OPERATIONALIZING CYBERSECURITY DUE DILIGENCE: A TRANSATLANTIC COMPARATIVE CASE STUDY

*Scott J. Shackelford JD, PhD**
*Scott Russell, JD***

Abstract

Although much work has been done on applying the law of warfare to cyber attacks, 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 the private sector, as well as how these obligations should be translated into policy. In this Article, we analyze how both the United States and the European Union are operationalizing the concept of cybersecurity due diligence, and then move on to investigate a menu of options presented to the European Parliament in November 2015 by the authors to further refine and apply this concept.

TABLE OF CONTENTS

INTRODUCTION

During the winter of 2015, more than 80,000 people in Western Ukraine lost power.[1] That, in itself, would not be newsworthy but for the fact that the outage was due not to a storm or fuel shortage, but "the first known cyber attack to take down an electric grid."[2] Although efforts to attribute the attack remain underway as of this writing,[3] the episode highlights the difficulty of establishing rules of the road for appropriate behavior in cyberspace, and what obligations nations owe to one another—and to the private sector—to help mitigate cyber risk. Unfortunately, though much work has been done on applying the law of warfare to cyber attacks,[4] less attention has been paid to defining a law of cyber peace applicable below the armed attack threshold.[5] Among the most important unanswered questions "below the threshold" is what exactly nations' due diligence obligations are to the public and private sectors,[6] as well as how these obligations should be translated into policy. In this Article, we analyze how both the United States and the European Union are operationalizing cybersecurity due diligence, and then move on to investigate a menu of options presented to Members of the European Parliament in November 2015 by the authors to further refine and apply this concept.[7]

---

*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, Indiana University.

[1] *See* Jim Finkle, *U.S. Power Companies Told to Review Defenses after Ukraine Cyber Attack*, REUTERS (Jan. 6, 2016), http://www.reuters.com/article/us-usa-utilities-cybersecurity-idUSKBN0UK2MM20160106.

[2] *Id*.

[3] *See id*.

[4] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICATION TO CYBER WARFARE 17 (Michael N. Schmitt ed., 2013).

[5] *See* Chapter 6 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014); 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.

[6] *See, e.g.*, Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VIRG. J. INT'L L. 697, 698 (2014).

[7] This presentation took place at a cybersecurity briefing organized by the German Institute for International and Security Affairs in Brussels, Belgium in November 2015. The Article represents a follow-up study to *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors* in which we explored the international law on cybersecurity due diligence by focusing here on how these conceptions are being translated by policymakers on both sides of the Atlantic. *See* Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence,* __ CHI. J. INT'L L. __ (forthcoming 2016).

"Cybersecurity due diligence," a term unpacked further in Part I, may be understood as the customary obligations of both State and non-State actors to help identify and instill cybersecurity and governance best practices so as to promote cyber peace, such as by enhancing the security of critical infrastructure.[8] As such, the field of cybersecurity due diligence must be understood as part of larger and ongoing conversations about Internet governance, and the search for a steady state of cybersecurity, and end game acceptable to various stakeholders. Although there are various concepts available for such a discussion, the focus in this Article is on how the burgeoning field of cybersecurity due diligence plays into conceptions of "cyber peace." For those unfamiliar with the term, 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 . . . ."[9] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term.[10] Cyber peace is defined here not as the absence of conflict, what may be called negative cyber peace.[11] 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—namely in the field of due diligence—to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. In other words, we are arguing for a *positive* vision of cyber peace that does three things: (1) respects human rights, (2) spreads Internet

[8] *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).

[9] Wegener, *supra* note 5, at 78, 82 (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace.").

[10] 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.").

[11] 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 "[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.").

access along with cybersecurity best practices, and (3) strengthens governance mechanisms by fostering effective multi-stakeholder collaboration.

To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to build robust, secure systems, and couches cybersecurity within the larger debate on Internet governance. There are various analytical tools available to conceptualize such an approach, but the one used here is polycentric governance. This multi-level, multi-purpose, multi-functional, and multi-sectoral model,[12] 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,"[13] and examining the extent to which national and private control can in some cases coexist with communal management. 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"[14] 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."[15] This approach has the promise of moving us beyond common classifications of cybersecurity challenges, recognizing that cyberspace is uniquely dynamic and malleable, and that its "stratified . . . structure [underscores] . . . a particularly complex regulatory environment, meaning that mapping or forecasting" the effects of regulations is problematic.[16] This, as we will see, has important implications in

[12] 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.").

[13] 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.

[14] 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.

[15] 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").

[16] ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 52-53 (2006).

the cybersecurity due diligence context, and is an idea that is enjoying increased traction with the likes of the President of Estonia, Hendrik Ilves, and the President of the Internet Corporation for Assigned Names and Numbers (ICANN), Fadi Chehadé, relying on the term to describe the Internet governance ecosystem.[17] Ultimately we argue that a menu of policy options are available that would enhance cybersecurity due diligence in both the U.S. and EU, but that certain market-orientated options likely will experience the greatest political support and as such could be an appropriate foundation on which to build.

This Article is structured as follows. Part I introduces the concept of cybersecurity due diligence, leveraging both the international law transactional literatures. Parts II and III then examine how it is being operationalized both within the United States and the European Union respectively. Part IV explores the utility of a menu of policy options ranging from publicly funded bug bounty programs and subsidized cyber risk insurance schemes to an EU-wide cyber hygiene campaign that are designed to further the cause of cybersecurity due diligence as part of an overarching campaign to foster cyber peace.

I. INTRODUCING "CYBERSECURITY DUE DILIGENCE"

What is cybersecurity due diligence? International law is not dispositive in this instance in that it does not spell out in detail *how* nations should go about enhancing their cybersecurity to account for emerging due diligence obligations. For example, in *Corfu Channel*, the International Court of Justice (ICJ) held that "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[18] In the cybersecurity context, this decision could be extended to hold 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, though a given cyber attack may be launched from within a State's territorial boundaries, attributing it back to that State's government is no simple matter.[19]

---

[17] *See, e.g.*, Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/10/07/internet-operations-chief-snowden-disclosures-make-my-job-easier/.

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

[19] 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).

Similar translational problems arise in other ICJ cases, including *Trail Smelter* and *Nicaragua*. This is true in the former instance given difficulties of extending what has come to be known as the "no harm" principle, which requires of States "that activities within their jurisdiction or control respect the environment of other States,"[20] to new arenas like cybersecurity.[21] In the latter case, making *Trail Smelter's* interpretation of due diligence jive with other ICJ precedent, like *Nicaragua* with regards to State sovereignty, is also challenging. In deciding *Nicaragua*, the ICJ found that unlawful State intervention in the inner workings of other nations was unlawful if it pertained to "the choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[22] This depiction of State sovereignty stands in juxtaposition to the Court's "no harm" decision in *Trail Smelter*, and in fact is arguably more consistent with those nations like China arguing for "Internet sovereignty" or "cyber sovereignty," the notion that "countries had the right to choose how to develop and regulate their internet."[23] The multilateral versus multi-stakeholder debate over the future of cyberspace (centering around how much power governments have a right to exercise online) will not be settled anytime soon, but 2014 did bring two notable successes for the prevailing multi-stakeholder model in Brazil and South Korea.[24] The future of multi-stakeholder Internet governance in the context of Westphalian conceptions of State sovereignty embodied in Chinese President Xi's proclamation of "cyber sovereignty" over the long run remains unclear, but the potential for domestic cyber policies to have international ramifications has never been greater.[25]

---

[20] 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).

[21] For more on this topic, see Shackelford, Russell, & Kuehn, *supra* note 7.

[22] Case Concerning the Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 106–108 (June 27).

[23] *China Internet: Xi Jinping Calls for 'Cyber Sovereignty*,' BBC (Dec. 16, 2015), http://www.bbc.com/news/world-asia-china-35109453.

[24] For more on this and other developments in the field of Internet governance, see Scott J. Shackelford et al., *Back to the Future of Internet Governance?*, GEO. J. INT'L AFF. 81 (2015). This debate has also played out in the context of "Internet freedom" versus "Internet sovereignty." *See, e.g.*, Scott J. Shackelford, *The Coming Age of Internet Sovereignty?*, HUFF. POST (Jan. 10, 2013), http://www.huffingtonpost.com/scott-j-shackelford/internet-sovereignty_b_2420719.html.

[25] *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).

Given the lack of clarity on the topic of cybersecurity due diligence in the international law literature, it is informative to consider the transactional context, in which this term has been defined as "the review of the governance, processes and controls that are used to secure information assets."[26] Or more simply, some have argued that "due diligence refers to your activities to identify and understand the risks facing your organization."[27] Such due diligence obligations may exist between States, between non-State actors (e.g., private corporations), and between State and non-State actors. However, under international law the emphasis is on State responsibilities particularly to safeguard vulnerable critical infrastructures from misuse, overuse, and attack. For example, the Obama Administration has defined cybersecurity due diligence as the requirement that States, "should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse."[28] The term is used here, as was stated in the Introduction, consistent with this latter interpretation, though the difficulty comes in operationalizing such necessarily vague obligations. That is why it is vital to review State practice, especially given regulatory movement in the U.S. with regards to cyber threat information sharing,[29] as well as in the EU with the recently agreed upon Network and Information Security (NIS) Directive and still pending as of this writing General Data Privacy Directive.[30]

II. OPERATIONALIZING CYBERSECURITY DUE DILIGENCE IN THE UNITED STATES

As Part I demonstrated, international law, while informative, does not spell out how nations (or companies under their jurisdiction) should go about enhancing their

---

[26] 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/.

[27] GREGORY J. TOUHILL & JOSEPH TOUHILL, CYBERSECURITY FOR EXECUTIVES: A PRACTICAL GUIDE 209 (2014).

[28] 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).

[29] *See, e.g.*, Paul Rosenzweig, *The Cybersecurity Act of 2015*, LAWFARE (Dec. 16, 2015), https://www.lawfareblog.com/cybersecurity-act-2015.

[30] *See, e.g.*, *The Network and Information Security Directive – Who is In and Who is Out?*, REGISTER (Jan. 7, 2016), http://www.theregister.co.uk/2016/01/07/the_network_and_information_security_directive_who_is_in_and_who_is_out/.

cybersecurity to account for emerging due diligence obligations. There is currently no consensus from the ICJ or elsewhere, for example, on when neutral transit countries must police their networks such as by detecting or blocking cyber attacks. As such, it is important to consider how leading cyber powers—such as the U.S. and the EU—consider the topic.

The Obama Administration has been a champion of cybersecurity due diligence, having first publicly referenced the topic in its 2011 International Strategy for Cyberspace.[31] In this document, the Administration makes the case that it is vital to crystallize a cybersecurity due diligence norm in international law, which they argue is "essential" as part of broader norm-building effort to enhance international critical infrastructure cybersecurity.[32] This notion of cybersecurity norm building is popular across myriad sectors as diverse as NATO and Microsoft.[33] The argument goes that, due to the practical and political difficulties surrounding multilateral treaty development in the cybersecurity arena, norms can help move the ball forward (though whether or not such reasoning stands in a post-Paris Accord world is an open question).[34] 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.[35] As a result, to be successful in such a difficult climate, norms must be "clear, useful, and do-able . . . ."[36] The question then becomes how to make cybersecurity due diligence clear and do-able. The U.S. has had some

[31] INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD, WHITE HOUSE 10 (2011).

[32] *Id*.

[33] *See* MICROSOFT, INTERNATIONAL CYBERSECURITY NORMS: REDUCING CONFLICT IN AN INTERNET-DEPENDENT WORLD (2014), http://tinyurl.com/ogv9qzq; Eneken Tikk*, Ten Rules of Behavior for Cyber Security*, SURVIVAL*,* June 2011*,* at 119.

[34] For more on applying lessons from the climate change movement to enhancing cybersecurity, see Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, __ VAND. J. ENT. & TECH. L. __ (forthcoming 2016); Scott J. Shackelford & Timothy L. Fort, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 UNIV. ILL. L. REV. __ (forthcoming 2016).

[35] James A. Lewis, *Confidence-Building and International Agreement in Cybersecurity*, DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 58 (2011).

[36] Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

success in applying international law to cybersecurity,[37], but translating due diligence obligations is no simple feat. 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 strategized about national cybersecurity arguably since the creation of the world's first Cyber Emergency Response Team at Carnegie Mellon University in 1988, which was in response to the Morris Worm—arguably the world's first documented cyber attack.[38] Today, though, the field is crowded with an alphabet soup of agencies and organizations responsible for various aspects of national cybersecurity. The U.S. Department of Defense alone reportedly operates more than 15,000 networks in 4,000 installations spread across some 88 nations.[39] 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 with a slew of sector-specific CI legislation,[40] successive administrations—including those of Presidents Clinton, Bush, and Obama—have also focused on securing vulnerable CI, a topic that was brought into sharp relief given revelations regarding the late 2015 cyber attacks on Ukrainian CI causing mass blackouts mentioned in the Introduction.[41]

President Obama unequivocally stated that U.S. CI was a "strategic national asset" in 2009, though a fully integrated U.S. cybersecurity policy for protecting it has yet to be

---

[37] *See* Elaine Korzak, *International Law and the UN GGE Report on Information Security*, JUST SEC. (Dec. 2, 2015), https://www.justsecurity.org/28062/international-law-gge-report-information-security/; 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.").

[38] *See* Scott J. Shackelford, *Another 'Back to the Future' Moment - 27 Years After the World's First Cyber Attack*, HUFFINGTON POST (Oct. 30, 2015), http://www.huffingtonpost.com/scott-j-shackelford/another-back-to-the-future-moment_b_8428352.html.

[39] 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).

[40] *See* John A. Fisher, *Secure My Data or Pay the Price: Consumer Remdedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 225-26 (2013).

[41] *See* Alex Hern, *Ukrainian Blackout Caused by Hackers that Attacked Media Company, Researchers Say*, GUARDIAN (Jan. 7, 2015), http://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company; *see infra* note 1 and accompanying text.

developed.[42] The process took a step forward, though, when after eight years of debate, Congress passed the Cybersecurity Act of 2015.[43] This Act does not reference "due diligence" per se, but it does impact the concept, in particular by offering a liability shield in exchange for private-public cyber threat information sharing with the U.S. Department of Homeland Security done "conducted in accordance" with the bill's provisions,[44] and by requiring the reporting of cyber attacks on CI.[45] President Obama has also 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.[46] This Framework is important since, even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges,[47] it is arguably spurring the development of a standard of cybersecurity care in the United States that plays into discussions of due diligence.[48] 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 CI in assessing and managing cyber risk.[49]

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

---

[42] *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.").

[43] *Cf.* Rosenzweig, *supra* note 29; Alina Selyukh, *Cybersecurity Legislation Finds A Place In U.S. Budget Bill*, NPR (Dec. 16, 2015), http://www.npr.org/sections/alltechconsidered/2015/12/16/459999069/cybersecurity-legislation-finds-a-place-in-u-s-budget-bill ("After years of debate, cybersecurity legislation may pass this week, tucked inside the trillion-dollar federal spending bill . . . The focus of this legislation, called 'The Cybersecurity Act of 2015,' is to encourage companies to share with the government and each other technical details of hacking threats (for example, IP addresses or malicious code), as close to in real time as possible.").

[44] Cybersecurity Act of 2015, Title I, § 106.

[45] *Id* at § 208.

[46] *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.

[47] 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.

[48] *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).

[49] *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. at 11,741.

'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[50] 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.[51]

III. OPERATIONALIZING CYBERSECURITY DUE DILIGENCE IN THE EUROPEAN UNION

The European Union's approach to operationalizing cybersecurity due diligence is, as with many aspects of the European Union, complicated. Viewed broadly, the EU strategy is two-fold: ensure the protection of EU citizen's personal data, and promote the development of cybersecurity standards for EU organizations. Yet despite employing broad-spectrum data protection laws since the 1990s,[52] and developing cybersecurity standards for CI since the early 2000s,[53] the EU's multipolar governance structure coupled with the difficulty in regulating cyberspace has historically limited significant progress on cybersecurity policymaking. This state of affairs is exacerbated by ongoing negotiations regarding the General Data Protection Regulation (GDPR) and the new Network and Information Security (NIS) Directive, both of which will bring significant changes to the legal environment of both European privacy and cybersecurity standards.[54] Yet despite continuing uncertainty, discussing these developments in the context of the evolution of

[50] *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

[51] 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.

[52] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

[53] Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final (Dec. 12, 2006) [hereinafter 2006 EPCIP COM], http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52006DC0786&from=EN.

[54] *EU Policy Updates for 2016*, NAT'L L. REV., (Jan. 6, 2016), http://www.natlawreview.com/article/eu-policy-update-january-2016.

EU cybersecurity policymaking helps derive a better understanding of comparative approaches to due diligence.

Before delving into the specifics of the EU approach to cybersecurity policymaking, it is important to highlight a recurring conflict in EU governance: the inbuilt power struggle between individual Member States and EU-wide institutions.[55] The EU's composition as a collection of sovereign States makes internal governance complicated,[56] as the desire for Member State autonomy is at odds with EU-wide policy goals, which often require greater uniformity and accountability.[57] These competing principles are realized through "directives" and "regulations," the two primary mechanisms for EU-wide legislation.[58] Directives require Member State implementation and therefore preserve greater autonomy than regulations, which are immediately enforceable across the EU.[59] This distinction may be particularly important in the cyber context, as the difficulty in regulating cyberspace has tended to centralize regulatory power,[60] as can be seen in the development of EU data protection law.

The foundations for EU cybersecurity due diligence are seen in the EU's historic approach to data protection, culminating in the recently introduced GDPR. The EU approach to data protection largely began with the Organization for Economic Cooperation and Development (OECD) guidelines, which articulated seven privacy principles governing national data protection policies among the adhering OECD nations.[61] Although non-binding, these even principles created a groundwork for data protection that has percolated through each subsequent iteration of EU data protection

---

[55] *Power Struggles Delay EU Data Protection Reform*, DW, (May 13, 2013), http://www.dw.com/en/power-struggles-delay-eu-data-protection-reform/a-17631222.

[56] This may be seen in the EU requirement that EU Member States ratify hybrid international treaties along with the EU as an independent entity. *See Procedure for the Adoption of International Agreements*, EUR-LEX http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14532 (last visited Jan. 12, 2015).

[57] *See* DW, *supra* note 55.

[58] See *Regulations, Directives and Other Acts*, EUROPA, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm (last visited Jan. 6, 2016).

[59] *Id.*

[60] The same process has played out in the EU sustainability context. *See* Elisa Morgera, *Introduction to European Environmental Law from an International Environmental Law Perspective* (Nov. 18, 2010), at 1-10, http://ssrn.com/abstract=1711372.

[61] Organization for Economic Co-operation and Development [OECD], *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*, C(80)58/FINAL (Sept. 23, 1980).

law.[62] The Data Protection Directive furthered the OECD guidelines by requiring each Member State to enact domestic legislation comporting with the privacy principles, which would be enforced by a national data protection authority and guaranteed through restrictions on the transfer of personal data to countries without "adequate" privacy protections.[63] Yet while the directive unified the EU approach to data protection, national variations in implementation coupled with the drastic expansion and development of the global Internet made the directive increasingly inadequate as a framework for data protection,[64] culminating in the development of the GDPR to update and unify data protection law for the entire EU.[65]

The GDPR, recently finalized, represents the most recent iteration of EU data protection law.[66] While there are numerous minor differences in implementation, the GDPR differs more substantially in a few notable ways from prior reform efforts. The largest distinguishing factor of the GDPR is that it centralizes data protection authority in the EU into a single regulatory body, as compared with the EU Data Privacy Directive's (DPD) utilization of national data protection authorities for each Member State.[67] This development is designed to unify the EU regulatory landscape while providing more parity in Member State representation, as the DPD tended to permit businesses to forum shop, seeking those Member States (such as historically Ireland) with the most business-friendly data protection authority.[68] Also notable is the apparent shift towards a risk-management model for implementing the privacy principles, as compared with the more

[62] *See, e.g.*, THIRTY YEARS AFTER THE OECD PRIVACY GUIDELINES, OECD 53 (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf.

[63] Data Protection Directive, *supra* note 52.

[64] *See, e.g.*, Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations*, __ SETON HALL JOURNAL OF DIPLOMACY AND INTERNATIONAL RELATIONS __ (forthcoming 2016).

[65] Reform of EU data protection rules, European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited Jan. 6, 2016).

[66] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2015) 15039/15 (Dec. 15, 2015) [hereinafter General Data Protection Regulation].

[67] *Id* at art. 64.

[68] Phil Lee, *Will the New EU General Data Protection Regulation Prevent Forum Shopping?,* FIELDFISHER (May 12, 2015), http://privacylawblog.fieldfisher.com/2015/will-the-new-eu-general-data-protection-regulation-prevent-forum-shopping.

direct regulatory approach seen previously.[69] While this may have been influenced by US policy, which has historically favored a risk-based approach to privacy and security, it may also be a logical progression from the difficulty of strict compliance.[70] Finally, the GDPR extends the jurisdictional reach of EU data protection requirements to data processing that occurs outside the territorial boundaries of the EU when the processor targets individuals within the EU for the offering of goods or services, or when the processor is monitoring EU persons that are located within the territorial bounds of the EU.[71] This broadening of the EU's interpretation of data jurisdiction, while of questionable regulatory value without international cooperation or corresponding territorial sovereignty, may be seen as a proclamation of EU due diligence expectations for foreign nations whose internal activities implicate EU interests online: specifically, the protection of personal data of EU citizens.[72]

With regard to direct cybersecurity regulations, the EU approach has historically resembled that of the U.S. by focusing on protecting CI, with the European Council first requesting a CI cybersecurity strategy in 2004,[73] which led to the development of the European Network and Information Security Agency (ENISA),[74] and was followed by the European Programme for Critical Infrastructure Protection (EPCIP) in 2008.[75] Yet the most substantial step towards a broad-spectrum cybersecurity policy came in 2013 with

---

[69] *Council of the European Union Proposes Risk-Based Approach to Compliance Obligations,* PRIVACY AND INFORMATION SECURITY LAW BLOG (Oct. 29, 2014), https://www.huntonprivacyblog.com/2014/10/29/council-european-union-proposes-risk-based-approach-compliance-obligations/.

[70] Katherine O'Keefe, Daragh O'Brien, *Subject Data Request: A Data Health Check*, Castlebridge Associates, 12, *available at* https://castlebridge.ie/system/files/private/whitepapers/subject_access_requests_-_a_data_health_check.pdf , ("40% of Data Controllers are failing to ensure adequate technological or organisational controls to prevent unauthorised access to or disclosure of personal data.")

[71] General Data Protection Regulation, supra note 66, art. 3.

[72] Omar Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, Future of Privacy Forum, 2 (Jan. 2013), https://fpf.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf.

[73] Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final (Dec. 12, 2006) [hereinafter 2006 EPCIP COM], http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52006DC0786&from=EN.

[74] Regulation No. 460/2004 of the European Parliament and of the Council of (Mar. 10, 2004), establishing the European Network and Information Security Agency, O.J. (L 077) (Mar. 3, 2004) 1, 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

[75] Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final (Dec. 12, 2006) [hereinafter 2006 EPCIP COM], http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52006DC0786&from=EN.

the Cybersecurity Strategy for the European Union.[76] The 2013 Strategy, while informative for elucidating broad policy goals, is most important for its initiation of the NIS Directive process, which would establish binding cybersecurity requirements for each Member State, and is therefore probably the best example of the EU approach to operationalizing due diligence to date.

The 2015 NIS Directive identifies broad cybersecurity requirements that serve as the foundation for cybersecurity policy in each respective EU Member State.[77] The first requirement is to create a standard of cybersecurity for all businesses based upon risk management, with exceptions only for the smallest businesses.[78] This is coupled with a requirement for each EU Member State to enact legislation establishing a national cybersecurity strategy, a national cybersecurity authority, and a national Cyber Emergency Response Team (CERT), if such entities do not exist already.[79] These national authorities are also obliged to participate in a "cooperative network" that includes, among other requirements, information sharing and breach reporting between Member States, as well as participation in coordinated responses to cyber threats.[80] The extent of these obligations, however, is still unclear, as States may see cyber threats as falling in the realm of national security, and therefore outside the scope of this strata of EU governance.[81] Finally, in furtherance of the emphasis on risk management, the 2013 Strategy led to the development of the NIS Platform, which establishes a framework for evaluating cybersecurity due diligence, and which largely incorporates the NIST

[76] Joint Communication to the European Parliament, the Council, the European and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, [2013 Cybersecurity Strategy] JOIN (2013) 1 final (Feb. 7, 2013).

[77] Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union, [NIS Directive] COM (2013) 48 final (July 2, 2013).

[78] *Id* at 9 ("the requirements are proportionate to the risk presented . . . and should not apply to micro enterprises.")

[79] *Id*, arts. 5, 7.

[80] *Id* at 8.

[81] Consolidated Version of the Treaty on European Union art. 4(2), 2010 O.J. C 83/01, ("national security remains the sole responsibility of each member state.")

Framework core elements – identify, protect, detect, respond, recover – as the standard approach for enterprise risk management.[82]

While these policies taken together outline a broad conception of the EU approach to cybersecurity due diligence, several questions remain unanswered. How the EU will balance its embrace of multi-stakeholder risk management with its increasingly centralized regulatory approach to both data privacy and cybersecurity remains to be seen, as do the practical ramifications of the EU's increasingly broad pronouncements of data jurisdiction. Subsequent to the approval of the EU Commission, the text of the NIS Directive now heads for formal approval to the European Parliament and the European Council.[83] After that, individual EU Member States will have twenty-one months to implement the deal.[84] Competing interests in cyberspace will certainly continue to muddy due diligence obligations throughout and after this period of time, particularly for organizations operating in multiple regions, and it is unclear whether national practices alone will be sufficient to develop an unambiguous standard of cybersecurity due diligence.

IV. OFFERING A MENU OF CYBERSECURITY DUE DILIGENCE OPTIONS FOR POLICYMAKERS AND MANAGERS

No nation is an island in cyberspace, however much they may sometimes wish to be.[85] To fulfill their international legal obligations, States arguably needs to be able to exercise control over Information and Communications Technology (ICT) and CI under their jurisdiction. Yet this is a difficult and complex undertaking given the challenges of jurisdiction, attribution, ambiguous norms, and extensive private-sector ownership of CI, among other challenges discussed above.[86] This final Part seeks to apply and build from lessons learned in Parts II and III to present a menu of policy options for the EU (given its

[82] NIS Platform (WG-1) Final Draft 220515, Network and Information Security Risk Management Organizational Structures and Requirements, *available at* https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-and-requirements-v2/at_download/file.

[83] *See* Commission Welcomes Agreement to Make EU Online Environment More Secure, Eur Comm'n Press Release (Dec. 8, 2015), http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

[84] *Id*.

[85] *See China Internet*, *supra* note 23.

[86] *See* Dep't Homeland Sec., Critical Infrastructure Sector Partnerships, http://www.dhs.gov/critical-infrastructure-sector-partnerships (last visited Dec. 17, 2015).

current status in enacting both the NIS Directive and GDPD), and other nations including the U.S. (especially given DHS's ongoing enactment of the Cybersecurity Act of 2015) wishing to enhance their cybersecurity preparedness. This menu is not meant to be a comprehensive rendering; it was first compiled in response to an invitation in November 2015 from the Permanent Representative of the Federal Republic of Germany to the European Union to prepare and present an academic input statement based on the authors' research to a multi-stakeholder gathering of Members of the European Parliament in Brussels, Belgium. Rather, the goal here is to think through mechanisms by which domestic policy could enhance cybersecurity due diligence such as through active private-sector partnerships. Specifically, to further their cybersecurity due diligence mandates, policymakers can consider a menu of options relevant to the NIS Directive, the GDPR, and the Cybersecurity Act of 2015. Five main overarching topics are addressed in turn: (1) tailored cybersecurity frameworks and certifications, (2) integrated reporting, (3) international cyber threat information sharing, (4) proactive cybersecurity policies including cyber risk insurance, and (5) cybersecurity capacity-building measures.

1) Policymakers could encourage the use of tailored frameworks, certifications, and incentives such as prizes to help identify firms with best-in-class cybersecurity, singling out those companies that use the power of their supply chains to enhance the security of vendors and business partners.

First, regarding prizes, policymakers could enact domestic policy regimes including laws, frameworks, and initiatives to incentivize—such as through tax breaks[87]—or even cajole private actors under their jurisdiction to invest in cybersecurity best practices. One example of this approach already being tried is the Obama Administration, which will reportedly offer prizes to firms that have done the best job at instilling and spreading knowledge about the NIST Framework.[88] The European Parliament could undertake a similar voluntary program to reward leading firms—or even Member States—that have done the most to advance the goals of the NIS Directive and the GDPR. Regular

[87] *See, e.g.*, House Republican Cybersecurity Task Force, 112th Cong., Recommendations of the House Republican Cybersecurity Task Force 5, 8, 14 (2011).

[88] *See* Kent Landfield & Malcolm Harkins, *We Tried the NIST Framework and It Works*, MCAFEE (Feb. 11, 2015), https://blogs.mcafee.com/executive-perspectives/tried-nist-framework-works-2/.

summaries or report cards as shown in Table 1 could be issued for EU Member States with rewards available for market leaders and norm entrepreneurs. Similarly, parliaments could either incentivize existing bug bounty programs being run by private firms that provide rewards to hackers who report vulnerabilities,[89] or create public versions of such programs given that such reporting is in the public good.[90]

Second, regarding certifications, policymakers could encourage the private sector to develop the digital equivalent of Leadership in Energy and Environmental Design (LEED standards), which would help identify firms with best-in-class cybersecurity. To those unfamiliar, LEED is a "voluntary, consensus-based, market-driven program that provides third-party verification of green buildings."[91] It provides a flexible framework to rank various projects along multiple dimensions. The NIS Directive (like the NIST Framework) could provide a foundation on which to build a LEED-type cybersecurity certification scheme. The UK's Cyber Essentials and Cyber Essentials Plus certificates could also be used as analogies, with the proviso being that any such approach should be voluntary and tailored to help guard against "checklist" cybersecurity.[92]

Third, policymakers could encourage firms to leverage the power of their supply chains to spread cybersecurity best practices akin to what companies such as IBM are doing with regards to promoting sustainability.[93] More companies are already requiring NIST Framework compliance in their supply chains and from their business partners, for example.[94] Incentives could be offered to have a similar level of uptake for the NIS Directive and other similar schemes across Europe and beyond.

---

[89] *The Bug Bounty List*, BUG CROWD, https://bugcrowd.com/list-of-bug-bounty-programs (last visited Dec. 17, 2015).

[90] *See* Eduard Kovacs, *Invitation-Only Bug Bounty Programs Becoming More Popular: Bugcrowd*, SEC. WK. (July 30, 2015), http://www.securityweek.com/invitation-only-bug-bounty-programs-becoming-more-popular-bugcrowd.

[91] *See LEED*, U.S. GREEN BUILDING COUNCIL, http://new.usgbc.org/leed (last visited Jan. 24, 2013). For more on this topic, see Shackelford & Fort, *supra* note 34.

[92] UK CABINET OFF., THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 27 (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[93] *See* Adriene Hill, *Wet Towels in Hotel Rooms is a Corporate Goal*, MARKETPLACE (Sept. 18, 2013), http://www.marketplace.org/topics/sustainability/wet-towels-hotel-rooms-corporate-goal.

[94] *See FACT SHEET: White House Summit on Cybersecurity and Consumer Protection*, WHITE HOUSE (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection.

2) Policymakers could expand integrated reporting requirements to include information on cybersecurity in their sustainability reports while encouraging firms—particularly critical infrastructure operators—to consider cybersecurity to be part their corporate social responsibility.

Policymakers could incentivize firms to take a wide view of risk management to encompass all of the dimensions of sustainability—economic, environmental, social, and potentially, security. To do this, it may be helpful to leverage the power of integrated reporting to better inform managers and other stakeholders including investors, about the impact of their business operations. Nearly 7,000 organizations have submitted more than 22,000 Global Reporting Initiative (GRI) reports as of December 2015, making the framework the dominant sustainability-reporting standard for international business.[95] Although submitting a report does not compel a given business decision, protagonists argue that the act of compiling and disclosing the information can have an impact on firm decision making.[96] Some thirty-three nations have either required publicly traded firms to submit sustainability reports or have encouraged such disclosure.[97] By April 2014, the European Parliament had passed an integrated reporting statute affecting companies of more than 500 employees.[98] Policymakers could either amend existing integrated reporting statutes or reinterpret them to include a good faith effort for how companies' operations—particularly CI operators—impact EU or U.S. cybersecurity, while being cognizant that no firm, or government for that matter, has total situational awareness. Relatedly, policymakers could suggest that cybersecurity should be treated as a firm's corporate social responsibility given the large number of businesses that depend on the

[95] *See* Sustainability Disclosure Database, GRI, http://database.globalreporting.org/ (last visited Jan. 12, 2015).

[96] Jo Confino, *What's the Purpose of Sustainability Reporting?*, GUARDIAN (May 23, 2013), http://www.theguardian.com/sustainable-business/blog/what-is-purpose-of-sustainability-reporting.

[97] ERNST & YOUNG, VALUE OF SUSTAINABILITY REPORTING 11 (2013), *available at* http://www.ey.com/Publication/vwLUAssets/ACM_BC/$FILE/1304-1061668_ACM_BC_Corporate_Center.pdf.

[98] *See It's the Law: Big EU Companies Must Report on Sustainability*, GREENBIZ (Apr. 17, 2014), http://www.greenbiz.com/blog/2014/04/17/eu-law-big-companies-report-sustainability.

proper functioning of CI networks, which is similar to calls by former U.S. cybersecurity coordinator Howard Schmidt.[99]

3) To help safeguard critical ICT, policymakers could provide incentives to deepen international information sharing while similarly expanding cyber attack reporting requirements.

Within this cybersecurity due diligence theme, public-private, private-private, and private-public information sharing could be incentivized with a particular emphasis on CI firms sharing cyber threat data and best practices with one another across borders and sectors in a manner consistent with existing EU privacy laws. This would represent a deepening of the cooperation network envisioned in the NIS Directive.[100] The U.S. took a step in this direction in December 2015 with the passage of the Cybersecurity Act of 2015 that incentivizes cyber threat information sharing by offering liability protections as was discussed above,[101] but more remains to be done.

Also in the vein of deepening the pool of information to help guide policymakers, cyber attack reporting requirements could be expanded and reinforced. In the U.S., as of June 2014, more than 1,500 companies traded on the NYSE included information regarding cybersecurity in their Securities and Exchange Commission (SEC) filings, which is "up from 1,288 in all of 2013."[102] Building on the NIS Directive,[103] policymakers in other jurisdictions could require such disclosure on that part of CI entities along with incentivizing the use of cybersecurity frameworks and the new ISO standards

---

[99] Howard A. Schmidt, *Price of Inaction Will Be Onerous*, N.Y. TIMES (Oct. 17, 2012), http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-ofinaction-on-cybersecurity-will-be-the-greatest.

[100] *See, e.g.*, *EU Reaches Agreement on Cybersecurity Rules*, JONES DAY (Dec. 7, 2015), http://thewritestuff.jonesday.com/rv/ff00244f33c81ad8c93fc552d943a31ce4517b34?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[101] *See infra* Part I; Jessica Davis, *5 Key Takeaways from Cybersecurity Act of 2015*, HEALTHCARE IT NEWS (Dec. 28, 2015), http://www.healthcareitnews.com/news/5-key-takeaways-cybersecurity-act-2015 ("The Cybersecurity Information Sharing Act protects the liability of private sector entities when sharing and receiving cyber threat information. It also establishes the personal data that needs to be removed before data sharing can occur and how quickly individuals must be notified their information was shared.").

[102] *See* Danny Yadron, *Corporate Boards Race to Shore Up Cybersecurity*, WALL ST. J. (June 29, 2014), http://online.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146.

[103] *See* Eur Comm'n Press Release, *supra* note 83 (noting that the NIS Directive "require[s] operators of essential services in the energy, transport, banking and healthcare sectors, and providers of key digital services like search engines and cloud computing, to take appropriate security measures and report incidents to the national authorities.").

for vulnerability disclosure. Further, incident "significance" could be amended to include not only the number of users, duration, and geographic spread of the incident, but also its *type*.[104]

4) Policymakers could encourage a more proactive cybersecurity stance on the part of CI operators including potentially offering subsidized cyber risk insurance schemes in exchange for in-depth cybersecurity audits as part of an overarching cyber hygiene campaign.

The proactive cybersecurity movement includes technological best practices ranging from real-time analytics to cybersecurity audits promoting built-in resilience. While "hacking back" is often a highly visible point of contention when discussing the role of private sector active defense, it is a small part of a growing field.[105] Many regulators, for example, continue to focus on the "hack back" question rather than on identifying, instilling, and spreading cybersecurity standards of behavior. Policymakers could, for example, encourage the creation of collective proactive cybersecurity forums. One example of this is Operation SMN, during which a group of private firms engaged in "the first ever private sponsored interdiction against a sophisticated state sponsored advanced threat group."[106] Overall, policymakers could encourage 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 advanced threats. CI operators in particular could be required to have a widely disseminated and regularly vetted cybersecurity strategy as part of their overarching enterprise risk management process, along with having an incident response plan in place that includes information sharing. The NIS Directive takes steps to make such ideas a reality for firms operating in Europe.[107] Similarly, the Federal Trade Commission seems to be taking a step in this

[104] *See id*.

[105] For more on the benefits of a more proactive approach to cybersecurity, see Amanda N. Craig, Scott J. Shackelford, & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721 (2015).

[106] NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT 4 (2014), https://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.

[107] *See* Eur Comm'n Press Release, *supra* note 83.

direction as part of its enforcement actions under Section 5(a) dealing with "unfair" trade practices, which could be copied in other jurisdictions.[108]

Related to the proactive cybersecurity movement, some commentators have been arguing that insurance a "key part of the [cybersecurity] solution" for years but it has only relatively recently begun to catch on.[109] Part of the reason for this delay lays in concerns surrounding the accurate assessment of risk, as well as geographical limitations. If managers are not forthcoming, or do not have adequate safeguard in place then the insurance company may decline coverage, as happened to British electrical grid operator in early 2014.[110] Still, despite the limitations, success stories abound—like Brookeland Fresh Water Supply in Texas, from which cybercriminals stole $35,000, but because of its insurance policy, instead of going out of business, it only lost its $500 deductible.[111] Policymakers could consider offering subsidized cyber risk insurance policies in exchange for in-depth cybersecurity audits of applying CI firms, having the dual benefit of mitigating cyber risk to those firms while potentially enhancing the overall level of private-sector cybersecurity due diligence.[112]

To help boost cybersecurity literacy, policymakers could incentivize stakeholders to make anti-malware and anti-spyware tools available to their citizens for free along with certain open source encryption technologies to better safeguard private data. Lists of other best practices and resources could be developed building on the UK's '10 steps to cybersecurity' guide.[113] It is worth noting, though, that in fact the U.S. seems to be going in the opposite direction, paying lip service as to the importance of building cybersecurity awareness while cutting the budget to do so. Sanctions and countermeasures could be used against nations that launch or sponsor cyber attacks, along with export controls being

---

[108] *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk*, FED. TRADE COMM'N (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

[109] Interview with Chris Palmer, Google engineer and former technology director, Electronic Frontiers Foundation, in San Francisco, Cal. (Feb. 25, 2011).

[110] *See* Mark Ward, *Energy Firm Cyber-Defense is 'Too Weak', Insurers Say*, BBC (Feb. 26, 2014), http://www.bbc.com/news/technology-26358042.

[111] *See The Case for Cybersecurity Insurance, Part II*, KREBS ON SEC., http://krebsonsecurity.com/2010/07/the-case-for-cybersecurity-insurance-part-ii/ (last visited Jan. 23, 2014).

[112] For more on this topic, see Scott J. Shackelford & Scott Russell, *Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy*, 24 MINN. J. INT'L L. ONLINE 33 (2015).

[113] U.K. CABINET OFFICE, TEN STEPS TO CYBER SECURITY (2012), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets.

placed on certain dual-use cyber weapons technologies including clarifying the legality of high-grade encryption.[114] Similarly legal assistance treaties could be strengthened and forums created to help prosecute attackers while encouraging State practice to further build out an international cybersecurity due diligence norm.

5) Policymakers could encourage the development of cybersecurity clinics for underserved stakeholders and otherwise help build the cybersecurity capacity such as through norm building measures.

Grants could be offered to universities and research institutions that are willing to create cybersecurity clinics, helping underserved stakeholders—including CI operators, small businesses, schools, and local governments—to enhance their cybersecurity due diligence once overall capability levels rise. Moreover, consistent with the draft NIS Directive, policymakers could setup cybersecurity training and education resources, as well as suggest ways in which new or revised national cybersecurity strategies could focus more on CI protection such as through information sharing and private-sector collaboration.[115] Finally, policymakers could encourage polycentric norm building, such as by States working in small groups to start building trust around the protection of critical international infrastructure like energy and finance.

More generally, as was referenced in the first cybersecurity due diligence stream, a cybersecurity due diligence matrix could be developed, a scorecard by which EU Member Nations' cybersecurity efforts could be readily compared. An example matrix is included below that simplifies these five themes into three more general due diligence categories, proposing a non-comprehensive, working set of domestic "State responsibilities" that contribute to fulfilling a state's international law obligation on cyber due diligence. 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 framework for cybersecurity standards (such as the NIS Directive or NIST Framework) or leave it to private industry associations to establish frameworks and standards for particular business sectors. To describe and

[114] *See* Dep't of St., International Traffic in Arms Regulations, Apr. 1, 1992, Sec 121.1.

[115] For more on this topic, see Scott J. Shackelford & Andraz Kastelic, *A State-Centric Cyber Peace? Analyzing the Current State and Impact of National Cybersecurity Strategies on Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGISLATION & PUB. POL'Y __ (forthcoming 2016).

measure a particular responsibility, we suggest adopting a maturity model, similar to that used in software development.

TABLE 1: STATE'S CYBER DUE DILIGENCE RESPONSIBILITIES[116]

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	●[117]	●[118]	●[119]
- Introduce or adopt *domestic laws and regulation* relevant to cybersecurity and cyber crime	●[120]	●[121]	●[122]
- Establish and maintain capabilities to respond and react to cyber incidents (e.g. computer security incident response team)	●[123]	●[124]	●[125]
- Define and implement *technical standards, measures, and best practices*	●[126]	●[127]	●[128]

[116] This research was first published in Shackelford, Russell, & Kuehn, *supra* note 7.

[117] *See*, *e.g.*, *Comprehensive National Cybersecurity Initiative*, WHITE HOUSE (2008), https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (summary); NIST Framework, *supra* note 46.

[118] *See*, *e.g.*, 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; 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.

[119] *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.

[120] For the U.S., the 2015 *Global Cybersecurity Index* lists nineteen laws and regulations related to cybercrime and cybersecurity. ITU, GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES 493 (2015), https://www.itu.int/pub/D-STR-SECU-2015.

[121] 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 120, at 206.

[122] 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 120, 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.

[123] *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).

[124] *See*, *e.g.*, CERT-Bund, https://www.bsi.bund.de/CERT-Bund_en (last visited Aug. 18, 2015).

[125] *See*, *e.g.*, CNCERT, http://www.cert.org.cn (last visited Aug. 18, 2015); CERT-Bund, *supra* note 124.

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

[127] *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.

(e.g., vulnerability patching) for cybersecurity			
- Define and maintain *organizational processes and mechanisms* for cybersecurity	●[129]	●[130]	
- Provide *training, education, and certification* for individuals and organizations	●[131]	●[132]	●[133]
- Engage in *collaboration on cybersecurity* such as through Budapest Convention (e.g., information sharing, law enforcement, intelligence) with domestic and international actors	●[134]	●[135]	●[136]
Control and Enforce			
- Hold ownership or exercise regulatory *control over critical*	●[137]	●[138]	●[139]

See GESETZ ZUR ERHÖHUNNG DER SICHERHEIT INFORMATIONSTECHNISCHER SYSTEME (IT-SICHERHEITSGESETZ) (July 17, 2015), Bundesgesetzblatt 2015, I(31), Bonn, July 24, 2015.

[128] 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 120.

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

[130] *See*, *e.g.*, BSI, *supra* note 127. 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 127.

[131] 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).

[132] 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 120, at 206.

[133] 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.

[134] 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, Cybersecurity 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).

[135] *See* Allianz für Cybersicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html (last visited June 16, 2015).

[136] 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 120, at 134.

infrastructure			
- Conduct *review and control of information technology deployed in critical infrastructure*	●[140]		●[141]
- Enforce *compliance with regulations and policies*	●[142]	●[143]	●[144]
Monitor and Assess			
- Monitor and assess *cyber risks and threats landscape*	●[145]	●[146]	

[137] 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).

[138] The 2015 IT Security Act addressed IT security requirements for CI. *See* IT-SICHERHEITSGESETZ, *supra* note 127.

[139] 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.

[140] 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.

[141] *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.

[142] 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 120, at 493.

[143] 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 120, at 206.

[144] 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 120, at 134.

[145] 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.

In addition to the elements from Table 1, low-hanging fruit should also not be ignored given that some of the reforms suggested in this Part are politically difficult to implement. The Australian government, for example, has reportedly 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."[147] This stuff isn't rocket science, after all; it's just computer science.

CONCLUSION

In short, an all-of-the-above approach is needed to build out the arena of cybersecurity due diligence. Working together through polycentric partnerships at the national, bilateral, and regional levels, we can mitigate cyber risk by laying the groundwork for a positive cyber peace that includes a robust cybersecurity due diligence norm. How this topic will be operationalized is ultimately in the hands of policymakers, but through some combination of the cybersecurity due diligence themes discussed in Part IV—including tailored frameworks, integrated reporting, information sharing, instilling active defense, cyber risk mitigation best practices, and cybersecurity capacity building—significant progress is possible. Indeed, with the recent passage of the NIS Directive and the GDPR, as well as developments in the U.S. such as the success of the NIST Framework, enactment of the Cybersecurity Act of 2015, and the FTC enforcement actions, the time is ripe for deeper engagement to help leverage the power of the market to operationalize cybersecurity due diligence.

---

[146] 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 127.

[147] 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.