a State's obligations.

Yet despite Gabčíkovo–Nagymaros hinging on proportionality, the ICJ went into relatively little detail on how the analysis should be structured.[81] Yet this vagueness might represent a consensus in the international community not to place too constrictive a legal regime on States engaging in such diplomatic behavior. While Slovakia's actions in Gabčíkovo–Nagymaros may have been clearly outside the bounds of customary international law, other cases adjudicating proportionality have allowed for some laxity in how proportionate "proportionate" must be. Arbitration between France and the United States over an airline dispute, for example, held that the U.S.'s countermeasures, although having a notably larger economic impact than France's actions, were not "clearly disproportionate," and therefore were justified under international law.[82] The adjudicating tribunal in the case held that economically disproportionate countermeasures

---

[77] *See* Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 AM. J. INT'L L. 715, 738 (2008).
[78] Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), 1997 ICJ Rep. 7 (Sept. 25).
[79] *Id.* at 56, para. 87.
[80] *See* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report of the Special Rapporteur on Key Trends and Challenges to the Right of All Individuals to Seek, Receive and Impart Information and Ideas of All Kinds Through the Internet, Human Rights Council, U.N. Doc. A/HRC/17/27, ¶¶ 49-50 (May 16, 2011).
[81] *See* Frank, *supra* note 77, at 716.
[82] Air Services Agreement of 27 March 1946 (U.S. v. Fr.), 18 R.I.A.A. 417 (1978).

can be justified when "enforcing a principle,"[83] thus allowing for laxity in the proportionality assessment.[84]

Applying these principles to cyber-countermeasures suggests that States will enjoy tentatively broad discretion in the choice of response to an internationally unlawful act. Since there is no requirement that countermeasures take the same form as the precipitating activity, cyber-countermeasures may be used in response to non-cyber unlawful activity, and vice versa. And among these cyber-responses, activities may vary widely, from more aggressive "hack back" operations against the offending State, to more passive activities, such as the termination of packets routed through the victim State.[85] Yet some activity will likely fall beyond the bounds of international law, such as the cyber equivalent of diverting a river,[86] and may be given a wide berth in turn.[87]

Adding upon this loose framework, the primary substantive limit on countermeasures – proportionality – is weakened by the dearth of cyber-examples, particularly in the due diligence context, as well as the difficulty in quantifying cyber-operations, and the principle that economically disproportionate countermeasures are

---

[83] *Id.* at 443-444.

[84] Although other requirements are often invoked regarding the legality of countermeasures, Gabčíkovo-Nagymaros only expressly acknowledged one: that the countermeasures must be to induce the offending State to comply with its international obligations. *See* Gabčíkovo-Nagymaros Project, *supra* note 78, at 56–57, para. 87. This is sometimes reframed to require that countermeasures not be punitive, and is generally accepted to encompass a requirement that countermeasures, when possible, be reversible (that the countermeasures can be undone once the offending State is in compliance with their international obligations). *See* Articles on State Responsibility, *supra* note 74, art. 49, commentary 9 ("States should as far as possible choose countermeasures that are reversible."). Moreover, although the ILC suggests that countermeasures should require the victim State to call upon the offending State to cease the activities prior to commencing countermeasures, even this is undermined by an exception for "urgent countermeasures." Articles on State Responsibility, *supra* note 74, art. 52(1–2). In the cyber context, this exception may trivialize the requirements for prior notification, since many incidents are likely to be deemed urgent in an arena as dynamic and fraught with attribution difficulties as cyber. *See* Katherine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, YALE J. INTL. L. 1, 11 (2011); Lotrionte, *supra* note 53, at 520–521. Even in the seemingly slower realm of due diligence, this "urgent" provision may still be utilized, as a State's failure to police cybercrime perpetrated within its borders, for example, could reasonably be interpreted as necessitating urgent countermeasures by the victim State to quash the threat posed by the cybercriminals.

[85] *See* Schmitt, *supra* note 73, at 704–705.

[86] For a discussion of the economic and environmental impact of Slovakia's actions, *see* Gabriel Eckstein, *Application of International Water Law to Transboundary Groundwater Resources, and the Slovak-Hungarian Dispute Over Gabickovo-Nagymaros*, 19 SUFFOLK TRANSNAT'L L. REV. 67, 102-106 (1995).

[87] There is even some acknowledgment that countermeasures may negatively impact innocent States, provided those impacts are not intentional and are minimized as much as possible. *See* Portugal v. Germany, 2 R.I.A.A. 1052, 1057 (1928).

allowable to enforce a principle.[88] While how to classify cyber-operations is still a contested topic, and will likely vary depending upon the specific context,[89] cyber-operations and cyber due diligence could both reasonably be interpreted as primarily "economic," and the further laxity allowed with economic countermeasures when "enforcing a principle" (say, the legality of economic espionage) may defang the primary restriction imposed on countermeasures. A State's failure with regard to due diligence may therefore give rise to disproportionate countermeasures, and so long as those countermeasures are not so disproportionate as to rise to a use of force,[90] or to being "clearly disproportionate," there appears to be little in the way of constraining legal factors on State cyber-countermeasures. However, the politics involved are another matter, such as may be seen in the Obama Administration's deliberations about how best to respond to the 2015 OPM breach such as by breaching the Great Firewall of China.[91]

The unwillingness to formally recognize cyber-operations likely stems from their legal ambiguity, particularly with regard to due diligence. Since the legality of economic espionage and the requirements for cyber due diligence are not clearly delineated under international law, the overt use of countermeasures is risky, as the invocation of countermeasures does not shield the victim State if the precipitating activity is later found to have been lawful.[92] Rather than rely purely on countermeasures and risk international liability, States currently seem to employ a middle ground between espionage and countermeasures, featuring a combination of public outrage with private culpability that can become self-perpetuating and is unlikely to be resolved in the near future.

C. Cybersecurity Due Diligence Obligations of Transit States

Cyber attacks are frequently routed through several transit states before reaching their ultimate targets so as to obfuscate the attack's origin by taking advantage of the distributed nature of the Internet's architecture.[93] As with attacks launched from within a

[88] *See* Air Services Agreement, supra note 82, at 443.
[89] TALLINN MANUAL, *supra* note 3, 43–45.
[90] *See id.*
[91] *See* David E. Sanger, *U.S. Decides to Retaliate Against China's Hacking*, N.Y. TIMES (July 31, 2015), http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.
[92] Articles on State Responsibility, *supra* note 74, art. 30 and accompanying commentary.
[93] Mudrinich, *supra* note 34, at 198.

State, the obligations of States that retransmit malicious Internet traffic originating elsewhere will likely depend upon that State's knowledge of the attack. The obligations of a State that knowingly allows a cyber attack to be transmitted through its domestic networks will likely be greater than those that do so without knowledge. Among those States that transmit the attack unwittingly, different standards could be applied to those that comply with cybersecurity best practices and those that fail to do so.[94] Furthermore, repeated or continuous cyber-activity through a State's domestic networks may give rise to a presumption of knowledge, and direct use of State controlled critical infrastructure could serve as evidence that the transit State knew or should have known of a cyber attack in progress.[95] Yet State knowledge must be understood in context, as the individual packets transmitted through the State's network may, taken alone, be innocuous.[96] Cyber attacks are complex, often made up of myriad components, and so knowledge of an individual exploit does not necessarily equate to knowledge of the overarching campaign. Attacks may be broken apart into bits of seemingly innocuous or unintelligible code, only to be recognizable as a cyber threat when reconstructed later. Stuxnet, for example, was designed in such a way that it would only be activated on specific hardware and systems.[97]

As for the due diligence duties that may be required of transit States, these would likely reflect the role that a given State's infrastructure played in the attack. The highest level of due diligence that could reasonably be required would be an affirmative obligation to monitor a nation's networks for cyber attacks and to mitigate any such threat. This would be akin to requirements of neutral States in time of war, which are told to disallow and resist any belligerent force from transporting troops or munitions through a neutral territory. Less potentially onerous, yet more likely, requirements would be a duty to warn target States of attacks detected on their networks (without a hard requirement to monitor and eliminate), and a duty to cooperate with cyber-forensics conducted by the target State to identify the cyber-attack's source.[98] The transit State

[94] Heinegg, *supra* note 36, 136–137.
[95] *Id.*
[96] *Id.*
[97] *See generally* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON passim (2014).
[98] Heinegg, *supra* note 36, at 140.

may still be under a general obligation to enact and enforce domestic cybercrime legislation, as is discussed above, although this is unlikely to be relevant for mere transmission. Most broadly, the State may be subject to a generalized duty to maintain a minimum standard of cybersecurity care, as discussed above for the States in which the attack originated.

The role of transit States ultimately will reflect the degree to which their actions and omissions contributed to the attack. While these obligations are certainly less demanding than those of the State where the attack originated, transit States nonetheless may have some obligations, and must consider the international implications of their domestic cybersecurity strategies. However, it should be noted that as command and control servers move to targeted States, due diligence standards might shift.[99] And regardless, there is a need to clarify the international law of neutrality more broadly to define whether or not victim States can or should hold neutral States through which cyber attacks transited accountable for not being diligent in repelling attackers.[100]

D. Caveats

Although all of these cases address the concept of international due diligence, it is unclear to what extent these opinions should shape international cybersecurity law and policy. Both *Corfu Channel* and *Trail Smelter* are arguably distinguishable on the grounds of physical proximity. *Corfu Channel* involved a State's obligations in their bordering sovereign waters and addressed issues raised by ships of other nations physically occupying those waters, while *Trail Smelter* involved environmental discharge across a neighbor's borders. Both cases recognize that actions undertaken by a State within its own territory can have consequences beyond that territory, but are nonetheless constrained to geographically proximate territories. This geographical constraint is not reflected in the cybersecurity realm, wherein actions taken within one's borders can impact diverse networks and systems distributed across myriad global networks. This substantial expansion of the territory on which harmful activity may occur may be the slippery slope that derails this aspect of cybersecurity due diligence requirements for

[99] *Botnet Control Servers Span the Globe*. MCAFEE (Jan. 23, 2013), https://blogs.mcafee.com/mcafee-labs/botnet-control-servers-span-the-globe.
[100] Schmitt, *supra* note 73, at 727.

States. After all, if it were otherwise many nations would be in breach of the environmental obligations to one another through the emission of greenhouse gases responsible for global climate change.[101] As a result, perhaps this aspect of international cybersecurity due diligence should be an arena of *lex feranda* that could lead to a change in attitudes within the international community. International environmental obligations, although originally geographically constrained, have increased in their scope of impact, with major environmental catastrophes such as the Fukushima Nuclear Reactor and the Deepwater Horizon oil spill showing that a single stakeholder's environmental actions and omissions can lead to global environmental challenges.[102] As the world shrinks through environmental and technological changes, geographic isolation, perhaps, should no longer be a viable excuse for neglecting common "no harm" obligations. Indeed, some commentators have already argued "that States have an obligation of due diligence to prevent significant transboundary cyberharm to another state's intellectual property."[103]

Another caveat to the above discussion that should be addressed is the exemption for national security under international law. Customary international law recognizes four national security exceptions: change of circumstances, the law of reprisal, self-defense, and the doctrine of necessity.[104] Each of these exceptions recognizes instances in which a State's international obligations can be stayed due to the actions or threat of action of another State. While narrow in scope, these exceptions insert more uncertainty into an already uncertain arena, as none have been clarified in the realm of cyber-activities, which often implicate issues of national security. For instance, the World Trade Organization ("WTO"), incorporating the General Agreement on Tariffs and Trade

---

[101] *See* Russell A. Miller, *Surprising Parallels Between Trail Smelter and the Global Climate Change Regime*, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW; LESSONS FROM THE TRAIL SMELTER ARBITRATION 167, 167 (Rebecca Bratspies & Russell A. Miller eds., 2006).

[102] *See, e.g.*, Steven Starr, *Costs and Consequences of the Fukushima Daiichi Disaster*, PHYSICIANS FOR SOCIAL RESPONSIBILITY, http://www.psr.org/environment-and-health/environmental-health-policy-institute/responses/costs-and-consequences-of-fukushima.html (last visited Aug. 28, 2015).

[103] Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm,* 52 COLUM. J. TRANSNAT'L L. 275, 279 (2013) ([A]ffected states may be entitled to reciprocate by . . . allowing their victimized nationals to hackback." (emphasis added)).

[104] Susan Rose-Ackerman and Benjamin Billa, *Treaties and National Security,* 40 N.Y.U. J. INT'L L. & POL. 437 (2008).

("GATT"), employs a broad exception for "essential security interests,"[105] which effectively serves as an un-appealable, self-determined "get out of jail free card." Despite the GATT's restriction on unilateral economic sanctions, the United States has on multiple occasions used the national security exception to impose unilateral economic sanctions, most recently against Russia.[106] This exception for national security is a frequently bemoaned aspect of international law, but nevertheless suggests a fundamental valuation on the part of the international community that State sovereignty is to be given preference on issues implicating essential security interests. Therefore, any cybersecurity due diligence standards must be understood to likely contain a national security exception, which could lead to the exception swallowing the rule. Ultimately, the existence of these caveats and exceptions makes any definitive statement regarding the status of international due diligence standards that much more difficult, leading to the necessity of examining public- and private-sector approaches to help clarify the missing elements to a cybersecurity due diligence norm.

II. NATIONAL AND PRIVATE-SECTOR APPROACHES TO CYBERSECURITY DUE DILIGENCE

As was discussed in the previous section, international law, while informative, does not spell out in detail how nations should go about enhancing their cybersecurity to account for emerging due diligence obligations. As a result, it is helpful to consider established and proposed both public-and private sector approaches for defining due diligence. Such national strategies could, in time, crystallize into customary international law as state practice clarifies.[107] Similarly, given the extensive public-private cross-pollination of cybersecurity best practices, private-sector efforts aimed at enhancing cybersecurity are informative given the extent to which they are shaping national

[105] GATT 1994: General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 17 (1999), 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994).
[106] *See, e.g.*, Robert Coalson, *Explainer: How The International Sanctions Game Is Played*, RADIO FREE EUR. (Mar. 21, 2014), http://www.rferl.org/content/russia-us-sanctions-explainer/25305528.html.
[107] *See* Jean-Marie Henckaerts & Louise Doswald-Beck, *Assessment of Customary International Law*, INT'L COMM. RED CROSS (2005), http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin.

policymaking with the NIST Framework being a case in point.[108] Thus, this final section begins by discussing several national case studies of cybersecurity due diligence including the United States, Germany, and China as a first step to uncovering a due diligence governance spectrum.[109] We then offer a due diligence matrix to better inform the discussion before moving on to examine the extent to which cybersecurity is entering the due diligence process of mergers and acquisitions in the U.S. private sector context. Finally, we conclude with several observations for how industry cybersecurity norms are translating into national policymaking, and what that means for managers, policymakers, and the field of cybersecurity due diligence generally.

A. National Approaches to Regulating Cybersecurity Due Diligence

This sub-section briefly reviews the national approaches of the United States, Germany, and China with regards to cybersecurity due diligence regulation. These case studies were chosen not only because these nations are among the world's leading cyber powers, but also to provide common and civil law, as well as developed and emerging market perspectives on this issue. This analysis is not meant to be dispositive of the topic under consideration, but rather to provide a snapshot for how this influential subset of nations is approaching the topic of cybersecurity due diligence.[110] Further research is required to flesh out whether the noted trends are playing out globally.

1. United States

The topic of cybersecurity due diligence per se has not received an inordinate amount of attention by the Obama Administration, though it has referenced the topic in its 2011 International Strategy for Cyberspace. In it, the Administration states of cybersecurity due diligence that: "States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or

[108] *See Update on the Cybersecurity Framework*, NIST (Dec. 5, 2014), http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf.
[109] For further information on how cybersecurity governance is playing out in the arena of critical infrastructure protection around the world, see generally Shackelford & Craig, 2014.
[110] *See* BOOZ ALLEN HAMILTON, CYBER POWER INDEX 2–3 (2014), http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf (discussing various indicators of cyber power in the public and private sectors and making the case that the US, Australia, the UK, Germany, and Canada are the top five cyber powers).

misuse."[111] This represents an effort to help crystallize a cybersecurity due diligence norm in international law essential to broader efforts to promote cyber peace. The argument goes that due to the practical and political difficulties surrounding multilateral treaty development in the cybersecurity arena, norm creation provides an opportunity to enhance global cybersecurity without waiting for a comprehensive global agreement, which could come too late if at all. Yet despite general agreement as to the value of cybersecurity norms including due diligence, "even simple norms face serious opposition. Conflicting political agendas, covert military actions, espionage[,] and competition for global influence" have created a difficult context for cyber norm development and diffusion[112]; a situation that NSA revelations arguably exacerbated. As a result, to be successful in such a difficult climate, norms must be "clear, useful, and do-able . . . ."[113] The U.S. has had some success in applying international law to cyber warfare, along with extending human rights protections online,[114] but more broadly what would a cybersecurity due diligence norm look like from the national perspective? It is helpful to briefly review U.S. approaches to this topic in order to provide a build out a framework for discussion.

The United States has been active in strategizing about national cybersecurity since the creation of the world's first Cyber Emergency Response Team at Carnegie Mellon University in 1988. Today, though, the field is crowded with an alphabet soup of agencies and organizations responsible for various aspects of the nation's cybersecurity. The Department of Defense alone reportedly operates more than 15,000 networks in

---

[111] INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD, WHITE HOUSE 10 (2011).
[112] James A. Lewis, *Confidence-Building and International Agreement in Cybersecurity*, DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 58 (2011).
[113] Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).
[114] Henry Farrell, *Promoting Norms for Cyberspace*, COUNCIL FOREIGN REL. (2015), http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358?cid=nlc-npbnews-2015_national_conference_confirmation_and_background--link22-20150602&sp_mid=48790069&sp_rid=a3plZ3VyYUBjZnIub3JnS0 (arguing that the U.S. government should take the following three steps to reinvigorate a norms-based approach to multilateral cybersecurity policymaking: "reform U.S. intelligence activities to make them more consistent with the publicly expressed norms of Internet openness that the United States is trying to establish; disclose more convincing evidence when trying to shame actors that do not abide by cybersecurity norms; and encourage other states and civil society actors to take a leading role in norm promotion—even when this cuts against U.S. interests.").

4,000 installations spread across some 88 countries.[115] Yet the majority of U.S. efforts in this space have been focused on securing vulnerable critical infrastructure ("CI"). Although Congress has been active in this regard, successive administrations—including those of Presidents Clinton, Bush, and Obama—have pushed the ball forward on securing vulnerable CI.

Most recently, President Obama declared the U.S. CI to be a "strategic national asset" in 2009 though a fully integrated U.S. cybersecurity policy has yet to be established.[116] In the face of Congressional inaction, President Obama issued an executive order that, among other things, expanded public-private information sharing and established the NIST Framework comprised partly of private-sector best practices that companies could adopt to better secure CI.[117] This Framework is important since, even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges,[118] it is arguably spurring the development of a standard of cybersecurity care in the United States that plays into discussions of due diligence.[119] In particular, the NIST Framework harmonizes industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk. Although the NIST Framework has only been out for a relatively short time, already some private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[120] Over time, the NIST

---

[115] Kristin M. Lord & Travis Sharp, Executive Summary, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 7, 12 (Kristin M. Lord & Travis Sharp eds., CNAS, 2011).
[116] *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*, GAO (May 7, 2013), http://www.gao.gov/products/GAO-13-462T ("Further, without an integrated strategy that includes key characteristics, the federal government will be hindered in making further progress in addressing cybersecurity challenges.").
[117] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.
[118] Taylor Armerding, *NIST's Finalized Cybersecurity Framework Receives Mixed Reviews*, CSO (Jan. 31, 2014), http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html.
[119] *See, e.g.*, Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. J. INT'L L. 287 (2015).
[120] *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

Framework not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large given active NIST collaborations with a number of nations including the United Kingdom, Japan, Korea, Estonia, Israel, and Germany.[121]

2. Germany

Germany's cybersecurity due diligence efforts rely on close collaboration between the public and private sectors, nationally and globally.[122] Long known for its strong national data protection law with fines up to EUR 300,000, Germany is moving now to mandate strict cybersecurity standards for CI, and assign the responsibility to protect users and secure CI to service providers and operators of CI.[123] In particular, the federal government approved the German Cybersecurity Strategy ("Cyber-Sicherheitsstrategie für Deutschland") in February 2011. The Strategy recognizes cyberspace as an essential domain for the German State, economy, and society, and emphasizes the protection of CI as a core cybersecurity policy priority. Moreover, it addresses cybersecurity due diligence by recognizing that "incidents in other countries' information infrastructures may also indirectly affect Germany."[124] The Strategy also calls for a code of conduct, international legal harmonization and cooperation, and states that service providers may need to assume greater responsibility for the security of their digital products and users.[125] In all, according to Booz Allen, Germany "is one of only five countries (the others being the UK, the US, France, and Japan) to have a

[121] There is some evidence that this may already be happening, including with regards to the Federal Trade Commission's cybersecurity enforcement powers. *See, e.g.*, Brian Fung, *A Court Just Made it Easier for the Government to Sue Companies for Getting Hacked*, WASH. POST (Aug. 24, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/08/24/a-court-just-made-it-easier-for-the-government-to-sue-companies-for-getting-hacked/?wpmm=1&wpisrc=nl_headlines.
[122] CYBER-SICHERHEITSSTRATEGIE FÜR DEUTSCHLAND, GERMAN FEDERAL MINISTRY OF THE INTERIOR (2011), http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html.
[123] BUNDESMINISTERIUM DES INNERN, SCHUTZ KRITISCHER INFRASTRUKTUREN – RISIKO- UND KRISENMANAGEMENT: LEITFADEN FÜR UNTERNEHMEN UND BEHÖRDEN (2008), http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf?__blob=publicationFile.
[124] GERMAN FEDERAL MINISTRY OF THE INTERIOR, *supra* note 122, at 4.
[125] *Id*. at 4–7.

comprehensive national cyber plan and a comprehensive cybersecurity plan" which has been "a key to its success."[126]

Germany has also been active in identifying and spreading cybersecurity best practices in a similar vein as the NIST Framework. The Federal Office for Information Security ("Bundesamt für Sicherheit in der Informationstechnik", BSI) first released its IT Baseline Protection ("IT-Grundschutz") in 1994. This set of BSI standards contains recommendations for cybersecurity and has been adopted by German corporations and international stakeholders; some of the standards are now available in English, Swedish, and Estonian. These standards are best practice recommendations that have become "de-facto standards for [the German] IT security," but are not legally enforceable save for data protection fines mentioned earlier.[127]

Efforts are also underway in Germany's private sector to widen the discussion and dissemination of cybersecurity best practices. For example, established in 2012, the Alliance for Cybersecurity ("Allianz für Cybersicherheit") is an initiative under the aegis of the Federal Office for Information Security.[128] It brings together more than a thousand public and private participating entities to share best practices and further the cause of German cybersecurity due diligence. The Alliance encourages voluntary reporting of cyber incidents and attacks to collect information about current cyber threats against German organizations. These private efforts help to shape industry norms and contribute towards responsible cyber behavior.

Germany's Minister of the Interior Dr. Thomas de Maizière recently addressed the topic of cybersecurity due diligence in particular during the 2014 Global Cyberspace Cooperation Summit in Berlin. Referring to the need to carefully consider the principle of responsibility in cyberspace, de Maizière, pointed to a basic tenet in law: he who creates a risk for others is responsible for it. The greater the risk, the larger the responsibility ("[…] wer ein Risiko für andere schafft, trägt dafür Verantwortung. Je

[126] CYBER POWER INDEX, *supra* note 110, at 3.
[127] OWASP REVIEW BSI IT-GRUNDSCHUTZ BAUSTEIN WEBANWENDUNGEN, https://www.owasp.org/index.php/OWASP_Review_BSI_IT-Grundschutz_Baustein_Webanwendungen.
[128] *See* Allianz für Cybersicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html (last visited June 16, 2015).

größer das Risiko ist, umso höher die Verantwortung").[129] Partly in response to this sentiment (and the 2013 NSA revelations), the German parliament adopted the IT Security Act ("Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)"), which became effective as of July 25, 2015. The new law requires companies to employ and comply with state of the art technology to secure their websites – or be held liable in the event of a breach. More stringent security requirements and responsibilities apply for CI operators.[130] The designated CI sectors are responsible for developing appropriate security standards (similar to the NIST Framework's approach), pending the Ministry of the Interior's approval. CI operators are also obligated to inform the authorities of cyber attacks. These cybersecurity policy efforts are estimated to create a need for between 200 and 425 new jobs across the federal government and cost for personnel and resources of up to EUR 38 million per year.[131] However, relative to the United States where, despite an overall shrinking defense budget, cybersecurity spending continues to increase (as is the case with China), such costs seem almost reasonable.[132]

3. China

According to Booz Allen, while the United States and Germany rank second and fourth respectively in terms of their 2015 global cyber power ranking, China comes in at a, perhaps somewhat surprising, thirteenth place.[133] Part of the reason for this lower ranking is that China applies tight controls over its domestic Internet in order to advance the Communist party's economic, political, and military interests and to help secure its rule while having a less robust legal and regulatory environment to enhance national

---

[129] Thomas de Maizière, Thomas, *Sichere Informationsinfrastrukturen in einem Cyber-Raum der Chancen und der Freiheit* (2014), http://www.bmi.bund.de/SharedDocs/Reden/DE/2014/12/east-west-cyber-summit.html?nn=3314802. This sentiment may also be considered another manifestation of the sliding scale approach discussed above.

[130] *See* Friendhelm Greis, *Kabinett Beschließt Meldepflicht für Cyberangriffe*, GOLEM.DE (2014), http://www.golem.de/news/it-sicherheitsgesetz-regierung-beschliesst-meldepflicht-fuer-cyberangriffe-1412-111234.html.

[131] *Id*.

[132] *See e.g.,* Andrea Shalal & Alina Selyukh, *Obama Seeks $14 Billion to Boost U.S. Cybersecurity Defenses*, REUTERS (Feb. 2, 2015), http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202.

[133] *See* CYBER POWER INDEX, *supra* note 110, at 4.

cybersecurity.[134] On the international stage, it continuous to seek cooperation "to promote the building of a peaceful, secure, open, and cooperative cyberspace" and attempts to shape international norms, particularly with regard to State sovereignty and censorship under the disguise of information security.[135] At the same time, there are increasing tensions between the U.S. and China about mutually alleged cyber exploitations including the millions of impacted current and former U.S. civil servants from the Office of Personnel Management breach referenced above.[136] In 2014, the U.S. indicted five hackers of the People's Liberation Army for economic cyber espionage; China protested sharply.[137] The U.S. government has billed China as the "world's most active and persistent perpetrators of economic espionage,"[138] while in June 2013, President Obama warned that the continuation of U.S. intellectual property theft is a serious matter that will hinder the further development of economic trade relations with China. The U.S reaction may be conceived as an approach to shape norms on cybersecurity due diligence, by calling out China to take responsibilities for alleged cyber exploitations. Ultimately, though, such norms have a strong political dimension, as the Chinese case study shows, and have not yet found a resolution.

As with the U.S., China's cybersecurity strategy is fragmented, but its development and implementation has garnered the political support of high-ranking senior government officials. In early 2014, Chinese President Xi Jinping stressed that a uniform and comprehensive approach to "network security" is necessary to turn China

---

[134] *See id*. at 5; Edward Wong, *For China, Cybersecurity Is Part of Strategy for Protecting the Communist Party*, N.Y. TIMES (Dec. 3, 2014), http://sinosphere.blogs.nytimes.com/2014/12/03/for-china-cybersecurity-is-part-of-strategy-for-protecting-the-communist-party/.

[135] *See* Sonya Sceats, *China's Cyber Diplomacy: a Taste of Law to Come?*, DIPLOMAT (Jan. 14, 2015), http://thediplomat.com/2015/01/chinas-cyber-diplomacy-a-taste-of-law-to-come/.
China is pursuing cyber diplomacy on an array of fronts. Among other actions, China is furthering the multilateral cybersecurity initiative with the Shanghai Cooperation Organization, is negotiating a bilateral cybersecurity treaty with Russia, is involved in a U.S.-China working group to diffuse tensions around mutually alleged cyber exploitations, and has been drafting cybersecurity-relevant proposals and declarations to garner support from like-minded states at the 2014 World Internet Conference in China and at various UN meetings.

[136] *See* Chappell, *supra* note 2 and associated text.

[137] *See* Chen Weihua, *China Protests Against US Indictment*, CHINA DAILY (May 20, 2014), http://usa.chinadaily.com.cn/world/2014-05/20/content_17519650.htm.

[138] DNI, OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE, REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE: 2009-2011 (Oct. 2011).

into a "cyber power."[139] The speech coincided with the establishment of the "Central Cyber Security and Informatization Leading Group," which under the leadership of President Xi Jinping will guide China's cybersecurity policy efforts.

In many ways, China's cybersecurity strategy is broader in scope than either its U.S. or German counterparts. In addition to addressing the security of networks and computers, it includes censorship of content and information control to a far greater extent than is the case in these Western nations. It is the Chinese government's official position that "properly guiding Internet opinion is a major measure for protecting Internet information security."[140] China's take on cybersecurity is reflected in the idea of Internet sovereignty and its use of the Internet as a means to build up a domestic information economy and secure network infrastructure that benefits domestic development and political stability.[141]

China's first cybersecurity strategy dates back to 2003. It is referred to as "Document 27: Opinions for Strengthening Information Security Assurance Work and covers – inter alia – CI protection.[142] The current 2012 cybersecurity strategy continues some of the earlier cybersecurity considerations (including CI protection) while also addressing China's dependency on foreign technology as a security issue, the promotion of Chinese cryptography standards, the build-up of broadband infrastructure, next-generation mobile technology, and e-government services.[143] Observers have criticized the document as an inconsistent "grab bag of vague policy proposals."[144]

---

[139] Xi Jinping, *China Must Evolve From a Large Internet Nation to a Powerful Internet Nation*, XINHUANET.COM (Feb. 27, 2014), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.
[140] Chris Buckley & Lucy Hornby, *China Defends Censorship after Google Threat*, REUTERS (Jan. 14, 2010), http://www.reuters.com/article/2010/01/14/us-china-usa-google-idUSTRE60C1TR20100114.
[141] *See, e.g.*, Shannon Tiezzi, *China's 'Sovereign Internet*,' DIPLOMAT (June 24, 2014), http://thediplomat.com/2014/06/chinas-sovereign-internet/.
[142] Adam Segal, *China Moves Forward on Cybersecurity Policy*, COUNCIL ON FOREIGN REL. (July 24, 2012), http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/.
[143] Hauke Johannes Gierow, *Cyber Security in China: New Political Leadership Focuses on Boosting National Security*, MERCATOR INST. FOR CHINA STUD. (2014), http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf. China is far from alone, though, in seeking to protect its domestic industry in the name of enhancing cybersecurity. *See* Karen Kornbluh, *Beyond Borders: Fighting Data Protectionism*, COUNCIL ON FOREIGN REL. (Dec. 16, 2014), http://www.cfr.org/united-states/beyond-borders-fighting-data-protectionism/p34008?cid=nlc-npbnews-2015_national_conference_confirmation_and_background--link25-20150602&sp_mid=48790069&sp_rid=a3plZ3VyYUBjZnIub3JnS0; Scott J. Shackelford, *How to Enhance Cybersecurity and Create American Jobs*, HUFF. POST (July 16, 2012), http://www.huffingtonpost.com/scott-j-shackelford/how-to-enhance-cybersecurity_b_1673860.html.
[144] Segal, *supra* note 142.

Some of these measures are in line with cybersecurity due diligence efforts; others are broader in scope and have raised concerns, particularly from U.S. and European counterparts. For example, in 2007, China established a set of security standards, the "Regulations on Classified Protection of Information Security" (which are also referred to as the Multi-Level Protection Scheme, "MLPS") with the objective of safeguarding information and protecting national security.[145] Western firms and organizations repeatedly expressed their disapproval since these technical standards are incompatible with international IT security standards. Rather than protecting national security, these standards have been perceived as protectionist measures that shield Chinese domestic IT firms from global competition. Some argue that such efforts have actually resulted in *less* secure Chinese standards and technology.[146] Leading cybersecurity companies such as Kaspersky and Symantec are barred from competing in China's corporate market for financial institutions and power utilities, for instance. Such developments may help open the door for cyber attacks on China's CI; a detriment to the cause of cybersecurity due diligence.[147]

Similar to MLPS, and as part of its economic policy, China has attempted to establish its own wireless network standard ("WAPI"). In reaction to NSA revelations, it announced work on independent, Chinese operating systems for desktop computers as well as mobile devices.[148] Other recent or pending Chinese legislation portend still more protection, such as requiring technology companies that sell to China's banks to submit

---

[145] Nathaniel Ahrens, *National Security and China's Information Security Standards: Of Shoes, Buttons, and Routers*, CTR. STRATEGIC & INT'L STUD. (Nov. 8, 2012), http://csis.org/publication/national-security-and-chinas-information-security-standards.

[146] *See* Gierow, *supra* note 143.

[147] Once again, though, China is not alone in striking the appropriate balance between promoting state sovereignty and digital protectionism and enhancing both cybersecurity and innovation. The European Union is also in the midst of a similar debate with behemoths of the Information Age including Google. *See, e.g.*, EU International Cyberspace Policy, http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm (last visited June 16, 2015); David Fidler, *Europe v. Google: A Dispute About Competition, Political Power, and Sovereignty*, COUNCIL ON FOREIGN REL. (Apr. 21, 2015), http://blogs.cfr.org/cyber/2015/04/21/europe-v-google-a-dispute-about-competition-political-power-and-sovereignty/?cid=nlc-npbnews-2015_national_conference_confirmation_and_background--link24-20150602&sp_mid=48790069&sp_rid=a3plZ3VyYUBjZnIub3JnS0.

[148] *Chinese OS Expected to Debut in October*, XINHUNET (Aug. 24, 2014), http://news.xinhuanet.com/english/china/2014-08/24/c_133580158.htm.

their source code for government inspection.[149] A proposed draft for a new anti-terror legislation has been stalled, but if implemented would similarly require companies to divulge encryption keys and install backdoors to give Chinese authorities access to secured data and communication. Such policies would impact Western tech firms in particular, and could even bar them from China's still growing market.[150]

In summary, China expresses the need for the control of information and exclusion of foreign owned-security technologies in order to protect its societal stability. As a result, its strategy focuses on national security and economic advancement. Elements of cybersecurity due diligence consequently look quite different when compared to the U.S. or German cases, demonstrating the difficulty of crafting a global norm in this space. However, one could potentially construe a Chinese version of cybersecurity due diligence that is at the other end of a possible spectrum from the U.S. and Germany and that includes domestic economic rationales and protectionist measures as opposed to a narrower focus on securing CI though a relatively well-developed system of legal checks and balances. In fact, many of the policy objectives are similar across the three case studies; what differs are the means.

Custom requires widespread State practice that is undertaken out of a sense of legal obligation. Depending on the type of norm involved, that State practice needs to be more or less widespread. For new norms, such as in the cybersecurity context, the standard generally is "virtually uniform" State practice.[151] This threshold has not yet been reached in the cybersecurity due diligence context, as may be seen by the three approaches taken by these nations with the U.S. being more voluntary, Germany taking a relatively more regulatory approach featuring a comprehensive cybersecurity policy that has long alluded U.S. policymakers, and China's broader economic and national security efforts. To get a better sense of how these nations vary in their treatment of cybersecurity due diligence, we have generated a matrix comparing these countries' due diligence responsibilities.

---

[149] Paul Mozur, *New Rules in China Upset Western Tech Companies*, N.Y. TIMES (Jan. 28, 2015), http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.

[150] *See* Gierow, *supra* note 143; Shara Tibken, *Apple's Cook: Don't Fret – China Growth Remains Strong*, CNET (Aug. 24, 2015), http://www.cnet.com/news/apples-cook-says-china-growth-remains-strong/.

[151] N. Sea Continental Shelf (F.R.G./Den. v. Neth.), 1969 I.C.J. 41, 72 (Feb. 20).

4. Cyber Due Diligence Matrix

Though there is not one definitive definition of cybersecurity due diligence as was discussed above,[152] for purposes of this matrix it is considered to be an obligation under international law that calls for a certain "form of conduct" from a State to be in line with its international law obligations toward other States.[153] While public international law is particularly concerned with the relations among States—as was discussed in the preceding three case studies—an international cyber due diligence obligation implicates domestic actors and legislation. To fulfill its international law obligations, a State arguably needs to be able to exercise control over ICT and critical information infrastructure within the territory and under its jurisdiction. Yet this is a difficult and complex undertaking given the difficulties of jurisdiction, attribution, ambiguous norms, and nearly ubiquitous private-sector ownership of critical infrastructure stemming from the wave of the liberalization and privatization of public infrastructure beginning in the late 1970s.[154] To further their cybersecurity due diligence mandates, States should, among other steps, establish domestic policy regimes including laws, frameworks (such as NIST and BSI), and initiatives that incentivize or even cajole private actors under their jurisdiction to behave in accordance with prevailing legal obligations. Table 1 proposes a non-comprehensive, working set of domestic "State responsibilities" that contribute to fulfilling a State's international law obligation on cyber due diligence.[155]

The responsibilities in Table 1 fall into three general activity categories: (1) Establish and Maintain, (2) Control and Enforce, and (3) Monitor and Assess.

---

[152] *See infra* Part I(B).

[153] Nicholas Tsagourias, *Economic Cyber Espionage and Due Diligence*, SYRACUSE UNIV. CONTROLLING ECONOMIC CYBER ESPIONAGE' WORKSHOP (June 18-19, 2015), *available at* http://insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf.

[154] *See, e.g.*, J.P. Singh, *The Institutional Environment and Effects of Telecommunication Privatization and Market Liberalization in Asia*, 24 TELECOMM. POL'Y 885, 886 (2000).

[155] The cyber due diligence matrix in Table 1 reflects key aspects of a due diligence obligation for cybersecurity as the authors perceive and define it. We gained analogical insights from key cases of international due diligence obligations as described above in Part I, and complemented those by looking for due diligence characteristics in three leading cyber powers: the U.S., Germany, and China. This helped us to chart out comparative factors applicable in the cyber domain. Nicholas Tsagourias's cyber due diligence paper, the 2015 ITU Global Cybersecurity Index, and conversations at the 2015 workshop on 'Controlling Economic Cyber Espionage' at Syracuse University, June 18-19, were used to help define and structure the cyber due diligence matrix. *See* Tsagourias, *supra* note 153; ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157. However, this constitutes merely a first effort and we welcome any and all feedback on refining the matrix.

Implementation of a given State's responsibilities varies across state and institutional settings. For instance, one State may legally mandate certain technological standards whereas another State may choose a voluntary structure for cybersecurity standards (such as the NIST Framework) or leave it to private industry associations to establish such standards for particular business sectors. The capacity among states to fulfill cyber due diligence as an international law obligation varies.[156] The ITU, the U.N.'s intergovernmental telecommunications authority, was mandated to build confidence and security in the use of ICTs.[157] The ITU's cyber mission includes a particular focus on developing countries where the necessary capabilities to ensure cyber due diligence may be lacking.[158] Indeed, in early 2011, the ITU and UN Office on Drugs and Crime (UNODC) signed a Memorandum of Understanding to work together to help member states fight cybercrime.[159] Such efforts help to establish a minimal shared standard that suffices international law obligations regarding cyber due diligence.[160] There is a need to establish clear notions about what domestic responsibilities a state needs to live up to in order to meet the cyber due diligence requirement. Due to technological and institutional development, however, those responsibilities are subject to change and need to be adjusted accordingly. To describe and measure a particular responsibility, we suggest adopting a maturity model, similar to that used in software development.[161] Such descriptive categories would allow one to compare responsibility statuses across various

[156] Nicholas Tsagourias (2015). Economic cyber espionage and due diligence. Paper presented at the Controlling Economic Cyber Espionage' Workshop, June 18/19, Syracuse University. http://insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf

[157] The ITU's cybersecurity mandate is based on the WSIS Action Line C5 - Building confidence and security in the use of ICTs; Resolution 69 (WTDC-10) and Resolution 58 (WTSA-12) Creation of national computer incident response teams; Resolution 130 (PP-14) - Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES (2015), https://www.itu.int/pub/D-STR-SECU-2015.

[158] *See*, *e.g.*, *IMPACT: Mission & Vision*, IMPACT, http://www.impact-alliance.org/aboutus/mission-&-vision.html (last visited June 30, 2013).

[159] *UN Agencies Team Up to Make the Online World Safer: MoU Signed Between ITU and UNODC at WSIS Forum 2011*, ITU NEWSLOG: CYBERSECURITY SPAM AND CYBERCRIME (May 19, 2011), http://www.itu.int/osg/blog/CategoryView,category,Cybersecurity%2BSpam%2Band%2BCybercrime.asp.

[160] Tsagourias argues for a need of a "common standard," because otherwise private or public actors may opt for operating from states with lesser developed cybersecurity capabilities; this could put the concept of a cyber due diligence obligation under international law at risk. *See* Tsagourias, *supra* note 153.

[161] *See* Mark C. Paulk et al., *Capability Maturity Model for Software*, (Carnegie Mellon Univ. Working Paper, 1993), *available at* http://www.sei.cmu.edu/reports/93tr024.pdf.

States, an application of the notion of common but differentiated responsibilities discussed further below.

TABLE 1: STATE'S CYBER DUE DILIGENCE RESPONSIBILITIES

State's Responsibilities	United States	Germany	China
Establish and Maintain			
- Define and implement *strategies, frameworks and policies* for cybersecurity (e.g., protection of critical information infrastructure), and its governance, for the state and private actors in its jurisdiction	●[162]	●[163]	●[164]
- Introduce or adopt *domestic laws and regulation* relevant to cybersecurity and cyber crime	●[165]	●[166]	●[167]
- Establish and maintain capabilities to respond and react to cyber incidents (e.g. computer security incident response team)	●[168]	●[169]	●[170]
- Define and implement *technical standards, measures, and best practices*	●[171]	●[172]	●[173]

[162] *See*, *e.g.*, *Comprehensive National Cybersecurity Initiative*, WHITE HOUSE (2008), https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (summary); NIST Framework, *supra* note 117.
[163] *See*, *e.g.*, GERMAN FEDERAL MINISTRY OF THE INTERIOR, *supra* note 122; NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP STRATEGY), GERMAN FEDERAL MINISTRY OF THE INTERIOR (2009), http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf.
[164] *See*, *e.g.*, *China's Current Cybersecurity Strategy*, OPINION OF THE STATE COUNCIL CONCERNING FORCEFULLY MOVING INFORMATIZATION DEVELOPMENT FORWARD AND REALISTICALLY GUARANTEEING INFORMATION SECURITY (2012), http://politics.gmw.cn/2012-07/17/content_4571519.htm.
[165] For the U.S., the 2015 *Global Cybersecurity Index* lists nineteen laws and regulations related to cybercrime and cybersecurity. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 493.
[166] For Germany, the 2015 *Global Cybersecurity Index* lists six laws and regulations related to cybercrime and cybersecurity. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 206.
[167] For China, the 2015 *Global Cybersecurity Index* lists five laws and regulations related to cybercrime and cybersecurity. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 134; China's National People's Congress released a first draft of its Network Security Law on July 6, 2015, *see*, 网络安全法 (草案) (Network Security Law (Draft), http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.
[168] *See*, *e.g.*, US-CERT, https://www.us-cert.gov (last visited Aug. 18, 2015); ICS-CERT, https://ics-cert.us-cert.gov (last visited Aug. 18, 2015).
[169] *See*, *e.g.*, CERT-Bund, https://www.bsi.bund.de/CERT-Bund_en (last visited Aug. 18, 2015).
[170] *See*, *e.g.*, CNCERT, http://www.cert.org.cn (last visited Aug. 18, 2015); CERT-Bund, *supra* note 169.
[171] *See*, *e.g.*, NIST, http://www.nist.gov (last visited Aug. 18, 2015); MITRE, http://www.mitre.org (last visited Aug. 18, 2015).
[172] *See*, *e.g.*, Federal Office for Information Security (BSI), which defines the IT Baseline Protection ("IT-Grundschutz") standards and processes. *See* BSI, https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html (last visited Aug. 18, 2015). The 2015 IT Security Act requires government agencies and CI operators to meet minimal IT security standards. *See* GESETZ ZUR ERHÖHUNNG DER SICHERHEIT INFORMATIONSTECHNISCHER SYSTEME (IT-SICHERHEITSGESETZ) (July 17, 2015), Bundesgesetzblatt 2015, I(31), Bonn, July 24, 2015.

(e.g., vulnerability patching) for cybersecurity			
- Define and maintain *organizational processes and mechanisms* for cybersecurity	●[174]	●[175]	
- Provide *training, education, and certification* for individuals and organizations	●[176]	●[177]	●[178]
- Engage in *collaboration on cybersecurity* such as through Budapest Convention (e.g., information sharing, law enforcement, intelligence) with domestic and international actors	●[179]	●[180]	●[181]
Control and Enforce			
- Hold ownership or exercise regulatory *control over critical*	●[182]	●[183]	●[184]

[173] For instance, the Network and Information Security Standardization Technical Committee of the China Communications Standards Association has issued numerous technical IT security standards. *See* CCSA, http://www.ccsa.org.cn/english/tc.php?tcid=is (last visited Aug. 18, 2015). The ITU Global Cybersecurity Index counted eighteen standards that were approved by this committee in 2010. ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157.

[174] *See*, *e.g.*, NIST, http://www.nist.gov (last visited Aug. 18, 2015); MITRE, http://www.mitre.org (last visited Aug. 18, 2015).

[175] *See*, *e.g.*, BSI, *supra* note 172. The 2015 IT Security Act requires CI operators to notify the BSI about significant cyber incidents; in addition, telecom service providers are required to inform their customers, if they detect malicious traffic from their customers' networks or computers such as botnets. *See* IT-SICHERHEITSGESETZ, *supra* note 172.

[176] U.S. educational and training efforts include, for instance, the National Cyber Security Awareness Month, the National Initiative for Cybersecurity Education (NICCS), and the designation of academic institutions as National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD) in education and research. *See, e.g.*, StaySafeOnline.org, https://www.staysafeonline.org/ncsam/ (last visited Aug. 18, 2015).

[177] The BSI, for instance, certifies individuals, service providers, systems, services, and products with regard to IT security and assurance. *See* ZERTIFIZIERUNG UND KONFORMITÄTSBEWERTUNG, FEDERAL OFFICE FOR INFORMATION SECURITY, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html (last visited Aug. 18, 2015). Germany has no federal authority charged with educational or professional training for cybersecurity and related public awareness that we could uncover. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 206.

[178] For instance, the July 2015 draft of China's Network Security Law addressed cyber education and training in articles 15, 16, and 28. *See*, 网络安全法 (草案) (Network Security Law (Draft), http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.

[179] The U.S. ratified the Budapest Convention and emphasized the importance of international collaboration in its 2011 International Strategy for Cyberspace. DHS, for instance, has international sharing agreements with India and Israel. *See* Andreas Kuehn & Milton Mueller, *Einstein on the Beach: Surveillance Technology, Cyersecurity and Organizational Change*, *in* SECURITY IN CYBERSPACE: TARGETING NATIONS, INFRASTRUCTURES, INDIVIDUALS 127, 143 (Giampiero Giacomello ed., 2014). Domestically, the 2015 Executive Order on Promoting Private Sector Cybersecurity Information Sharing encourages information sharing and analysis organizations. *See* WHITE HOUSE, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (Feb. 13, 2015).

[180] *See* Allianz für Cybersicherheit, *supra* note 128. Internationally, Germany cooperates with the U.S. on cybersecurity through a joint cyber bilateral mechanism. *See Joint Statement on U.S.-Germany Cyber Bilateral Meeting*, U.S. DEP'T ST. (June 27, 2014), http://www.state.gov/r/pa/prs/ps/2014/06/228543.htm.

[181] According to the 2015 *Global Cybersecurity Index*, cooperation and information sharing is established on the national level within the public sector. In addition, there is "massive cooperation" among China's telecom operators, the China Internet Network Information Center, and CNCERT. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 134.

infrastructure			
- Conduct *review and control of information technology deployed in critical infrastructure*	●[185]		●[186]
- Enforce *compliance with regulations and policies*	●[187]	●[188]	●[189]
Monitor and Assess			
- Monitor and assess *cyber risks and threats landscape*	●[190]	●[191]	

[182] For instance, the U.S. Federal Energy Regulatory Commission adopted critical infrastructure protection standards. *See* Peter Behr, *A Decade After the Northeast Blackout, Reliability Increases but Human Issues Persist*, E&E (Aug. 12, 2013), http://www.eenews.net/stories/1059985876/print. While the 2014 NIST Framework does not establish additional regulatory requirements, utilities and operator of critical infrastructure may find it hard to avoid implementation. *See* Stephen M. Spina & J. Daniel Skees, *Electric Utilities and the Cybersecurity Executive Order: Anticipating the Next Year*, *in* 26 ELECTRICITY J. 61, 61 (2013).

[183] The 2015 IT Security Act addressed IT security requirements for CI. *See* IT-SICHERHEITSGESETZ, *supra* note 172.

[184] It is generally understood that China's government holds more direct control over CI than its Western counterparts. In the telecom sector, for instance, the major operators are state-owned; in addition, there are limitations on foreign investments, and thus foreign ownership and control are limited. *See* Yukyung Yeo, *Between Owner and Regulator: Governing the Business of China's Telecommunications Service Industry*, CHINA Q. 200, 200 (2009), http://dx.doi.org/10.1017/S0305741009990609. On July 1, 2015 China adopted a new National Security Law that reinforced Chinese authorities' control to maintain security in all fields, including cyber; it mandates national security reviews for foreign investments in Internet technologies and ICT. *See, e.g.*, Edward Wong, *China Approves Sweeping Security Law*, *Bolstering Communist Rule*, N.Y. TIMES (July 1, 2015), http://www.nytimes.com/2015/07/02/world/asia/china-approves-sweeping-security-law-bolstering-communist-rule.html; Timothy P. Stratford et al, *China's New National Security Law*, NAT'L L. REV. BLOG (July 7, 2015), http://www.natlawreview.com/article/china-s-new-national-security-law.

[185] In 2012, the U.S. House Intelligence Committee warned U.S. telecom operators not to buy network equipment from Chinese equipment manufacturers ZTE and Huawei. Since 2013, certain U.S. federal departments and agencies require governmental approval before sourcing information technology from Chinese companies. *See, e.g.*, Megha Rajagopalan, *China "Resolutely Opposes" U.S. Curbs on IT Imports: State Media*, REUTERS (Mar. 3, 2013), http://www.reuters.com/article/2013/03/30/us-china-us-trade-idUSBRE92T01J20130330.

[186] *See*, *e.g.*, NATHANIEL AHRENS, NATIONAL SECURITY AND CHINA'S INFORMATION SECURITY STANDARDS: OF SHOES, BUTTONS, AND ROUTERS (2012), http://csis.org/publication/national-security-and-chinas-information-security-standards.

[187] The authors are not aware of any systematic study that addresses the compliance and degree of enforcement with domestic cyber regulations and policies. However, the U.S. has implemented various legislation and regulation that target cybersecurity and cybercrime. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 493.

[188] The authors are not aware of any systematic study that addresses the compliance and degree of enforcement with domestic cyber regulations and policies. Germany has implemented various legislation and regulation that target cybersecurity and cybercrime. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 206.

[189] The authors are not aware of any systematic study that addresses the compliance and degree of enforcement with domestic cyber regulations and policies. China has implemented various legislation and regulation that target cybersecurity and cybercrime. *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157, at 134.

[190] The US-CERT provides threat information through its National Cyber Awareness System. *See* US-CERT, *National Cyber Awareness System*, https://www.us-cert.gov/ncas (last visited Aug. 18, 2015). The U.S. intelligence community addresses cyber threats in its annual Worldwide Threat Assessment. *See*, *e.g.*, James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community* (Feb. 26, 2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

- Monitor and evaluate *technological developments*	●[192]		
- Monitor and assess state's overall cybersecurity efforts across all domains; adjust and enforce where necessary	●[193]		

Table 1 includes areas of domestic responsibilities that we have analyzed in the U.S., Germany, and China case studies. The objective of this Article, however, is not to provide a comprehensive comparative reckoning, but rather to provide illustrative examples of various domestic responsibilities and approaches to meeting them in the due diligence context. The proposed list of domestic responsibilities requires testing and revision to determine its utility in meeting international law obligations. Given the variety of institutional and jurisdictional settings across states, it is likely that various combinations of domestic responsibilities and their different implementations may satisfy a cyber due diligence obligation under international law.[194] Yet aside from national case studies, there are also valuable lessons from the private sector that could inform the eventual shape of a cybersecurity due diligence norm, which we turn to next.

B. Lessons from the Private Sector

Among the criticisms of the NIST Framework is that, although it does a good job at promoting general "cyber hygiene" for those organizations that implement it, it is less well suited to protecting firms from sophisticated and targeted cyber attacks sometimes called Advanced Persistent Threats ("APTs"). Indeed, there is a cybersecurity due diligence industry emerging in which the NIST Framework, and for that matter the German BSI Standards, play a role but are only one aspect of a larger decision-making

---

[191] The BSI issues an annual report on the state of cybersecurity that addresses cyber risks and threats. *See, e.g.*, DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2014, BSI (Dec.15, 2014), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.html. The 2015 IT Security Act requires CI operators to provide regular proof of compliance regarding IT security requirements in form of audits, evaluation, or certification. *See* IT-SICHERHEITSGESETZ, *supra* note 172.

[192] Various U.S. federal entities, including the National Institute of Standards and Technology and the White House Office of Science and Technology Policy, assess technological development with resources dedicated on cyber.

[193] While authorities and responsibilities with regard to cyber are allocated across numerous U.S. federal agencies, the U.S. Cybersecurity Coordinator at the White House occupies a central function in coordinating U.S. cybersecurity policies and activities. *See* Michael Daniel, https://www.whitehouse.gov/blog/author/michael-daniel (last visited Aug. 18, 2015).

[194] *See* ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES, *supra* note 157 (including some level of detail on legal, organizational, and technical measures, as well as capacity building and cooperation from ITU nations that can be construed as emerging norms relevant to cyber due diligence).

process that companies contemplating all sorts of business decisions from mergers and acquisitions to supply chain management must consider.[195] This section investigates some hallmarks of this trend primarily in the U.S. mergers and acquisitions context but with other related asides.

U.S. law helps to inform a host of legal questions faced by the private sector as part of an overarching cybersecurity due diligence process,[196] though legal requirements do vary in large part by industry sector.[197] It is critical for companies, for example, to have detailed cybersecurity strategies in place on what employee and customer data has been retained and used, and how that data is secured. If unsatisfactorily undertaken, potential resulting causes of action include negligence, breach of contract, breach of fiduciary duty, and invasion of privacy, to name a few.[198] This can lead to the ousting of managers up to and including the C-Suite as seen in the aftermath of the Target and Sony cyber attacks, but still many organizations have not taken the necessary steps to internalize cybersecurity due diligence. For example, roughly two thirds of surveyed companies use encryption for data in transit,[199] but only about half use intrusion prevention systems and encryption for data in storage, and still fewer, approximately one-third, use public-key encryption, specialized wireless security systems, or content-monitoring systems to prevent data loss.[200] Even more dramatic, just thirteen percent of respondents to a 2012 PwC survey made the survey's "leader cut," a label used to identify respondents that measured and reviewed their cybersecurity policies annually,

---

[195] *See, e.g.*, GREGORY J. TOUHILL & JOSEPH TOUHILL, CYBERSECURITY FOR EXECUTIVES: A PRACTICAL GUIDE 123 (2014).
[196] *See* Jamie Barnett et al., *Cybersecurity Issues in Dealmaking: What You Need to Know*, ACG (2014), http://www.acg.org/UserFiles/file/Cybersecurity%20Webinar%20-Final.pdf.
[197] *What is Critical Infrastructure*, DHS, http://www.dhs.gov/what-critical-infrastructure (last visited Jan. 16, 2014); *see What is the ICS-CERT Mission?*, http://ics-cert.us-cert.gov/Frequently-Asked-Questions (last visited Jan. 17, 2014) (The U.S. Cyber Emergency Response Team, which is part of DHS, identifies sixteen critical infrastructure sectors consistent with Homeland Security Presidential Directive 7, including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems).
[198] *See, e.g.*, Barnett et al., *supra* note 196.
[199] Robert Richardson, *CSI Computer Crime & Security Survey*, CSI at 19 (2008), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf; VERIZON, DATA BREACH INVESTIGATIONS REPORT 63 (2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.
[200] *See id*.

had "an overall information security strategy in place[,]" analyzed the types of cyber attacks hitting their networks, and had a CISO or equivalent reporting to "the top of the house[.]"[201] Those organizations that made the cut reported half as many incidents as those that did not.[202] Yet some progress is being made; by 2014 PwC found that while sixty-nine percent of surveyed U.S. executives were "worried that cyber threats will impact growth[,]" overall awareness as to the importance of cybersecurity is increasing as may be seen by the rise in cyber information sharing.[203] One arena with application to due diligence showing increasing promise is mergers and acquisitions.[204]

Jason Weinstein, former deputy assistant attorney general at the U.S. Department of Justice, summarized the issue of cybersecurity due diligence succinctly when he said: "When you buy a company, you're buying their data, and you could be buying their data-security problems."[205] In other words, "[c]yber risk should be considered right along with financial and legal due diligence considerations."[206] Already a majority of respondents in one 2014 survey reported that cybersecurity challenges are altering the M&A landscape, while eighty-two percent said that cyber risk would become more predominant over the following eighteen months.[207] A majority of surveyed firms also said that a cyber attack during the M&A negotiation process could scuttle the deal, which is a concern given the range of serious cyber attacks coming to light on a regular basis in an era of increasing mergers.[208] Managers now considering what form cybersecurity due diligence should take have a wealth of resources (as well as a growing array of compliance obligations) to consider.[209] These include, in the U.S. context, the NIST

---

[201] *See Eye of the Storm: Key Findings from the 2012 Global State of Information Security Survey*, PwC at 33 (2012), http://www.pwc.co.nz/global-state-of-information-survey.aspx.
[202] *Id.*
[203] *See US Cybercrime: Rising Risks, Reduced Readiness: Key Findings from the 2014 US State of Cybercrime Survey*, PwC at 6 (2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.
[204] *See* TOUHILL & TOUHILL, *supra* note 195, at 209 ("due diligence refers to your activities to identify and understand the risks facing your organization.").
[205] Ensign, *supra* note 6.
[206] Erin Ayres, *Cybersecurity Easing its way into M&A Due Diligence*, Cyber Risk Network (Aug. 22, 2014), http://www.cyberrisknetwork.com/2014/08/22/cybersecurity-easing-way-ma-process/.
[207] *Id*.
[208] *Id*.
[209] *See* Stone v. Ritter*,* 911 A.2d 362, 370 (Del. 2006) ("To establish a failure of oversight, a shareholder must plead and prove that: (a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee

Framework, as well as guidance from the Securities and Exchange Commission, National Association of Corporate Directors, and the PCI Security Standards Council.[210] Together, these frameworks, and others, provide the beginnings of a cybersecurity due diligence standard guiding judges as they work through causes of action such as breach of fiduciary duty and negligence resulting from data breaches.[211] The same goes for partnerships with vendors. The Target breach, for example, which wound up exposing some 40 million credit card numbers, was the result of lax security from a HVAC (heating, ventilation, and air conditioning) vendor that for some reason had access to myriad Target systems well beyond HVAC networks.[212]

Despite some progress, there is still a long way to go to enhance private-sector cybersecurity due diligence, including in the M&A context. Freshfields Bruckhaus Deringer, a global law firm, for example, conducted a survey in which they found that "78 per cent of global respondents believe cyber security is not analysed in great depth or specifically quantified as part of the M&A due diligence process, despite 83 per cent saying they believe a deal could be abandoned if previous breaches were identified and 90 per cent saying such breaches could reduce the value of the deal."[213] Similarly, only 39 percent of respondents "say they make cyber security policies . . . a condition precedent that is addressed prior to completion" of a transaction.[214] In other words, despite growing recognition as to the scale and scope of the multifaceted cyber threat facing firms, many remain predominantly reactive.[215] In order to improve the status quo firms must leverage the above cybersecurity best practices among many others ranging

---

its operations thus disabling themselves from being informed of risks or problems requiring their attention.").

[210] *See* Ayres, *supra* note 206.

[211] *Cf.* Willingham v. Global Payment, 2013 WL 440702 at 19 (N.D. Ga. 2013) (unreported) (reflecting an alternative view in which courts are reluctant rely on data security standards as a means of determine whether a duty was owed, let alone whether they should be used to determine a reasonable standards of care).

[212] *See Target Hackers Broke in via HVAC Company*, KREBS ON SEC. (Feb. 5, 2014), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[213] FRESHFIELDS BRUCKHAUS DERINGER, CYBER SECURITY IN M&A 7 (2014), http://www.freshfields.com/uploadedFiles/SiteWide/News_Room/Insight/Campaigns/Cyber_security_in_MandA/01214_BS_MBD_Media_MA%20Cyber%20Security%20Report_WEB_AW.PDF.

[214] *Id*.

[215] *See* MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf (comparing cybersecurity investment rates across countries and concluding that "[i]t appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive.").

from utilizing risk-based data management to minimizing the danger of insider threats through meshing corporate and human resources policies and reviewing the cybersecurity track records of vendors and potential partners.[216] Still, that might not be enough.

The end result of all this is that there is a push among IT professionals to go beyond mere due diligence and move toward the use of real-time analytics and other cybersecurity best practices to monitor vendors' systems.[217] The lesson here is constant vigilance, e.g., letting an initial process of cybersecurity due diligence be the first, and not the last, word in an ongoing proactive and comprehensive cybersecurity policy that promotes cyber hygiene along with the best practices essential for battling APTs.[218] Such a policy should be widely disseminated and regularly vetted as part of an overarching enterprise risk management process, along with having an incident response plan in place that includes private and public information sharing mechanisms.[219]

C. A Polycentric Approach to Promoting Due Diligence and Cyber Peace

These private sector best practices should inform national and indeed international debates playing out in the field of cybersecurity due diligence. Together, such bottom-up experimentation could be considered a polycentric approach to unpacking the field of cybersecurity due diligence. This multi-level, multi-purpose, multi-functional, and multi-sectoral model,[220] championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-

---

[216] *See* FRESHFIELDS, *supra* note 213, at 10.
[217] Steven Norton, *Going Beyond Due Diligence to Monitor Vendor Cybersecurity*, WALL ST. J., (Mar. 21, 2014), http://blogs.wsj.com/cio/2014/03/21/going-beyond-due-diligence-to-monitor-vendor-cybersecurity/.
[218] *See* TOUHILL & TOUHILL, *supra* note 195, at 291 ("You should measure your cybersecurity posture as part of your efforts to practice due care and due diligence, monitor and control your information systems, maintain legal and regulatory compliance, meet contractual obligations, and maintain certifications.").
[219] For more on this topic, see Amanda N. Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, __ AM. BUS. L. J. __ (forthcoming 2015). *See also US Cybercrime*, *supra* note 203, at 7 (noting that the best policy among those studied to help detect and deter cybercriminals was having an incident response team practicing vulnerability management).
[220] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) POL'Y STUD. J. 163, 171–72 (Feb. 2011), *available at* http://php.indiana.edu/~mcginnis/iad_guide.pdf (defining polycentricity as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes.").

organization, networking regulations "at multiple scales,"[221] and examining the extent to which national and private control can in some cases coexist with communal management as may be seen in the success of the Internet Engineering Task Force.[222] It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems"[223] such as cyber attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[224] Such an approach, in other words, recognizes both the common but differentiated responsibilities of public- and private-sector stakeholders as well as the potential for best practices to be identified and spread organically generating positive network effects that could, in time, result in the emergence of a cascade toward a cybersecurity due diligence norm.[225] Such a norm should not only focus on the cyber hygiene referenced in the NIST Framework but should also encourage the uptake of proactive cybersecurity best practices so as to secure our networks along with clarifying the rights and responsibilities of transit states to help foster cyber peace.

As applied to cybersecurity due diligence, the field of polycentric governance has an array of more particularized lessons drawn from Professor Ostrom's work summarized in her Institutional Analysis and Design (IAD) Framework. This is a Framework of governance best practice gleaned from decades of commons field studies and applied, among other contexts, to global commons issues including atmospheric governance. Some of these principles similarly have resonance to the cause of cybersecurity due

---

[221] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.
[222] *See* Shackelford, *supra* note 7.
[223] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.
[224] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").
[225] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

diligence, including the need to undertake effective cost-benefit analysis,[226] conduct supply chain monitoring with an eye toward spotting hardware and software vulnerabilities, and institute governance strategies that permit ample space for innovation while still mandating proven best practices.[227] The latter goal may be furthered by, for example, requiring NIST Framework compliance for all suppliers and potential partners, something that more firms are undertaking. For example, in early 2015 Bank of America will announced "that it is using the Framework and will also require it of its vendors[,]" while "QVC is announcing that it is using the Cybersecurity Framework in its risk management."[228]

Such innovative efforts are critical to furthering the cause of cyber peace, especially when coupled with effective cybersecurity regulation as was discussed in the German case study. The International Telecommunication Union (ITU), a UN agency specializing in information and communication technologies, pioneered some of the early work in the field by defining "cyber peace" in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence . . . ."[229] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term.[230] That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be called negative cyber peace.[231]

---

[226] Cost-benefit analysis in the cybersecurity context is challenging both because of the difficulty in defining all the associated costs of a successful data breach as well as determining an investment strategy to identify and instill technological, budgetary, and organizational best practices. *See, e.g.*, TOUHILL & TOUHILL, *supra* note 195, at 31; Chapter 5 of SHACKELFORD, *supra* note 17.

[227] *See* Ostrom, Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 tbl. 5.3 (Eric Brousseau et al. eds., 2012) (citing ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (1990)).

[228] FACT SHEET: White House Summit on Cybersecurity and Consumer Protection, https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection (last visited June 17, 2015).

[229] Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace.").

[230] To its credit, though, the ITU report recognizes this fact, and that the concept of cyber peace should be broad and malleable given an ever-changing political climate and cyber threat landscape. *Id*. at 78 ("The definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.").

[231] The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, *Non-Violence and Racial Justice*, CHRISTIAN CENTURY 118, 119 (1957) (arguing

Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships, we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[232] Already some of the public- and private-sector efforts highlighted in this paper may be bearing fruit with, by some estimates, the severity of cyber attacks beginning to plateau and "an emerging norm against the use of severe state-based cybertactics" emerging.[233]

CONCLUSION

The field of international cybersecurity due diligence remains a complex, demanding, and difficult arena, but one that requires sustained academic, private, and public engagement if progress is to be made. An array of paths forward beckons. For example, States could exercise due diligence through passive means, promoting resiliency in domestic and partner nation's networks.[234] Warning systems for various

---

"[t]rue peace is not merely the absence of some negative force – tension, confusion or war; it is the presence of some positive force – justice, good will and brotherhood.").

[232] *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 1, 1 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace). Definitions of positive peace vary depending on context, but the overarching issue in the cybersecurity space is the need to address structural problems in all forms, including the root causes of cyber insecurity such as economic and political inequities, legal ambiguities, as well as working to build a culture of peace. *Id*. ("The goal is to build a structure based on reciprocity, equal rights, benefits, and dignity . . . and a culture of peace, confirming and stimulating an equitable economy and an equal polity."); *see also A Declaration on A Culture of Peace*," UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm (offering a discussion of the prerequisites for creating a culture of peace including education, multi-stakeholder collaboration, and the "promotion of the rights of everyone to freedom of expression, opinion and information.").

[233] Brandon Valeriano & Ryan C. Maness, *The Coming Cyberpeace: The Normative Argument Against Cyberwarfare*, FOREIGN AFF. (May 13, 2015), https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace.

[234] Dennis Edwards et al., *Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture*, SYS. OF SYS. ENGINEERING 1, 1 (2007), doi:10.1109/SYSOSE.2007.4304228.

types of cyber attacks facilitated by cyber emergency response teams, active (and two-way) private-sector information sharing and collaboration on identifying and spreading cybersecurity best practices, and a robust cyber hygiene campaign may be considered other essential elements of cybersecurity due diligence. Other best practices include partioning access to code and systems, audits and regular penetration testing, and promoting redundancy and parallel network construction to build further resiliency, as well as harnessing cybersecurity expertise beyond one's own organizational boundaries through bug bounty and vulnerability reward programs.[235] The NIST Framework, and the related standards it references, provides a conceptual toolbox to identify gaps in an organization's cybersecurity readiness that both public and private sector actors should be aware, along with the German BSI Standards and Chinese equivalents. There is plenty of low-hanging fruit. After all, the Australian government hasreportedly been succcessful in preventing 85 percent of cyber attacks through following three common sense techniques: application whitelisting (only permitting pre-approved programs to operate on networks), regularly patching applications and operating systems, and "minimizing the number of people on a network who have 'administrator' privileges."[236]

Over time, as legal harmonization progresses, there will be increasing opportunities to build out cybersecurity norms, including those surrounding the question of due diligence. Already, a number of national governments referenced above, and even some companies such as Microsoft, have released lists of draft norms for stakeholder consideration.[237] Given both the rich cross-pollination of cybersecurity best practices and the cyber threat posed by a huge range of attackers to the public and private sectors, conceptions of cybersecurity due diligence should be gleaned from existing customary international law but built out through a review of industry norms that are in turn informing national policies. Achieving some measure of cyber peace requires the active

---

[235] *See* Robert Westervelt, *Kaspersky: Redundancy, Offline Backup Critical For Cyberdefense*, CRN (Feb. 8, 2013), http://www.crn.com/news/security/240148219/kaspersky-redundancy-offline-backup-critical-for-cyberdefense.htm; Andreas A. Kuehn & Milton Mueller, *Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities*, PROC. OF THE 42ND RES. CONF. ON COMM., INFO., AND INTERNET POL'Y (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418812.

[236] James A. Lewis, *Raising the Bar for Cybersecurity*, CSIS, at 1, 7–8 (Feb. 12, 2013), http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf.

[237] *See* MICROSOFT, INTERNATIONAL CYBERSECURITY NORMS: REDUCING CONFLICT IN AN INTERNET-DEPENDENT WORLD (2014), http://tinyurl.com/ogv9qzq.

involvement of public and private stakeholders. It may be time for more international lawyers to reach out to CISOs, and vice versa.