Chapter 16

Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector

Scott J. Shackelford, JD, Ph.D.*, 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 their respective private sectors and to one another. The International Court of Justice ("ICJ") has not explicitly considered the legality of cyber weapons to this point, 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 University Hoover Institution.
**Post-Graduate Fellow, Center for Applied Cybersecurity Research.
*** Zukerman Cybersecurity Predoctoral Fellow, Center for International Security and Cooperation, Stanford University; PhD Candidate School of Information Studies, Syracuse University.

TABLE OF CONTENTS

16.1 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. Yet 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 (Schmitt, 2013). This is surprising since the vast majority of cyber attacks do not cross the armed attack threshold. Among the most important unanswered questions is what exactly are nations' due diligence obligations to secure their networks and 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" (Corfu Channel Case, 1949, para. 22). 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 have to take to secure their networks, along with clarifying the rights and responsibilities of transit states.

This chapter 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 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 (Ensign, 2014). 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.

This chapter 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 United States, Germany, and China. Finally, we review lessons from the private-sector cybersecurity due diligence context focusing on mergers and acquisitions to better understand where the rubber meets the road and conclude with some implications for managers and policymakers.

16.2 Unpacking Due Diligence Under International Law

International law may be 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 (International Labor Organization, 2013). The primary sources of international law are treaties, general principles of law, and custom, the third of which requires evidence of state practice that nations follow out of a sense of legal obligation (Statute of the International Court of Justice, 1945, art. 38). 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. 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.

16.2.1 An Introduction to Customary International Cybersecurity Law

A vital component of customary international law was articulated by the ICJ case of *Nicaragua v. United States*, which involved a dispute over the United States' involvement with the Contra rebellion in Nicaragua (Nicaragua Case, 1986). In *Nicaragua*, the ICJ held that customary international obligations would arise from the consistent, widespread practice of States to engage 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 by a significant number of states, would give rise to international obligations under customary

international law. The underlying rationale is that this combination reflects a consensus in the international community that the actions taken represent an unspoken international obligation. Depending on the type of norm involved, that state practice needs to be more or less widespread. For new norms, such as regarding cybersecurity, the standard generally is "virtually uniform" state practice (N. Sea Continental Shelf, 1969). That is a high bar, as we discuss further below.

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 therefore the prior existence of the customary international law (Bradley, 2013). To help resolve this dilemma, Professor Frederic Kirgis, in response to *Nicaragua,* argued for what he called a "sliding scale approach" (Kirgis, 1987). 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. This sliding scale approach may prove particularly important in the realm of cyber activities, 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 realm. The temporal dilemma makes pointing to existing rules complicated, so the preferred method is to identify broad principles. The ICJ suggests that these broad principles can be found by looking to treaties, as multilateral treaties evidence a widespread agreement among States, and indeed most courts rely on treaties to identify *opinio juris*, often exclusively so (Gulati, 2013). Yet in the cyber realm, treaties thus far have largely focused on implementing domestic cybercrime laws, and have done little to address cybersecurity standards leaving such decisions to the private sector and standards bodies as embodied in the NIST Framework discussed below. 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 language. Similarly, the Organization of American States has also encouraged member states to join the Budapest Convention and to ratchet up regional cooperation to mitigate cybercrime, whereas a nonbinding UN General Assembly Resolution calls on states to "eliminate safe havens" for cybercriminals (G.A. Res. 55/63, 2001). 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 form the foundation for international obligations.

The search for *opinio juris* is further complicated by the widespread use of State-sponsored cyber-activity, from cyber-espionage to State-sponsored cyber-crime. While the classification of State cyber-activities is a well-known problem, 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 the *Tallinn Manual's* discussion of the international law relating to espionage, which is ostensibly legal as a matter of international law (Schmitt, 2013). 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 (Gruener, 2012). Given the relative lack of multilateral progress, claiming a widespread consensus for an underlying cybersecurity principle would be challenging in this area.

16.2.2 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 these cases all arose prior to the rise of cyber attacks, but some of the principles that underlay them may still have some applicability including *Corfu Channel*, *Trail Smelter*,

and *Nicaragua*.[2] 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" (Ryan & Navarro, 2015). 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 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.

16.2.2.1 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 (Corfu Channel Case, 1949). In this disagreement, 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 State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States" (Corfu Channel Case, 1949, 22).

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

[2] 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; *Gabcikovo-Nagymaros Project* (Hungary v. Slovakia), Judgment, 25 September 1997, ICJ Reports (1997), at 7, para. 53; *Case concerning pulp mills on the river Uruguay* (Argentina v. Uruguay), Judgment, 20 April 2010, para. 193.

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 (Tikk, 2011). While this principle is unlikely to require the warning State to identify vulnerabilities with particularity, it could require that State to warn other States of the existence of the equivalent of 'cyber mines' (such as logic bombs). 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. Nor is how this reasoning jives with the increasing use of cloud-based computing by companies and governments and the related jurisdictional issues raised.

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" (Corfu Channel Case, 1949, 17–18). Some commentators have suggested that this reflects a higher burden of proof for omissions than direct actions (Mar, 2012). 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. 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 is no easy feat (Mudrinich, 2012).

The attribution problem may become less burdensome, however, when attempting to prove the State's knowledge of attackers within its territory, as Corfu's allowance for "more liberal recourse to inferences of fact and circumstantial evidence" when the

evidence is controlled by the opposing State may make proving knowledge easier. 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 (Heinegg, 2013). Some commentators go even further, and assert that States can 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 (Sklerov, 2009). 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 their territory solely due to a lack of direct attribution to the State.

16.2.2.2 Trail Smelter

The ICJ also dealt with the issue of due diligence in the *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, the ICJ 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" (Trail Smelter Case, 1938, 1965). Although directed towards the emission of "fumes," the Trail Smelter case 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 . . ." (Bodle, 2012, 457).

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 activity that results 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 host 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 have been called a form of "information pollution," and distributed denial of service attacks, which can cause targeted websites to crash through too many requests for site access (Ophardt, 2010; Hurwitz, 2009). However, though recognized by the ICJ, this precedent does not enjoy significant State practice since recognizing it widley would likely mean the end of much 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.

16.2.2.3 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" (Nicaragua, 1986, 106–08). 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 nations asserting varying degrees of national sovereignty over their domestic intranets even as others espouse the virtues of a "global networked commons" (Clinton, 2010). Indeed, several dozen nations now routinely filtering traffic, threatening the dawn of a new age of Internet sovereignty (Lewis, 2011a). How multi-stakeholder Internet governance will jive with classic conceptions of State sovereignty is unclear, but the potential for domestic cyber policies to have international ramifications has never been greater; a fact that may entail obligations on the cyber powers in particular, some of which are discussed below.

16.2.2.4 Cybersecurity Due Diligence Obligations of Transit States

Cyber attacks are frequently routed through several transit states before reaching their ultimate targets, both to obfuscate the attack's origin and to stir international tensions as well as because of the distributed nature of the Internet's architecture (Mudrinich, 2012). As with attacks launched from within a State, the obligations of States that merely transmit 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 (Heinegg, 2013). 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 (Heinegg, 2013).

Yet State knowledge must be understood in context, as the individual packets transmitted through the State's network may, taken alone, be innocuous (Heinegg, 2013). 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 at a particular target. Stuxnet, for example, was designed in such a way that it would only be activated on specific hardware and systems (Zetter, 2014).

As for the specific duties that may be required of transit States, these would likely reflect the role that a given nation'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 far 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 (Heinegg, 2013). The transit State may still be under a general obligation to enact and enforce domestic cybercrime legislation, as 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 target nations, due diligence standards may shift (Mcafee, 2013). And regardless, there is a need to clarify the international law of neutrality more broadly to define whether or not victim nations can or should hold neutral nations through which cyber attacks transited accountable for not being diligent in repelling attackers (Schmitt, 2013).

16.2.2.5 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. But this geographical constraint is not reflected in the realm of cybersecurity, wherein actions taken within one's borders can impact anywhere accessible via 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 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.

Yet perhaps this aspect of international 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. 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" (Messerschmidt, 2013, 279).

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 (Rose-Ackerman, 2008). 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 (Schmitt, 2014). For instance, the World Trade Organization ("WTO"), incorporating the General Agreement on Tariffs and Trade ("GATT"), employs a broad exception for "essential security interests," which effectively serves as an un-appealable, self-determined "get out of jail free card" (GATT 1994). 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. This exception for national security is a frequently bemoaned aspect of international law, but nevertheless suggests a fundamental valuation in 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, and the ever-increasing importance of cybersecurity for national security interests may lead such an exception to ultimately swallow 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 some of the missing elements to a cybersecurity due diligence norm.

16.3 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 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 (ICRC, 2014). Similarly, given the extensive public-private cross-pollination of cybersecurity best practices, private-sector efforts aimed at enhancing cybersecurity are similarly informative to consider given the extent to which they are informing national policymaking with the NIST Framework being a case in point. 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.[3] We then move on to discuss 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.

16.3.1 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

[3] 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.

studies were chosen 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. Further research is required to flesh out whether the noted trends are playing out globally.

16.3.1.1 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 misuse" (International Strategy for Cyberspace, 2011, 10). This represents an effort to help crystallize a cybersecurity due diligence norm in international law essential to broader efforts to promote cyber peace (Shackelford, 2014). 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, still "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 (Lewis, 2011b, 58); 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 . . . ." (Finnemore, 2011, 90). What would a cybersecurity due diligence norm look like, then? It is helpful to briefly review U.S. approaches to this topic in order to provide a build out the framework for discussion discussed above.

The United States in many ways pioneered cybersecurity at the national level, beginning with the creation of the first Cyber Emergency Response Team at Carnegie Mellon University in 1988 in response to a growing number of network intrusions. 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 alonem reportedly operates more than 15,000 networks in 4,000 installations spread across some 88 countries (Lord & Sharp, 2011). Yet the majority of U.S. efforts in this space have been focused on securing vulnerable critical infrastructure ("CI"). Although Congress have 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 (Obama, 2009). 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 (White House, 2013). This Framework is important since, even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges (Armerding, 2014), it is arguably spurring the development of a standard of cybersecurity care in the United States that plays into discussions of due diligence. In particular, the NIST Framework harmonizes consensus standards and 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" (Information Security, 2014). Over time, the NIST 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.

16.3.1.2 Germany

Germany's cybersecurity due diligence efforts rely on close collaboration between the public and private sectors, nationally and globally (German Federal Ministry of the Interior, 2011). Long known for its strong national data protection law with fines up to EUR 300,000, Germany is moving now to: (a) mandate strict cybersecurity standards for CI, and (b) assign the responsibility to protect users and secure CI to service providers and operators of CI, respectively (Bundesministerium des Innern, 2008). 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, the Strategy addresses cybersecurity due diligence by recognizing that "incidents in other countries' information infrastructures may also indirectly affect Germany" (German Federal Ministry of the Interior, 2011, 4). It 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 (German Federal Ministry of the Interior, 2011, 4–7).

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" (OWASP Review), but are not legally enforceable save for data protection fines mentioned earlier.

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. 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 größer das Risiko ist, umso höher die Verantwortung") (de Maizière, 2014).[4] Partly in response to this sentiment (and the 2013 NSA revelations), the German government drafted the IT Security Act ("Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)"), which is pending as of this writing. If enacted, the new law would require companies to employ state of the art security standards to secure their websites – or be held liable in the event of a breach. More stringent security requirements and responsibilities would apply for CI operators. 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 would also be 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 (Greis, 2014).

16.3.1.3 China

China applies tight controls over its domestic Internet in order to advance the Communist party's economic, political, and military interests and to secure its rule (Wong, 2014). 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 the sovereign state's control over the domestic Internet and censorship under the disguise of information security (Sceats,

[4] This sentiment may also be considered another manifestation of the sliding scale approach discussed above.

2015).[5] At the same time, there are increasing tensions between the U.S. and China about mutually alleged cyber exploitations. In 2014, the U.S. indicted five hackers of the People's Liberation Army for economic cyber espionage; China protested sharply (Weihua, 2014). The U.S. government has billed China as the "world's most active and persistent perpetrators of economic espionage" (DNI, 2011), 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 can 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 recently garnered 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 into a "cyber power" (Jinping, 2014). 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" (Buckley & Hornby, 2010). 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.

[5] 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.

China's first cybersecurity strategy goes back to 2003. It is referred to as "Document 27: Opinions for Strengthening Information Security Assurance Work and covers – inter alia – CI protection (Segal, 2012). 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, and the build-up of broadband infrastructure, next-generation mobile technology, and e-government services (Gierow, 2014). Observers have criticized the document as an inconsistent "grab bag of vague policy proposals" (Segal, 2012).

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 (Ahrens, 2012). 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 (Gierow, 2014). 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.

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 an independent, Chinese operating systems for desktop computers as well as mobile devices (Xinhunet, 2014). Other recent or pending Chinese legislation portend still more protection, such as requiring technology companies that sell to China's banks to submit their source code for government inspection (Mozur, 2015). 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 growing market (Gierow, 2014).

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 cyber 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 and that includes domestic economic rationales and protectionist measures as opposed to a narrower focus on securing CI. 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 cybersecurity, the standard generally is "virtually uniform" state practice.[6] This threshold has not yet arguably 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, and China's broader economic and national security efforts. 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.

16.3.2 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

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

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

U.S. law includes a host of relevant legal questions faced by the private sector as part of an overarching cybersecurity due diligence process (Barnett, 2014). 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. 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 (PwC, 2012). One arena in which some progress is being made, though, is mergers and acquisitions.

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" (Ensign, 2014). In other words, "Cyber risk should be considered right along with financial and legal due diligence considerations" (Ayres, 2014). 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 (Ayres, 2014). 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 (Ayres, 2014). 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. These include, in the U.S. context, the NIST Framework, as well as guidance from the Securities and Exchange Commission, National Association of Corporate Directors, and the PCI

Security Standards Council (Ayres, 2014). 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.[7] 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.

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 (Norton, 2014). 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. 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.[8]

16.3.3 A Polycentric Approach to Cybersecurity Due Diligence

These private sector best practices should inform national and indeed international debates playing out in the field of cybersecurity due diligence. This multi-level, multi-purpose, multi-functional, and multi-sectoral model (McGinnis, 2011), championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales," and examining the extent to which national and private control can in some cases coexist with communal management (Ostrom, 2008). It also posits that, due to the existence of free riders in a multipolar world, "a single

[7] *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).

[8] 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).

governmental unit" is often incapable of managing "global collective action problems"[9] such as cyber attacks (Ostrom, 2009, 35). 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" (Keohane & Victor, 2009, 9). 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.[10] 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 referenced above so as to secure our networks along with clarifying the rights and responsibilities of transit states.

16.3.3 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. There is an array of paths forward. For example, States could exercise due diligence through passive means, promote resiliency in domestic and partner nation's networks (Edwards, 2013). Warning systems for various 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 (Westervelt, 2013, Kuehn &

[9] Ostrom, *supra* note **Error! Bookmark not defined.**, at 35.
[10] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

Mueller, 2014). 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" (Lewis, 2013).

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 (Microsoft, 2014). 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 involvement of public and private stakeholders. It may be time for more international lawyers to reach out to CISOs, and vice versa.

16.4 Works Cited

Ahrens, Nathaniel. 2012. National Security and China's Information Security Standards: Of Shoes, Buttons, and Routers. Center for Strategic and International Studies, November 8. http://csis.org/publication/national-security-and-chinas-information-security-standards. Accessed 26 March 2015.

Armerding, Taylor. 2014. NIST's Finalized Cybersecurity Framework Receives Mixed Reviews. *CSO,* January 31. http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html. Accessed 26 March 2015.

Ayres, Erin. 2014. Cybersecurity Easing its way into M&A Due Diligence. *Cyber Risk Network,* Aug. 22. http://www.cyberrisknetwork.com/2014/08/22/cybersecurity-easing-way-ma-process/. Accessed 26 March 2015.

Barnett et al. 2014. Cybersecurity Issues in Dealmaking: What You Need to Know. ACG. http://www.acg.org/UserFiles/file/Cybersecurity%20Webinar%20-Final.pdf. Accessed 26 March 2015.

Bodle, Ralph. 2012. Climate Law and Geoengineering. In *Climate Change and the Law, Ius Gentium: Comparative Perspectives on Law and Justice*, eds. Erkki Hollo, Kati Kulovesi, and Michael Mehling, 447-470. Dordrecht: Springer.

Botnet Control Servers Span the Globe. Mcafee. https://blogs.mcafee.com/mcafee-labs/botnet-control-servers-span-the-globe. 23 January 2013.

Bradley, Curtis A. 2013. The Chronological Paradox, State Preferences, and Opinio Juris. Duke Law. http://law.duke.edu/cicl/pdf/opiniojuris/panel_1-bradley-the_chronological_paradox,_state_preferences,_and_opinio_juris.pdf. Accessed 26 March 2015.

Buckley, Chris and Hornby, Lucy. 2010. China Defends Censorship after Google Threat. *Reuters*, January 14. http://www.reuters.com/article/2010/01/14/us-china-usa-google-idUSTRE60C1TR20100114. Accessed 26 March 2015.

Bundesministerium des Innern. 2008. Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf?__blob=publicationFile. Accessed 26 March 2015.

Case Concerning the Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. U.S.), 1986 I.C.J.14, 183 (June 27).

Chinese OS expected to debut in October. Xinhunet, August 24, 2014. http://news.xinhuanet.com/english/china/2014-08/24/c_133580158.htm. Accessed 26 March 2015.

Clinton, Hillary Rodham. 2010. Remarks on Internet Freedom. U.S. Department of State. http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm. Accessed 26 March 2015.

Corfu Channel Case (United Kingdom v. Albania), 1949 I.C.J. 244 (Dec.15).

Definition of International Law. Int'l Labor Org. http://www.actrav.itcilo.org/actrav-english/telearn/global/ilo/law/lablaw.htm. Accessed 25 Mar. 2015.

Del Mar, Katherine. 2012. 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*, 98-123. London: Routledge.

DNI, Office of the National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage: 2009-2011, October 2011.

Edwards, Dennis, Simmons, Sharon, and Wilde, Norman. 2007. Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture. *Systems of Systems Engineering*,1-6. doi:10.1109/SYSOSE.2007.4304228.

Ensign, Rachel Louise. 2014. Cybersecurity Due Diligence Key in M&A Deals. *Wall Street Journal*, April 24. http://blogs.wsj.com/riskandcompliance/2014/04/24/cybersecurity-due-diligence-key-in-ma-deals.

Eye of the Storm: Key Findings from the 2012 Global State of Information Security Survey. PwC. http://www.pwc.co.nz/global-state-of-information-survey.aspx. Accessed 26 March 2015.

Finnemore, Martha. 2011. Cultivating International Cyber Norms. In *America's Cyber Future: Security and Prosperity in the Information Age* eds. Kristin M. Lord and Travis Sharp, 87-102. Washington, D.C.: CNAS.

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).

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.

German Federal Ministry of the Interior. 2011. Cyber-Sicherheitsstrategie für Deutschland. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html. Accessed 26 March 2015.

Gierow, Hauke Johannes. 2014. Cyber Security in China: New Political Leadership Focuses on Boosting National Security. Mercator Institute for China Studies. http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf. Accessed 26 March 2015.

Greis, Friendhelm. 2014. Kabinett beschließt Meldepflicht für Cyberangriffe. *Golem.de*, December 17. http://www.golem.de/news/it-sicherheitsgesetz-regierung-beschliesst-meldepflicht-fuer-cyberangriffe-1412-111234.html. Accessed 26 March 2015.

Gruener, Wolfgang. 2012. Many New PCs in China Come With Malware Preinstalled. *Tom's Hardware*, September 24. http://www.tomshardware.com/news/microsoft-pc-windows-security-china,17758.html. Accessed 26 March 2015.

Gulati, Mitu. 2013. How Do Courts Find International Custom? Duke Law. http://law.duke.edu/cicl/pdf/opiniojuris/panel_6-gulati-how_do_courts_find_international_custom.pdf. Accessed 26 March 2015.

von Heinegg, Wolff Heintschel. 2013. Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies* 89: 123-156.

Henckaerts, Jean-Marie, and Doswald-Beck, Louise. 2005. Assessment of Customary International Law. ICRC. http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin. Accessed 26 March 2015.

Hurwitz, Roger. 2009. The Prospects for Regulating Cyberspace: A Schematic Analysis on the Basis of Elinor Ostrom. MIT. http://web.mit.edu/ecir/pdf/hurwitz-ostrom.pdf. Accessed 26 March 2015.

Keohane, Robert O., and Victor, David G. 2011. The Regime Complex for Climate Change. *Perspectives on Policy*, 9:7-23.

Kirgis, Frederic L. 1987. Custom on a Sliding Scale. *The American Journal of International Law* 81(1): 146-151.

Kuehn, A., Mueller, M. 2014. Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities. *Proceedings of the 42nd Research Conference on Communication, Information, and Internet Policy*. 12-14September, 2014, Arlington, VA. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418812.

Lewis, James A. 2013. Raising the Bar for Cybersecurity. CSIS. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf. Accessed 26 March 2015.

Lewis, James A. 2011a. Why Privacy and Cyber Security Clash. In *America's Cyber Future: Security and Prosperity in the Information Age,* eds. Kristin M. Lord and Travis Sharp, 123-142. Washington, D.C: CNAS.

Lewis, James A. 2011b. Confidence-Building and International Agreement in Cybersecurity. In *Disarmament Forum: Confronting cyberconflict.* 51-59. United Nations Institute for Disarmament Research. http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf. Accessed March 26 2015.

Jinping, Xi: China must evolve from a large internet nation to a powerful internet nation. *Xinhuanet.com*, February 27, 2014. http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm. Accessed 26 March 2015.

Lord, Kristin M. and Sharp, Travis. 2011. Executive Summary. In *America's Cyber Future: Security and Prosperity in the Information Age*. Washington, D.C.: CNAS.

de Maizière, Thomas. 2014. Sichere Informationsinfrastrukturen in einem Cyber-Raum der Chancen und der Freiheit. http://www.bmi.bund.de/SharedDocs/Reden/DE/2014/12/east-west-cyber-summit.html?nn=3314802. Accessed 26 March 2015.

McGinnis, Michael D. 2011. An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework. *Policy Studies Journal* 39(1): 169-183.

McKay et al. 2014. International Cybersecurity Norms: Reducing conflict in an Internet-dependent world. Microsoft. http://tinyurl.com/ogv9qzq. Accessed 26 March 2015.

Messerschmidt, Jan E. 2013. Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm. *Columbia Journal of Transnational Law* 52: 275-323.

Mozur, Paul. 2015. New Rules in China Upset Western Tech Companies. *New York Times*, January 28. http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html. Accessed 26 March 2015.

Mudrinich, Erik M. 2012. Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem. *The Air Force Law Review* 68: 167-206.

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

Norton, Steven. 2014. Going Beyond Due Diligence to Monitor Vendor Cybersecurity. *Wall Street Journal*, March 21. http://blogs.wsj.com/cio/2014/03/21/going-beyond-due-diligence-to-monitor-vendor-cybersecurity/. Accessed 26 March 2015.

Obama, Barack. 2013. Executive Order on Improving Critical Infrastructure Cybersecurity. White House, Office of the Press Secretary. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed 26 March 2015.

Obama, Barack. 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. White House. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Accessed 26 March 2015.

Obama, Barack. 2009. Remarks by the President on Securing Our Nation's Cyber Infrastructure. White House, Office of the Press Secretary. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure. Accessed 26 March 2015.

Ophardt, Jonathan A. 2010. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law and Technology Review* 3: 1-76.

Ostrom, Elinor. 2009. A Polycentric Approach for Coping with Climate Change. The World Bank. http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf. Accessed 26 March 2015.

Ostrom, Elinor. 2008. Polycentric Systems as One Approach for Solving Collective-Action Problems. Indiana University. http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1. Accessed 26 March 2015.

OWASP Review BSI IT-Grundschutz Baustein Webanwendungen. https://www.owasp.org/index.php/OWASP_Review_BSI_IT-Grundschutz_Baustein_Webanwendungen. Accessed 26 March 2015.

Rose-Ackerman, Susan and Billa, Benjamin. 2008. Treaties and National Security. *New York University Journal of International Law and Politics* 40: 437-495.

Ryan, Tim, and Navarro, Leonard. 2015. Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks. Kroll, Jan. 28. http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/.

Sceats, Sonya. 2015. China's Cyber Diplomacy: a Taste of Law to Come? *The Diplomat*, January 14. http://thediplomat.com/2015/01/chinas-cyber-diplomacy-a-taste-of-law-to-come/.

Segal, Adam. 2012. China Moves Forward on Cybersecurity Policy. *Council on Foreign Relations*, July 24. http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/. Accessed 26 March 2015.

Schmitt, Michael N. 2014. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law* 54: 697-732.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Shackelford, Scott J. and Craig, Amanda N. 2014. Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity. *Stanford Journal of International Law* 50: 119-184.

Shackelford, Scott J. 2014. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge: Cambridge University Press.

Sklerov, Matthew J. 2009. Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent. Military Law Review 201: 1-84.

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.
Tikk, Eneken. 2011. Ten Rules of Behavior for Cyber Security. *Survival,* 53(3): 119-132.

Trail Smelter Arbitration (U.S. v. Can.), 3 Rep. Int'l Arb Awards (R.I.A.A.) 1905 (1941).

Verry, John. 2014. Why the NIST Cybersecurity Framework Isn't Really Voluntary. Info. Sec. Blog. http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework. Accessed 26 March 2015.

Weihua, Chen. 2014. China protests against US indictment. *China Daily*, May 20. http://usa.chinadaily.com.cn/world/2014-05/20/content_17519650.htm. Accessed 26 March 2015.

Westervelt, Robert. 2013. Kaspersky: Redundancy, Offline Backup Critical For Cyberdefense. *CRN,* February 8. http://www.crn.com/news/security/240148219/kaspersky-redundancy-offline-backup-critical-for-cyberdefense.htm. Accessed 26 March 2015.

Wong, Edward. 2014. For China, Cybersecurity Is Part of Strategy for Protecting the Communist Party. *New York Times*, December 3. http://sinosphere.blogs.nytimes.com/2014/12/03/for-china-cybersecurity-is-part-of-strategy-for-protecting-the-communist-party/. Accessed 26 March 2015.

Zetter, Kim. 2014. *Countdown to Zero Day*. New York: Random House.