BOTTOMS UP:
A COMPARISON OF "VOLUNTARY" CYBERSECURITY FRAMEWORKS

Scott J. Shackelford, JD, PhD*, Scott Russell, JD**, & Jeffrey Haut***[1]

Abstract

Although there is a spectrum of cybersecurity regulatory frameworks emerging around the world ranging from more state-centric approaches to voluntary initiatives, more and more nations—including the United States—seem to be settling on a bottom-up approach to enhancing private-sector cybersecurity. Emblematic of this movement in the U.S. context is the 2014 National Institute for Standards and Technology (NIST) Cybersecurity Framework. This Framework, which is comprised partly of regularly updated cybersecurity best practices, has already been influential in shaping the field of cybersecurity due diligence not only in the United States, but also in nations ranging from Canada to India. However, there has not yet been a thorough examination of the similarities and differences between these various bottom-up approaches and the extent to which they are promoting the harmonization of cybersecurity best practices. This Article addresses this omission by investigating a subset of national approaches to cybersecurity policymaking highlighting the extent to which they are converging and diverging using the NIST Framework as a baseline for comparison. Such an understanding is vital not only to businesses operating across these jurisdictions, but also to policymakers seeking to leverage the expertise of the private sector in promoting cyber peace.

[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.

***Law student, Maurer School of Law.

Table of Contents

INTRODUCTION

Governments around the world are considering how best to regulate an array of topics in the cybersecurity context. Canada, for example, has long debated how best to limit the proliferation of cyber weapons.[2] The U.S. government has similarly considered diverse schemes designed to safeguard critical infrastructure,[3] settling on a largely voluntary approach through the National Institute of Standards and Technology supplemented by sector-specific regulation and U.S. Cyber Command.[4] Israel has created a National Cyber Bureau to aid in standards setting.[5] However, none of these nations could be said to have gotten the mix regulatory exactly right given the continuing prevalence of cyber attacks across them.[6] Still, learning can and does happen across nations and sectors that could lead to what Professors Jack Goldsmith and Tim Wu call "regulatory spillover effects," which can "be good or bad, depending on which regulatory scheme prevails."[7]

Among the lessons learned in light of the regulatory experimentation happening around the world is a growing preference for a largely bottom-up approach to cybersecurity policymaking. Indeed, although there is a spectrum of cybersecurity regulatory frameworks ranging from more state-centric approaches to voluntary initiatives, more and more nations—including the United States—seem to be settling on a bottom-up approach to enhancing private-sector cybersecurity. Emblematic of this movement in the U.S. context is the 2014 National Institute for Standards and Technology (NIST) Cybersecurity Framework.[8] This Framework

---

[2] *See* Matthew Braga, *Canada Wants to Regulate the Sale of Cyberweapons, But Hasn't Decided How*, MOTHERBOARD (Sept. 8, 2014), http://motherboard.vice.com/read/canada-wants-to-regulate-the-sale-of-cyberweapons-but-hasnt-decided-how.

[3] *See, e.g.*, Paul Rosenzweig, *The Unpersuasiveness of the Case for Cybersecurity Regulation – An Introduction*, LAWFARE (May 17, 2012), https://www.lawfareblog.com/unpersuasiveness-case-cybersecurity-regulation-%E2%80%93-introduction; Michael Daniel, *Assessing Cybersecurity Regulation*, WHITE HOUSE (May 22, 2014), https://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations ("The major outcome is that the Administration's analysis supports our current voluntary approach to address cyber risk.").

[4] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2014), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [hereinafter NIST Framework].

[5] *See, e.g.*, Daniel Benoliel, *Toward a Cyber Security Policy Model: Israel National Cyber Bureau (INCB) Case Study* (Univ. of Haifa Discussion Paper, July 2014), http://weblaw.haifa.ac.il/he/Faculty/BenOliel/Publications/TOWARDS%20A%20CYBER%20SECURITY%20POLICY%20MODEL-ISRAEL%20NATIONAL%20CYBER%20BUREAU%20CASE%20STUDY%20-%20Daniel%20Benoliel.pdf.

[6] *See, e.g.*, Kaspersky Cybermap, https://cybermap.kaspersky.com/ (last visited Sept. 7, 2015).

[7] Jack Goldsmith, *Response to Paul on Cyber-Regulation for Critical Infrastructure*, LAWFARE (May 21, 2012), https://www.lawfareblog.com/response-paul-cyber-regulation-critical-infrastructure.

[8] *See* NIST Framework, *supra* note 4.

comprised partly of regularly updated cybersecurity best practices has already been influential in shaping the field of cybersecurity due diligence not only in the United States, but also in nations ranging from Canada to India.[9] However, there has not yet been a thorough examination of the similarities and differences between these various bottom-up approaches and the extent to which they are promoting the harmonization of cybersecurity best practices. Such harmonization is a necessary first step toward norm development that could, in time, give rise to customary international cybersecurity law on the topic. Surprisingly, though, this is a topic that has received relatively little attention in the literature.[10] This Article addresses this omission by investigating a subset of national and regional approaches to cybersecurity policymaking—including the UK, Italy, European Union, Japan, South Korea, and Australia—highlighting the extent to which they are converging and diverging using the NIST Framework as a baseline for comparison through the use of primary source materials including national policies and stakeholder interviews. Such an understanding is vital not only to businesses operating across these jurisdictions, but also to policymakers seeking to leverage the expertise of the private sector in promoting "cyber peace."[11]

Part I introduces the NIST Framework to provide grounding for the comparative discussion to follow. Part II then summarizes six national and regional approaches to cybersecurity from the UK, Italy, the European Union, Japan, South Korea, and Australia concluding with a summary regulatory matrix comparing them across several indices in an effort to uncover to what extent they are converging or diverging. Finally, Part III analyzes the data amassed in Part II to examine to what extent cybersecurity legal harmonization may be moving

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

[10] *Cf.* Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. REV. 613, 631 (2015) ("These detailed requests loosely incorporate the NIST framework, but they contain additional pointers for proactive boards."); Robert Gyenes, *A Voluntary Cybersecurity Framework Is Unworkable--Government Must Crack the Whip*, 14 PGH. J. TECH. L. & POL'Y 293, 314 (2014) ("The NIST Framework and the overall voluntary structure of the Presidential strategy acquiesce too much to public pressure."); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. L. REV. 287, 288 (2014) (comparing and contrasting the benefits and drawbacks of federal and state-based approaches to enhancing cybersecurity); 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. INT'L L.J. 287, 287 (2015); Scott J. Shackelford, Timothy L. Fort, & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 UNIV. PENN. J. INT'L L. 353, 353 (2015).

[11] For more background on the theory and practice of cyber peace, see SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

forward to such an extent that it could lead to cybersecurity norm development and the crystallization of customary international law thereby promoting the cause of cyber peace.[12]

I. ENHANCING CYBERSECURITY FROM THE BOTTOM-UP: INTRODUCING THE NIST FRAMEWORK

Reasonable people disagree about the utility of so-called bottom-up and top-down approaches to regulating cybersecurity, as may be seen in the debate between Professors Jack Goldsmith and Paul Rosenzweig.[13] Policymakers are similarly split between those taking a more regulatory or market-driven stance on cybersecurity reform.[14] This Part analyzes the benefits and drawbacks of top-down and bottom-up approaches to enhancing cybersecurity focusing on the NIST Framework to provide a foundation for discussion.

A. From CERT to CYBERCOM: A Brief History of U.S. Cybersecurity Policymaking

Cybersecurity reform has long been a point of interest for the United States since the Morris Worm was first reported on November 2, 1988 when a Cornell graduate student targeted MIT's networks.[15] The U.S. approach to cybersecurity regulation has evolved during the following nearly three decades extending from the creation of the world's first Cyber Emergency Response Team in 1988 to U.S. Cyber Command in 2009.[16] Still, a single, comprehensive approach to U.S. cybersecurity law and policy has yet to emerge with a veritable alphabet soup of agencies including the Department of Homeland Security, NSA, and Federal Trade Commission responsible for various aspects of the nation's cyber defense; the Department of Defense alone reportedly operates more than 15,000 networks in 4,000 installations spread

---

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

[13] *See* Goldsmith, *supra* note 7; Rosenzweig, *supra* note 3.

[14] *See, e.g.*, *Congress, not Obama, Should Crack Down on Cybercrime*, L.A. TIMES (Apr. 5, 2015), http://www.latimes.com/opinion/editorials/la-ed-cyber-security-sanctions-20150405-story.html.

[15] HOSSEIN BIDGOLI, HANDBOOK OF BUSINESS DATA COMMUNICATIONS: A MANAGERIAL PERSPECTIVE 318 (2000). *See also* Scott J. Shackelford, *Another 'Back to the Future' Moment - 27 Years After the World's First Cyber Attack*, HUFF POST (Oct. 30, 2015), http://www.huffingtonpost.com/scott-j-shackelford/another-back-to-the-future-moment_b_8428352.html (discussing the Morris Worm).

[16] *See* U.S. Cyber Command, https://www.stratcom.mil/factsheets/2/Cyber_Command/ (last visited Sept. 21, 2015).

across 88 countries.[17] Still, the majority of U.S. efforts in this space have been focused on securing vulnerable critical infrastructure (CI). Although Congress has been active in this regard, successive administrations—including those of Presidents Clinton, Bush, and Obama—have kept reform so focused, including the Obama Administration, which has made CI protection a key piece of its cybersecurity strategy as may be seen in the NIST Framework itself.

B. Enter the NIST Framework

President Obama declared U.S. CI to be a "strategic national asset" in 2009, but little in the way of legislative initiative followed this pronouncement.[18] In the face of ongoing Congressional inaction to safeguard CI, President Obama issued an executive order in 2013 that, among other things, expanded public-private information sharing and established the NIST Framework process comprised partly of private-sector best practices that companies could adopt to better secure CI.[19] This Framework is important since—even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges[20]—it is arguably spurring the development of a standard of cybersecurity care in the United States, which is an important development given how fragmented this process has been to date.[21] In particular, the NIST Framework harmonizes industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk. Although the NIST Framework has

[17] 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).

[18] *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.").

[19] *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.

[20] 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. 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. __ (2015).

[21] *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).

only been public for a relatively short time,[22] 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."[23] 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 UK, Japan, and Korea, as is discussed further in Part II.[24]

Before delving into the NIST Framework itself, though, it is first important to note the process for how the Framework was created. That is, over a series of five multi-stakeholer meetings in which hundreds of representatives from business, civil society, and government from the U.S. and around the world came together to create and revise the NIST Framework, showing a remarkable ability to build consensus across numerous sectors and industries in a complex and dynamic arena.[25] This type of active dialogue is a crucial piece of the NIST Framework's success—as well as that of the more general bottom-up approach to cybersecurity regulation—in the United States, and is one that other nations are seeking to emulate. Before we delve into the experience of other nations, though, it is first crucial to introduce the NIST Framework itself.

In particular, the NIST Framework takes a risk-based approach for organizations to detect, mitigate, and respond to cyber threats; however, it is not a prescriptive document telling companies, for example, how much cyber risk they should tolerate in a given segment of their

---

[22] *See Framework for Improving Critical Infrastructure*, NIST (Apr. 2015), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf ("To allow for adoption, Framework version 2.0 is not planned for the near term.").

[23] *See* INFO. SEC. BLOG, *supra* note 9.

[24] 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.

[25] *See, e.g.*, Cybersecurity Framework Frequently Asked Questions, http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm (last visited Sept. 21, 2015) ("Among other things, the EO directed NIST to work with industry leaders to develop the Framework. The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. That took place via workshops, extensive outreach and consultation, and a public comment process. NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. This collaboration continues as NIST works with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework.").

operations.[26] Rather than reinventing the wheel by developing an entirely new set of cybersecurity standards, the NIST Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," which allows the Framework to "scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements."[27] The NIST Framework does this by providing a "common language" for entities to evaluate their current cybersecurity posture; determine their targeted state, or "tier," for cybersecurity; prioritize opportunities for improvement; assess progress toward their targeted state; and establish sufficient methods of communication among internal and external stakeholders about cybersecurity risk.[28] The substance of the Cybersecurity Framework is composed of three parts: (1) The Framework Core, (2) The Framework Implementation Tiers, and (3) The Framework Profile. Each component is briefly addressed in turn.

The NIST Framework begins by laying out the Framework Core, which "provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes."[29] While neither an exhaustive list nor a checklist, the Framework Core is an organizational map of industry-recognized cybersecurity best practices that are helpful in managing cyber risk and provides unified terminology for organizations to communicate more effectively such as through now emerging Information Sharing and Analysis Organizations (ISAOs) trumpeted by the Obama Administration.[30] The Framework Core is, in turn, broken

---

[26] *See* NIST, *supra* note 22. Risk assessment and management is a complex process that has developed into its own, distinct area of expertise. "Risk," generally, refers to the "effect of uncertainty on objectives." INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 3100: RISK MANAGEMENT –PRINCIPLES AND GUIDELINES (2009). As the International Organization for Standardization's has further described:

> Whenever we try to achieve an objective, there's always the chance that things will not go according to plan. There's always the chance that we will not achieve what we expect to achieve. Every step we take to achieve an objective involves uncertainty. Every step has an element of risk that needs to be managed. In short, risk is the chance that there will be a positive or negative deviation from the objectives we expect to achieve.

Id. The process of identifying, assessing, and responding to risk is referred to as "risk management," and while the Framework itself is not a risk management process, it "uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity." NIST CYBERSECURITY FRAMEWORK, *supra* note 4, at 5.

[27] *Id.* at 4

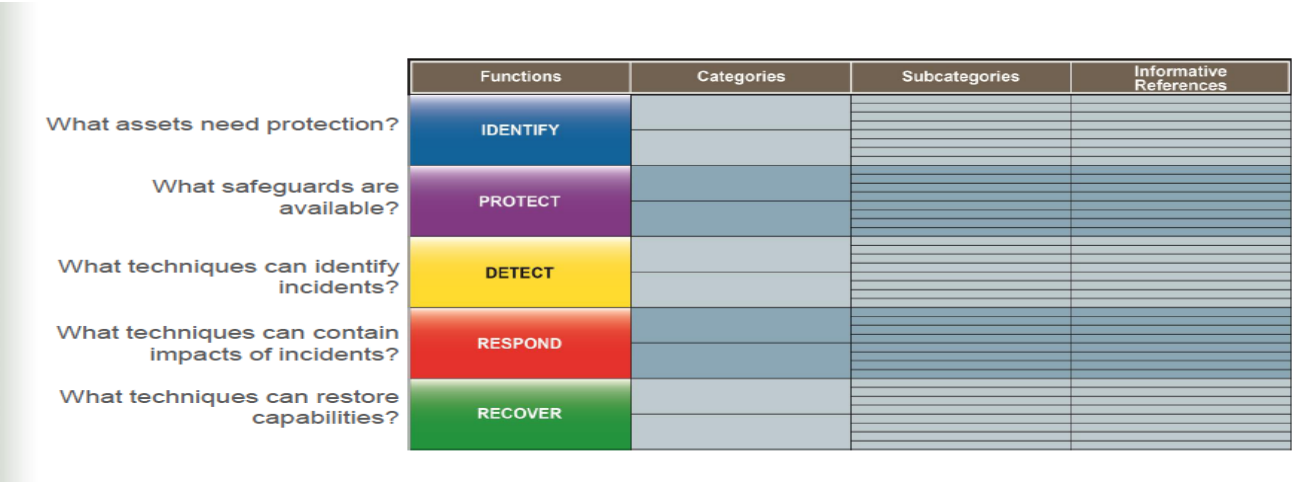
[28] *Id.* at 1.

[29] *Id.* at 7.

[30] *Id. See also Information Sharing and Analysis Organizations*, DEP'T HOMELAND SEC., http://www.dhs.gov/isao (last visited Sept. 21, 2015) ("America's cyber adversaries move with speed and stealth. To

down into four categories—Functions, Categories, Subcategories, and Informative References—that may be used to map an organization's approach to applicable cybersecurity standards, guidelines, and best practices. These Core categories are summarized in Figure 1 along with cells to better understand how these functions are built upon in the NIST Framework through various categories, subcategories, and references.

FIGURE 1: NIST FRAMEWORK CORE[31]



After mapping out cybersecurity activities, the Framework provides a method for an organization to understand the degree to which a firm's Enterprise Risk Management (ERM) practices match the characteristics described within the Framework[32]—this layer is known as the Framework Implementation Tiers. These Tiers provide a vehicle illustrating how organizations manage cyber risk within their overall ERM strategy, taking into consideration an entity's current practices, the multifaceted cyber threat environment, regulatory requirements, business objectives, and organizational constraints, among other considerations.[33] Based upon an organization's evaluation of its practices, the organization can identify to which Tier it belongs. The Implementation Tiers consist of a range of four Tiers (Partial; Risk Informed; Repeatable; and Adaptive) and are progressive, with each tier building on the previous one.[34]

---

keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share and respond to cyber risk in as close to real-time as possible.").

[31] NIST, *supra* note 22, at 10.

[32] NIST CYBERSECURITY FRAMEWORK, *supra* note 4, at 5.

[33] *Id.* at 9. It is important to note that the "Tiers do not represent maturity levels," but that advancing to a higher tier "is encouraged when such a change would reduce cybersecurity risk and be cost effective." *Id.*

[34] *Id.* at 10–11; NIST, *supra* note 22, at 14.

Finally, while the Framework's Implementation Tiers are designed to help gauge an organization's overall cybersecurity risk management practices, the Framework Profiles are meant to align the particular NIST Framework Core Functions and Categories.[35] For example, an organization could create a "Current Profile" that would indicate "the cybersecurity outcomes that are currently being achieved" and a "Target Profile" that would specify "the outcomes needed to achieve the desired cybersecurity risk management goals,"[36] e.g., how to boost their performance to reach a higher tier that may better match their designated cyber risk Profile. Comparing these Profiles would allow an organization to reveal governance "gaps" that should be addressed to meet the organization's cyber risk management objectives.[37] Success in the NIST Framework context is defined on an organization's ability to achieve such Targeted Profiles,[38] which, its proponents argue, will help not only individual firms enhance their cybersecurity preparedness, but through such actions boost the overall economy's cybersecurity resilience. Other nations have seen the value of this approach, while taking into account the drawbacks of the NIST Framework as well. Some, for example, have cautioned that the Framework does not go far enough in terms of its scope, influence, and impact.[39] One of the main questions surrounding the NIST Framework is how "voluntary" it will actually turn out to be—as well as how voluntary it should be.[40] Both the U.S. and other similarly minded jurisdictions are debating such issues contributing to different rates and types of uptake, as is discussed next in Part II.

---

[35] NIST CYBERSECURITY FRAMEWORK, *supra* note 4, at 5.

[36] *Id.* at 11.

[37] *Id.* (stating that that the Target Profiles should be "well aligned with organizational and sector goals, consider[] legal/regulatory requirements and industry best practices, and reflect[] risk management priorities").

[38] *Id.* at 9 ("Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s).").

[39] *See, e.g.*, Tony Romm, *Cybersecurity in Slow Lane One Year After Obama Order*, POLITICO (Feb. 9, 2014), http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html?hp=f1 ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate."); Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

[40] *See e.g., NIST's Voluntary Cybersecurity Framework May Be Regarded as De Facto Mandatory*, HOMELAND SEC. NEWS WIRE (Mar. 4, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution").

II. A COMPARATIVE ANALYSIS OF REGULATORY APPROACHES TO ENHANCING CYBERSECURITY

This Part compares and contrasts a subset of nations pursuing analogies to the NIST Framework in an attempt to ascertain to what extent these approaches are converging leading to the beginnings of a global standard of cybersecurity care. These country case studies were chosen out of the more than twenty nations with which NIST is currently collaborating to represent a spectrum of European and Asian cyber powers including the UK, Italy, the European Union, Japan, South Korea, and Australia. Following these case studies a summary matrix is offered in the form of Table 1 to more easily compare areas of convergence and divergence across these countries again using the NIST Framework as a baseline.[41]

A. United Kingdom

In December 2014, the UK's third-largest broadband service provider, TalkTalk,[42] suffered a data breach that exposed the account numbers, addresses, and phone numbers of many of the company's four million customers.[43] TalkTalk acknowledged the data theft in February 2015, stating that a third-party contractor who had legitimate access to its customer accounts allegedly perpetrated the breach.[44] In October 2015, TalkTalk suffered another "significant" attack on its website, which allowed hackers to "[access] up to 28,000 obscured credit and debit card details, with the middle six digits removed, and 15,000 customer dates of birth."[45] Cyber attacks such as the TalkTalk breach seem to be becoming more common among British companies. The 2015 Information Security Breaches Survey, commissioned by

[41] The authors are aware that other "voluntary" cybersecurity frameworks exist around the world in addition to the NIST Framework. The focus here is on NIST for two reasons. First, it is out of a desire to see how a given voluntary framework from one of the world's leading cyber powers influences the behavior of peer nations. Second, the NIST Framework, although recent, is fast becoming known throughout not only the U.S. economy but in large parts of the world as a leading benchmark, highlighting the desirability to focus on its evolving status and impact. *See, e.g.*, Sean Lyngoos, *NIST Goes Global with Cybersecurity Framework*, FCW (July 3, 2014), https://fcw.com/articles/2014/07/03/nist-global-cyber-framework.aspx.

[42] TalkTalk Telecom Group PLC 2015 Annual Report, http://www.talktalkgroup.com/~/media/Files/T/TalkTalk-Group/2015/Annual%20Report%202015/Annual%20Report%202015%20Final.pdf.

[43] Charles Arthur, *TalkTalk Customers Hit by India-Based Scam Calls Prompting Fears of Data Leak*, GUARDIAN (Dec. 5, 2014), http://www.theguardian.com/business/2014/dec/05/talktalk-customers-india-based-scam-calls-prompting-fears-data-leak/.

[44] Conspirators used the stolen subscriber information to pose as TalkTalk account representatives and to convince customers to transfer small sums of money overseas using one-time use codes in order for the representative to remotely repair "viruses" found on the customers' computers, and then charged the customers large sums of money. *See* Miles Brignall, *Fraud Threat to Millions of TalkTalk Customers*, GUARDIAN (Feb. 27, 2015), http://www.theguardian.com/money/2015/feb/27/threat-to-millions-of-talktalk-customers/.

[45] *TalkTalk Hack: Twenty-Year-Old Man Released on Bail*, BBC (Nov. 1, 2015), http://www.bbc.com/news/uk-34694965 (noting that the alleged perpetrators' demographics underline the nontraditional nature of the cyber threat landscape, as police arrested a 20-year old Staffordshire man, a 16-year-old boy from west London, and a 15-year-old boy from Northern Ireland in connection with the cyber attack).

the UK Department for Business, Innovation and Skills ("BIS"), revealed that ninety percent of large organizations that were surveyed had suffered from a data breach in the previous year.[46] The average cost to a large organization ranged from £1.46 to £3.14 million — more than double the upper range of £1.15 million reported in the same survey in 2014.[47] Such statistics reinforcethe need for greater collaboration and for the spread of proactive cybersecurity best practices in both the public- and private- sectors to better meet the multifaceted cyber threat.

The UK's cybersecurity policymaking efforts have generally focused on developing voluntary standards to enhance CI protection. The 2011 UK Cyber Security Strategy ("2011 Strategy") is the overarching cybersecurity policy promulgated by the British government.[48] The 2011 Strategy focused on tackling cybercrime, increasing overall resilience to cyber attacks, and encouraging the development of industry-led cybersecurity norms.[49] However, the 2011 Strategy did not specifically address cybersecurity awareness-raising for individuals and businesses that were not identified as components of the UK's critical infrastructure.[50] Further, the 2011 Strategy revealed that the UK's national cybersecurity investment allocations from 2011 to 2015 through the National Cyber Security Programme ("NCSP") would primarily be centralized to government entities, such the Home Office, the Ministry of Defence, and the Cabinet Office, with just two percent allocated to the Department for Business, Innovation, and Skills.[51]

As a component of the 2011 Strategy, in June 2014, the GCHQ, BIS, and Cabinet Office created Cyber Essentials, a best practices certification program backed by the British government, which was supported by industry leaders.[52] The Cyber Essentials program's primary purpose is to "incentivize widespread adoption of basic security controls that will help to protect organizations against the commonest kind of internet attack."[53] The Cyber Essentials certification program is mandatory for all UK government contractors handling personal or sensitive information.[54] Yet in an effort to encourage voluntary adoption, the UK government opened up the program to the general public. The Cyber

---

[46] UK DEP'T BUS., INNOVATION & SKILLS, 2015 INFORMATION SECURITY BREACHES SURVEY (June 4, 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.

[47] *Id.* at 6.

[48] 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.

[49] *Id.*

[50] *Id.*

[51] *Id.* at 25.

[52] *Id.* at 7.

[53] *Id.*

[54] Cabinet Office, Policy Paper, "2010 to 2015 Government Policy: Cyber Security" (updated May 8, 2015), https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-7-working-with-industry-on-minimum-standards-and-principles.

Essentials program has two schemes: Cyber Essentials and Cyber Essentials Plus.[55] Cyber Essentials' requirements involve self-certification for basic organizational cyber hygiene practices, such as firewalls, secured configuration, user access control, and patch management.[56] The Cyber Essentials Assurance Framework is intended for supplementation of existing organizational approaches to risk management.[57] Specifically, the Cyber Essentials certification calls on businesses to follow the British government's Ten Steps to Cyber Security.[58]

In December 2014, the UK Cabinet Office released a progress report on the 2011 Strategy, laying out enhanced programs for small to medium enterprises,[59] and a Cyber Security Information Sharing Partnership comprised of more than 750 organizations, to share cyber threat information and best practices among businesses.[60] The report also explained the expansion of cybersecurity guidance in high-risk sectors, such as finance.[61] Perhaps the most important recent development, though, came in January 2015 with the addition of the Advice Sheets ("Advice Sheets") to the 10 Steps to Cyber Security program.[62] The Advice Sheets set out "[the] actions and measures . . . [that represent] a good foundation for effective information risk management . . . to safeguard a company's most valuable assets"[63] while acknowledging that the degree of implementation may be variable, depending upon the cyber risks to a given organization.[64]

Unlike the NIST Framework, the UK's Advice Sheets do not specifically categorize best practices within a core function/category/subcategory paradigm. Rather, the Advice Sheets are broken

---

[55] UK DEPT. BUS., INNOVATION & SKILLS, CYBER ESSENTIALS SCHEME SUMMARY (June 2014), http://www.cyberstreetwise.com/cyberessentials/files/scheme-summary.pdf.

[56] UK DEPT. BUS., INNOVATION & SKILLS, CYBER ESSENTIALS SCHEME REQUIREMENTS (June 2014), http://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf.

[57] UK DEPT. BUS., INNOVATION & SKILLS, CYBER ESSENTIALS SCHEME ASSURANCE FRAMEWORK (Jan. 2015), http://www.cyberstreetwise.com/cyberessentials/files/assurance-framework.pdf.

[58] UK DEPT. BUS., INNOVATION & SKILLS, CYBERSECURITY GUIDANCE FOR BUSINESS (Jan. 16, 2015), https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.

[59] In July 2015, the Cyber Growth Private-Public Partnership, spearheaded by the UK Trade and Investment Defense and Security Organization, and the Cabinet Office's National Cyber Security Program, developed a partnership with over 2,000 companies, which are mostly Small Medium Enterprises. *See* Press Release, UK Trade & Investment Defence & Security Organization, New UK Cyber Demonstration Centre opens today (July 21, 2015), https://www.gov.uk/government/news/new-uk-cyber-demonstration-centre-opens-today. The Cyber Growth Partnership will "support the growth of the sector," and provides "a focal point for cyber security businesses to engage, connect and collaborate and for non-cyber businesses to better understand cyber security and how to protect their business." CGPExchange Landing Page (n.d.), https://cgp.uk.net/#/home (last visited Dec. 3, 2015).

[60] U.K. CABINET OFF., THE UK CYBER SECURITY STRATEGY: REPORT ON PROGRESS AND FORWARD PLANS 4 (Dec. 2014).

[61] *Id.* at 3.

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

[63] *Id*.

[64] *Id.*

down into ten individual sheets.[65] Yet, many of the NIST Framework's categories and subcategories objectives have in fact been adopted by the Advice Sheets. Within the NIST Identify Core Function, the Advice Sheets emphasize the importance of maintaining the key stakeholders' engagement in the risk management process, including discussions about the corporation's risk appetite, and recommend establishing a governance framework that sets out a regularly updated overall information risk management strategy.[66] Within the NIST Protect and Detect Core Functions, the Advice Sheets explain the importance of monitoring user activities and network traffic, aligning incident management polices within the organization, locking down operating systems and software, and conducting regular vulnerability scans and penetration tests.[67] The Advice Sheets also advise the application of "recognized sources of security management good practice," such as ISO/IEC 27000 series of standards for physical, personnel, and technical security.[68] The Advice Sheets advocate for strong user education and awareness practices, including regular training and strong policies and standards for user identification and access controls – particularly limiting user privileges to only such access as is necessary to fulfill business roles, limiting access to audit and system activity logs, and strong account management processes.[69] The Advice Sheets also place a great deal of focus on mobile device protocols such as "BYOD" policies, specifically focusing on protecting data at rest and data in transit.[70] Within the NIST Respond and Recover Core Functions, the Advice Sheets advise alignment of incident management policies, employing a specialist (such as forensic investigation), performing data back-ups, sharing information among with necessary individuals, and conducting a "lessons learned" review to improve future responses.[71]

The 10 Steps: Advice Sheets in January 2015 coincided with a joint announcement by Prime Minister David Cameron and President Barack Obama, proclaiming a shared intention to "work with

---

[65] The ten Advice Sheets are: Information Risk Management Regime, Secure Configuration, Network Security, Managing User Privileges, User Education and Awareness, Incident Management, Malware Prevention, Monitoring, Removable Media Controls, and Home and Mobile Working. *See* UK CABINET OFF., *supra* note 62.

[66] U.K. CABINET OFFICE, 10 STEPS: INFORMATION RISK MANAGEMENT (Jan. 16, 2015), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-information-risk-management-regime--11.

[67] U.K. CABINET OFFICE, 10 STEPS: SECURE CONFIGURATION (Jan. 16, 2015), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-secure-configuration--11.

[68] *See* UK CABINET OFF., *supra* note 62.

[69] UK CABINET OFF., 10 STEPS: MANAGING USER PRIVILEGES (Jan. 16, 2015), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-managing-user-privileges--11; U.K. CABINET OFFICE, 10 STEPS: USER EDUCATION & AWARENESS (Jan. 16, 2015), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-user-education-and-awareness--11.

[70] U.K. CABINET OFFICE, 10 STEPS: HOME & MOBILE WORKING (Jan. 16, 2015), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-home-and-mobile-working--11.

[71] U.K. CABINET OFFICE, 10 STEPS: INCIDENT MANAGEMENT (Jan. 16, 2015), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-incident-management--11.

industry to promote and align [the UK] cybersecurity best practices and standards,"[72] similar to the U.S.-South Korea announcement discussed below.[73] The announcement included an intention to harmonize the NIST Framework and the UK's Cyber Essentials scheme.[74] While the harmonization does not appear to include a dissemination of a separate cybersecurity strategy, the timing of the Advice Sheets' release and the correlations between the advice given within those sheets and the NIST Framework indicate that the Advice Sheets are one of the steps toward the international harmonization of transatlantic cybersecurity best practices.[75]

On May 8, 2015, the UK government released a policy paper – 2010 to 2015 Government Policy: Cyber Security – as an update to the 2011 Strategy.[76] The Policy Paper discussed building out the Cyber Essential scheme, and strengthening the UK's cooperation with the United States, including "aligning [UK] cyber security best practices and standards, including the [NIST] Cybersecurity Framework and the UK's Cyber Essentials scheme."[77] However, as of this writing, the UK has not released any additional overarching policies to achieve this objective, apart from the correlations in the Advice Sheets.

B. Italy

Like the UK, Italian firms have not been immune from an increasing number of cyber attacks. Italian-based cybersecurity firm Hacking Team, for example, which sells its surveillance tools to law enforcement agencies and national security organizations,[78] fell victim to a cyber attack on July 5, 2015.[79] The attackers hijacked the firm's Twitter account, and provided a link to a Torrent file that contained 400 gigabytes of confidential company documents, employee emails, and financial records.[80] The breach

---

[72] US-UK Cybersecurity Cooperation (White House Press Release, Jan. 16, 2015), https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

[73] *See infra* Part II(E).

[74] US-UK Cybersecurity Cooperation, *supra* note 72.

[75] Furthermore, as of the first quarter of 2015, one third of organizations are using the Cyber Essentials guide, and forty-nine percent of all organizations have achieved a Cyber Essentials badge. UK DEP'T BUS., INNOVATION & SKILLS, *Government Urges Business to Take Action As Cost of Cyber Security Breaches Double* (June 2, 2015), https://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles.

[76] Cabinet Off., *supra* note 54.

[77] *Id*.

[78] Hacking Team reportedly sold its mobile phone spyware Remote Control System, which is capable of tracking a target's location, and taking control of a smartphone's microphone and camera, to nearly 100 governmental agencies in thirty-five countries. *See Attack on Hacking Team Spills Global Cyber-Spying Secrets*, CBC NEWS (July 16, 2015 7:49 PM), http://www.cbc.ca/news/technology/attack-on-hacking-team-spills-global-cyber-spying-secrets-1.3155981.

[79] Alex Hern, *Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim*, GUARDIAN (July 6, 2015, 7:46 AM), http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim/.

[80] Jeremy Kirk, *Hacking Team Spyware Company Allegedly Breached, 400GB of Data Dumped Online*, PC WORLD (July 6, 2015, 6:34 AM), http://www.pcworld.com/article/2944372/italian-surveillance-software-maker-hacking-team-allegedly-breached.html.

exposed significant software vulnerabilities for two major international software developers, Adobe and Microsoft[81]: on July 7, two Adobe Flash Player exploits, one of which was a "zero-day" vulnerability, and one Windows kernel exploit were found in the confidential company data[82]; on July 11, two additional Adobe Flash Player zero-day vulnerabilities were discovered,[83] at least one which was tied to a campaign of cyber attacks against Taiwanese educational, religious, and political websites, and a Hong Kong news site;[84] on July 13, a zero-day vulnerability was found in Internet Explorer,[85] and finally, on July 20, the last zero-day vulnerability gleaned from the data breach – affecting Windows operating systems running a certain program – was found and patched.[86]

[81] At least one member of the cybersecurity industry described the data dump as "akin to the fall of the Soviet Union," comparing the widespread publication of Hacking Team's high-level surveillance tools, cybersecurity research, and hacking "cookbooks" – which could allow even novice hackers to extrapolate the knowledge needed to engage in sophisticated hacking and covert cyber operations against businesses– to the surge in black market weapons and dissemination of knowledge concerning WMD's following the USSR's collapse. *See* Lior Div, *Why the Hacking Team Breach Further Tips the Scales Against Business*, FORBES (Aug. 4, 2015, 12:53 PM), http://www.forbes.com/sites/frontline/2015/08/04/why-the-hacking-team-breach-further-tips-the-scales-against-businesses/.

[82] Moony Li, *Hacking Team Leak Uncovers Another Windows Zero-Day, Fixed in Out-of-Band Patch*, TRENDLABS SECURITY INTELLIGENCE BLOG (July 20, 2015, 6:56 PM), http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-leak-uncovers-another-windows-zero-day-ms-releases-patch/. The Flash Player zero-day exploit was used to launch limited attacks in Korea and Japan a few days before the Hacking Team leak. *See* Weimin Wu, *Hacking Team Flash Zero-Day Tied to Attacks in Korea and Japan . . . on July 1*, TRENDLABS SECURITY INTELLIGENCE BLOG (July 8, 2015, 10:06 AM), http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-tied-to-attacks-in-korea-and-japan-on-july-1/. In a zero-day attack, a hacker creates an exploit before the vendor knows about the vulnerability, so the attack base is broader. Zero-day exploits have been called the "the Holy Grail" of exploits. *See* Gregg Keizer, *Microsoft's Reaction to Flame Shows Seriousness of 'Holy Grail' Hack*, COMPUTERWORLD (June 7, 2012), http://www.computerworld.com/s/article/9227860/Microsoft_s_reaction_to_Flame_shows_seriousness_of_Holy_Grail_hack

[83] See Peter Pi, *Another Zero-Day Vulnerability Arises from Hacking Team Data Leak*, TRENDLABS SEC. INTELLIGENCE BLOG (July 11, 2015, 12:43 AM), http://blog.trendmicro.com/trendlabs-security-intelligence/another-zero-day-vulnerability-arises-from-hacking-team-data-leak/; Peter Pi, *New Zero-Day Vulnerability (CVE-2015-5123) in Adobe Flash Emerges from Hacking Team Leak*, TRENDLABS SECURITY INTELLIGENCE BLOG (July 11, 2015, 10:58 PM), http://blog.trendmicro.com/trendlabs-security-intelligence/new-zero-day-vulnerability-cve-2015-5123-in-adobe-flash-emerges-from-hacking-team-leak/.

[84] Joseph Chen, *Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIvy*, TRENDLAB SEC. INTELLIGENCE BLOG (July 28, 2015, 2:01 PM), http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-attacks-spread-compromised-tv-and-government-sites-in-hong-kong-and-taiwan-lead-to-poisonivy/.

[85] Peter Pi, *"Gifts" From Hacking Team Continue, IE Zero-Day Added to Mix*, TRENDLABS SEC. INTELLIGENCE BLOG (July 14, 2015, 10:00 AM), http://blog.trendmicro.com/trendlabs-security-intelligence/gifts-from-hacking-team-continue-ie-zero-day-added-to-mix/.

[86] Microsoft released an "out-of-band patch" that same day– a software fix that can be downloaded and installed automatically – to address the critical vulnerability, which could allow attackers to take remote control of an affected system. *See* Li, *supra* note 82.

Despite this highly damaging breach, Italy's overall cyber threat landscape is reported to be relatively moderate.[87] In part, this may be due to Italy's comparably limited Internet connectivity and usage. In 2006, only forty percent of Italian households had Internet access, and Italy did not cross the fifty percent threshold until 2009.[88] By 2014, 73 percent of households had internet access compared with 84 percent in the U.S. and 90 percent in the UK.[89] Nevertheless, the most recent Eurostat survey on usage, conducted in 2013, revealed about one-third of Italians still had never used the Internet, and only 54 percent reported using the Internet on a daily basis.[90] Still, some progress is apparent with many Italian businesses having built out their IT infrastructure in recent years – particularly in the use of cloud computing.[91] In some respects, Italian Internet usage and connectivity practices have paralleled Italy's approach to cybersecurity governance – as more Italians connect to the internet, more comprehensive cyber risk management strategies have emerged, but the latter is nonetheless a recent development.

Italy's first generation of cybersecurity initiatives were primarily top-down regulatory measures focused on law enforcement and the prevention on cybercrime rather than creating voluntary standards to achieve greater cyber resilience, have largely been enacted to comply with European Union initiatives. Initial cybersecurity efforts began by legislative decree in 2005 with the Ministry of Communication's establishment of a working group to analyze Critical Information Infrastructure ("CII") and potential vulnerabilities to it posed by information technology.[92] In 2011, Italy enacted its implementation of the European Directive on Critical Infrastructure,[93] which granted authority to the Secretariat for Critical

---

[87] In 2014, Italy fell out of the "Top 20" countries where users face the greatest risk of cyber exploitation. *See* Garnaeva, et. al., *Kaspersky Security Bulletin 2014. Overall Statistics for 2014*, SECURELIST (Dec. 8, 2014, 9:00 AM), https://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/.

[88] EUROSTAT, LEVEL OF INTERNET ACCESS – HOUSEHOLDS, http://ec.europa.eu/eurostat/web/information-society/data/main-tables (Select the "Information Society Statistics" folder, then "Computers and the Internet in households and enterprises," sub-folder, and click the icon containing the alt-text "Tables, Graphs, and Maps interface.") (last accessed on Dec. 1, 2015).

[89] By comparison, the overall 2014 EU household access level was 81%. *See* Eurostat, *supra* note 88; Internet Live Stats, http://www.internetlivestats.com/internet-users-by-country/ (last visited Dec. 8, 2015).

[90] News Release, EUROSTAT, *More Than 60% of Individuals in the EU28 Use the Internet Daily*, No. 199/2013 (Dec. 18, 2013), *available at* http://ec.europa.eu/eurostat/documents/2995521/5168694/4-18122013-BP-EN.PDF/b92e0257-3dba-4eb1-97ce-0b42a736dee0?version=1.0.

[91] In 2014, forty percent of Italian enterprises used cloud computing services (primarily for e-mail services), trailing only Finland's fifty-one percent usage rate. *See* News Release, EUROSTAT, *Cloud Computing Services Used By One Out of Every Five Enterprises in EU28*, No. 189/2014 (Dec. 9, 2014), *available at* http://ec.europa.eu/eurostat/documents/2995521/6208098/4-09122014-AP-EN.pdf/627ddf4f-730a-46ca-856b-32532d8325c5.

[92] Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale [Decree-Law of 27 July 2005, no. 144 on urgent measures to combat international terrorism], *available at* http://www.camera.it/parlam/leggi/05155l.htm.

[93] Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, O.J. (L. 345/75), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

Infrastructure to identify CI and to be developing security measures to better protect it.[94] The Italian government took key steps in 2012 and 2013 with the promulgation of the Italian Digital Agenda, which was in response to the Digital Agenda for Europe.[95] In 2013, comprehensive cyber legislation was passed, which granted the Italian Prime Minister authority to implement cyber defensive measures, and promoted governmental cooperation with the private sector, an effort that has largely involved outreach from the Intelligence and Security Department (DIS) and the Inter Ministerial Committee for the Security of the Republic (CISR).[96]

In December 2013, two comprehensive strategies were released by the Presidency of the Council of Ministers: The National Strategic Framework for Cybersecurity ("National Framework")[97] and the National Plan for Cyberspace Protection and ICT Security ("National Plan").[98] The National Plan focused on strategic development of future measures, such as enhancing coordination and dialogue between national private and public stakeholders, and identifying "international best practices" to include in the National Framework.[99] The National Plan also included broad strategic goals about inter-governmental cooperation with NATO and the EU, and plans for expanding the National CERT.[100] Comparatively, the National Framework espoused a number of specific best practices that are identified in the NIST Core Framework: analyzing, preventing, mitigating, and reacting to cyber threats.[101] The National Framework arranges these practices in the form of a pyramid, with risk analysis, risk management, and risk mitigation forming the base, physical, logical and procedural measures stacked above, and the capstone reflecting user training, awareness, and empowerment.[102] Similar to the NIST Framework, the National Framework identifies the key requirements of organizational cybersecurity policies to include setting up "a risk assessment, mitigation and management plan," raising awareness

---

[94] Decreto Legislativo 11 aprile 2011, n. 61 [Implementation of Directive 2008/114/EC on the identification and designation of European Critical Infrastructure] (Apr. 11, 2011), *available at* http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=5299.

[95] *See* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe [European Digital Agenda], COM (2010) 245 final.

[96] Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale [Directive regarding national cybersecurity], GU no.66 del 19-3-2013, *available at* http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=false.

[97] PRESIDENCY OF THE COUNCIL OF MINISTERS, NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY [National Framework] (Dec. 2013), *available at* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

[98] PRESIDENCY OF THE COUNCIL OF MINISTERS, THE NATIONAL PLAN FOR CYBERSPACE PROTECTION & ICT SECURITY [National Plan] (Dec. 2013), *available at* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf.

[99] *Id.* at 12, 15.

[100] *Id.* at 17, 20.

[101] National Framework, *supra*, note 97, at 20.

[102] *Id.* at 18.

through training and education, and setting up reliable norms and procedures for physical and role-based security protocols.[103] The National Framework also called for identifying best practices and procedures for supply chain risks, and audit mechanisms.[104] In comparison to the NIST Framework, however, the National Framework places a great deal of emphasis on defining the nature of the threat in terms of cyber crime, and specific malevolent actors and actions, such as "hacktivism," "cyber terrorism," "cyber warfare," and the "computer crime market."[105] Furthermore, the National Framework views the adoption of strategies as integral to protecting and strengthening the nation's cybersecurity infrastructure as a whole, rather than being a general framework for an enterprise to enact for its own tailored cybersecurity needs.[106]

Although the National Framework called for enhanced public-private partnerships in Italy's future cybersecurity framework, only a handful of significant developments have occurred since the National Plan and National Framework were released. One instance occurred in June 2014, when the Italian government, in partnership with IT firm Finmeccanica –Selex Es, opened the Cyber Security Center of Excellence.[107] The center contains a supercomputer that detects and helps to defeat cyber attacks, and the company offers cybersecurity services to the Italian Ministry of Defense as well as roughly 70,000 international users.[108] The center employs a number of cyber specialists, and is hoped to have a role in the establishment of a local CERT, and to assist a local university in the future. More recently, following the November 2015 attacks in Paris, Italian Prime Minister Matteo Renzi announced that five-hundred million euros would be earmarked for cyber-security.[109] Although as of this writing, specific details have not been released about how the funds will be expended or prioritized.

C. European Union

The EU as a region faces a dynamic cyber threat landscape emerging from its Member States' concerns including the UK and Italy. Through 2015, the EU saw increases in cyber threats, such as data losses from cyber attacks perpetrated by "social hackers, hacktivists, script kiddies, cyber criminals," and

[103] *Id*.
[104] *Id*. at 25.
[105] *Id*. at 13-16.
[106] *Id*. at 20.
[107] Tom Kington, *Finmeccanica Opens Cyber Defense Center*, DEF. NEWS (June 8, 2014, 1:49 PM), http://archive.defensenews.com/article/20140608/DEFREG01/306080008/Finmeccanica-Opens-Cyber-Defense-Center.
[108] *Id*.
[109] AFP, *Italy to Spend 1 Billion More on Security*, LOCAL IT (Nov. 25, 2105, 8:06 AM), http://www.thelocal.it/20151125/italy-to-boost-security-spending-by-a-billion-euros.

even nation states.[110] Indeed, much like the United States, the EU faces increasing trends of identity theft, spam, and malware propagation against its citizens.[111] Considering the unique composition of the EU – with Member States in many cases having the ultimate responsibility to implement state-specific solutions – the EU has faced unique challenges in promoting the adoption and harmonization of cybersecurity best practices, including in the CI context.

In 2004 when the European Council – a body composed of each EU member's head of state – requested the preparation of a CI protection strategy.[112] That same year, the European Parliament and the Council established the European Network and Information Security Agency (ENISA) to promote "a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organizations in the European Union."[113] ENISA was primarily tasked with tracking information security risks, facilitating cooperation and information-sharing between public and private sector entities, and assisting Member States in their development of industry-specific cybersecurity strategies.[114]

Among the more recent significant updates to the EU's overall cybersecurity stance came with the promulgation of the 2013 EU Cybersecurity Strategy.[115] Acknowledging the EU's unique governance structure, the 2013 Cybersecurity Strategy does not centralize supervision, but rather encourages Member States to organize and respond to cyber threats at the national level.[116] In conjunction with the 2013 Cybersecurity Strategy's release, the European Parliament and the Council also proposed a Network and Information Security Directive (NIS Directive) to "ensure a high common level of network and information security" standards among member states.[117] The 2013 Cybersecurity Strategy introduced the NIS Directive's goal to "facilitate exchange of best practices," and enhance "risk management practices and information sharing."[118] The Strategy also empowered ENISA to work with the public and private sectors to further the adoption of NIS standards, and to assist in the development of guidelines that

---

[110] ENISA, *Threat Landscape and Good Practice Guide for Internet Infrastructure* (Jan. 2015) at 49, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure.

[111] *Id.*

[112] 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.

[113] 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.

[114] *Id.*

[115] 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).

[116] *Id.*

[117] 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).

[118] *Id.*

reflect industry best practices. To accomplish these goals, the NIS Public-Private Platform (NIS Platform) was established with a goal to help public and private stakeholders facilitate EU-wide adoption of "industry-led security standards, [and] technical norms."[119]

Following the release of the 2013 Strategy and the proposed NIS Directive, the NIS Platform set up three working groups to develop the standards: WG1, "on risk management, including information assurance, risk metrics, and awareness raising"; WG2, "on information exchange and incident coordination, including incident reporting and risk metrics for the purpose of information exchange"; and WG3, "on secure ICT research and innovation."[120] The NIS Platform held three plenary meetings between June 2013 and April 2014, each laying the groundwork for a "commission recommendation on good cybersecurity practices" by the end of 2015.[121] In the days leading up to the fourth Plenary Meeting on November 24, 2014, the NIS Platform held a workshop to evaluate the merits of standardizing cyber norms between the NIST Framework and the NIS Platform. The summary report of the meeting concluded that "sufficient efforts should be devoted to raising awareness about the existence of voluntary good practice guidance initiatives and frameworks," and that the findings would be presented at the platform plenary the following day.[122] Less than one year later, at the fifth NIS Platform Plenary Meeting in Brussels, WG1 introduced and disseminated chapter one, version two of the NIS Platform ("NISP"), which specifically adopts the NIST core – identify, protect, detect, respond, recover – as the industry-standard approach for enterprise risk management.[123] NIS Program takes a similar approach to the role that the Platform should play in enterprise risk management: that the "guidelines will highlight existing risk management standards and best practices that organizations . . . can use and tailor to their own approach to risk management."[124] While maintaining the same NIST core paradigm, there are notable areas of difference in the NIS Platform, which are summarized below.

---

[119] 2013 Cybersecurity Strategy, *supra* note 115, at 13.

[120] NIS Platform, European Union Agency for Network and Information Security, https://resilience.enisa.europa.eu/nis-platform.

[121] NIS Platform, Minutes of the Fourth Plenary Meeting of the Public-Private Network and Information Security Platform (Nov. 25, 2014), *available at* https://resilience.enisa.europa.eu/nis-platform/shared-documents/4th-plenary-meeting/4th-nis-platform-plenary-meeting-minutes/view.

[122] Summary Report, Preliminary Workshop Comparing U.S. Cybersecurity Framework and EU NIS Platform Approaches (Nov. 24, 2014), https://resilience.enisa.europa.eu/nis-platform/shared-documents/eu-us-preliminary-workshop-comparing-approaches/Summary_report_US-EU_preliminary_workshop-24_November_2014.pdf/view.

[123] 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.

[124] *Id.* at 4.

TABLE 1. NIST FRAMEWORK VS. EU NIS PLATFORM[125]

NIST Categories/Subcategories	NIS Platform
Identify • Asset management; prioritization of resources based on their classification, criticality, and business value. • Risk assessment; potential business impacts and likelihoods are identified. • Organizational risk tolerance is informed by CI role.	**Identify** • Key assets, vulnerabilities and impacts from cyber compromises. • Threats and the likelihood of attack, overall risk, and prioritization of assets key to the survival of the organizations, and its customers.
Protect • Focused on access control and user permissions. • Raising awareness and training. • Protecting the confidentiality, integrity, and availability of data.	**Protect** • Emphasis on tracking and reporting risks to the right level in the organization. • Tracking changes in the risk drivers within an enterprise risk area. • Preventing events from happening, containing events from expanding, and/or preventing events from causing damage if they occur.
Detect • Detecting anomalous events in a timely manner. • Security continuous monitoring, emphasizing specific benchmarks, such as malicious code, unauthorized personnel, and devices. • Event detection is communicated to appropriate parties. • Well-defined roles. • Detection processes are tested.	**Detect** • Calls for dedicated threat intelligence, internal teams, and "incredibly skilled forensic investigators equipped with cutting-edge tools and resources." • Emphasizes continuous monitoring, appropriate monitoring capabilities. Divides monitoring services into three categories: base-level for broad detection of malicious or anomalous network activity, specialized security monitoring for critical assets and processes, data analysis and reporting to other key internal security detection and response partners.
Respond • Response planning with timely procedures. • Communicating with external stakeholders, such as law enforcement, information is shared in a consistent manner. • Analysis is conducted, forensics are performed, notifications are inspected. • Activities are performed to prevent expansion of event, incidents are mitigated, and eradicated. Improvements are made.	**Respond** • Limited emphasis. Notes that "Incident response is a priority for all organizations."
Recover • Recovery processes are executed, and lessons learned are incorporated. Recovery plans are improved. • Public relations managed, and activities are restored with partners, reputation is repaired.	**Recover** • Design for recoverability; test for recoverability; defense-in-depth; use diagnostic aids; recovery of key assets.; automated rollback; forensics important for detection.

[125] *Id.* at 14-16.

Moving forward, the NIS Platform plans to disseminate WG1's recommendations concerning risk management best practices for adoption.[126] Nevertheless, the NIS Directive has faced a lengthy road to enactment. "Negotiations over the directive have stumbled along," and a number of "trialogue" negotiations between the European Parliament, European Commission, and the European Council have taken place since the NIS Directive was proposed.[127] On June 6, 2015, an "understanding with the European Parliament on the main principles to be included in the draft [NIS directive]" was reached.[128] In general, Member States have disagreed about a number of the NIS Directive's requirements, including the applicability to individual economic sectors, and the extent of information sharing between EU states.[129] As of the time of this writing, neither the NIS directive nor the General Data Privacy Directive have yet been adopted; however, the EU Digital Commissioner believes that a deal on the NIS directive is imminent, though its final shape may be influenced by events such as the November 2015 Paris attacks.[130] Indeed, word came in December 2015 that a tentative deal on the NIS Directive had been reached that would: (1) oblige EU Member States to develop national cybersecurity strategies and Computer Security Incident Response Teams; (2) engage in international information sharing; (3) require reasonable security measures and incident reporting for cyber attacks on critical infrastructure.[131] However, time will tell how well this agreement is implemented, and to what extent the NIST Framework influences its interpretation.

D. Japan

The cyber threat landscape facing Japan is similar to that of the United States and the EU, and Japan's national strategy to combat this threat reflects this similarity by likewise emphasizing private sector self-governance over top-down direct regulation. In 2014 alone, Japan suffered an estimated 12.8 billion unauthorized cyber attacks, up from the 7.8 billion in 2012, and substantially greater than the estimated 300 million when monitoring began in 2005.[132] In addition to this increasing volume of cyber

---

[126] WG1 Presentation, NIS Platform Plenary Meeting (May 2015), *available at* https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/wg1-presentation/at_download/file.

[127] Catherine Stupp, EurActive, *Oettinger: Deal on Cybersecurity Directive Close*, EURACTIV (Nov. 10, 2015 7:30), http://www.euractiv.com/sections/digital/oettinger-deal-cybersecurity-directive-close-319325

[128] Press Release, Council of the European Union, Network and Information Security: Presidency Re-Launches Talks with EP (June 29, 2015), http://www.consilium.europa.eu/en/press/press-releases/2015/06/29-network-information-security/.

[129] Stupp, *supra* note 127.

[130] *Id.*

[131] *See* Günther H. Oettinger, *First EU-Wide Legislation on Cybersecurity Agreed*, EUR. COMM'N (Dec. 8, 2015), https://ec.europa.eu/commission/2014-2019/oettinger/blog/first-eu-wide-legislation-cybersecurity-agreed_en.

[132] *Record 12.8 Billion Cyberattacks Seen in Japan Last Year*, JAPAN TIMES (Feb. 11, 2014), http://www.japantimes.co.jp/news/2014/02/11/business/tech/record-12-8-billion-cyberattacks-detected-in-japan-last-year/#.VgLPg9VVhBd.

attacks, the sophistication of cyber attacks is increasing, with a seven-fold increase in targeted attacks in 2015 alone.[133] These numbers are indicative of a mounting cyber threat, but one that is perhaps most acutely felt by businesses and government agencies. Yet this state of affairs changed in March of 2015 when Japan's Pension Service suffered a massive data breach, resulting in the leak of personal data for an estimated 1.25 million individuals.[134] Apart from the notable similarities with the 2015 OPM data breach in the United States, this seems to have triggered sufficient public backlash for the Japanese government to modify its cybersecurity strategy.[135] While not a dramatic shift, the updated cybersecurity strategy better motivates private sector self-governance, primarily through incentivizing adherence to collaboratively generated cybersecurity standards similar to the NIST framework.

The Japanese approach to cybersecurity regulation has historically mirrored the U.S. one, minimizing direct regulation and favoring a private sector-led approach to generating cybersecurity standards. This approach has been realized through broad national strategies that promote important policies in lieu of a more restrictive regulatory framework. The First National Strategy on Information Security (FSIS), promulgated in 2006, represented Japan's first attempt at addressing the problem of cybersecurity on a nationwide level.[136] Prior to 2006, the Japanese approach to cybersecurity was disjointed, with no clear authority and a purely reactive approach to cyber threats.[137] FSIS sought to create a centralized voice for cybersecurity, focusing on recognition, development of cybersecurity infrastructure, and the protection of critical sectors. This was followed in 2009 with the Second National Strategy on Information Security[138]—which reemphasized the principles of FSIS while placing a greater emphasis on risk-management—and then the Cybersecurity Strategy in 2013[139]—which moved towards resilience.

This progression of cybersecurity strategies seems to reflect both a growing understanding of the threat and the increasing sophistication of the attacks being perpetrated. In 2006, cybersecurity was viewed as a relatively straightforward matter, which could be easily appended to existing systems, and

---

[133] *Surge in Targeted Cyber-Attacks in Japan in 2015*, GADGETS 360 (Sept. 17, 2015), http://gadgets.ndtv.com/internet/news/surge-in-targeted-cyber-attacks-in-japan-in-2015-report-741206.

[134] William Mallard and Linda Sieg, *Japan Pension System Hacked, 1.25 Million Cases of Personal Data Leaked*, REUTERS (June 1, 2015), http://www.reuters.com/article/2015/06/01/us-japan-pensions-attacks-idUSKBN0OH1OP20150601.

[135] *Japan Government Adopts Draft Cybersecurity Strategy*, JAPAN TIMES (Aug. 21, 2015), http://www.japantimes.co.jp/news/2015/08/21/national/japan-government-adopts-draft-cybersecurity-strategy/#.ViT0S9WrSHs.

[136] First National Strategy on Information Security, Information Security Policy Council, Feb. 2, 2006, *available at* http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

[137] Yasu Taniwaki, Cybersecurity Strategy in Japan, 7, Oct. 9, 2014, *available at* http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/keynotelecture.pdf.

[138] The Second National Strategy on Information Security, National Information Security Policy Council, Feb. 3, 2009, *available at* http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

[139] Cybersecurity Strategy, Info. Sec. Pol'y Council, June 10, 2013, http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf [hereinafter "2013 Strategy"].

indeed which should seek cybersecurity that is "perfect without any mistakes."[140] By 2009, the Strategy recognized that cybersecurity could not achieve perfect results, and instead shifted towards risk management.[141] By 2013, the mounting cyber threat pushed Japan towards resilience instead of prevention, emphasizing the maintenance of operability in the face of near constant cyber attacks.[142]

Yet the clearest trend through each Japanese cybersecurity strategy is an emphasis on bottom-up, voluntary private sector involvement, referred to as "autonomy" and "self-governance"[143] Despite frequent national strategies and the initiation of several government cybersecurity organizations, like the National Information Security Council, the Information Security Policy Council, and the CEPTOAR Council, the Japanese approach to cybersecurity has involved relatively little direct regulation. While Japan does provide basic privacy protections, and requires that data controllers "take necessary and proper measures for the prevention of leakage, loss, or damage; and for other security control of the personal data,"[144] the implementation of these laws is left to sector-specific agencies, of which there are twenty-seven,[145] whereas common protections, like data breach notifications, are often absent or only recommended.[146] This regulatory framework largely seeks to promote cybersecurity without imposing it.

The 2015 Cybersecurity Strategy reaffirms Japan's commitment to private sector self-governance, albeit with a greater emphasis on the development of national and international standards like the NIST Framework,[147] and on information sharing between the public and private sector.[148] The 2015 Strategy states from the outset that "Autonomy" and "Collaboration among Multi-stakeholders" are two of the five core principles that should inform the entire strategy, emphasizing the role that private sector self-governance has played in fostering the growth and development of cyberspace.[149] Yet the mounting threat posed by inadequate cybersecurity also suggests that greater government involvement in developing standards is needed to inform and incentivize private sector self-governance, prompting the

---

[140] *See* Second National Strategy on Information Security, *supra* note 138, at 27.

[141] *Id*.

[142] 2013 Strategy, supra note 139.

[143] Cybersecurity Strategy, Government of Japan, Sept. 4, 2015, available at http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf [hereinafter "2015 Strategy."].

[144] Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information (APPI)], Act No. 57 of 2003, art. 20 (Hōrei hon'yaku dētashū [Hon'yaku DB]), http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=02&dn=1&yo=Act+on+the+Protection+of+Personal+Information&x=29&y=10&ia=03& ky=&page=2, archived at http://perma.cc/GY4M-CF3W (Japan).

[145] See, e.g., Lynn M. Marvin & Yohance Bowden, Conducting U.S. Discovery in Asia: An Overview of e-Discovery and Asian Data Privacy Laws, 21 Rich. J.L. & Tech. 12, 57 (2015).

[146] 2015 International Compendium of Data Privacy Laws, BakerHostetler, 110, *available at* http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.

[147] The 2015 Strategy does not explicitly reference the NIST Framework, preferring to allude more broadly to "international frameworks," see, e.g., 2015 Strategy at 20, although Japan has met with NIST officials, *see* http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf.

[148] 2015 Strategy, supra note 143, at 9.

[149] *Id*. at 9.

Japanese government to "build a guiding framework that enables stakeholders . . . to properly evaluate enterprises' efforts to address cybersecurity as a critical management challenge; and a framework that gives financial advantages, e.g. fund-raising, to enterprises making such efforts."[150] This two-fold strategy of creating standards and rewarding stakeholders that meet those standards represents a compromise between outright self-governance and top-down regulatory oversight, and views the role of the government as emphasizing policies that will "catalyze [the private sector's] self-motivated activities and their own initiatives."[151]

In creating incentives, the Strategy seeks to identify business practices that it deems particularly important for strong cybersecurity and reward investment and development in businesses that support those practices. The Strategy specifies "security by design"—where cybersecurity is central to new products' development cycles—as a particularly important cybersecurity practice that should warrant government incentives.[152] Using as an example the development of Internet of Things (IoT) devices, the Strategy specifies that "the Government will promote security measures for these systems in a cross-sectoral manner, based on the Security by Design approach, and will give its prioritized support to the growth of such new business."[153] However, the Strategy recognizes that new technologies involve multiple stakeholders, often with ambiguous requirements and expectations, and that cross-sectoral involvement is necessary to develop cybersecurity standards. The Strategy therefore seeks to promote dialogue in these multi-stakeholder areas, first to assess the benefits and risks of potential policies, and then to establish explicit security obligations for the various stakeholders.[154] Using the example of Intelligent Transport Systems, the Strategy recognizes that this industry involves numerous manufacturers, government agencies, and academics, and that these bodies should come together to develop appropriate standards by which they will hold themselves accountable.[155] This once again affirms a commitment to a bottom-up, collaborative approach to cybersecurity policy, and while the Strategy anticipates the government taking a leading role in areas of considerable importance, (through the Cybersecurity Strategic Headquarters), the overall focus is still self-governance. This strategy is particularly notable when contrasted with the greater government intervention seen with other regionals powers, such as Japan's close neighbor, South Korea.

E. Republic of Korea

[150] *Id*. at 16.
[151] *Id*. at 11.
[152] *Id*. at 13.
[153] *Id*.
[154] *Id*. at 14.
[155] *Id*.

South Korea is well known as one of the most "connected" countries in the world, with more than eighty percent of its population having access to a broadband Internet connection.[156] Yet this connectivity also makes South Korea particularly vulnerable to cyber attacks, of which it has had its fair share, with the South Korean government suffering an estimated 114,000 cyber attacks since 2011.[157] Furthermore, while South Korea is subject to the usual cybercriminals, state-sponsored espionage, and other traditional cyber threats, it also has a unique position as the focus of North Korean cyber activities. Despite North Korean involvement with the 2014 Sony hack receiving more press in the United States, the bulk of North Korean cyber activity seems to be targeted at South Korea, with several high profile cases involving the disruption of nuclear facilities,[158] banks,[159] communications companies,[160] and potentially the Seoul Metro system[161] in recent years. Yet as is often the case, arguably the most pivotal cyber attack felt by South Korea involved the theft of personal data, specifically credit card numbers. In 2014, a worker at Korea Credit Bureau, a South Korean credit monitoring firm, downloaded and sold over 20 million credit card numbers, impacting more than forty percent of South Korea's citizenry.[162] This incident highlighted both the complexity of cybersecurity issues and the apparent failure of South Korean cybersecurity policy to protect basic consumer information, and may serve to shift its national cybersecurity policy.

South Korea has historically taken a more hands-on approach to cybersecurity regulation than either the United States or Japan, combining strong broad-spectrum legislation protecting personal data with sector specific regulations governing other aspects of cybersecurity. The single most important cybersecurity regulation is the Personal Information Protection Act (PIPA), passed in 2011.[163] PIPA regulates the collection and use of personal information by data controllers and data processors, and requires particular protection of South Korean resident registration numbers (an analogue of U.S. Social Security Numbers).[164] PIPA also requires companies to take certain minimum cybersecurity precautions,

---

[156] *See, e.g.*, State of the Internet Q2 2015, Akamai, *available at* https://content.akamai.com/PG3046-Q2-2015-SOTI-Report.html.

[157] Conor Gaffey, *South Korea Suffered 114,000 Cyberattacks in Five Years*, NEWSWEEK (Sept. 21, 2015), http://europe.newsweek.com/south-korea-suffered-114000-cyberattacks-five-years-333371.

[158] *South Korea Accuses North of Cyber-Attack on Nuclear Plants*, SEC. WK. (Mar. 17, 2015), http://www.securityweek.com/south-korea-accuses-north-cyber-attacks-nuclear-plants.

[159] Choe Sang-Hun, *Computer Networks in South Korea are Paralyzed in Cyberattacks*, N.Y. TIMES (Mar. 20, 2013), http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0.

[160] *South Korea on Alert for Cyber-Attacks After Major Network Goes Down*, GUARDIAN (Mar. 20, 2013), http://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack.

[161] Shannon Hayden, *Cyber Attack on South Korean Subway System Could be a Sign of Nastier Things to Come*, VICE NEWS (Oct. 8, 2015), https://news.vice.com/article/cyber-attack-on-south-korean-subway-system-could-be-a-sign-of-nastier-things-to-come.

[162] *Credit Card Details on 20 Million South Koreans Stolen*, BBC (Jan, 20, 2014), http://www.bbc.com/news/technology-25808189.

[163] Personal Information Protection Act, Act. No. (10465), Sept. 30, 2011, (S.Kor.), *available at* http://koreanlii.or.kr/w/images/a/a3/PIPAct_1308en.pdf.

[164] *Id*. at Art. 34-2.

and specifies South Korea's general-purpose breach notification requirements.[165] While the rules propagated through PIPA are generally vague, they serve as the foundation for the more specific, sector-based rules that are generated by those sector's respective ministries. South Korea also recently created a presidential post, similar to a cabinet official, specifically for cybersecurity, designed to serve as a "control tower" for cybersecurity issues.[166]

Yet South Korea's cybersecurity regulation has drawn a fair amount of criticism, claiming that this heavily regulated approach adapts too sluggishly to new cyber threats, and forces companies to use outdated security tools and procedures.[167] For instance, South Korean regulations from the 1990s still require all online financial transactions to be authenticated using the SEED cipher, a relatively obscure authenticator not supported by most browsers and operating systems.[168] This lack of support requires the widespread use of ActiveX, despite frequent complaints that ActiveX is outdated and insecure.[169] South Korean reliance on SEED has led to historically bizarre outcomes, as an otherwise technologically sophisticated culture is forced overwhelmingly to use Microsoft operating systems and the Internet Explorer browser exclusively, as they are one of the only ways to engage in encrypted online commercial transactions.[170] Although appropriate when implemented, the fallout from these regulations shows how quickly technology can outpace legislation, suggesting that more agile approaches may be necessary.

Whereas from a policy perspective, South Korea's approach to cybersecurity is heavily influenced by its position internationally as a "middle power," referred to as "medium-size states with the capability and willingness to employ proactive diplomacy with global visions."[171] As a middle power, South Korea can act as a broker between the disparate cybersecurity strategies of the United States and China, two generally accepted "great powers" operating in the region.[172] The blend of South Korea's economic and political ties with the United States and its physical proximity to China has led South Korea

---

[165] *Id*. at Art. 34.

[166] *South Korea Army General Assumes Cyber-Security Post*, SEC. WK. (Apr. 3, 2015), http://www.securityweek.com/south-korea-army-general-assumes-cyber-security-post.

[167] Gen Kanai, *The Cost of Monoculture*, KANAI (Jan. 26, 2007), http://kanai.net/weblog/archive/2007/01/26/00h53m55s#003095.

[168] Chico Harlan, *South Korea is Stuck with Internet Explorer for Online Shopping Because of Security Law*, WASH. POST (Nov. 5, 2013), https://www.washingtonpost.com/world/asia_pacific/due-to-security-law-south-korea-is-stuck-with-internet-explorer-for-online-shopping/2013/11/03/ffd2528a-3eff-11e3-b028-de922d7a3f47_story.html.

[169] *See, e.g.*, Designing Secure ActiveX Controls, MICROSOFT, https://msdn.microsoft.com/en-us/library/aa752035(v=vs.85).aspx (last visited Nov. 30, 2015) ("an ActiveX control is particularly vulnerable to attack").

[170] *Id*.

[171] Kim Sung-han, *Global Governance and Middle Powers: South Korea's Role in the G20*, COUNCIL ON FOREIGN REL., http://www.cfr.org/south-korea/global-governance-middle-powers-south-koreas-role-g20/p30062.

[172] Minghao Zhao, *South Korea's Middle-Power Diplomacy*, PROJECT SYNDICATE, (Sept. 9, 2015) https://www.project-syndicate.org/commentary/china-south-korea-warming-relations-by-minghao-zhao-2015-09.

to employ a cybersecurity strategy that is similarly "in between" those of China and the United States.[173] While not reaching the level of state intervention seen in China, South Korea employs a notably stronger cybersecurity regulatory approach than the United States and other Westernized regional powers, like Japan, where multistakeholderism is the predominant strategy.[174] Indeed South Korea often serves as a bridge between these disparate regimes, and it sees itself as an important diplomatic force in the development of international cybersecurity policy.[175]

South Korea's cybersecurity policy is further complicated by North Korea, which is arguably the State's single strongest policy determinant. North Korea's frequent belligerence is largely targeted at South Korea, and North Korea's cyber-capabilities, while not fully understood, are a constant source of worry in South Korean policymaking. This threat of "6000 North Korean cyber-soldiers," as estimated by the South Korean military, is frequently cited by South Korean sources,[176] and fear of North Korean cyber attacks, particularly preceding a kinetic attack, has tended to centralize cybersecurity efforts into the government. This is reinforced by the most recent development, the presidential cybersecurity post, which seems poised to further centralize the various regulatory agencies employed.[177]

Therefore, despite vowing closer ties with the US on cybersecurity,[178] South Korea has not formally indicated any willingness to fundamentally change its cybersecurity policy towards a more bottom-up approach. However, discontent with the immobility of this regime may nonetheless be driving some change, as seen by the recent efforts to replace ActiveX with a more modern and secure online authenticator. In April of 2015, for example, the South Korean Ministry of Science, ICT, and Future Planning announced a plan to move away from ActiveX by incentivizing the most highly trafficked websites to develop new authentication methods more in keeping with modern Internet standards, like HTML5.[179] The plan will offer the equivalent of $90,000 dollars to each of the top 100 most trafficked South Korean websites to develop new standards, which will eventually be utilized by other local and less popular websites. The overall goal is to update an outdated cybersecurity policy through a private-sector

---

[173] Sangbae Kim, *Cyber Security and Middle Power Diplomarcy: A Network Perspective*, 12 KOREAN J. INT'L STUD. 323, 338–45 (2014).

[174] *Id* at 329.

[175] *Id*.

[176] *North Korea has 6,000-Strong Cyber-Army, Says South*, GUARDIAN (Jan. 6, 2015), http://www.theguardian.com/world/2015/jan/06/north-korea-6000-strong-cyber-army-south-korea.

[177] This troubled relationship with North Korea may also contribute to South Korean desires to strengthen ties with China, North Korea's largest trade partner and one of its few diplomatic supporters. *See*, e.g., Beina Xu & Jayshree Bajora, *The China-North Korea Relationship*, COUNCIL ON FOREIGN REL., (Aug. 22, 2014) http://www.cfr.org/china/china-north-korea-relationship/p11097.

[178] Cory Bennet, *US Vows Tighter Cyber Cooperation with South Korea*, HILL (May 18, 2015), http://thehill.com/policy/cybersecurity/242369-us-vows-tighter-cyber-cooperation-with-south-korea.

[179] Simon Sharwood, *South Korea to Nuke Microsoft ActiveX*, REGISTER (Apr. 2, 2015), http://www.theregister.co.uk/2015/04/02/south_korea_to_deport_microsoft_activex/.

driven initiative, with the hope that similar initiatives will be extended to other areas, such as finance and education.[180]

This approach to ActiveX suggests again a blend between entirely State-imposed and entirely private sector driven models for implementing cybersecurity. Recognizing the weaknesses of their preceding model, South Korea may be attempting to better harness the benefits of bottom-up cybersecurity initiatives while still retaining the degree of control and accountability that the State-imposed model allows. While it is unclear if this reflects a fundamental shift in policy, South Korean officials have recently met with NIST representatives, perhaps signaling a willingness to try more market-driven approaches to cybersecurity.[181] This may also be signaled by South Korea strengthening cybersecurity ties with more market-driven regional powers, like Australia.[182]

F. Australia

To quote the Australian Cyber Security Center's 2015 Threat Report, the cyber threat faced by Australia is "undeniable, unrelenting, and continues to grow."[183] Meanwhile, the Australian Federal Police reported 3,500 breaches in April alone, and a twenty percent rise in cyber attacks during 2014.[184] While Australia has mostly avoided the massive data breaches that have shocked other countries into action, it does not have to look too far into the past to see how vulnerable its systems can be to cyber attack. For instance, in February of 2010, in response to Internet regulations designed to restrict access to "unwanted" content, the hacker group Anonymous subjected Australian government websites to a two-day distributed denial of service attack, rendering the sites largely inoperable, and placing Australian cyber-insecurity at the forefront of public scrutiny.[185] But perhaps the paradigmatic example of Australian cybersecurity failings is the telecommunications company Telstra, the single largest provider of telecom services in Australia. In 2011, Telstra was found to have publically exposed the personal data

---

[180] Cho Mu-hyun, *South Korea to remove 90 percent of ActiveX by 2017*, ZDNET, (April 2, 2015), http://www.zdnet.com/article/south-korea-to-remove-90-percent-of-activex-by-2017/.

[181] *Board Agenda: Cyber Conference*, NIST (2015), http://nist.gov/director/speeches/2015-board-agenda-cyber-speech.cfm.

[182] Rohan Pearce, *Australia, South Korea Seek to Boost Cyber Security Cooperation*, COMPUTERWORLD, (Sept. 11, 2015), http://www.computerworld.com.au/article/584322/australia-south-korea-seek-boost-cyber-security-cooperation/.

[183] ACSC 2015 Threat Report, Australian Cyber Security Center, 2, (July 2015), https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf .

[184] Conor Duffy, *Cyber Attacks: More than 3,500 breaches in April and Threats Set to Rise, AFP Says*, ABC (June 15, 2015), http://www.abc.net.au/news/2015-06-15/threat-of-cyber-attacks-set-to-increase-says-afp/6547696.

[185] David Kravets, *Anonymous Unfurls 'Operation Titstorm'*, WIRED (Feb. 10, 2010), http://www.wired.com/2010/02/anonymous-unfurls-operation-titstorm/.

of over 700,000 individuals online for a period of eight months.[186] Despite the scale of the breach, the Australian government was not empowered to impose financial penalties for privacy violations at the time, so Telstra faced little in the way of direct consequences.[187] And while the breach partly served as the motivation for Australian privacy reform, when Telstra found itself again facing privacy violations in 2014 (this time for exposing personal data on over 15,000 individuals), these bolstered privacy laws only imposed a sanction of AU$10,200: less than a dollar per individual affected.[188]

The Australian model of cybersecurity regulation could be described as a mix between that of the EU and the U.S., employing a small number of broad-spectrum data protection laws, which are supplemented with sector specific laws in areas of heightened cybersecurity concern.[189] The single most important law is the Privacy Act, Australia's data protection law for all federal government entities and private organizations with revenues over $3 million annually.[190] The Privacy Act, most recently amended in 2014, articulates thirteen Australian Privacy Principles, one of which is the "data security principle," which requires entities that hold personal information to take "such steps as are reasonable in the circumstances to protect the information" and to delete information that is no longer relevant for any purpose.[191] Whereas for sector-specific regulations, Australia employs specific laws for Healthcare, Finance, and Internet Service Providers similar to the U.S. approach, although the specific requirements are typically minimal with regard to cybersecurity, and instead recommend voluntary frameworks, like ISO 27001/2 and COBIT 5.[192]

Adding to the complexity of this system, some "voluntary frameworks" are effectively mandatory due to private sector self-regulation, as with credit card processors and PCI-DSS,[193] whereas other industries, like those frequently classified as critical infrastructure, may be required to adhere to standards

---

[186] Stephanie McDonald, *Telestra found in breach of privacy and telco laws*, COMPUTERWORLD, (June 29, 2012) http://www.computerworld.com.au/article/429127/telstra_found_breach_privacy_telco_laws/

[187] *Id*.

[188] Allie Coyne, *Telstra Breached Privacy Act by Exposing User Data*, ITNEWS, (Mar. 11, 2014), http://www.itnews.com.au/news/telstra-breached-privacy-act-by-exposing-user-data-374722.

[189] Alexandra McKay, *The Private Sector Amendment to Australia's Privacy Act: A First Step on the Road to Privacy*, 14 PAC. RIM. L. & POL'Y J. 223, 224 (2005).

[190] The Privacy Act, 1988 (Austl.), *available at* https://www.comlaw.gov.au/Details/C2015C00534 (last visited Oct 19, 2015).

[191] Privacy Fact Sheet 17: Australian Privacy Principles, Office of the Australian Information Commissioner, available at http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-17-australian-privacy-principles_2.pdf (last visited Oct. 19, 2015); However, Australia also imposes data retention requirements in certain circumstances, see, e.g., Josh Taylor, Mandatory Data Retention Passes Australian Parliament, ZDNet, Mar. 26, 2015, http://www.zdnet.com/article/mandatory-data-retention-passes-australian-parliament/.

[192] Babu Veerappa Srinivas, A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains, SANS Institute, June 15, 2015, available at https://www.sans.org/reading-room/whitepapers/legal/concise-guide-australian-laws-related-privacy-cybersecurity-domains-36072

[193] PCI SSC Data Security Standard Overview, PCI Security Standards Council, https://www.pcisecuritystandards.org/security_standards/index.php (last visited Oct. 19, 2015).

developed for government agencies, like the Protective Security Policy Framework.[194] Further muddying the waters, the amended Privacy Act allows for the private sector to register privacy codes of practice (APP codes), which effectively serve to codify voluntary standards for specific industries.[195] APP codes, although not required to be developed in an industry-wide manner, are nonetheless binding on all organizations in that industry.[196] Despite this option for self-regulation, comparatively few APPs have been enacted.[197] Notwithstanding this web of cybersecurity standards, for most businesses the important regulation is the Privacy Act's data security principle, which sets a minimum, albeit a vague one, for cybersecurity among larger businesses. And while the data security principle is good in theory, the Australian Privacy Commission has relatively limited options for enforcement, as discussed above, and cybersecurity failing are nonetheless difficult to assess in practice, as Australia does not require breach reporting or breach notification to affected individuals,[198] although both are recommended.[199][200]

In articulating national cybersecurity strategies, however, Australia has been somewhat behind the curve, with the first Australian Cybersecurity strategy not being released until 2009.[201] In the 2009 strategy, Australia emphasized bolstering cybersecurity awareness, promoting and developing cybersecurity technologies, and fostering public-private partnerships.[202] Although the Strategy included the government taking a "leading role," it ultimately relied on the private sector to self-regulate their cybersecurity standards, primarily through the adoption of APP codes.[203] Furthermore, Australia has recently undertaken a comprehensive Cybersecurity Review designed to better address cybersecurity

---

[194] Protective Security Policy Framework, Australian Government, available at https://www.protectivesecurity.gov.au/ExecutiveGuidance/Documents/ProtectiveSecurityPolicyFrameworkSecuringGovernmentBusiness.pdf (last visited Oct. 19, 2015) ("The Australian Government requires non-government organisations that access security classified information to enter into a Deed of Agreement to apply the PSPF to that information").

[195] *See* Privacy Codes Register, Office of the Australian Information Commissioner, http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/privacy-codes/ (last visited Oct. 19, 2015).

[196] *Id*.

[197] *Id*.

[198] DATA BREACH NOTIFICATION — A GUIDE TO HANDLING PERSONAL INFORMATION SECURITY BREACHES (Off. of the Australian Info. Comm'r, 2014), http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/data-breach-notification-guide-august-2014.pdf (last visited Oct. 19, 2015).

[199] *Id*. at 6 ("Notification of a data breach in compliance with this guide is not required by the Privacy Act. However, the steps and actions in this guide are highly recommended by the OAIC").

[200] The Australian parliament has expressed its intent to make breach notification mandatory, and plans to introduce legislation this year. *See* Chris Duckett, *Australian Data Breach Notification Laws will Not be Passed in 2015*, ZDNET (Oct. 13, 2015), http://www.zdnet.com/article/australian-data-breach-notification-laws-will-not-be-passed-in-2015-brandis/.

[201] Cyber Security Strategy, Australian Attorney General (Nov. 23, 2009), *available at* https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

[202] *Id*.

[203] *Id*. at 17.

concerns in this evolving cyber-landscape.[204] Although originally scheduled to release by the end of 2015, this has been pushed back due to initial critiques that the draft lacked "teeth or funding."[205]

This updated Australian cybersecurity strategy is believed to be incorporating elements of the NIST framework, specifically by creating a national voluntary cybersecurity standard defining the various levels of cybersecurity preparedness, thereby allowing private companies to determine the appropriate level of cybersecurity for their business needs and risk tolerance.[206] Rather than rely solely on APP codes, whose binding requirements on the entire sector make them difficult to pass, this would allow for companies to self-regulate in a less restrictive manner, and may better incentivize the establishment of best practices by private sector actors. While the NIST Framework is already recommended by some Australian government agencies,[207] creating or adopting a broad spectrum framework would help simplify the current model, and would be in keeping with Australia's historic mix of government and private sector regulation.[208]

G. Summary

This Part has summarized the cybersecurity policymaking of five nations (the UK, Italy, Japan, the Republic of Korea, and Australia) and one region (EU) as they pertain to the NIST Framework. The following Part will parse these findings beginning with a summary matrix to help identify areas of convergence and divergence that could help set the stage for trust and norm building measures as part of a polycentric program to promote international critical infrastructure cybersecurity.

III. A POLYCENTRIC PATH FORWARD

This final Part analyzes the case studies and summary matrix of Part II in an attempt to delineate areas of regulatory convergence and uncover what that portends for cybersecurity norm building. To accomplish this, lessons from national case studies are amalgamated and digested into recommendations

---

[204] Cyber Security Review, Department of the Prime Minister and Cabinet, http://www.dpmc.gov.au/pmc/about-pmc/core-priorities/national-security-and-international-policy/australian-governments-cyber-security-review, (last visited Nov. 30, 2015).

[205] Allie Coyne, *Turnbull orders rewrite of draft Australian cyber strategy*, ITNEWS, (Nov. 16, 2015), http://www.itnews.com.au/news/turnbull-orders-rewrite-of-draft-australian-cyber-strategy-411749.

[206] Robert Parker, *Developing and Australian Cybersecurity Framework*, TECH. SPECTATOR (Sept. 18, 2015), http://www.businessspectator.com.au/article/2015/9/18/technology/developing-australian-cybersecurity-framework.

[207] Cyber Resilience: Health Check, AUST. SEC. & INVESTMENT COMM'N, (Mar. 2015), *available at* http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.

[208] Paul Kelly, *Recent Developments in Private-Sector Personal Data Protection in Australia: Will There Be an Upside Down Under?*, 19 J. Marshall J. Computer & Info. L. 71, 80, 85 (2000).

for managers and policymakers and are couched within the theoretical literature on polycentric governance to help enrich the discussion.

A. Areas of Convergence and Divergence and Impact on Norm Building

Table 2 summarizes some areas of convergence and divergence across the five nations and one region surveyed using the NIST Framework as a baseline for comparison.

TABLE 2. CYBERSECURITY REGULATORY SUMMARY MATRIX

	UK	Italy	EU	Japan	South Korea	Australia
Overall NIST Framework Implementation Status	No new, updated strategy has been released since the NIST Framework was released. However, intent to harmonize NIST and UK practices has been announced formally by US and UK leaders. The recent release of 10 Steps: Advice Sheets track elements of NIST Framework.	General intention to identify international best practices announced. No specific mention of NIST harmonization or implementation, but certain language overlaps imply NIST influenced Italian cybersecurity strategies.	NIS Directive still in flux, but is close to implementation. At least one meeting was held regarding the merits of standardizing NIST and NIS Platform, and results of latest NIS Working Group meeting indicate implementation is likely.	Pending[209]	Pending[210]	Pending[211]
Overlap with NIST Framework Approach	Emphasis that implementation of framework may be variable depending on the business, and is adaptable over time. Enables internal risk management processes, implementation variable based on risk appetite.	Espouses best practices in the language of the NIST Core: analyzing, preventing, mitigating, and reacting to cyber threats.	Exact language of NIST core has been proposed for formal adoption into NIS Directive.	Emphasis on voluntary standards and public/private cooperation.	Utilizes some market-developed standards.	General emphasis on voluntary standards and public/private cooperation, and risk management.
Differences with NIST Framework Approach	Not broken down by Function, etc. Rather, collected in "Advice Sheets" intended to assist firms. Compliance is required to achieve Cyber Essentials certification.	Broken down in a pyramid structure, with risk analysis, management, and mitigation forming the base, and identifying training, awareness and "empowerment" as the capstone. Emphasis on preventing cybercrime.	Less focus on responding to cyber threats, and does not emphasize public relations and reputational damage caused by incidents. Steps for detecting and protecting against intrusions sometimes overlap.	(Unavailable at this time.) Potentially a greater reliance on government incentives than risk management.	Mandatory. Standards primarily government developed. More top-down than NIST Framework.	(Unavailable at this time.) Potentially a greater reliance on private/private partnerships.

[209] Japan is currently developing its own cybersecurity framework, believed to be partly modeled on the NIST Framework. Currently, similarities and differences are extrapolated from the 2015 Japanese Cybersecurity Strategy, *supra* note 143.

[210] South Korea has been involved in talks with NIST regarding the NIST Framework, although it is unclear to what degree, if any, it will be adopted.

[211] Australia is currently developing its own cybersecurity framework, based partly on the NIST Framework.

As Table 2 helps exemplify, these nations and the EU generally (out of the more than twenty with which NIST has had active consultations) are, to a greater or lesser extent, emulating various aspects of the NIST Framework in their domestic policymaking. The UK, Japan, and to a lesser extent Australia seem to be the most supportive of many aspects of the NIST Framework, as does the EU as seen in its support of core NIST Framework terminology. In contrast, the Italian approach is more prescriptive than the NIST Framework, as is South Korea's philosophy of more top-down cybersecurity policymaking even as it engages with the U.S. on NIST Framework deployment.

Such State practice is informative in discussions relating to cybersecurity norm development, the argument being 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, "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[212]; 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 . . . ."[213] Potentially, cyber norms generated from arguably bottom-up processes, though admittedly with some degree of centralized facilitation, could help engender trust across multiple stakeholders that could make them more clear and useful than top-down schemes. This leads to the question: Might the rise of bottom-up measures to enhance particularly critical infrastructure cybersecurity help point to an emerging governance norm that could help to build out the field of cybersecurity due diligence?[214] It is too soon to tell, but the recent pronouncement by a group of twenty influential cyber powers is indicative perhaps of the polycentric shape of things to come, stating, "The Group recommended that States cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT."[215] How precisely states should go about operationalizing such cybersecurity due diligence requirements is left unstated, but the role of voluntary bottom-up frameworks is central to such efforts, as is discussed next with regards to implications for businesses and policymakers.

B. Implications for Businesses and Policymakers

---

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

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

[214] *See* INFO. SEC. BLOG, *supra* note 9.

[215] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, at 2 (July 22, 2015).

There is an array of takeaways for both managers and policymakers from the prior analysis. In particular, the UK's experimentation with "Cyber Essentials Certification" requires further unpacking in terms of its potential to help realize the goals for bottom-up cybersecurity policymaking, as does the utility of offering incentives such as prizes to those firms exhibiting "best-in-class" cybersecurity. First, regarding certifications, public- and private-sector stakeholders are at odds regarding the benefit of certifications fearing that they send the wrong signal and could contribute to "check box" security. There seems to be more support for purely private-sector certification schemes to help identify market leaders and norm entrepreneurs, though there is also the potential for public-private schemes to emerge. Indeed, the NIST Framework could provide a foundation on which to build a LEED-type certification scheme as a middle ground between purely public and purely private cybersecurity certification efforts. The flexibility inherent in the NIST Framework could be leveraged as more organizations adopt it to begin the task of comparing what has, until recently, been difficult: the cybersecurity competence of organizations. Eventually, this could allow for the type of approach advocated by the Heritage Foundation, which has put forward the idea of rewarding market leaders with the most secure supply chains through some type of certificate scheme.[216] However, elements of the private sector will wish to ensure that such certifications are bottom-up and not used as a backhanded regulatory tool that, they argue, could be too blunt to meet diverse risk positions.

Parliaments could also enact domestic policy regimes including laws, frameworks, and initiatives to incentivize—such as through tax breaks—or even cajole private actors under their jurisdiction to invest in cybersecurity best practices. One example 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 similar to Japan's two-fold strategy of creating standards while working to catalyze self-motivated activities.[217] The European Parliament could also undertake a similar voluntary program to reward leading firms—or even Member States—that have done the most to spread awareness of the NIS Directive and/or have taken the largest advances in the field of cybersecurity due diligence. Regular summaries or report cards 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 or create public versions of such programs.[218]

---

[216] *See* David Inserra & Steven P. Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Mar. 6, 2014), http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

[217] *See* 2015 Strategy, supra note 143, at 11.

[218] *See, e.g.*, Kacy Zurkus, *Have Bug Bounties Finally Become Mainstream?*, CIO (Aug. 7, 2015), http://www.cio.com/article/2966121/security/have-bug-bounties-finally-become-mainstream.html.

Elements of the private sector have been active in pushing the NIST Framework globally as a helpful tool to strategize about cybersecurity resilience as part of an overarching strategy for enterprise risk management, though some elements do not see the need for additional carrots to use the NIST Framework in particular beyond a desire to enhance their own resilience. Indeed, the U.S. Chamber of Commerce has plans to work with their foreign counterparts to this end, along with helping to shape a common vision of "shared responsibility" for protecting critical systems from misuse, overuse, and attack. The word seems to be getting out, with more than ninety percent of businesses recently surveyed by IBM having heard of the NIST Framework, while sixty percent have had a conversation with their Boards about the Framework.[219] How then might such initiatives fit into an approach to foster a global culture of cybersecurity? That conceptualization is what we turn to next as part of the overarching literature on polycentric governance and cyber peace.

C. A Polycentric Cyber Peace?

Bottom-up regulation such as the NIST Framework should inform global debates playing out in the field of CI cybersecurity, and indeed the importance of "co-regulation" has been recognized in the literature.[220] Together, such bottom-up experimentation could be considered a polycentric approach to promoting cyber peace. This multi-level, multi-purpose, multi-functional, and multi-sectoral model,[221] 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,"[222] and examining the extent to which national and private control can in some cases coexist with communal management, as may be seen in the success of the Internet Engineering Task Force. It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems"[223] such as cyber attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility

---

[219] *See generally* FROM CHECKBOXES TO FRAMEWORKS, IBM (2014).

[220] TATIANA TROPINA & CORMAC CALLANAN, SELF- AND CO-REGULATION IN CYBERCRIME, CYBERSECURITY AND NATIONAL SECURITY 36 (2015).

[221] 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.").

[222] 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.

[223] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

across issues and adaptability over time."[224] Such an approach, in other words, recognizes both the common but differentiated responsibilities of public- and private-sector stakeholders as well as the potential for best practices to be identified and spread organically, generating positive network effects that could, in time, result in the emergence of a cascade toward cybersecurity critical infrastructure norms.[225] Such norms should not only focus on the NIST Framework but should also encourage the uptake of proactive cybersecurity best practices so as to secure vulnerable critical infrastructure.

Such innovative efforts are critical to furthering the cause of cyber peace, especially when coupled with effective cybersecurity regulation. 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 . . . ."[226] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term.[227] That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be called negative cyber peace.[228] Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships, we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[229]

---

[224] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

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

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

[227] 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.").

[228] 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.").

[229] *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 1, 1 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace). Definitions of positive peace

Already some of the public- and private-sector efforts highlighted in this paper may be bearing fruit with, by some estimates, the severity of cyber attacks beginning to plateau and "an emerging norm against the use of severe state-based cybertactics" emerging.[230]

CONCLUSION

This Article has examined the extent to which five nations—the UK, Italy, Japan, the Republic of Korea, and Australia—and one region—the EU—are coalescing around the NIST Framework as a model of bottom-up cybersecurity governance. As has been shown, several of these nations—including the UK and Japan—have incorporated aspects of the NIST Framework, as has the EU with its deployment of NIST Framework terminology in its cybersecurity policymaking. Moreover, even those nations with a traditionally more top-down approach to cybersecurity policymaking, such as Italy and the Republic of Korea, have seen the benefits of the NIST Framework and are working to include elements of it in their cybersecurity reform efforts. Certainly, the NIST Framework is not a panacea, and it should be tailored to meet unique national circumstances. Increasingly, though, it is helping to inform debates over both what counts as a reasonable level of cybersecurity care and cybersecurity due diligence. As State practice crystallizes further it will be possible to better gauge what impact the NIST Framework may have on norm building measures and the field of international cybersecurity law as part of a polycentric approach to secure CI and promote cyber peace.

---

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

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