2020

National Cybersecurity Innovation

Tabrez Y. Ebrahim

NATIONAL CYBERSECURITY INNOVATION

*Tabrez Y. Ebrahim**

Abstract

National cybersecurity plays a crucial role in protecting our critical infrastructure, such as telecommunication networks, the electricity grid, and even financial transactions. Most discussions about promoting national cybersecurity focus on governance structures, international relations, and political science. In contrast, this Article proposes a different agenda and one that promotes the use of innovation mechanisms for technological advancement. By promoting inducements for technological developments, such innovation mechanisms encourage the advancement of national cybersecurity solutions. In exploring possible solutions, this Article asks whether the government or markets can provide national cybersecurity innovation. This inquiry is a fragment of a much larger literature on various innovation policy options (including patents, prizes, grants, and research and development tax credits). It requires determining whether national cybersecurity is a public good and an examination of market

---

* Associate Professor of Law, California Western School of Law; Visiting Associate Professor, University of California, San Diego; Ostrom Visiting Scholar (Program on Data Management and Information Governance) & Affiliate (Program on Cybersecurity and Internet Governance), Indiana University (Bloomington); Visiting Fellow, University of Nebraska (Lincoln): Nebraska Governance & Technology Center; Thomas Edison Innovation Fellow & Leonardo da Vinci Fellow, George Mason University Antonin Scalia Law School; Visiting Scholar, University of California, Los Angeles School of Law; Registered U.S. patent attorney; J.D., Northwestern University Pritzker School of Law; M.B.A., Northwestern University Kellogg School of Management; LL.M., University of Houston Law Center; Graduate Entrepreneurship Certificate, Stanford Graduate School of Business; M.S. Mechanical Engineering, Stanford University School of Engineering; B.S. Mechanical Engineering, University of Texas at Austin Cockrell School of Engineering.

I am grateful for helpful comments and suggestions from Tejas Narechania, Gus Hurwitz, Deven Desai, Charlotte Tschider, Jeff Kosseff, Alan Rozenshtein, Josephine Wolff, Asaf Lubin, Kaspar Rosager Ludvigsen, Janet Freilich, Camilla Hrdy, Rachel Sachs, Brian L. Frye, Amy Semet, Brian E. Ray, Anjanette Raymond, Abbey Stemler, John Bagby, Gregory Day, Kimberly A. Houser, Janine Hiller, Lawrence J. Trautman, Laura M. Padilla, William J. Aceves, Nancy S. Kim, Kevin Tamm, and Daniel R. Peterson. Additionally, I am thankful for insightful guidance from Vice Admiral Bruce MacDonald, JAGG, USN (Ret.).

Thanks to the following forums for presenting this Article and their participants for insightful comments: Cybersecurity Law & Policy Scholars Conference, Works-In-Progress Intellectual Property (WIPIP) at Santa Clara University School of Law, 2020 Annual Conference of the Academy of Legal Studies in Business (ALSB): Technology Section Colloquium, and Intellectual Property Theory Seminar at University of Kentucky J. David Rosenberg College of Law.

failure and government failure. Along the way, it draws on a property-liability rules theoretical framework to argue that the patent system's invention secrecy restrictions and government patent use are ineffective for national cybersecurity innovation. On a normative level, the interface between government intervention and markets presents innovation mechanisms for national cybersecurity. Turning to prescriptions, expansion of prizes should rapidly promote national cybersecurity innovation, and reciprocal public–private research and development interactions should gradually multiply knowledge spillovers.

I. INTRODUCTION

In 2010, the Stuxnet computer virus caused a sophisticated cyber-attack against a nuclear power plant in Iran.[1] This malicious computer virus Stuxnet, which was found to be conducted with nation-state support, replicated itself in software, proliferated over computer networks, and comprised systems that controlled the country's nuclear program.[2] This high-profile national cybersecurity incident caused concern and is notable because Stuxnet could have been adapted to attack communications and electronic power infrastructure that could cripple the U.S.[3] Following Stuxnet, in 2012, U.S. Secretary of Defense Leon Panetta warned that the U.S. was vulnerable to a "cyber Pearl Harbor" that could derail trains, ruin water supplies, and cripple electricity power grids.[4] In 2013, U.S. officials claimed that Iranian cyber hackers infiltrated the computerized controls of a flood-control dam near New York City through a cellular modem in a retaliatory cyber-attack for the Stuxnet computer virus.[5] This trend of cyber-attacks that impact critical infrastructure has included halting

---

1 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 817, 819–20, 828, 839, 884 (2012) (proposing a new comprehensive legal framework to more effectively address cyber-attacks, which as an example, include one against Iran's nuclear program by the Stuxnet computer worm that was claimed to be tested by the U.S. and Israel).

2 Christopher S. Yoo, *Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures*, *in* CYBER WAR (Jens David Ohlinet et al. eds., 2015); David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM, Mar. 2013, at 49, 50 (describing the malicious computer code's infiltration of Iran's nuclear fuel enrichment program).

3 Carol M. Hayes & Jay P. Kesan, *Law of Cyber War*, INT'L ENCYCLOPEDIA DIGIT. COMMC'N & SOC'Y 1, 12 (2015).

4 SEAN T. LAWSON, CYBERSECURITY DISCOURSE IN THE UNITED STATES 1918, 1953 (Taylor & Francis ed. 2019); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 347.

5 *See* Robert M. Lee, *Protecting Industrial Control System in Critical Infrastructure*, *in* CYBER INSECURITY 31–32 (Rowman & Littlefield ed. 2016) (suggesting that Iranian cyber-attackers, who were sanctioned by the Iranian government targeted U.S. infrastructure in response to the Stuxnet worm launched previously against Iran, attempted to gain access to a 245 feet tall and 800 feet wide dam that could have resulted in deaths of thousands of New York residents, but were stopped by the U.S. intelligence community).

operations of a German steel mill in 2014,[6] leaving thousands without electricity from shut-down utility operations in Ukraine in 2015,[7] and grounding airplanes in Poland in 2015.[8] Nation-states have begun to engage in cyber warfare, and national cybersecurity is an increasing concern and considered the next threat to national security and for critical infrastructure.[9] Computer-induced failures of U.S. power grids, transportation networks, and financial systems could cause massive physical damage, take down the stock exchange and the Internet, and disrupt the nation's economy.[10]

Nation-state warfare, which began on the ground between soldiers and transitioned to ships at sea and planes in the sky, now has shifted to computers and software.[11] Military battles between nations are no longer limited to mechanical, chemical, and nuclear weapons but instead, must consider computer and software weapons that could cripple infrastructure once considered invulnerable to digital attacks.[12] Critical infrastructure, which includes communication systems, electricity grids, and transportation networks, are becoming more complex and reliant on connected devices and data transmission,

---

6 Scott J. Shackelford, *Smart Factories, Dumb Policy?: Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things*, 21 MINN. J.L. SCI. & TECH. 1, 3 (2019).

7 Scott J. Shackelford, Michael Sulmeyer, Amanda N. Craig Deckard, Ben Buchanan et al., *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What To Do About It*, 96 NEB. L. REV. 320, 321, 324–38 (2017); Donghui Park, Julia Summer & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukranian Power Grid Attacks*, HENRY M. JACKSON SCH. INT'L STUDS. (Oct. 11, 2017), https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

8 *Hackers Ground 1,400 Passengers in Attack on Polis Airline LOT (Update)*, PHYS.ORG (June 21, 2015), https://phys.org/news/2015-06-airline-cancels-flights-hacker.html.

9 *See generally* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 100–01 (Harper Collins ed. 2010) (suggesting that cyberwar is the next great threat to national security, which cause power grids and critical systems to shut down).

10 ANDREW F. KREPINEVICH, CYBER WARFARE: A "NUCLEAR OPTION"? 4 (2012).

11 Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 603, 603–04 (2011) (describing the evolving history of war and the recent radical shift to the information age of utilizing emerging computer technologies for military purposes).

12 KREPINEVICH, *supra* note 10, at i–iii, 2–4 (suggesting a major shift in military conflict with expansion into the cyber domain and critical infrastructure more vulnerable to cyber-attacks that would produce catastrophic destruction); U.S. CYBERSPACE SOLARIUM COMM'N, EXECUTIVE SUMMARY i (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (stating that "[a] major cyberattack on the nation's critical infrastructure and economic system would create chaos").

such that vulnerability or failure of a link could result in a devastating chain reaction and debilitate society.[13]

Technological innovation is necessary to foster the development of digital solutions to defend, maintain, and advance critical infrastructure from cyber-attacks and to present new offensive capabilities to keep pace in cyber warfare.[14] Cybersecurity legal and policy scholarship has emphasized the nature and function of government and private-sector actors, the role of regulators, and frameworks for governance and international relations,[15] but technological innovation has been underappreciated and underdeveloped. Surprisingly little meaningful cybersecurity scholarship has addressed the crosscutting realities of technological innovation, yet technology is the underlying force that drives cybersecurity law and policy.[16] Society needs to consider what institution and policy choices can best foster technological innovation to protect critical infrastructure.

National cybersecurity involves tradeoffs with government intervention and market-based incentives for technological innovation, and theoretical reformulation of innovation mechanisms towards this lens is the subject of this Article. The patent system has been considered as supporting the establishment of a market of new technologies by providing incentives for invention, promoting the financing of innovation, and stimulating competition through exclusion. As such, while the patent system is a government-driven mechanism, the market foundation role of patents supports the market development of new technologies.

---

13 *See generally* Michael A. Mullane, *Cyber Attacks Targeting Critical Infrastructure*, IEC E-TECH (Feb. 15, 2019), https://etech.iec.ch/issue/2019-02/cyber-attacks-targeting-critical-infrastructure (stating that cyber-attacks on the critical infrastructure could cut off the supply of electricity to hospitals, homes, schools and factories); Craig Rieger & Milos Manic, *On Critical Infrastructures, Their Security and Resilience*, https://arxiv.org/ftp/arxiv/papers/1812/1812.02710.pdf (suggesting that the critical infrastructure is increasingly interconnected and interdependent).

14 DEF. SCI. BD. TASK FORCE ON COMPUT. SEC., SECURITY CONTROLS FOR COMPUTER SYSTEMS A.1 (1979) (suggesting that security is an increasing concern for military operations); Nat'l Inst. of Standards & Tech., *Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, *in* GUIDELINES FOR SMART GRID CYBERSECURITY ix, xi (2014) (specifying that advancements in information technologies are essential to building a reliable smart grid).

15 Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 431 (2016) (defining cybersecurity as "the protection of information and communication technologies from unauthorized access and attempted access").

16 *See* INT'L TELECOMM. UNION, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY 2 (2008) (providing as a definition: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure that the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment").

The parsing out of the government's need to provide national cybersecurity versus the private market in being able to provide national cybersecurity raises the question as to whether the patent system provides sufficient incentives for national cybersecurity innovation. A variety of innovation mechanisms could promote national cybersecurity innovation, and a comparison of the role of government and the market presents innovation policy considerations for society.

Implicit in this analysis is that the patent system has some role in technological advancement for national cybersecurity. However, inventors and patent holders lack inadequate incentives from the patent system for national cybersecurity inventions, for which the guarantee of the reward is too small, the possibility of the reward is uncertain, or the transaction cost is too high. As a result, the patent system is inadequate to promote national cybersecurity innovation. Such limitations may push some national cybersecurity innovators towards trade secrecy, which presents a different set of problems, including whether and how they can help foster technological advancement to protect the critical infrastructure. The purpose of this Article is to assess how important the patent system is to national cybersecurity. If one unequivocal conclusion follows from this Article in addressing this tradeoff for achieving national cybersecurity, it is that patents may not be a good match when their disclosure is kept secret or when their interests can be taken by government, and technological innovation for critical infrastructure protection can be better oriented through prize funding or a better way to encourage public–private research and development ("R&D").

Innovation mechanisms for technological advancement present unique challenges for national cybersecurity, including market failure, government failure, and co-mingled public–private infrastructure elements. At a theoretical economic level, inventors and innovators will not make investments in national cybersecurity R&D and individuals hope to reap its benefits without contribution to its technology development—a conundrum that warrants government intervention.[17]

In exploring national cybersecurity innovation, this Article highlights and challenges the particularized, traditional conception of national security innovation embedded in the patent system. Among other characteristics, innovation in patent law for the national security context prohibits disclosure on inventions, allows for eminent domain power with government patent use, and protects government from patent infringement causes of action. National cybersecurity innovation, however, should arise from government and private sector collaboration (rather than solely market forces such as through the patent system) and emerge from non-patent incentives. This Article further argues that, notwithstanding patent law's particular conception of innovation, these dynamics often apply as well to technological domains where the innovation produces significant positive externalities beyond the implementing firm (such

---

17 Paul Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership"*, TASK FORCE ON NAT'L SEC. & L. 7, 7–8 (2011).

as for environmental, public health, and public safety). Along these lines, the analysis reveals previously unrecognized benefits of public finance mechanisms, particularly prizes and Cooperative Research and Development Agreements ("CRADAs") for national cybersecurity innovation.

Before proceeding, several terminological notes are in order. First, this Article focuses on "national cybersecurity" rather than "corporate cybersecurity." While it certainly addresses corporate cybersecurity (and the corporate enterprises that seek cybersecurity solutions) and recognizes that interconnectedness of corporate insecurity affects national cybersecurity,[18] its emphasis on national cybersecurity innovation offers a mechanism to serve public objectives. Second, although this Article focuses on "national cybersecurity innovation," it posits no sharp distinction between the field of cybersecurity and the more traditional forms of information security.[19] Indeed, it argues that labels signifying "cyber" and "information" reflect differences of emphasis and degree of new forms of cyber-physical interconnectedness rather than fundamental differences of kind, and therefore, the underlying innovation dynamics are often generalizable across overlapping contexts. Third, this Article uses the term "innovation" rather than the term "invention" to describe the novel creations that serve societal public needs and not solely market needs.[20] Thus, the term "invention" has limited meaning in the national cybersecurity innovation context, other than for technologies subject to the Invention Secrecy Act or subject government patent use and government exemption from patent infringement under 28 U.S.C. § 1498—each of which this Article argues against and considers a particularized, traditional conception.

Turning from the descriptive to the normative and prescriptive, this Article proposes mechanisms for accelerating national cybersecurity innovation. In so doing, it helps fill a significant gap on technological innovation in the cybersecurity literature, for,

> [while] [c]omputers and networks essentially run the critical infrastructures that are vital to our national defense, economic security, and public health and safety, [u]nfortunately, many

---

18 Gabriele Lattanzio & Yue Ma, *Corporate Innovation in the Cyber Age*, 1–3 (SMU Cox Sch. of Bus., Research Paper No.20-04, 2020).

19 *See generally* ROSS ANDERSON, SECURITY ENGINEERING (Wiley ed. 2008) (describing the differences between various forms of security in describing specialized protection mechanisms and how to build systems that stay dependable); Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109, 1113 (2018) (distinguishing between cybersecurity and information security).

20 Traditional patent parlance distinguishes between "invention," which refers to creating a new technology applicable for market need, and of "innovation," which entails the technological development and commercialization processes a technology that could serve broader societal public needs as well. Kim Bhasin, *This Is the Difference Between "Invention" and "Innovation"*, BUS. INSIDER (Apr. 2, 2012, 3:46 PM), https://www.businessinsider.com/this-is-the-difference-between-invention-and-innovation-2012-4 ("If invention is a pebble tossed in the pond, innovation is the rippling effect that the pebble causes.").

> computer systems and networks were not designed with security in mind, [and] as a result, the core of our critical infrastructure is riddled with vulnerabilities that could enable an attacker to disrupt operations or cause damage to these infrastructures.[21]

In drawing upon a rich body of scholarship comparing the relative merits of patents, grants, prizes, R&D tax credits, and other inducement mechanisms to promote national cybersecurity innovation, this Article argues against extending exclusive patent rights to national cybersecurity innovations and applies several economic and theoretical insights for promoting such innovation. It draws upon the theoretical Calabresi–Melamed typology of property rules and liability rules to serve as a guidepost for examining why the patent system inadequately incentivizes national cybersecurity innovation.

The normative vision rooted in this Article for national cybersecurity innovation is that the current patent system is slow and hampers innovation, whereas prizes rapidly place an invention into the public domain without possible significant deadweight losses, and reciprocal public–private R&D interactions in the form of a CRADA can recalibrate the patent bargain. While there are some benefits with other innovation mechanisms—such as basic research at universities, applied research and commercialization non-profit organizations, small business innovation funding, and public subsidies (research grants and tax incentives)—this Article argues that national cybersecurity innovation is best achieved via government intervention through prizes and CRADAs. In particular, it argues that national cybersecurity is a public good and that public funding can quickly promote and steer national cybersecurity innovation, while recognizing biases and information costs raised by public choice theory. In reciprocal fashion, this Article shows that national cybersecurity innovation has much to teach legal scholars and policymakers about accelerating more traditional types of technological innovation. In particular, it argues that innovation policy should focus more on fostering public finance innovation mechanisms for technological areas serving societal public needs (such as national cybersecurity, environmental public health, and public safety) and providing reciprocal public–private enhancing interactions for the rapid development of technologies that co-mingle private and public infrastructure elements.

This Article develops analysis and arguments grounded in theory and proceeds in four parts. Part II summarizes the contours of national cybersecurity technology (including through graphical representations), identifies the problem and need for protection of critical infrastructure, and assesses the problem and need in preparedness of national cybersecurity to defend against cyber-attacks and foster the development of new technologies. Part III turns to theory to serve

---

21 U.S. GEN. ACCT. OFF., TECHNOLOGY ASSESSMENT: CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION (2004), https://www.gao.gov/assets/160/157541.pdf.

as a foundation for delineating the appropriate scope of government invention in the national cybersecurity domain. It explores whether national cybersecurity is a public good in the economic sense and how it compares to a public good in the patent law context to conclude that mischaracterization can lead to government failure or market failure. Moreover, it considers the theoretical Calabresi–Melamed typology of property rules and liability rules to argue against the patent system for incentivizing national cybersecurity innovation. It argues that technological co-mingling of critical infrastructure necessitates integration of public and private inducements for innovation. Part IV draws on theories from Part III to assess normative implications, costs, and benefits of various incentive mechanisms for national cybersecurity development. Turning to prescriptions, it argues that prizes should incentivize rapid cybersecurity development and CRADAs should gradually multiply knowledge spillovers with reciprocal public–private R&D interactions. Part V concludes, including a discussion on innovation policy and on cybersecurity scholarship.

II. CHARACTERIZING CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

Cyber-attacks involve more than theft of corporate information; they can damage or destroy critical infrastructure, which in turn, can lead to a catastrophic shutdown of society. The threat of cyber-attacks against critical infrastructure deserves special attention in cybersecurity scholarship and requires some foundational background, including definitions and descriptions, the problem and need, and the role of innovation mechanisms in creating a state of preparedness or lack thereof.

A. Defining & Describing "National Cybersecurity"

What exactly is "national cybersecurity," or "cybersecurity" for that matter? A part of the challenge of analyzing national cybersecurity (or, in general, cybersecurity) entails defining what that term means and its boundaries. Various definitions abound about the term "cybersecurity," which in isolation can be so capacious as to encompass fields as diverse as corporate cybersecurity, information (data) security, and national security. Scholars have pointed out that there is not a crisp definition of cybersecurity.[22]

---

[22] JEFF KOSSEFF, CYBERSECURITY LAW xxiv–xxv (2020) ("Cybersecurity encompasses all of those subjects [data security, anti-hacking, privacy] and more. . . .and cybersecurity law [consists] of six broad areas of law: private sector data security laws, anti-hacking laws, public–private cybersecurity efforts, government surveillance laws, cybersecurity requirements for government contractors, privacy law"); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works*, J.L. & CYBER WARFARE 1, 5 (2015) (stating "[t]he terms cybersecurity and cyberattack have become broadly used without widespread acceptance as to their exact meaning"); *What Is Cybersecurity and What Does It Mean for You?*, GET SMARTER (Feb. 13,

As Professor Andrea Matwyshyn has noted, legal scholarship and policy has become "cyberized" to the point that the "current rhetoric is so muddled."[23] Professor John Bagby conceptualizes security in the cyber or digital context as connoting "the quality or state of being secure, freedom from danger, fear, or anxiety [which] includes undertakings to guard against various threats," which he states can be termed "computer security, cybersecurity, network security, cloud security, critical infrastructure (security) protections, and national security and the like."[24] Even if there are various definitions, Professor Orin Kerr has noted that "there isn't much clarity about what 'cybersecurity' law actually means" but acknowledges that one set of special issues concerns "government network offense and defense."[25] Professor Jeff Kosseff has determined that not only has legal scholarship not coalesced around a definition for cybersecurity law but that cybersecurity legislation provisions have failed to define cybersecurity.[26] Despite the lack of a uniformly agreed upon definition of "cybersecurity" among cybersecurity law scholars, it does not lessen the fact the technology is at the core of cybersecurity law and policy as Professor Scott Shackelford has noted, stating, "[d]ifficulties stem in part from the rate of technological advancement . . . [and] [i]nformation technology is no exception [since] [n]etworked computers have given tremendous advantages to and exposed vulnerabilities of the cyber power[]."[27] "Technology has raced ahead of both military doctrine and international law."[28]

Rather than offer a categorical definition, this Section contends that the "national" nature of "national cybersecurity" suggests protection that impacts the nation and serves public interest. Thus, the field of cybersecurity represents a continuum, which includes national cybersecurity that serves public interests and corporate cybersecurity that serves private interests. However, national cybersecurity is connected with corporate cybersecurity, since the critical infrastructure occupies the boundary between the private sector's responsibilities

---

2019), https://www.getsmarter.com/blog/career-advice/what-is-cybersecurity-and-what-does-it-mean-for-you/.

23 Matwyshyn, *supra* note 19, at 1114.

24 John W. Bagby, Security Law, Regulation and Public Policy for Accounting Professionals 3–4 (Aug. 11, 2018) (on file with author).

25 Orin Kerr, *What Is "Cybersecurity Law"?*, WASH. POST (May 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/14/what-is-cybersecurity-law/.

26 Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 988 (2018) (stating that "the U.S. legal system lacks a consistent definition of the term 'cybersecurity law' [and that] no scholarship has stepped back to define exactly what 'cybersecurity law' is and the goals of statutes and regulations that aim to promote 'cybersecurity'").

27 SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS xvii (Cambridge Univ. Press 2014).

28 *Id.*

and the government's national security responsibilities.[29] There is a reciprocal security relationship between the public and private sectors that are "inextricably interwoven."[30] Along these lines, corporate cybersecurity is not necessarily incompatible with national cybersecurity since the private sector owns, operates, and maintains approximately 85% of the critical infrastructure (with the remaining 15% owned by the government).[31] Information (data) security refers to the information and communication technologies that underlie any type of cybersecurity.[32] The following Venn diagram provides a taxonomy of these various terms, and the scope of cybersecurity.

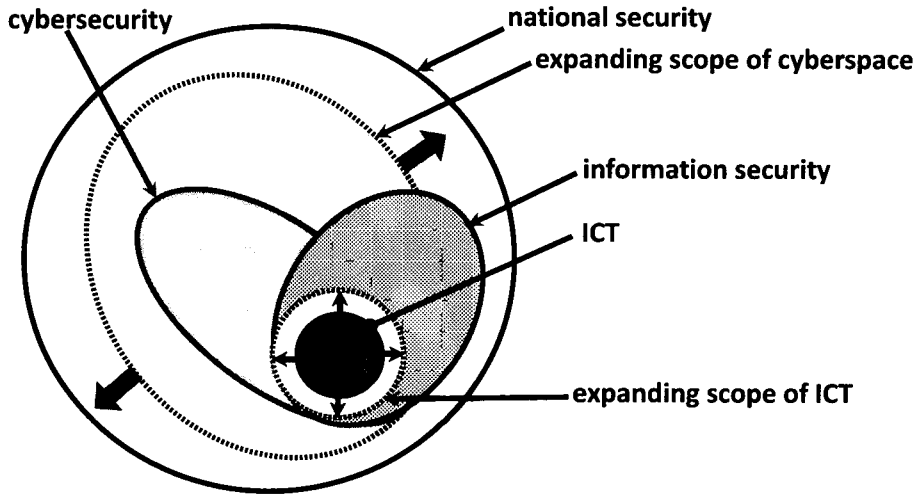

Figure 1: Taxonomy of Security Technologies

This Article characterizes national cybersecurity innovations based on the degree to which they substantially serve the public interest and produce changes in national security. This characterization considers cybersecurity as a subset of national security and information security as being comprised of information and communications technologies ("ICT") which is the underlying technology of cybersecurity. The reciprocal relationship between corporate cybersecurity and national cybersecurity is shown in *Figure 1* graphically as simply "cybersecurity," which comprises both private sector owned

---

29 John W. Bagby, Cyber-Infrastructure Protection Policy: On resolving Ostensibly Intractable Posistions 1, 6 (Jan. 16, 2013) (on file with author).

30 Matwyshyn, *supra* note 19, at 1114, 1116–17, 1119, 1121, 1126–27.

31 Bagby, *supra* note 29, at 4.

32 Kosseff, supra note 26, at 995.

cybersecurity and government owned cybersecurity.[33] As shown by the arrows in *Figure 1*, with an expanding scope of cyber space (including cyber-physical systems[34]) and an expanding scope of ICT (including the Internet of Things, or the IoT[35]), the field of cybersecurity will begin to encompass national security.[36] Lack of cybersecurity is the new national security threat.[37] In sum, *Figure 1* demonstrates that ICT is an increasing part of each of information security, cybersecurity, and national security. Additionally, as cyberspace expands, cybersecurity will become synonymous with national security.

As a result of an expansive scope of corporate (privately-owned) cybersecurity technologies, vulnerabilities in software and the security ecosystem have a reciprocal and inextricably interwoven nature that couples the private sector with the public sector,[38] thereby implicating national cybersecurity. This Article characterizes national cybersecurity based on the degree that it serves critical infrastructure[39] and as being co-mingled of private

---

33 As shown in *Figure 1*, the term "cybersecurity" refers to a broad approach captured by various technologies that enable and promote a protected, reliable, and stable national critical infrastructure. Underlying this graphical representation is the understanding that "national cybersecurity" has both public sector and private sector elements, whereas "corporate cybersecurity" has purely private sector elements. More specifically, the private sector measures in the form of corporate cybersecurity have the potential to impact public sector critical infrastructure in the form of national cybersecurity. In particular, effective corporate cybersecurity can led to stronger national cybersecurity, in part due to the interconnectedness; in turn, corporate cybersecurity affects national security.

34 *See infra* note 78.

35 *See id.*

36 In other words, *Figure 1* demonstrates that national cybersecurity can be conceptualized as an expansive cybersecurity (including expansive corporate cybersecurity), which implicates increasing aspects of national security.

37 J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 Yale L.J. 1020, 1024, 1034 (2020).

38 Johnathan Pincus, Sarah Blakinship & Thomasz Ostwald, *Looking at Information Security Through an Interdisciplinary Lens*, *in* HARBORING DATA 19, 26–27 (Andrea M. Matswyshyn ed., Standford Univ. Press ed. 2009) (describing a vulnerability as "any flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy" and the security ecosystem as "organizations and individuals around the world with a stake in information security: corporations, governments, individual security researchers, information brokers, bot herders, and so on"); Matwyshyn, *supra* note 19, at 1109, 1113–14, 1116–17.

39 42 U.S.C.A. § 5195c(e) (West 2020); BOBBY CHESNEY, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS 81–82 (2020) (ebook) (characterizing critical infrastructure as "provid[ing] the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health . . . [known] as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family." Further listing distinct sectors of critical infrastructure as being: chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, emergency

and public sectors elements.[40] The interplay between national cybersecurity's private sector and public sector stems from the characteristics of ICT.[41] Characterizing national cybersecurity in this manner helps to show the interconnected nature of the private–public sectors that are necessary for innovation applicable for critical infrastructure.

1. Securing the Critical Infrastructure

This Article characterizes national cybersecurity innovations based on the degree to which they substantively serve critical infrastructure and produce changes in the level of security from cyber-attacks. Innovations that are intertwined with critical infrastructure impact modern business practice and national security.[42] This sense of technological security of national cybersecurity is not a dichotomy of security or insecurity alone, but instead it is a sliding scale and spectrum with a range of level of security.[43] Moreover, there are varied types critical infrastructure, which are regulated differently and present a continuum of systemic vulnerability to cyber-attacks.[44] Even with a sliding scale of technological security and a continuum of critical infrastructure, a common theme in achieving national cybersecurity is to attain information assurance with network defense.[45] Thus, national cybersecurity technologies promote links and network effects among computer systems that distribute data and share information among multiple dimensions of critical infrastructure. These effects have private sector and public sector elements.

First, national cybersecurity inventions can be secure (or insecure) through links between software, devices, and the nation's critical infrastructure.[46]

---

services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear reactors/materials/waste sector, transportation systems sector, water and wastewater systems sector).

40 Matwyshyn, *supra* note 19, at 1121.

41 *See* Melissa E. Hathaway & Alexander Klimburg, *Preliminary Considerations: On National Cyber Security*, *in* NATIONAL CYBER SECURITY FRAMEWORK MANUAL 1, 1–2 (Alexander Klimburg ed., 2012).

42 John Bagby & David Reitter, Anticipatory FinTech Regulation: On Deploying Big Data Analytics to Predict the Direction, Impact and Control of Financial Technology (Oct. 1, 2019) (available at https://ssrn.com/abstract=3456844).

43 Lee, *supra* note 5, at 33–34.

44 Bagby, *supra* note 29, at 1–2.

45 Trey Herr & Eric Ormes, *Understanding Information Assurance*, 10 AM. FOREIGN POL'Y COUNCIL, Apr. 2015, at 1.

46 *Cyber Attacks on Critical Infrastructure*, ALLIANZ GLOB. CORP. & SPECIALTY, https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html (last visited Oct. 11, 2020) (specifying that "critical infrastructure . . . is becoming more complex and reliant on networks of connected devices" and that "everyday devices

National cybersecurity technologies have a direct or indirect impact on physical hardware, equipment, devices, and software of critical infrastructure. Such technologies provide security in relation to authentication, covertness, and fault tolerance through security linking mechanisms through access controls, ciphers, and hardware tamper-resistance.[47] Digitization provides links between the physical and cyber worlds, such that the critical infrastructure is exposed to physical attacks or cyber-attacks.[48] Connectivity, control, and prevention of attack onto vulnerabilities of critical infrastructure are important in characterizing a national cybersecurity innovation as being secure. In general, the primary motivation of national cybersecurity innovation is to secure the fundamental facilities and systems of our critical infrastructure that serve the country and are necessary for the operation of the economy.[49] This is a complicated inquiry, however, because critical infrastructure is composed of public and private physical improvements, and this co-mingling necessitates a closer inspection of innovation policy that fosters the development of technology to provide greater national cybersecurity.[50] Critical infrastructure is composed of inter-connected government services and a large private sector system, such that interdependencies stress the role of cybersecurity in nearly all aspects.[51] As a general matter, however, as Professor Bagby has noted, "critical infrastructure [protection] stubbornly occupies the boundary between the private-sector's responsibilities and national security realms [and] private sector risks are often insurable but national security risks are frequently framed as tantamount to risking cataclysmic failure."[52] National cybersecurity innovation aims to create national security value rather than market value.

Second, national cybersecurity technologies can be secure (or insecure) in that they enhance public safety through thwarting deleterious network effects. Threats in data emerging from the cloud, mobile/wireless, and other computer systems can transmit vulnerabilities through a variety of data center, routers, and

---

embedded with electronics that collect information and connect to a network . . . could create a perfect cyber security storm").

47 ANDERSON, *supra* note 19, at 4.

48 Yagnyasenee Sen Gupta & Shyamapada Mukherjee, *A Survey on Security Issues in Cyber-Physical Systems*, PROCS. INT'L CONF. ON COMPUTATIONAL INTEL. & IoT 137, 137–38 (2018) (describing how links between cyber and physical elements can be provided by actuators and sensors with communications and software capabilities, and that "physical attacks are the ones that tamper physical elements" and "cyber-attacks are the ones whose deployment takes place through software, malware or accessing the communication network in an unauthorized way and thereby tampering the transmitting data").

49 *See* sources cited *supra* note 39.

50 Bagby, *supra* note 29, at 4; Herr & Ormes, *supra* note 45, at 9.

51 PETER SOMMER & IAN BROWN, REDUCING SYSTEMIC CYBERSECURITY RISK 23 (2011), https://www.oecd.org/gov/risk/46889922.pdf.

52 Bagby, *supra* note 29, at 6.

hosts. Such is the case with other interconnected computing approaches that rely on security to prevent, detect, mitigate, or restore threats and attacks in data before spreading to the computing system. National cybersecurity is akin to a chain, such that it is only as strong as the weakest link, and a vulnerability on the weakest link can spread through communication in networks. Cyberattacks against networks can be against vulnerabilities in network protocols, on local networks use Internet protocols, or use malicious code but can be defended against by filtering and firewalls, intrusion detection, and encryption.[53] Similarly, classic data (information) security innovation suggests that threats to physical facilities of the critical infrastructure occur through random and unauthorized access to that data and among interconnection of networked devices and systems.[54] Two-way information communication and network effects presents risks to critical infrastructure.[55] Along similar lines as the impact on security via interconnections between external features with critical infrastructure, vulnerabilities and security breaches can be multiplied via network effects. Vulnerabilities in software can impact an entire ecosystem,[56] and leakage points in hardware, software, and communication can exacerbate vulnerabilities.[57] The result is that network effects of insecurity can result in co-mingled, or public and private, elements.[58] The impact to critical infrastructure for public and national security interests, however, helps distinguish such innovation from other ICT that may only enhance corporate cybersecurity.

National cybersecurity technologies prevent adversaries from producing harm (whether intentionally or otherwise) via access, attack, exploit, exposure, threats, and vulnerability to protect the sovereignty of the state, and its assets,

---

53 ANDERSON, *supra* note 47, at 636, 638, 644, 652.

54 Michael E. Whitman & Herbert J. Mattord, *Introduction to Information Security*, *in* PRINCIPLES OF INFORMATION SECURITY 6, 6–7 (2012).

55 Nat'l Inst. of Standards & Tech., *supra* note 14, at 1–2 (specifying that additional risks include: "[i]nterconnected networks [that] introduce common vulnerabilities"; "communication disruptions and the introduction of malicious software/firmware or compromised hardware" that results in malicious attacks; "[i]ncreased number of entry points and paths available for potential adversaries to exploit"; "interconnected systems [that] increase the amount of private information exposed and increase the risk when data is aggregated"; and "expansion of the amount of data that will be collected that can lead to the potential for compromise of data confidentiality").

56 *See* sources cited *supra* note 38.

57 DEF. SCI. BD. TASK FORCE ON COMPUT. SEC., *supra* note 14, at 7–8 (defining hardware leakage points as "hardware portions of the systems [that] are subject to malfunctions that can result directly in a leak or cause a failure of security protection mechanisms elsewhere in the system, including a software malfunction"; defining software leakage points as "all vulnerabilities directly related to the software in the computer system"; defining communication leakage point as "the communications linking the central processor, the switching center and the remote terminals").

58 *See infra* Section III.B.1.

resources, and people.[59] These characteristics present links and network effects that present private sector and public sector dimensions of critical infrastructure that necessitate a closer inspection of the technologies for its protection and the concomitant evolution of critical infrastructure.[60]

2. Mapping of Critical Infrastructure with Technological Innovation

Perhaps the best way to elucidate national cybersecurity innovation is by discussing specific examples. Representative examples to defend against cyber-attacks illustrate the "security" nature of such innovation and provide a basis for comparison with other cybersecurity innovation. The highly interconnected nature of the public and private sector elements demands a significant degree of contextual innovation policy to foster development of such innovations.[61]

Furthermore, national cybersecurity innovation is both similar to and different from other forms of corporate forms of cybersecurity. In corporate domains, cybersecurity is critical for identity theft prevention, protection of consumer data, and preventing corporate information leakage and data breaches.[62] For example, Professor Matwyshyn has described the importance of corporate cybersecurity to businesses by stating that, "[i]n the broader business context, the business environment in our society has been dramatically altered by the integration of information technology into corporate governance and operations over the last two decades. Businesses have become progressively more technology-centric and, consequently, organized in large part around their unifying computer systems."[63] National cybersecurity innovations are different in that they protect industrial control systems in critical infrastructure. In this sense, the motivations of national cybersecurity development are more akin to environmental innovation and public health innovation, where advancements serve public interests in order to benefit society broadly rather than solely market based objectives. As will be shown, however, innovators can seldom develop national cybersecurity innovation in isolation. Instead, the highly interconnected nature between corporate cybersecurity and national cybersecurity leads to effective national security.

In exploring national cybersecurity, it is useful to provide a representative mapping for the current analysis. Although there are many axes upon which to order national cybersecurity innovations, two are particularly useful. The first is the degree to which a technology is connected with a public-owned (government-owned) versus private-sector-owned part of the critical

---

59 *See* Whitman & Mattord, *supra* note 54, at 8–11.

60 *See supra* Section II.A.1.

61 *See infra* Part IV.

62 *See generally* HARBORING DATA, *supra* note 38.

63 Andrea M. Matswyshyn, *Introduction* to HARBORING DATA, *supra* note 38.

infrastructure. National cybersecurity innovations run the gamut from large infrastructures, such as dams and electricity grids that are owned by government, to privately-owned technologies that interface with such public infrastructure.[64] The second is the degree to which a national cybersecurity innovation is oriented towards cyberspace versus the degree to which it exists in the tangible, physical world. At one end of this spectrum are data-centric or information technological innovations that reside in software and do not directly address the physical world, and at the other end of this spectrum are tangible and physical devices.

The distinctions in this representative mapping matter, since there has been and continues to be a historical technological shift in protection of critical infrastructure,[65] which is demonstrated in figures that characterize critical infrastructure in response to national cybersecurity innovation. The representative mapping shown in the ensuing figures influences how law and innovation policy should evolve, according this Article's prescriptions.[66]

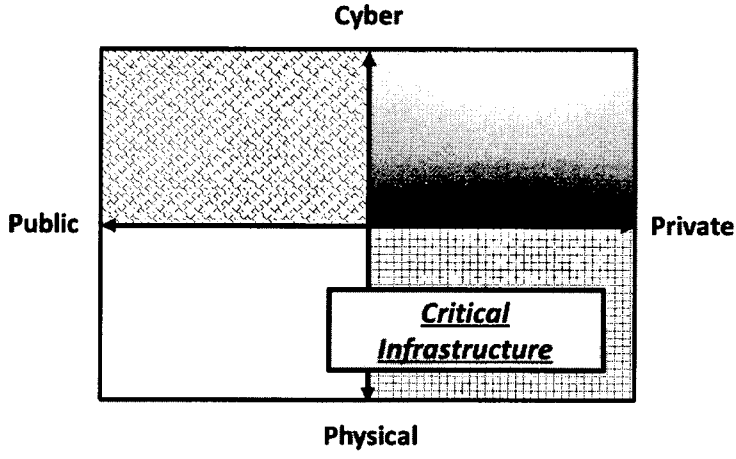

Figure 2.A: Representative mapping of the traditional view of critical infrastructure

64 *See generally* U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE AND KEY ASSETS vii, xii, 35–70 (2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

65 *See generally* U.S. DEP'T OF HOMELAND SEC., BUDGET-IN-BRIEF FISCAL YEAR 2021, 49–54 (2020), https://www.dhs.gov/sites/default/files/publications/fy_2021_dhs_bib_web_version.pdf (showing a budgetary shift in priority by the U.S. government towards the critical infrastructure).

66 *See infra* Part IV.

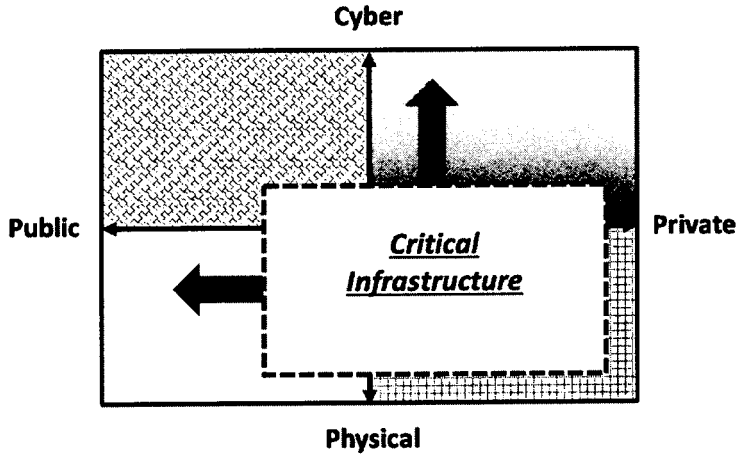

Figure 2.B: Representative mapping of the evolving view of critical infrastructure coincident with national cybersecurity innovation

These figures reflect many of the characteristics of national cybersecurity and their impact on critical infrastructure. They address technological innovation of ICT that protects critical infrastructure.[67] The nature of the critical infrastructure which is susceptible to cyber-attacks[68] is affected by innovation in interconnected hardware and software,[69] with the effect that public-owned (government-owned) elements are increasingly connected to cyber technologies through data. And while it is difficult to quantify the degree of this change, it is fair to say it is largely motivated by advances in information and communication technologies that detect, prevent, and mitigate cyber risk.[70] Furthermore, these cyber innovations, which are being developed and deployed by the private sector, increasingly interconnect and link with public-owned (government-owned) elements of the critical infrastructure.[71]

These innovations impact national cybersecurity in that they increasingly cause critical infrastructure to be exposed to cyber-attack.[72] This is

---

67 *See generally* Finnemore & Hollis, *supra* note 15.

68 *See generally* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429 (2012).

69 DEF. SCI. BD. TASK FORCE ON COMPUT. SEC., *supra* note 14, at 3–4.

70 NATIONAL CYBER SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 9 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

71 *See generally* Rieger & Manic, *supra* note 13 (describing the increasing interdependencies and interconnectedness of the national critical infrastructure).

72 U.S. DEP'T OF HOMELAND SEC., CYBER RISK ECONOMICS CAPABILITY GAPS RESEARCH STRATEGY 2 (2018), https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf.

a vibrant, incredibly valuable area of technological innovation, and yet as is shown, it proceeds more quickly and efficiently outside of the patent system.[73] Indeed, the reality of national cybersecurity helps illustrate a narrow and highly particularized conception of innovation embedded in patent law for national security that runs counter the incentive-laden goals of the patent system, a unique phenomenon that the next Part explores further from a theoretical lens.[74] Of course, to say that national cybersecurity innovation is hampered by deficiencies in the patent system for national security is not to say that all national cybersecurity innovation should proceed outside of the patent system. Patents and the market system are a robust source of corporate cybersecurity, and national cybersecurity melds some corporate cybersecurity with public-owned (government-owned) elements of critical infrastructure through cyber advancements in new technologies. This represents an innovative twist on empowering innovators through government intervention on national cybersecurity innovation policy.[75]

A few, modern-day and developing technological examples reflect many of the characteristics of national cybersecurity innovations. These technologies have different attributes and definitions yet share a common characteristic of ensuring security through interconnections between data and devices.[76] These examples all address substantive national cybersecurity, ranging from

---

73 *See infra* Part III and Part IV.

74 *See infra* Part III.

75 *See infra* Part IV.

76 *See* Christian Reuter, Larissa Aldehoff, Thea Riebe & Marc-André Kaufhold, *IT in Peace, Conflict, and Security Research*, *in* INFORMATION TECHNOLOGY FOR PEACE AND SECURITY 22–24 (Christian Reuter ed., 2019).

cryptography,[77] cyber-physical systems,[78] IoT,[79] information security,[80] and the SmartGrid.[81] A rich technological literature had demonstrated that these new

---

[77] Cryptography refers to embeddable technology that secures information storage, communication, and transactions through concealment or extraction of concealed information. *See generally* Greg Vetter, *Information Security and Patents*, *in* HARBORING DATA, *supra* note 38, at 64, 77, 79 (defining cryptography as "a versatile, foundation technology with wide applicability [and one that] can hide information in data or implement secure communication" by the use of a key that serves a translation function); Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 762 (2010) (defining cryptography as "us[ing] a key to convert plaintext to ciphertext and to reverse the operation when necessary" for the purpose being to "keep everyone else from accessing the protected data"); *Cryptography*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/web/patents/classification/uspc380/defs380.htm (last visited Oct. 11, 2020) (describing that this class of technologies includes "equipment and processes which (a) conceal or obscure intelligible information by transforming such information so as to make the information unintelligible to a casual or unauthorized recipient, or (b) extract intelligible information form such a concealed representation, including breaking down of unknown codes and messages").

[78] Cyber-physical systems refer to elements that link between the cyber and physical world and impact security, integrity, and/or privacy of the information of devices and impact critical infrastructure. *See generally* NAT'L INST. OF STANDARDS & TECH., STRATEGIC R&D OPPORTUNITIES FOR 21ST CENTURY CYBER-PHYSICAL SYSTEMS 5 (2013), https://storage.ey.md/Technology%20Related/PDFs%20and%20Books/Foundations%20for%20Innovation%20Strategic%20R%26D%20Opportunities%20for%2021st%20Century%20Cyber-Physical%20Systems.pdf (providing as examples of cyber-physical systems as being active monitoring and control systems, smart grids for water and wastewater, and early warning systems; providing as corresponding innovative products or applications as being bridges and dams and municipal water and wastewater treatment); Gupta & Mukherjee, *supra* note 48, at 138 (suggesting that cyber-physical systems' elements are actuators and sensors with communication or software capabilities; providing as examples pertaining to infrastructure as being smart grids, industrial control systems, intelligent transportation); Amy J. C. Trappey, Charles V. Trappey, Usharani Hareesh Govindarajan, John J. Sun et. al., *A Review of Technology Standards and Patent Portfolios for Enabling Cyber-Physical Systems in Advanced Manufacturing*, 4 IEEE ACCESS 7356 (2016) (defining cyber-physical systems as "a collection of transformative technologies for managing interconnected physical and computational capabilities," through "sensors, data acquisition systems, and computer networks"); Florian Ernst & Patrick Frische, Industry 4.0/Industrial Internet of Things–Related Technologies and Requirements for a Successful Digital Transformation: An Investigation of Manufacturing Businesses Worldwide 8 (2015) (M.S. thesis, University of Strathclyde), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698137 (stating cyber-physical systems are a "combination of IT with mechanical and electronic components connected to online networks that allow machine-to-machine communication in a similar way to social networks").

[79] IoT refers to interconnected devices networked together with computers for data collection and exchange, and more specifically Industrial IoT refers to IoT applied to industrial uses. *See generally* IGOR MIKOLIC-TORREIRA, RYAN HENRY, DON SNYDER, SINA BEAGHLEY ET. AL., A FRAMEWORK FOR EXPLORING CYBERSECURITY POLICY OPTIONS xii (2016); SANDRA WACHTER, NORMATIVE CHALLENGES OF IDENTIFICATION IN THE INTERNET OF THINGS (Elsevier Ltd. ed. 2018) (defining the IoT as "objects [that] can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet," and furthermore, "objects embedded with RFID tags, allowing for unique identification and monitoring of object movement and consumption"); Adam

national cybersecurity innovations are utilized in applications such as Industrial Control Systems ("ICS")[82] and Supervisory Control and Data Acquisition ("SCADA"),[83] which interact with critical infrastructure. The biggest challenges towards ensuring critical infrastructure include fostering national cybersecurity innovation and integrating the resulting advanced technologies into the critical infrastructure.[84]

Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, RICHMOND J.L. & TECH. 8 (2015) (describing the IoT as being machine-to-machine connectivity and communication that enables computers to observe, identify, and understand the world without limitations of human-entered data and increasingly through wireless technologies and protocols; further quoting Morrision Foerster analysts as defining the IoT as "the network of everyday physical objects which surround us and that are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings"); William H. Dutton, The Internet of Things 8–11 (2013) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324902; Ernst & Frische, *supra* note 78, at 11 (referring to the Industrial IoT as "connect[ing] the physical world with the virtual world" for industrial transformation of power distribution, manufacturing, wind, rail, mining, oil and gas, power generation).

80 Information security is a broad term that refers to securing hardware, software, and physical locations from threats. *See generally* Whitman & Mattord, *supra* note 54, at n.3.

81 The SmartGrid refers to modernization of the electricity grid with computer hardware and software. *See generally* 42 U.S.C.A. § 17381 (West 2020) (characterizing the Smart Grid as having "increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid"); NAT'L INST. OF STANDARDS & TECH., *supra* note 14, at 4 (describing the smart grid as involving electricity infrastructure that is characterized by "(1) increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid. (2) dynamic optimization of grid operations and resources"); Joel B. Eisen, *An Open Access Distribution Tariff: Removing Barriers to Innovation on the Smart Grid*, 61 UCLA L. REV. 1712, 1719, 1721 (2014) (suggesting that the Smart Grid "consist[s] of improvements to the old [electricity] infrastructure, such as deployment of smart meters and digital technology across the existing network"; also suggesting that "data gathered by smart meters may well create a 'big data' ecosystem").

82 KEITH STOUFFER, SUZANNE LIGHTMAN, VICTORIA PILLITTERI, MARSHALL ABRAMS ET AL., NAT'L INST. STANDARDS & TECH., UNITED STATES DEPARTMENT OF COMMERCE, SPECIAL PUB. NO. 800–82 REV. 2, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY 1, 1 (2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (stating that "ICS are found in many industries such as electric, water and wastewater, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverage, automotive, aerospace, and durable goods" and includes SCADA systems).

83 U.S. DEP'T OF ENERGY, 21 STEPS TO IMPROVE CYBER SECURITY OF SCADA NETWORKS 2 (2005), https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (describing SCADA networks as "contain[ing] computers and applications that perform key functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste treatment, transportation) [and are] potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure).

84 Lee, *supra* note 5.

B. The Problem, The Need, & Preparedness

National cybersecurity is one of the most pressing domestic policy issues in the U.S. today.[85] While the new coronavirus has caused a crisis, a malicious cyber-attack could cause the next crisis—one that would spread faster than a biological virus and with greater economic impact.[86] The U.S. has come to recognize that cyber-insecurity could cripple the nation's security, economic structure, public health and safety, or any combination thereof.[87] The U.S. is dangerously cyber insecure and is facing a catastrophic cyber-attack that requires greater investment preparation.[88] The economic impact of cyber-attacks is about 6% of the U.S. GDP, or over $ 1 trillion dollars.[89] Cyber-attacks against critical infrastructure would result in high damage to the U.S. economy and generate spillovers to the wider economy.[90] Without adequate national cybersecurity, connected devices, communication networks, and electricity grids are vulnerable to being hacked at an unprecedented scale.[91]

---

85 RAUL KIKK, NATIONAL CYBER SECURITY INDEX (2018), https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf; NATIONAL CYBER SECURITY FRAMEWORK MANUAL (Alexander Klimburg ed., 2012); Klon Kitchen, *A Major Threat to Our Economy—Three Cyber Trends the U.S. Must Address To Protect Itself*, HERITAGE FOUND. (Oct. 2, 2019), https://www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect.

86 This includes widespread disruption, fundamental shifts in the way we live our lives, an extremely challenging recovery ahead, and a growing uncertainty about the stability of the U.S. economy from the shutdown. Most readers may think the most likely cause of the crisis that fits this description would be COVID-19. Instead, prior to the start of 2020, many policymakers would have considered the cause to be a cybersecurity incident. While the new coronavirus has caused a crisis, a malicious cyberattack could cause the next crisis—one that would spread faster than a biological virus and with greater economic impact.

87 Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. STATE U. L. REV. 515, 519 (2017); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 215 J.L., TECH. & POL'Y 341, 345, 349 (2015) (specifying "grave danger and potential consequences of cyberattack[s]" and noting that there are "many entry points for attackers to find vulnerabilities" such that there is "an arms race between attackers and defenders").

88 U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 12.

89 JOHN GILLIGAN, AFCEA INT'L CYBER COMM., THE ECONOMICS OF CYBERSECURITY 1 (2013), https://www.afcea.org/committees/cyber/documents/cybereconfinal.pdf.

90 COUNCIL OF ECON. ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

91 PUB. SAFETY CANADA, NATIONAL CYBER SECURITY STRATEGY: CANADA'S VISION FOR SECURITY AND PROSPERITY IN THE DIGITAL AGE 15, 18 (2018), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

Cyber-attacks are inevitable.[92] Cyber-risk is considered a major concern for society and is getting exponentially worse.[93] Resilient cybersecurity would thwart bad actors from unlawfully and maliciously disabling, intruding on, or otherwise impeding the use of computers and networks that protect cyber-based and physical assets of critical infrastructure.[94] However, underinvestment in cybersecurity technology has made U.S. critical infrastructure woefully cyber-insecure.[95] Cybersecurity of the software, hardware, and the cloud that is

---

92 KARINE BANNELIER & THEODORE CHRISTAKIS, CYBER-ATTACKS 7 (2017) (defining cyber-attacks as "malicious acts against, *inter alia*, vital infrastructure of [the United] States [that] threaten[s] critical infrastructure"); CHESNEY, *supra* note 39, at 3 (describing a cyber-attack as "using cyber capabilities directly to disrupt the capabilities an adversary would need [through] access, disrupt[ion], manipulate[ion], or damage [to] a system in an unauthorized way"); SHACKELFORD, *supra* note 27, at xix (stating that "[a] serious cyber attack may disrupt critical networks, damage 'military command or information systems,' and interrupt 'electrical power . . . or . . . financial services.' Or, in a worst-case scenario, cyber attacks could trigger satellites to spin out of control, power grids to crash, economies to collapse, and societies—deprived of basic services—to begin to self-destruct"); Dan Assaf, *Government Intervention in Information Infrastructure Protection*, *in* CRITICAL INFRASTRUCTURE PROTECTION 31, 34 (E. Goetz & S. Shenio, eds., 2008) (describing the use of information warfare through the application of information technology having a debilitating impact on a power grid or a communication network, such that a disruption leads to cascading failures, which would lead to a failure of practically every critical infrastructure due to cyber-interdependency of an infrastructure's operability relying on its information systems); Matwyshyn, *supra* note 19, at 1121–23 (giving as an example of a cyber-attack being the use of malware to "compromis[e] networks of personal computers, consumer smartphone, and even Internet of Things (IoT) webcams [that] can easily be remotely repurposed for attacking critical national assets such as stock exchanges, dams, or power grids [and] vulnerable critical infrastructure systems [such as] smart grids, power and water stations, air traffic control systems, and other communication systems, health systems, and nuclear power plants—all blend private and public-sector elements").

93 Jay P. Kesan & Linfeng Zhang, *Analysis of Cyber Incident Categories Based on Losses*, ACM TRANS. MANAG. INFORM. SYST. (forthcoming 2020).

94 Critical Infrastructures Protection Act of 2001, 42 U.S.C.A. § 5195c(e) (West 2020) (defining critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"); CHESNEY, *supra* note 39, at 81–82 (characterizing critical infrastructure "provid[ing] the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health . . . [known] as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family"; further listing distinct sectors of critical infrastructure as being: chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear reactors/materials/waste sector, transportation systems sector, water and wastewater systems sector).

95 RICHARD HARRISON & TREY HERR, CYBER INSECURITY (2016); INT'L TELECOMM. UNION, *supra* note 16 ("Cybersecurity is the collection of tools, policies, security concepts, security

connected to networks requires research and development of defensive countermeasures.[96] The nation should not fall victim to being caught off guard by another threat that could cause a severe crisis, and one response is to foster the development of adequate national cybersecurity of critical infrastructure.[97]

The U.S. critical infrastructure and computer networks have been built with vulnerable technologies designed with easy access—whether licit or illicit—that are in need of improvement. Cybersecurity forms the backbone of the information age and technological improvements, including developing better products, reducing the porous structure and vulnerabilities of unsecured network systems, replacing legal systems, and improving reliability.[98] Existing national cybersecurity technologies may be limited or not working and render critical infrastructure vulnerable to attack.[99] Cyber-attackers are constantly devising new technologies for launching cyber-attacks.[100] The U.S. struggles to address the changing character of cyber threats, lacks a clear cybersecurity response mechanism, and faces gaps in cyber deterrence of new technological

---

safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure that the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."); U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 12; Finnemore, *supra* note 15, at 431 (defining cybersecurity as "the protection of information and communication technologies from unauthorized access and attempted access"); Barrie Sander, *Cyber Insecurity and The Politics of International Law*, 6 ESIL REFLECTIONS 1, 1, 8 (2017).

96 I define "cybersecurity" throughout this Article as encompassing technology, such as information and communication technology, that permits resilience of critical infrastructure and a state of being secure from cyber-attacks. In other words, "cybersecurity" means "cybersecurity technology" for the purposes of this Article, which focuses on "national cybersecurity" (not solely "corporate cybersecurity"). For a discussion that is solely on "corporate cybersecurity," see generally HARBORING DATA, *supra* note 38.

97 I define "national cybersecurity" as cybersecurity applicable for critical infrastructure. Given that the choice of governing arrangement—whether a government provision, private provision, or any combination thereof—is essential to ensuring critical infrastructure protection, a distinction between "national cybersecurity" and "corporate cybersecurity" is warranted and acknowledges the reasons for the ability of the private sector to provide adequate incentives for technological innovation to protect against cyber-attacks. *See generally* Matwyshyn, *supra* note 19, at 1113, 1119, 1120–23 (differentiating corporate cybersecurity and national cybersecurity, but recognizing that they are reciprocal and inextricably interwoven).

98 Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1503 (2013).

99 JOHN R. VACCA, CYBER SECURITY AND IT INFRASTRUCTURE PROTECTION 121 (Elsevier Science 2013).

100 SCOTT A. WEED, U.S. POLICY RESPONSE TO CYBER ATTACK ON SCADA SYSTEMS SUPPORTING CRITICAL NATIONAL INFRASTRUCTURE 11 (2017), https://media.defense.gov/2017/Nov/20/2001846609/-1/-1/0/CPP0007_WEED_SCADA.PDF.

development.[101] In order to respond to technological advances being developed by adversaries, the U.S. should proactively develop and incorporate breakthrough and incremental national cybersecurity technologies to protect its critical infrastructure.[102] There is a national need for innovation and evolution of cybersecurity technological capabilities,[103] which are a porous structure of legacy and unsecured systems.

Cyber-attacks have risen exponentially in recent decades and have impacted the critical infrastructure, producing devastating effects on society.[104] Increased data connectivity, quick expansion of cyber-physical systems, and the on-going development of artificial intelligence and new technologies in the cybersecurity field have all contributed to an increased frequency and magnitude of cyber-attacks.[105] These same forces are predicted to erupt in the foreseeable future with potentially catastrophic effects on critical infrastructure.[106] The Department of Homeland Security has estimated that in the short run a cyber-attack is likely to result in catastrophic damage to industrial control systems, which would jeopardize electricity, energy, transportation, and water networks.[107]

Against this backdrop, national cybersecurity systems are faced with insurmountable challenges in anticipating and proactively addressing future cyber-attacks with preparedness.[108] Chief among these challenges is the fact that

---

101 U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 12, at 14, 17, 27–28, 36–39, 71, 75, 82, 84, 88.

102 DIV. OF NAT'L INTEL., NATIONAL INTELLIGENCE STRATEGY OF THE UNITED STATES 5, 21 (2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf; Mullane, *supra* note 13 (suggesting that cyber-attacks targeting critical infrastructure would jeopardize transport systems, supply of fresh water, communications, banking, power plants, national railway and local underground systems, other forms of public transport, and electricity to hospitals, homes, schools and factories).

103 NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 20 (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; James Kaplan, Chris Toomey & Adam Tyra, *Critical Resilience: Adapting Infrastructure To Repel Cyberthreats*, MCKINSEY & CO. (Jan. 15, 2019), https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/critical-resilience-adapting-infrastructure-to-repel-cyberthreats#.

104 U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY STRATEGY 2 (2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

105 Tabrez Y. Ebrahim, *Artificial Intelligence in Cyber Peace in* CYBER PEACE: CHARTING A PATH TOWARDS A SUSTAINABLE, STABLE, AND SECURE CYBERSPACE (Cambridge Univ. Press) (forthcoming 2021).

106 Rebecca Moore, *Expansion of Technology Will Increase Cyber Security Threats*, PLANSPONSOR (Feb. 15, 2019), https://www.plansponsor.com/expansion-technology-will-increase-cyber-security-threats/.

107 WEED, *supra* note 100, at 3–7.

108 COMM'N ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY 2–3 (2016),

cyber-attacks remain inherently unpredictable, and the U.S. is cyber-insecure and underprepared to respond to upcoming cyber-attacks.[109] One strategy to help reduce the severity and scale of advanced persistent threats and their impact on the cyber-physical system is centered on innovation mechanisms for the development of national cybersecurity to provide information assurance, vulnerability management, and critical infrastructure protection.[110] Innovation policy should promote and direct R&D of national cybersecurity towards architecture, defense, intelligence, and offense measures in computing and information technologies. In some cases, national cybersecurity measures are urgently necessary, and in other cases, they are needed as soon as possible. However, national cybersecurity development in this context faces hurdles that vastly surpass the unpredictability of cyber-attacks and insufficient level of R&D.

When approached through a specific lens (such as in the case of this Article, which focuses on innovation mechanisms), the development of national cybersecurity innovation necessitates fostering targeted technological development. Such innovation can occur through government-oriented and market-oriented approaches,[111] as well as at different paces.[112] A more appropriate calibration of innovation policy is critically needed for national cybersecurity, and a failure to do so may come at a heavy cost for society.

This Article thus advocates for an expanded focus on the multifaceted roles of innovation mechanisms in national cybersecurity development to better suit the critical infrastructure needs that are prone to cyber-attacks. While providing a theoretical foundation based on public–private goods[113] and on property-liability rules,[114] this Article seeks to describe innovation mechanisms and their role in national cybersecurity preparedness.[115]

---

https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

109 Hathaway & Klimburg, *supra* note 41, at 4, 8.

110 DIV. OF NAT'L INTEL., *supra* note 102.

111 *See infra* Part III.

112 For example, short term objectives could prompt incentives to fix security in software code that may address immediate vulnerabilities; long term objectives could prompt incentive to develop integration among cyber and physical system to enable resilience, safety, and scalability, as well as integration of artificial intelligence and new technologies, to prevent gradual or catastrophic destruction.

Given multiple paces of technological development necessary to protect critical infrastructure against cyber-attack, innovation mechanisms may play another role, with licensing of technology. Thus, innovation mechanisms may have effects on multiple time horizons and multiple ways in which they can shape a response to national cybersecurity development to protect against cyber-attacks and point to different paths forward.

113 *See infra* Section III.A.1.

114 *See infra* Section III.A.2.

115 *See infra* Part IV.

III. THEORETICAL FOUNDATIONS

A theoretical foundation to national cybersecurity innovation seeks to align legal incentives and innovation inducement mechanisms with socially optimal level of security for critical infrastructure. National cybersecurity innovation requires establishing whether government intervention or the market should foster its technological development.[116] But conflicts have to be resolved between the society's interest in cybersecurity as a public good and the individual interests of inventors and innovators.

National cybersecurity's biggest problem stems from a policy failure to balance market-based incentives with government intervention, and society must consider that, "given the significance of the private sector in [national cybersecurity] settings, structuring incentives properly is critical [and] the benefits of any government intervention must be weighed against the costs of ineffective or excessively costly interventions."[117] The core problem is that protection of the critical infrastructure should benefit all, but the government must rely on the private sector to provide national cybersecurity, even though it has little incentive to do so. As such, determining whether and to what level national cybersecurity can be considered a public good and how the law can influence the behavior of actors for innovation can serve as a guidepost for normative implications, prescriptions, and innovation policy.

This Part compares and contrasts national cybersecurity innovation within patent law's conception of legally protectable technologies as public goods with cybersecurity law and policy's conception of public goods. The objective of this Part is to lay out the theoretical foundations and justifications for: (1) arguing against extending patent protection further for national cybersecurity innovation; and (2) arguing for considering national cybersecurity as a public good in order to provide the basis for alternative innovation mechanisms.

A. Patent Law's Conception & Taking of National Cybersecurity

Much is at stake in determining whether the patent system can be reformulated to promote national cybersecurity innovation since computer

---

116 Daniel R. McCarthy, *Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order*, 6 POL. & GOVERNANCE 5, 8 (2018).

117 Peter R. Orszag, *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives*, BROOKINGS (Sept. 4, 2003), https://www.brookings.edu/testimonies/critical-infrastructure-protection-and-the-private-sector-the-crucial-role-of-incentives/ (stating, "[w]e must therefore alter the structure of incentives so that market forces are directed towards reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted."; furthermore, while describing how "private markets by themselves do not generate sufficient incentives for homeland security" through seven reasons, also suggesting the need for government intervention").

networks and cyber-physical systems increasingly impact communication networks, dams, electrical grids, pipelines, and transportation. Critical infrastructure will function better when the federal government integrates its efforts with those of the private sector, and the patent system reflects that concept.

Drawing upon economic theory, this Section aims to bring to the forefront that patent law's conception of innovation deviates sharply from national cybersecurity technological development needs. The patent system's goal of encouraging innovation, which occurs through a quid pro quo exchange of the legal right to exclude for an inventor's full disclosure of the invention,[118] breaks down for national cybersecurity technologies. The legal basis for the restriction of information from the public secretly and steadily due to concerns of national security has negative implications.[119] Thus, this Section argues that patent law's unique policy mechanism of encouraging disclosure as a social contract metaphor leads to a distorted conception of the innovative process that it seems to promote for national cybersecurity.

The patent system enables market-based incentives to promote technological innovation and views innovation through the lens of exclusive rights.[120] By attributing temporary exclusionary rights, the patent system is meant to enhance the prospect of appropriating economic returns on investments in inventive activities.[121] However, exclusive rights produce deadweight loss[122] and perhaps result in a decrease in public-sector innovations. Economic-based rationales suggest that a patent would provide temporary monopoly rights over the technological development that is awarded but would also lead to a corresponding deadweight loss.[123] Thus, a market-based framework for driving national cybersecurity innovation may not adequately address the needs of critical infrastructure development.

---

118 *See generally* Jay P. Kesan, *Economic Rationale for the Patent System in the Current Context*, 22 GEO. MASON L. REV. 897, 898 (2015) (examining several theories that explain and justify the role of patents in the modern economy, including traditional *ex ante* justifications and *ex post* justifications, as well as how these economic rationales may differ across industries).

119 Amanda Fitzsimmons, *National Security or Unnecessary Secrecy? Restricting Exemption 1 To Prohibit Reclassification of Information in the Public Domain*, 4 J.L. & POL'Y INFO. SOC'Y 479, 479–80 (2008).

120 35 U.S.C.A. §§ 1–2 (West 2020).

121 Liliane Hilaire-Perez, Christine MacLeod & Alessandro Nuvolari, *Innovation Without Patents*, 64 REVENUE ECONOMIQUE JANVIER 5 (2013).

122 WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 16–21 (Harvard Univ. Press ed. 2003).

123 RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 301–03 (9th ed. 2014).

1. Public Goods in the Patent Context

National cybersecurity technologies, like other patentable technologies, should qualify as public goods.[124] The technical knowledge embedded within ICT is a public good since it is both nonrival (multiple parties can use it without diminishing its availability)[125] and nonexcludable (absent legal intervention, it is nearly impossible to exclude others from appropriation).[126] Essentially, these national cybersecurity technologies are knowledge assets, and as such, are theoretically capable of inexhaustible appropriability.[127] Economic theory holds that competitive markets will produce a suboptimal level of new technologies since free riders will appropriate such assets, leading to diminished incentives to invent unless and until a patent system provides legal rights to exclude others.[128] Thus, the patent system mitigates market failure by enhancing the incentive to invent, and in the absence of the patent system, the inventions would exhibit public good attributes.[129] In effect, a patent is a legal right on a public good. Moreover, absent patent law, an inventor that develops a better technology cannot prevent others from copying it without paying royalties. In sum, an inventor will put in effort into invention by recognizing the potential for reaping rewards in prices that approach the social value of the invention.

The foregoing analysis applies reasonably well to most technologies, but national cybersecurity innovation, however, adds another twist. While national cybersecurity technologies share these public good attributes,[130] they entail different challenges for underproduction in comparison to other technologies. Exclusive patent rights play different roles in motivation of the invention of national cybersecurity technologies. There are substantive differences between innovation of other technological domains and the patent framework for national cybersecurity technologies. Because national cybersecurity innovation produces significant positive externalities by reducing threats to critical infrastructure and to national security beyond the implementing inventor or firm,[131] inventors do

---

124 *See infra* Section III.B.1 and Section III.C.

125 R. A. Musgrave, *Provision for Social Goods*, *in* PUBLIC ECONOMICS 124, 126–29 (Julius Margolis & Henri Guitton eds., St. Martin's Press 1969).

126 Corinne Langinier & GianCarlo Moschini, *The Economics of Patents: An Overview* 2 (Iowa State Univ., Working Paper No. 335, 2002).

127 Kesan, *supra* note 118, at 897, 898–99.

128 *See* Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 285 (1977).

129 Langinier & Moschini, *supra* note 126.

130 Nicola Jentzsch, *State-of-the-Art of the Economics of Cyber Security and Privacy*, 4 IPACSO 1, 24 (2016).

131 Allen Friedman, *Economic and Policy Frameworks for Cybersecurity Risks*, CTR. FOR TECH. INNOVATION AT BROOKINGS (July 21, 2011), https://www.brookings.edu/wp-content/uploads/2016/06/0721_cybersecurity_friedman.pdf.

not face adequate incentives.[132] Thus, national cybersecurity innovation faces another type of market failure, one which is based on its positive externalities since its salutary effects are gained by members of society, far beyond the inventor or firm that implements the invention. Framed another way, national cybersecurity innovation has significant benefits beyond those received by the consumer.

Technological advancement in national cybersecurity provides benefits to the cost of national security, thwarts catastrophic failure of electricity grids and communication networks, and protects public health and safety.[133] Thus, there are significant, potential welfare gains as both industry and the general public could be made significantly better off by national cybersecurity innovation. Similar to the impact of technological innovation on the environment and for public health, innovators' incentives are not in accord with the social value of the innovation unless the public benefits are internalized in some fashion. A rational profit-maximizing inventor or firm will not develop and implement a national cybersecurity innovation unless it expects to benefit from it in some manner and to benefit from it in a greater amount than the cost of research, development, and implementation.[134] In general, an inventor or firm considering whether to invest into national cybersecurity innovation will not take into account the benefit that society reaps from the innovation in the form of improved critical infrastructure conditions but only accounts for the benefit that the inventor or firm itself will receive in the marketplace.

Because inventors and firms do not consider the full social benefits of implementing national cybersecurity innovation, they do not face socially optimal incentives to invent under the patent system. Thus, the patent system is not significantly successful in driving national cybersecurity innovation. United States patent law offers certain, limited opportunities to promote technological innovation that has national cybersecurity benefits but, ironically, opposes the aims of the patent system. There is a limited subset of national cybersecurity technologies that has a connection with patent law. Technologies pertaining to

---

132 Jentzsch, *supra* note 130, at 7 (specifying cybersecurity amplifies network externalities).

133 *President Donald J. Trump Is Strengthening America's Cybersecurity*, WHITE HOUSE (Sept. 20, 2018), https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/.

134 MARKET FORCES AND GOVERNMENT ACTION IN SECURING CYBERSPACE PRELIMINARY REPORT 7, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/001213_cybersec_marketforces_govt.pdf (last visited Oct. 11, 2020) (describing that, to the extent that critical infrastructure is a public good, then there is less reason for the market to invest into it).

information security are classified as Class 726[135] and cryptography are classified as Class 380[136] at the United States Patent & Trademark Office ("USPTO").

To clarify why patent law does not adequately incentivize national cybersecurity innovation, it is useful to describe the conceptual limitation of a compulsory license (that creates eminent domain power) and provide support under a theoretical framework. Understanding the patent system's inefficiencies with national cybersecurity innovation provides guidance as to other innovation mechanisms in order to provide socially optimal results.

2. Property-Liability Rules Theoretical Framework for Patents

A theoretical framework for predicting and explaining how property and liability rules influence the behavior in legal actors is useful in understanding the role and limitations of the patent system,[137] including for national cybersecurity innovation. Drawing from the Calabresi–Melamed typology towards a new application of patents for national cybersecurity technology has not been addressed in scholarship and would provide a way to analyze virtues and vices for protecting legal entitlements to promote economic efficiency and social welfare. An extension of this framework to an unaddressed field sheds new theoretical insights promoting national cybersecurity innovation.

As a theoretical framework, Calabresi–Melamed property-liability typology denies the holder of the asset the power to exclude others and allows the third party to keep the asset and objectively determine the value of it.[138] The owner of the asset must accept the value, and as a consequence, society benefits from the resources available to it for a particular technological field, whereas the owner of the asset accepts the uncertainty of the objectively determined value.[139] The normative insight from the Calabresi–Melamed property-liability rules

---

[135] *Information Security*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/web/patents/classification/uspc726/defs726.htm (last visited Oct. 16, 2020) (describing that this class of technologies includes "a computer or digital data processing system, for processes or apparatus for increasing a system's extension of protection of system hardware, software, or data from maliciously caused destruction, unauthorized modification, or unauthorized disclosure").

[136] *Cryptography*, *supra* note 77 (describing that this class of technologies includes "equipment and processes which (a) conceal or obscure intelligible information by transforming such information so as to make the information unintelligible to a casual or unauthorized recipient, or (b) extract intelligible information form such a concealed representation, including breaking down of unknown codes and messages").

[137] Andrew W. Torrance & Bill Tomlinson, *Property Rules, Liability Rules, and Patents: One Experimental View of the Cathedral*, 14 YALE J.L. & TECH. 138, 143 (2011).

[138] Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1108 (1972).

[139] Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CALIF. L. REV. 1293, 1302–04 (1996).

framework is that the choice of rules in a next context should be based on the degree of transaction costs.[140] In distinguishing between various types of transaction costs, liability rules are favored when voluntary bargaining is not expected and transaction costs are high, whereas property rules are favored when parties can cost-effectively bargain with each other and transaction costs are low.[141]

Liability rules, which are known as "take-any-pay" regimes, allow an option for a third party to take an entitlement and pay that entitlement owner some price.[142] By contrast, property rules would require obtaining permission from the right's owner and would necessitate transaction costs associated with the bargaining and licensing process.[143] Under a system of liability rules, however, a third party would be able to take a technology, thereby eliminating the need to negotiate a license and lowering the transaction cost by reducing the bargaining process to determine a value of the entitlement.

The field of patent law has gradually shifted away from property rules and towards liability rules.[144] Liability rules in patent law allow for the government to take a technology and provide a government-run reward. As such, a liability rule (such as eminent domain power in the form of compulsory licensing) frustrates the goal of incentivizing innovation through the patent system.[145]

3. Suppressing National Cybersecurity Inventions by Eminent Domain

The framework for a liability rule is embedded in patent law and arises under the Invention Secrecy and 28 U.S.C. § 1498, which are forms of eminent domain for patented inventions.[146] These exemptions to patent protection for government based public interest provides for a government-run reward system for which the state offers to pay monetary award.[147]

---

140 Mark A. Lemley, *Contracting Around Liability Rules*, 100 CALIF. L. REV. 463, 466 (2012).

141 Abraham Bell & Gideon Parchomovksy, *Pliability Rules*, 101 MICH. L. REV. 1, 37 (2002).

142 Calabresi & Melamed, *supra* note 138.

143 Ana Santos Rustchman, *The Vaccine Race in the 21st Century*, 61 ARIZ. L. REV. 729, 765 (2019).

144 eBay, Inc. v. Mercexchange, L.L.C., 547 U.S. 388, 394 (2006); Dan L. Burk, *Property Rules, Liability Rules, and Molecular Futures: Bargaining in the Shadow of the Cathedral*, *in* GENE PATENTS AND LEARNING MODELS: FROM CONCEPTS TO CASES (Geertrui van Overawlle ed., 2009).

145 Scott F. Kieff, *Patents for Environmentalists*, 9 WASH. U. J.L. & POL'Y 307, 314 (2002) (arguing that a liability rule, such as compulsory licensing, for patent law would frustrate the goals of incentivizing innovation).

146 28 U.S.C.A § 1498 (West 2020); 35 U.S.C.A. § 181.

147 Gary L. Hausken, *The Value of a Secret: Compensation for Imposition of Secrecy Orders Under the Invention Secrecy Act*, 119 MIL. L. REV. 201, 203 (1988); Joel Dodge, *The Government*

In the U.S., the Fifth Amendment to the Constitution expressly reserves the right of the federal government to take personal property from private individuals for public use, provided that the individual receive just compensation for such a taking.[148] Eminent domain powers of the government have increased with time,[149] with more uses being considered for public benefits, including in patent law.[150] In technological domains where eminent domain powers are applicable, the patent system is converted from an incentive-centric, market-based system to a reward system that provides a reasonable royalty.[151] The government can revoke a patent right and force the inventor to share its invention under compulsory licensing.[152] United States patent law provides for compulsory licensing for specialized subject matter and certain circumstances wherein a government entity can use the inventor's patent without the inventor's consent.[153] Thus, the government has statutory authority for compulsory licensing on patents for non-voluntary use of patented inventions.[154] These licenses limit the scope of what may be patentable and can involve inventions that are vital to the public interest, such as for national defense or public health and welfare.[155] Such compulsory licensing of inventions is deemed a type of eminent domain, wherein the government must compensate the inventor of the patent.[156] Two main forms of compulsory licensing are relevant for national cybersecurity—invention secrecy and government patent use.

Under the Invention Secrecy Act, inventors cannot receive patents on inventions that pose national security risks.[157] Whenever publication or

---

Can Legally Commandeer Drug Patents, PEOPLE'S POL'Y REP. (Oct. 2, 2017), https://www.peoplespolicyproject.org/2017/10/02/the-government-can-legally-commandeer-drug-patents/ (describing that under government patent use, the federal government must provide reasonable compensation to the patent holder for legally commandeering the patented product).

148 *See* U.S. CONST. amend. V (elaborating on the "Takings Clause," which allows the government to take property if just compensation is provided).

149 Jeremy A. Blumenthal, *Legal Claims as Private Property: Implications for Eminent Domain*, 36 HASTINGS CONST. L.Q. 373, 373–423 (2009).

150 Michael Abramowicz, *Cost-Plus Patent Damages*, 73 WASH. & LEE L. REV. 719, 761–62, 772, 775 (2016).

151 Hausken, *supra* note 147, at 201, 203, 228–31.

152 Cole M. Fauver, *Compulsory Patent Licensing in the United States: An Idea Whose Time Has Come*, 8 NW. J. INT'L L. & BUS. 666, 667–68 (1988).

153 CONG. RSCH. SERV., R43266, COMPULSORY LICENSING OF PATENTED INVENTIONS 6 (2014) (defining compulsory license as the grant of permission for an enterprise seeking to use another's patent without the consent of the inventor, wherein the grant of the compulsory license requires sanction of a government entity and provides compensation to the patent owner).

154 *Statutory Authority for Compulsory Licenses of Patents in the United States*, KNOWLEDGE ECOLOGY INT'L, https://www.keionline.org/cl/statutory-authority-us (last visited Oct. 16, 2020).

155 Fauver, *supra* note 152, at 668, 670.

156 CONG. RSCH. SERV., *supra* note 153, at 9.

157 35 U.S.C.A. § 181 (West 2020).

disclosure of an invention may be detrimental to national interests (such as national security), the government can determine that the invention be kept secret.[158] The result is that the inventor is notified that the patent application will not continue in the patent prosecution process and is withheld from being granted a patent for a period required for national interests.[159] The USPTO has the power to flag patent applications for review by government agencies, which could request certain inventions be kept secret under a secrecy order.[160] USPTO officials weigh the government's national security interests against the inventor's exclusion rights of the invention.[161] The leaderships of a government agency, such as the Secretary of Defense or chief officer of another government department or agency, can order the UPSTO to maintain the patent application in a sealed condition, through a secrecy order, if they determine that it could jeopardize national interest.[162] Such a secrecy order provides the government with the right to exploit an invention in a patent application and constitutes a taking by the government.[163]

The inventor whose patent application is held under a secrecy order has the right to apply for compensation based on damage caused by the secrecy order.[164] Thus, inventors who seek inventions that are deemed important to national interests (such as national security), however, may receive a patent reward.[165] The reward is set by a Patent Compensation Board, based in part upon the actual use and importance of the invention.[166] If a full settlement of the compensation cannot be determined, then the government can provide to the inventor "a sum not exceeding 75 per centrum of the sum which the head of the department or agency considers just compensation for the damage and/or use," or alternatively, the inventor can bring suit against the U.S. in the Court of Federal Claims.[167]

---

158 Arvind Dilawar, *The U.S. Government's Secret Inventions*, SLAT (May 9, 2018, 9:00 AM), https://slate.com/technology/2018/05/the-thousands-of-secret-patents-that-the-u-s-government-refuses-to-make-public.html.

159 35 U.S.C.A. § 181.

160 CONG. RSCH. SERV., RL32051, INNOVATION AND INTELLECTUAL PROPERTY ISSUES IN HOMELAND SECURITY 15 (2008).

161 GEOFFREY MCGOVERN, MARIA MCCOLLESTER, DOUGLAS C. LIGOR, SHENG TAO LI ET. AL., THE ROLE OF INTELLECTUAL PROPERTY IN U.S. HOMELAND SECURITY 21 (2019).

162 Hausken, *supra* note 147, at 201, 203, 228–31.

163 *Id.*

164 35 U.S.C.A. § 183.

165 Hausken, *supra* note 147, at 243–47.

166 *Id.*

167 Halpern v. United States, 258 F.2d 36, 39 n.3 (2d Cir. 1958).

Patent applications that are subject to invention secrecy have steadily increased.[168] According to reported statistics, an average of 117 secrecy orders have been imposed annually since passage of the 1952 Invention Secrecy Act, and 5,784 inventions have been under secrecy orders as of 2018.[169] While the number of secrecy orders remained constant from 1952 to 1979, since 1979 the number of active secrecy orders has steadily increased—a trend that has received attention from scholars, Congress, and courts.[170] Yet scholars have commented that such statistics are suspect, since the entire process is secret and invention secrecy has been overused.[171] While the aim of invention secrecy is to protect national interests, "[a]t best, government agencies err on the side of caution and impose secrecy orders on patents that present even the slightest threat. . . . At worse, bureaucrats mindlessly impose secrecy orders and then forget about them, because that's simpler than carefully considering the implications of new technologies becoming public."[172]

Additionally, government patent use of 28 U.S.C. § 1498 presents another form of eminent domain power by the government for patents.[173] Under 28 U.S.C. § 1498, the government can use a patent at any time without permission of the patent holder, so long as the inventor is provided reasonable compensation for the government's use of the patent.[174] This form of compulsory licensing is justified on the ground that it increases public access to inventions when there are governmental concerns about a lack of adequate supply and public interest.[175] This statute allows federal agencies and third party government contractors to manufacture and use the patented invention without authorization and without obligation of prior negotiation from the patent holder, whose only source of redress is the Court of Federal Claims.[176]

---

168 Steven Aftergood, *Invention Secrecy Increased in 2016*, FED'N AM. SCIENTISTS (Oct. 31, 2016), https://fas.org/blogs/secrecy/2016/10/invention-secrecy-2016/#:~:text=There%20were%205%2C680%20invention%20secrecy,101%20over%20the%20year%20before.

169 Dilawar, *supra* note 158.

170 Hausken, *supra* note 147, at 202–03.

171 Dilawar, *supra* note 158 (stating that "with so many inventions deemed secret, so few eventually publicized, and the entire process itself obfuscated in classification, it's no wonder that critics have questioned whether the current invention-secrecy regime is really working").

172 *Id.*

173 28 U.S.C.A. § 1498 (West 2020).

174 Hannah Brennan, Amy Kapczynski, Christine H. Monahan & Zain Rizvi, *A Prescription for Excessive Drug Pricing: Leveraging Government Patent Use for Health*, 18 YALE J.L. & TECH. 275, 279–80, 299 (2016).

175 Fauver, *supra* note 152, at 668, 671.

176 Judge Mary Ellen Coster Williams & Diane E. Ghrist, *Intellectual Property Suits in the United States Court of Federal Claims*, U.S. CT. FED. CLAIMS (Nov. 4, 2017), https://www.uscfc.uscourts.gov/node/2927.

The inventor whose patent is commandeered by the government under 28 U.S.C. § 1498 is entitled to just compensation under the Fifth Amendment.[177] The patent holder is paid a "reasonable compensation," which is usually 10% of sales or less[178]—a standard that is vague, and also non-applicable when there are not yet any sales. There are three methods to ascertain "reasonable compensation": (1) reasonable royalty of a license; (2) lost profits and (3) savings to the government.[179] The government can effectively force the compulsory licensing of the patented inventions for its own use. However, where negotiations over the value of the license fail, the government may still use the patented invention. In effect, 28 U.S.C. § 1498 results in a takings claim by the patent owner, and a court must fix the value of the patent.[180] Some scholars have argued that government patent use can be beneficial over other policy tools for a speedy response to some national emergency situations.[181] In particular, government patent use has been a strategy that has been suggested by scholars to promote pharmaceutical innovation and provide a response to a public health crisis.[182]

---

177 28 U.S.C.A. § 1498.

178 35 U.S.C.A. § 183.

179 Lionel M. Lavenue, *Patent Infringement Against the United States and Government Contractors Under 28 U.S.C. § 1498 in the United States Court of Federal Claims*, 2 J. INTELL. PROP. L. 389, 423 (1995).

180 Brennan et al., *supra* note 174, at 311.

181 *See generally* Christopher J. Morten & Charles Duan, *Who's Afraid of Section 1498? A Case for Government Patent Use in Pandemics and Other National Crisis*, YALE J.L. & TECH. (forthcoming 2020) (suggesting that government patent use provides speed, flexibility, ex post remedy determination, and impartial adjudication to the COVID-19 national emergency).

182 While scholars have argued that government patent use under 28 U.S.C. § 1498 may not undermine incentives to innovate in pharmaceuticals and for vaccines, and could result in net economic and healthcare gains, it may not be as effective for national cybersecurity (where it could be problematic). These perspectives consider that government patent use increase access to life-saving medicines and address the high cost of drugs caused by monopolistic pricing, but do not necessarily address innovation. Thus, the theoretical defense to government patent use under 28 U.S.C. § 1498 for commandeering inventions is based on access and efficiency caused by pricing, and not inadequacy in government or market driven motivations to promote innovation.

These features of liability regimes render them especially apt at a time of a prolonged crisis, in particular for a severe pandemic outbreak of an infectious disease, such as COVID-19. In such cases, the patent system present barriers to rapid R&D necessary to achieve a vaccine cure, and a liability regime would remove the barrier by facilitating compulsory licensing. However, such a feature would not apply to national cybersecurity where a disruption, even while catastrophic, is not biological but instead is caused by hardware and software. Unlike the race to find a cure for COVID-19, where the patent system imposes impediments over a relatively prolonged time period (estimated at optimistically 12–18 months, albeit intense R&D) to find a cure, a national cybersecurity breach would require a hardware and/or software solution (or a cyber-physical system) that would be a fix or repair. Thus, unlike vaccine R&D, where a take-and-pay liability regime would ease the R&D pathway after a crisis, a take-and-pay liability regime with national cybersecurity would not ease reduction of a crisis that could be solved with a technological fix. In other words, government patent use under 28 U.S.C.A. § 1498, which may aid R&D in some

The framework for a liability rule is embedded in government patent use under 28 U.S.C. § 1498, which is a form of eminent domain for patented inventions and provides for a government-run reward system for which the state offers to pay monetary award.[183] It gives the federal government the right to use patented inventions without permission, while paying the patent holder a "reasonable and entire compensation."[184] As such, it operates as a form of government immunity from patent rights, where patent holders can demand royalties but cannot stop the government from producing the invention or allowing others to do so.[185]

A liability regime is not desirable for all types of innovation, such as with national cybersecurity. Furthermore, a liability regime specific for certain types of technology presents challenges for delineating technology specific boundaries and for political economy. This Article takes the position that a liability regime would hamper national cybersecurity R&D following a cyber-attack, and also, the current system of government patent use under 28 U.S.C. § 1498 (a type of liability regime) is a barrier to national cybersecurity development even absent a catastrophic crisis.[186]

Consider as examples for government patent use under 28 U.S.C. § 1498 for non-biological technologies in the defense technology field. While a defense related technology is not necessarily within the characterization of national cybersecurity for this Article, it represents an example of the government commandeering a hardware-software technology. In the example of night-vision goggles, the patent owner sued the federal government under government patent (under 28 U.S.C. § 1498) for "reasonable and entire" compensation based on direct infringement by the government.[187] In the example of lead free bullets (or green bullets), the patent owner sued the U.S., and the Department of Defense invoked government patent use.[188] Thus, these examples demonstrated that

---

technological domains such pharmaceuticals and vaccines, does not advance R&D of national cybersecurity.

183 Amy Kapczynski & Aaron S. Keeselheim, *Why "Government Patent Use" To Lower Drug Costs Would Stifle Innovation*, HEALTH AFFS. (July 28, 2016), https://www.healthaffairs.org/do/10.1377/hblog20160728.055969/full/.

184 28 U.S.C.A. § 1498 (West 2020).

185 Dennis Crouch, *Can the U.S. Government Infringe a U.S. Patent? (The U.S. Government Says It's Impossible)*, PATENLYO (Sept. 20, 2015), https://patentlyo.com/patent/2015/09/government-infringe-impossible.html.

186 *See supra* Section III.A.3.

187 Philip A. Janquart, *Night-Vision Goggles Spat Resolves for $75 Million*, COURTHOUSE NEWS (Feb. 18, 2014), https://www.courthousenews.com/night-vision-goggle-spat-resolved-for-75-million/.

188 Stew Magnuson, *Ammunition Inventor Wins $15 Million Patent Infringement Case Against Army*, NAT'L DEF. (Jan. 14, 2015), https://www.nationaldefensemagazine.org/articles/2015/1/14/ammunition-inventor-wins-15-million-patent-infringement-case-against-army.

government patent use is a remedy for the patentee ex post of issuance and not an ex ante incentive, similar to pharmaceuticals and vaccines.

The current application of government patent use of 28 U.S.C. § 1498 for national cybersecurity related inventions has not adequately incentivized innovation. This statute, which is a form of liability rule under the Calabresi–Melamed property-liability typology,[189] is optimal to utilize when transaction costs are high or in a field where transactions are infeasible. Instead, alternative incentive mechanisms would yield more promising avenues for national cybersecurity development.

4. Limitations with Patent Rewards Based on Eminent Domain

A patent rewards system attempts to capture the social returns of innovation that are generally not reflected in the market.[190] The primary difficulty with a patent rewards system for inventions that are suppressed from disclosure under the Invention Secrecy Act, is that an administrative body has to determine the value of the invention.[191] The identification of the social value of an invention is not an easy task. There are criticisms leveled against such patent rewards in general.

First and foremost, a patent rewards system for inventions suppressed under the Invention Secrecy Act fails to result in commercialization of the inventions. The market for national cybersecurity innovations is the government or defense sector, and as such, this market does not provide adequate incentives for the adoption of such innovation.

Second, a patent rewards system for inventions suppressed under the Invention Secrecy Act is expensive to administer. There are costs with administration of the Patent Compensation Board and with resources spent in calculating the social value of the innovation. Furthermore, there is the cost of the reward itself. Determining the exact social value of an invention is a near impossible task that would require calculating how society benefits from the particular national cybersecurity innovation. This calculation would require determining secondary effects, such as the impact of the innovation on future inventive activity in the same technological domain, effect of multiple inventive efforts at various stages of the invention, and distortions in national cybersecurity caused by the grant of the reward.

Third, the amount of the reward is based on pricing of the social value of the invention and not simply on the marginal cost. Furthermore, the patent could be found to be invalid in post-issuance proceedings or in district courts had

---

189 *See supra* Section III.A.2.

190 Michael Kremer, *Patent Buyouts: A Mechanisms for Encouraging Innovation*, 113 Q.J. ECON. 1137, 1141 (1998).

191 Hausken, *supra* note 147, at 234.

there not been such a reward, and therefore, some rewards could be provided for patents that should have been deemed unworthy of the patent system as invalid patents.

These difficulties with a patent rewards system for inventions suppressed under the Invention Secrecy Act suggest that inventors have no ex ante knowledge of how their national cybersecurity invention will be treated and valued in this system. The lack of accuracy in valuing the invention and the high cost of administration of such a reward suggest that such a system is not adequate for incentives to national cybersecurity innovation.

B. Public Goods Characterization, Market Failure, & Government Failure

Public goods refer to a good that is both non-excludable and non-rivalrous, such that individuals cannot be excluded from use or could benefit from it without paying for it and where use by one individual does not reduce availability to others or the good can be used simultaneously by more than one person.[192] The notion of public goods in the patent context refers to the knowledge embedded within a technology that is nonrival and nonexcludable, and as such, the knowledge asset is capable of being inexhaustibly appropriable, wherein the patent system mitigates the free rider problem.[193] The notion of public goods in the cybersecurity context refers to a social good (or a collective good), which is non-excludable and non-rivalrous, such as national security, for which it applies to all citizens in a society that live under its protection (not just those who paid for it).

1. Public Goods in the National Cybersecurity Context

Is national cybersecurity a public good in the economic sense? At first glance, it would appear to be the case since national cybersecurity should be made available to society and there appears to be no buyer except the government, government agencies, or government contractors.[194] A deeper analysis reveals, however, that such a characterization is not so simple, and there is more subtlety to whether national cybersecurity is a purely public good.

National cybersecurity reveals an idiosyncratic nature of public goods in the social good context. One of the primary requirements for a public good (in the social good context) is that one's consumption of the good does not reduce the consumption left for another person.[195] In other words, public goods are made

---

192 *See generally* HAL R. VARIAN, MICROECONOMIC ANALYSIS (W.W. Norton & Co. ed. 1992).

193 *See supra* Section III.A.1.

194 A number of government services are considered public goods, which includes public health, fire department services, and national defense.

195 Joseph E. Stiglitz, *Economic Foundations of Intellectual Property Rights*, 57 DUKE L.J. 1693, 1699–1700 (2008).

available to everyone in society and the end product or service has only one customer—the government.[196] Public goods have two defining characteristics, that they are nonexcludable and nonrivalrous.[197]

Scholars have debated how to define the public good nature with regards to national cybersecurity.[198] The majority of scholars consider national cybersecurity a public good that should be provided by the U.S. government to the population.[199] However, a minority of scholars suggest that national cybersecurity is not a single public good, but it is a bundle of public goods and private goods that are networked with a cyber infrastructure owned mostly by private entities.[200]

Some scholars have argued that since ICT and data (that is increasingly part of national cybersecurity) are inherently commercial and operate as an

---

196 Nish Acharya, *COVID-19 Reminds Us Why Innovation Is Often a Public Good*, FORBES: ENTREPRENEURS (Mar. 23, 2020, 1:31 PM), https://www.forbes.com/sites/nishacharya/2020/03/23/covid-19-reminds-us-why-innovation-is-often-a-public-good/#637818681f7e.

197 The first characteristic of a public good is that it is nonexcludable, which means it is costly or impossible to exclude someone from using the good. More specifically, a public good cannot apply to everyone and exclude one member of society. The second characteristic of a public good is that it is nonrivalrous, which means when one member of society uses it, another can also use it. *See* Christopher S. Yoo, *Public Good Economics and Standard Essential Patents* 4 (Univ. Pa., Inst. for L. & Econ., Research Paper No. 14-27, 2014).

198 Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TX. L. REV. 87, 95 (2012).

199 John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 453 (2018) (stating that "[n]ational security (which cybersecurity protection of [critical infrastructure]) is a public good"); Deirde K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 J. AM. ACAD. ARTS & SCI. 70, 80 (2011) (stating "[o]ur doctrine of *public cybersecurity* is rooted in the thesis that cybersecurity is a public good"; furthermore, suggesting that "[c]ybersecurity is non-rivalrous and non-excludable so, by definition, it is a public good"); Benjamin Powell, *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry* 2 (Indep. Inst., Working Paper No. 57, 2001) (stating that "cybersecurity is often assumed to be a 'public good' that will be underprovided or fail to be provided at all in the private market"); Peter Magemeso, *Cyber Security a Public Good*, INST. FORENSICS & ICT SEC. (Jan. 8, 2020), https://www.forensicsinstitute.org/cyber-security-a-public-good/.

200 Rosenzweig, *supra* note 17, at 8–9 (stating, "[i]t is commonplace to note that private entities own and operate 85–90% of the cyber infrastructure"; furthermore, suggesting that "[s]ecurity in cyberspace is a market good [and that] security in cyberspace is not a singular good—rather it is a bundle of various goods, some of which operate independently and others of which act only in combination. . . . Given the vast scope of cybersecurity goods, it is no surprise that different aspects of the bundle may be provided by different sources . . . cybersecurity is, to a very large degree, a private good, adequately provided by the private sector."); Assaf, *supra* note 92, at 29–32 (stating that "most critical infrastructure assets are owned and operated by the private sector"; furthermore, recognizing "interdependencies between the public and private sectors" while pointing out that "cyber security is considered to be a public good, although not a pure public good. It has strong public good characteristics [but] it is not considered to be a pure public good because it is, at least to some extent, excludable").

interaction between individuals and firms, national cybersecurity cannot be considered a purely public good. This perspective suggests that national cybersecurity's reliance on the private sector indicates that it is a market good.[201]

Another perspective has argued that national cybersecurity *can* be characterized as a purely public good.[202] This viewpoint suggests that some elements of national cybersecurity can fairly be characterized as public goods, and remaining elements are either private goods with externalities that present challenges for government regulation or are co-mingled public–private goods that equally present challenges for private sector incentives.[203] This view considers national cybersecurity as not purely a public good, but instead a co-mingled public and private good. National cybersecurity has a dual nature of public and private goods that introduce externalities that point to different government and market policy solutions.

While some form of government or a government organization is the sole customer of public goods, private companies can contribute towards producing public goods, although private companies may find it difficult to produce them.[204] A free rider problem arises, such that people have an incentive to let others pay for the public good while benefiting from the purchases of others.[205] A key issue in paying for public goods is to find a way for everyone to make a contribution and prevent free riders. Relatedly, another important issue is how to provide for and incentivize the creation of the public good—this may be done via government or via markets.[206]

This analysis poses two countervailing considerations in the national cybersecurity economics discourse—the free rider problem and continued investment into corporate cybersecurity by the private sector. First, since individuals and firms want to benefit from others' efforts to develop and pay for national cybersecurity innovation, they fail to deal with the problem of national cybersecurity themselves. Firms and individuals hope to benefit from another firm's development of a national cybersecurity innovation and also fail to report data breaches as they arise, with the result that firms may not innovate as quickly

---

201 Rosenzweig, *supra* note 17, at 8; James Pattison, *From Defence to Offence: The Ethics of Private Cybersecurity*, 5 EUR. J. INT'L SEC. 233, 244 (2020).

202 Mischa Hansel, *Cyber Security Governance and the Theory of Public Goods*, E-ITN'L RELS. (June 27, 2013), https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/.

203 Kosseff, *supra* note 26, at 995; Shane, *supra* note 198, at 95; Tyler Moore, *The Economics of Cybersecurity: Principles and Policy Options*, 3 INT'L J. CRITICAL INFRASTRUCTURE PROT. 110–11 (2010).

204 Powell, *supra* note 199.

205 Chung, *supra* note 199, at 445–46.

206 *See infra* Part IV.

as they should.[207] As a result, the private sector underinvests in cybersecurity due to negative externalities, positive externalities, and free riding.[208] Second, the private sector has continued to invest dollars into cybersecurity—largely corporate cybersecurity—development to protect against cyber-attack, which impacts national cybersecurity.[209] Thus, there must be enough of a private return to cause firms to invest so much into cybersecurity, and as a result national cybersecurity may not have a purely public characteristic. Given that the private sector owns about 85–90% of the critical infrastructure in the U.S., innovations in corporate cybersecurity have positive effects in national cybersecurity.[210] However, many firms are not adequately investing into corporate cybersecurity, which is a growing priority among most companies.[211] Against this backdrop, and in assessing whether national cybersecurity is a public good, the relevant deeper question is whether private businesses on their own accord will provide adequate national cybersecurity or if some form of government involvement is necessary.[212]

2. Market Failure and Role of Government

The effect of the countervailing forces of the free rider problem and continued investment into corporate cybersecurity does not produce sufficient national cybersecurity.[213] While there may be some innovation in national cybersecurity, it may not be quick enough both in the short term or the long term. Markets may not provide sufficient national cybersecurity, resulting in a classic market failure that necessitates government involvement through some

---

207 Shana Kayne Beach, *Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula*, 1 NAT'L CYBERSECURITY INST. J. 4, 10 (2014) (describing that with "the current misalignment of incentives, asymmetries, and externalities of the traditional security-based approaches, [if] the costs of insecurity are borne by others in the network, there is limited incentive to increase security").

208 Chung, *supra* note 199, at 441, 476, 455 (explaining that a free rider problem occurs when an individual enjoys as much of the public good as someone who pays for it); Sales, *supra* note 98, at 1507–08, 1519–20 (describing that positive externalities happen when an activity generates benefits that an actor cannot internalize, and negative externalities occur when an activity imposes costs on others that are not transmitted through prices).

209 Trautman, *supra* note 4, at 355–58.

210 Sales, *supra* note 98, at 1506.

211 Lawrence A. Gordon & Martin P. Loeb, *The Economics of Security Investment*, 5 ACM TRANSACTIONS ON INFO. & SYSTEM SEC. 438, 438–39 (2002) (describing inadequate investments in corporate cybersecurity to reduce data breaches and develop encryption, access control, and firewalls to protect information).

212 *See infra* Part IV.

213 Assaf, *supra* note 92, at 32 (suggesting that government intervention is necessary due to various market failures, externalities, and information deficits with protection of the critical infrastructure).

appropriate innovation mechanisms.[214] Government intervention is justifiable when there is some public interest that impacts the relevant societal good.[215]

According to economic theory, government should seek to correct the market failure of national cybersecurity that arises due to its public good-like characteristics. However, even if government intervention helps to correct the market failure problem, there may still be government failure with over correction.[216] Government regulation could over-correct and overregulate, such that direct government regulations may not lead to an optimal level of national cybersecurity, resulting in a government failure.[217]

National cybersecurity faces market failures, but increased government efforts may lead to government failures. A balanced approach to national cybersecurity innovation should seek to provide additional government intervention to address market failure but remain careful not to over-impose and lead to government failure. While in a perfect market, the private sector would develop or purchase adequate cybersecurity technological solutions, indication of market failure necessitates some form of government intervention.[218] The market failure of cybersecurity stems from obstacles including: (1) a lack of incentives to pay for a public good; (2) high transaction costs; and (3) government restrictions. These obstacles are interrelated and necessitate a new approach to fostering cybersecurity innovation.

Consequently, government intervention is necessary since the private sector will not pay for a public good as long as someone else does.[219] Because the market by itself does not provide sufficient incentives for optimal resources towards cybersecurity, the private sector will not bear the full costs of its vulnerabilities.[220] As a result, the private sector has weaker incentives to secure its cybersecurity technological systems.[221] Thus, the market by itself does not provide sufficient incentives for optimal resources towards national cybersecurity. The problem is compounded by the government's reliance on the

---

214 Alain Marciano & Steven G. Medema, *Market Failure in Context*, HIST. POL. ECON. (2015).

215 J. Janewa OseiTutu, *Private Rights for the Public Good?*, SMU L. Rev. 767, 807 (2013).

216 Eli Dourado & Jerry Brito, *Is There a Cybersecurity Market Failure?*, (Geo. Mason Univ., Mercatus Ctr., Working Paper No. 12-05, 2012).

217 CLIFFORD WINSTON, GOVERNMENT FAILURE VERSUS MARKET FAILURE (2006).

218 MARKET FORCES AND GOVERNMENT ACTION IN SECURING CYBERSPACE PRELIMINARY REPORT, *supra* note 134.

219 Niva Elkin-Koren & Eli M. Salzberger, *The Effects of Cyberspace on the Economic Theory of the State*, 2004 LAW, ECON. & CYBERSPACE 144, 146.

220 Haber & Zarsky, *supra* note 87, at 515, 543–44 (noting that the market alone is insufficient to ward off cybersecurity risks since private sector critical infrastructure owners do not have sufficient incentives, thereby leading to insufficient cybersecurity protection).

221 Mariarosaria Taddeo & Francesca Bosco, *We Must Treat Cybersecurity as a Public Good: Here's Why*, WORLD ECON. F. (Aug. 22, 2019), https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/.

private sector to develop technologies to provide cybersecurity technology even if there is little economic incentive to do so.[222] Since market forces will not naturally provide for adequate cybersecurity, government intervention is necessary. As with other approaches to increase the development of and investment into public goods, the government can act as a facilitator to build a framework for strengthening cybersecurity.

C. *Comparing Public Goods in Patent Law & Cybersecurity Policy*

National cybersecurity is a "public good," not only because it serves the public but also because it emanates from a knowledge asset. The patent system is meant to provide a legal right on public goods.[223] The government has to strike a complex balance between national cybersecurity public interest concerns and exempting a legal right on public good inventions concerning national cybersecurity. Achieving this balance is even more difficult since ICT introduces more cyber and data connections with the critical infrastructure, which as a result, has become more of a public interest concern.[224] In the age of expansion of the critical infrastructure to being increasingly connected with the cyber domain,[225] it is necessary to consider national cybersecurity as a public good.

A similar public goods story applies both in the patent law context and in the cybersecurity policy context. While national cybersecurity inventions are *subject to eminent domain*,[226] they are also the *subject of government interest* in national security technological innovation.[227] This quality of pluralistic public goods in national cybersecurity is more evident with a deeper than from a high level of abstraction. Indeed, national cybersecurity innovation at large, such as cryptography,[228] percolated from government initiatives.[229]

In a similar sense, the notion of national cybersecurity also arose from government interests. At an even more discrete level, national cybersecurity innovation tends to arise from government interest in protecting the critical infrastructure.[230] Indeed, national cybersecurity innovation itself has been intrinsically a government-driven initiative to date, largely driven by the

222 Rosenzweig, *supra* note 17.

223 *See supra* Section III.A.1.

224 *See supra* Section II.A.1 and Section II.A.2; *Figure 2.B.*

225 *See supra* Section II.A.2; *Figure 2.B.*

226 *See supra* Section III.B.3.

227 *See supra* Section III.B.3 and Section III.B.4.

228 *See supra* Section II.A.2.

229 Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 761 (2010).

230 *See id.*

Department of Homeland Security.[231] As such, emphasizing the market-driven patent system for national cybersecurity innovation is a potentially distorting innovation mechanism. Public goods are likely to be under-produced if left to the private market, and markets for public goods will not form.[232]

The public goods nature of national cybersecurity, which is justified by economic reasoning,[233] contrasts sharply with the market-based conception that is celebrated by the patent system. Based on its very nature and purpose, patent law is preoccupied with market-based justifications. In so doing, however, it may reflect and corroborate a distorted perception of national cybersecurity innovation dynamics. In fact, much national cybersecurity innovation has arisen from outside of the patent system. For instance, the National Security Agency had been the main supporter of digital signatures research relevant for information security in computer networks.[234] Patent law's insistence on providing a market of inventions that is embodied in goods and services—and firms themselves—obscures the reality that research, development, and implementation of some technological domains reveal themselves through government funding and initiatives.[235]

In sum, national cybersecurity is a key component for protecting America's critical infrastructure from risks and entails some elements that are public goods requiring collective action. To the extent that cybersecurity technology that protects critical infrastructure is a public good, there is less incentive for the market to invest in it and a gap with the commercial sector's ability to protect critical infrastructure.[236] Market forces are at odds with the public safety and security needed to promote resilience to cyber-attack vulnerabilities.[237] There is a cybersecurity risk gap between protecting national infrastructure and the adequacy of technology to address it.[238]

---

231 COMM'N ON ENHANCING NAT'L CYBERSECURITY, *supra* note 108; National Cybersecurity and Critical Infrastructure Protection Act, H. R. 3696, 113th Cong. (2014).

232 Bell & Parchomovksy, *supra* note 141.

233 *See supra* Section III.B.

234 *See generally* NAT'L RSCH. COUNCIL ET AL., CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 227 (Kenneth W. Dam & Herbert S. Lin eds., 1996) (suggesting that the concepts of cryptography were developed at universities with federal research support).

235 *See generally* Daniel F. Spulber, *How Patents Provide the Foundation of Markets for Inventions*, J. COMPETITION L. & ECON. 271 (2015) (developing a framework that demonstrates patents provide a foundation of the market of inventions).

236 MARKET FORCES AND GOVERNMENT ACTION IN SECURING CYBERSPACE PRELIMINARY REPORT, *supra* note 134.

237 *See supra* Section III.A and Section III.B.2.

238 Haber & Zarsky, *supra* note 87, at 515; U.S. DEP'T OF HOMELAND SEC., *supra* note 72; NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA, *supra* note 70.

IV. NORMATIVE IMPLICATIONS & PRESCRIPTIONS

Turning from the descriptive to the normative and prescriptive, this Part draws from the prior analysis to propose various strategies for accelerating national cybersecurity innovation. In so doing, it fills a gap in the cybersecurity literature, which overwhelmingly focuses on maintaining technology resilience with traditional information assurance,[239] rather than incentivizing innovation.

This Article's examination of innovation mechanisms for incentivizing national cybersecurity intersects with a long-standing normative debate over what innovation policies promote research and development of innovative technologies. The optimal innovation policy—whether patents,[240] prizes,[241] grants,[242] or R&D tax credits[243]—are normatively preferable in certain contexts. Some scholars have argued in favor of market-based mechanisms,[244] whereas other scholars prefer government-driven initiatives[245] (or via so called public finance[246]). The U.S. government and private firms alike want innovative technological solutions to detect, prevent, and provide responses to future cyber-attacks, and in so doing, protect our nation's security, economic structure, and public health and safety.[247]

---

239 *See* Herr & Ormes, *supra* note 45, at 3 (suggesting that the goal of cybersecurity in the technological community is information assurance, or maintenance of integrity, reliability, and availability of data and equipment and minimization of the risk of compromise).

240 *See generally* Michael Abramowicz & John F. Duffy, *Intellectual Property for Market Experimentation*, 83 N.Y.U. L. Rev. 337 (2008); Steven P. Calandrillo, *An Economic Analysis of Property Rights in Information: Justifications and Problems of Exclusive Rights, Incentives To Generate Information, and the Alternative of a Government-Run Reward System*, 9 FORDHAM INTEL. PROP. MEDIA & ENT. L.J. 301 (1998); Ted Sichelman, *Commercializing Patents*, 62 STAN. L. REV. 341 (2010); Spulber, *supra* note 235.

241 Benjamin N. Roin, *Intellectual Property Versus Prizes: Reframing the Debate*, 81 U. CHI. L. REV. 999 (2014); Ted M. Sichelman, *Patents, Prizes, and Property*, 30 HARV. J.L. & TECH. 279 (2017).

242 W. Nicholson Price II, *Grants*, 34 BERKELEY TECH. L.J. 1 (2019).

243 Charles Delmotte, *The Case Against Tax Subsidies in Innovation Policy*, 48 FLA. STATE U. L. REV. (forthcoming 2021); Daniel J. Hemel & Lisa Larrimore Ouellette, *Beyond the Patent-Prizes Debate*, 92 TEX. L. REV. 303 (2013).

244 *See generally* Abramowicz & Duffy, *supra* note 240; Calandrillo, *supra* note 240; Sichelman, *supra* note 240; Spulber, *supra* note 235.

245 Eric E. Johnson, *Intellectual Property and the Incentive Fallacy*, 39 FLA. STATE U. L. REV. 623, 629–30 (2012); Peter Lee, *Towards a Distributive Agenda for U.S. Patent Law*, 55 HOUS. L. REV. 321 (2017); Peter Lee, *Social Innovation*, 92 WASH. U. L. REV. 1 (2014).

246 Camilla A. Hrdy, *Innovation or Jobs: An Inconvenient Truth About Public Financing for Innovation*, 3 J.L. & INNOVATION 69 (2020).

247 Ebrahim, *supra* note 105; Bannelier & Christakis, *supra* note 92; Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive: Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, (2015) (providing a survey of private sector proactive cybersecurity practices, including auditing, data mining, detection systems, analytics, testing, virus

Accordingly, this Part builds upon a rich body of scholarship comparing the relative merits of exclusive rights with patents, public funding, prizes, and other inducement mechanisms to promote national cybersecurity innovation.[248] It addresses the following questions. First, when should society utilize certain innovation mechanisms to incentivize national cybersecurity development and how should it allocate the corresponding costs? Second, what is the optimal innovation policy mix, and what multiple incentive mechanisms should be utilized in combination? Indeed, not only have these questions gone unanswered, but with few exceptions, they have gone unasked in cybersecurity scholarship. These analyses, moreover, provide a framework for selecting one or several of the mechanisms to promote particular kinds of breakthrough national cybersecurity innovation.[249] Innovation mechanisms, such as basic research at universities, applied research and commercialization non-profit organizations, small business innovation funding, and public subsidies (research grants and tax incentives), have some benefits, but this Article argues that national cybersecurity innovation is best achieved via government intervention through prizes and CRADAs. This Part argues against extending patents to national cybersecurity innovation too far, and instead, it argues that selection of prizes[250] and close public and private interactions[251] can each accelerate national cybersecurity innovation.

A. Normative Implications of Various Innovation Mechanisms

The fundamental principle for incentivizing national cybersecurity is to bring incentives to develop socially useful results in line with critical infrastructure needs. Various innovation mechanisms exist to encourage the production of new

---

trends, consulting, case management, compliance, training, insider threats, mobile security, honeypots, and patching); Vignesh Ramachandran, *Cybersecurity and Patent Law–Let's Work Together*, 10 AM. U. INTELL. PROP. BRIEF 1 (2019).

248 *See, e.g.*, Brett Frischman, *Innovation and Institutions: Rethinking of the Economics of U.S. Science and Technology Policy*, 24 VT. L. REV. 347 (2000); Hemel & Ouellette, *supra* note 243; Amy Kapczynski, *The Cost of Price: Why and How To Get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970 (2012); Amy Kapczynski & Talha Syed, *The Continuum of Excludability and the Limits of Patents*, 122 YALE L.J. 1900, 1902 (2013); Stiglitz, *supra* note 195; Brian D. Wright, *The Economics of Invention Incentives: Patents, Prizes, and Research Contracts*, 73 AM. ECON. REV. 691 (1983).

249 *See generally* JERRY SCHAUFELD, COMMERCIALIZING INNOVATION (Apress 2015) (describing how to turn ideas from research and development laboratories, universities, patent offices, and inventors into commercially successful products and services).

250 *See infra* Section IV.C.1.

251 *See infra* Section IV.C.2.

knowledge and technological innovation.[252] Society should want technological solutions where their development cost is less than their societal value, and some sort of incentive mechanism should serve that purpose.

There are numerous mechanisms for incentivizing the research and development of innovative technologies, such as cybersecurity for critical infrastructure. The choice among innovation mechanisms depends upon the model of knowledge creation, and requires assessing a range of policy levers and institutions that affect the incentives effects.[253] In comparing mechanisms that spur innovative technology development requires answering three distinct questions.

> (1) *Who decides* how to spur the innovative activity—a central planner (i.e., the government) or decentralized actors (i.e., the market)? (2) *When* is the reward transferred—before the outcome of a project is known or only after a project is successful? (3) *Who pays* for the reward—all taxpayers, or only user of any resulting products?[254]

A number of policies can increase innovation by encouraging the rate of return for new technology and encouraging its development.[255]

B. *The Limitations of Patents for National Cybersecurity Innovation*

One seemingly obvious incentive mechanism candidate for accelerating national cybersecurity innovation is to extend and promote exclusive rights over such technological inventions. For a variety of reasons, however, this Article argues against patents as such a potential incentive policy intervention.[256] Exclusive rights in national cybersecurity inventions would not be a prudent innovation policy instrument, since the societal costs would be high relative to benefits. Patent law's conception of legally protectable innovation includes assigning individual exclusive rights in inventions, requiring robust disclosure to meet statutory patentability requirements, and emphasizing discrete patent claiming[257]—each of these facets of patents makes patented technologies to be

---

252 *See generally* Matthew S. Clancy & GianCarlo Moschini, *Incentives for Innovation: Patents, Prizes, and Research Contracts*, 35 APPLIED ECON. PERSPS. & POL'Y 206 (2013) (discussing the economics of institutions and policies meant to provide incentives for innovation).

253 Peter S. Menell & Suzanne Scotchmer, *Intellectual Property*, *in* HANDBOOK OF LAW & ECONOMICS 1473–1557 (A. Mitchell Polinsky & Steven Shavell eds., 2007).

254 Hemel & Ouellette, *supra* note 243, at 327.

255 OPENSTAX, *How Governments Can Encourage Innovation,* in PRINCIPLES OF ECONOMICS 13.2 (2d ed. 2017).

256 *See supra* Section III.A.4 and Section IV.B.

257 *See generally* Michael Risch, *Everything Is Patentable*, 75 TENN. L. REV. 591 (2008).

tradable in markets.[258] Thus, in the classic profit-driven formulation for innovation, markets motivate the generation of new technologies and help to disseminate them in the commercial marketplace, such as through licensing, mergers, and acquisitions.[259] This model, of course, works best for technologies that are disclosed through quid pro quo, whereupon patent protection for inventions is attained in exchange for robust disclosure and patented technologies enter the public domain upon the expiration of the patent.[260] This market-driven model does not work well for innovations with any semblance of national security concerns, which present risk of government intervention of some sort and inadequacies with the patent system.

Notwithstanding potential difficulties with patenting national security inventions, such as those established by the Invention Secrecy Act,[261] other considerations should represent formidable obstacles to societal benefit from patenting of national cybersecurity technologies. As mentioned, many national cybersecurity inventions are not strictly patentable since they raise national security implications and are subject to government secrecy suppression.[262] Even if a national cybersecurity invention might technically meet patentability, it would likely be subject to government patent use and subject the government to exemption from patent infringement.[263] Further complicating attempts to patent national cybersecurity is the mysterious nature of the secrecy criteria, which the USPTO has noted is held under national security.[264] As previously mentioned, the patent system is typically not meant to keep innovation secret,[265] and in fact aims to disclose and disseminate inventions to the public through its quid pro quo.[266] Unless the practice of the government commandeering national security inventions is made less secretive (which seems highly unlikely), the Invention

---

258 Feng Gu & Baruch Lev, *Markets in Intangibles: Patent Licensing* (N.Y.U., Working Paper No. 2451/275465, 2001).

259 Paul J. Heald, *A Transaction Costs Theory of Patent Law*, 66 OHIO STATE L.J. 473 (2005).

260 Shubha Ghosh, *Patents and the Regulatory State: Rethinking the Patent Bargain Metaphor After* Elfred, BERKELEY TECH. L.J. 1315, 1354 (2004).

261 35 U.S.C.A. § 181 (West 2020).

262 Within the United States' Invention Secrecy Act, if an inventor files a patent that may be detrimental to the national security in the opinion of an interested government agency, then that inventor will be ordered to keep the invention secret, resulting in withholding the grant of the patent. *See* Dilawar, *supra* note 158 (noting "that, on top of patent being withheld for national security, 'the criteria is also held under national security'").

263 *See supra* Section III.A.3.

264 *See id.*

265 *See supra* Section III.A.1 and Section III.A.3.

266 *See* 35 U.S.C.A § 112; John R. Allison & Lisa Larrimore Ouellette, *How Courts Adjudicate Patent Definiteness and Disclosure*, 65 DUKE L.J. 609, 611 (2016); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974).

Secrecy Act and government patent use will continue to defeat attempts to patent national cybersecurity inventions.

Even if national cybersecurity inventions were kept patentable, exclusive rights would not be a prudent innovation policy instrument for incentivizing them. Patents (in theory) represent an intrinsic tradeoff: they enhance incentives to invent, but at the expense of providing disclosure to the public.[267] In the context of national cybersecurity inventions, the benefits of patent protection are nearly nonexistent since they can be commandeered by the government and the costs of losing patent protection would be highly deleterious to potential national cybersecurity inventors.[268] On the benefits side, patents resolve market failures by granting patentees a right to exclude others from using their inventions, thus shoring up incentives to invent, assuming that, however, those rights will not be taken by the government.[269] Thus, although patents enable market incentives to incentivize inventors to invent, they do not create market incentives.[270] Ultimately, it is the market demand that drives the generation of patented technologies.

The patent paradigm fails to translate to national cybersecurity inventions, for almost by definition, there is relatively little market demand for such innovations. That is, assuming the government is the main potential purchaser of national cybersecurity inventions and there is not a private sector market for them, patenting of national cybersecurity invention would be unlikely to generate significant revenues, thus defeating incentives for invention. Additionally, even if exclusive rights provided significant financial return on national cybersecurity inventions, such incentives are not particularly germane to them. As noted earlier, the motivations underlying national cybersecurity inventions are generally economic only when the invention would be known to advance a corporate cybersecurity interest. In particular, the challenge of determining whether a cybersecurity innovation benefits only corporate interests provides ample motivation for society to consider alternative innovation policies aside from the patent system. Furthermore, profit motives are not the driving force for creating technological solutions for achieving national cybersecurity.

Moreover, exclusive right on national cybersecurity innovations are plagued by difficulties of patent enforcements, which is more difficult than other technologies. National cybersecurity inventions are subject to government patent use, which allows the government to use patented inventions through a taking of

---

267 Jay P. Kesan, *Economic Rationales for the Patent System in Current Context*, 22 GEO. MASON L. REV. 897, 898–99 (2015).

268 *See supra* Section III.A.3.

269 Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property*, 71 UNIV. CHI. L. REV. 129 (2004).

270 *See generally* Kapczynski & Syed, *supra* note 248.

a patent license.[271] Even if national cybersecurity inventions were subject to exclusive rights, patentees would face significant challenges in bringing enforcement actions against the government,[272] which further depresses incentives to patent national cybersecurity inventions in the first place.

Lastly, the perceived informational benefits of utilizing patents and markets to allocate resources for national cybersecurity innovation would not apply and are largely inapposite. A classical argument in favor of patents for technological development is that market exchanges create price signals that allocate resources for invention more efficiently than centralized planning.[273] While the information efficiency of markets justifies the patent system in many technological contexts to incentivize research and development, it fares poorly when the market signals are weak. In the case of national cybersecurity innovations, their demand does not translate into commensurate market demand since there are few purchasers (other than government) who value the innovation and there is risk of government secrecy and eminent domain.

The misalignment of the traditional view of the patent system with an expansive, modern critical infrastructure can be demonstrated with a graphical representation in *Figure 3*. As national cybersecurity technologies have increasingly connected data to the critical infrastructure, more of the critical infrastructure is becoming a public good. By contrast, the patent system, which scholars have commented provides incentives for physical creations, has remained rooted in providing a market-based innovation mechanism for the physical world.[274] The physicality in the form of the invention, whether by actual reduction to practice or constructive reduction to practice, suggests that the patent system historical basis for incentivizing innovation is in the physical world.[275] Commentators have noted that the patent system is ineffective for software-based and digital inventions, which obfuscate the underlying innovation and do not promote adequate incentives.[276] The misalignment of the

---

271 Williams & Ghrist, *supra* note 176 (describing the eminent domain and taking patent license authority of the U.S. government in allowing an inventor to obtain money damages for the government's use of patented inventions while at the same time not restricting the government's use of the invention).

272 *See supra* Section III.A.3.

273 Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J.L. & ECON. 1, 11–13 (1969).

274 Christopher A. Cotropia, *What Is the Invention*, 53 WM. & MARY L. REV. 1855, 1897 (2012) ("The incentive-to-invent story assumes patent law will use this contextualized invention and demands that patent law provide protection for an invention that is both created and eventually sold to the public.").

275 *See* Christopher A. Cotropia, *Physicalism and Patent Theory*, 69 VAND. L. REV. 1543, 1545 (2016).

276 Bronwyn H. Hall & Meagan MacGarvie, *The Private Value of Software Patents*, 39 RSCH. POL'Y 994, 1003–05 (2010) (summarizing the critique of information and software patenting,

proper innovation mechanism, with the changing nature of critical infrastructure, suggests that another type of innovation mechanism is more appropriate for fostering the developing national cybersecurity for critical infrastructure.[277]

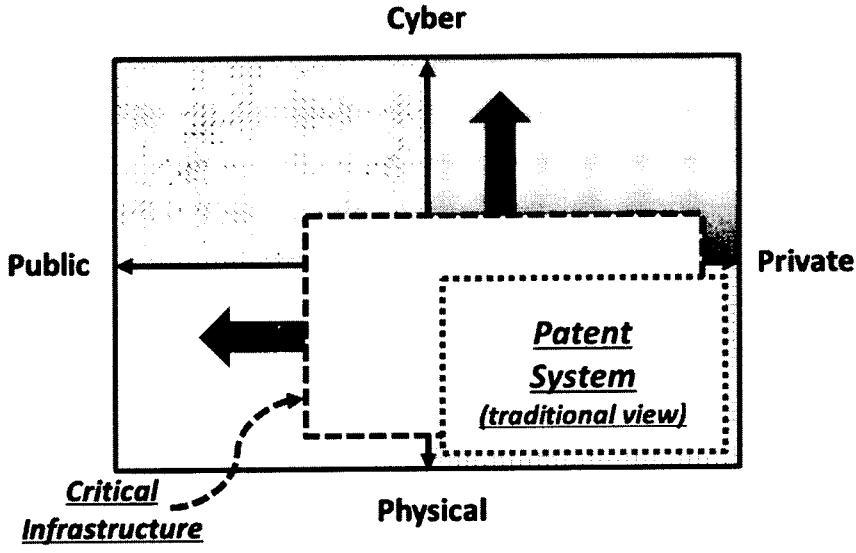

Figure 3: Graphical representation of the misalignment of the traditional view of the patent system with an expansive, modern critical infrastructure

Thus, the benefits of patent protection on national cybersecurity inventions would be mostly absent, and there would be a significant societal cost. Exclusive rights for national cybersecurity inventions would produce deadweight loss, which is deleterious for protection of critical infrastructure. Moreover, extending patent rights to national cybersecurity too far could even dissuade would-be inventors of technologies that would protect the critical infrastructure, resulting in perhaps decreasing national cybersecurity innovation. It appears that introducing exclusive rights and profit motives for national cybersecurity may actually undermine efforts to protect the critical infrastructure. For these reasons, extending exclusive rights to national cybersecurity innovations would be ineffective and is ill advised for innovation policy.

---

including being of low quality, lacking adequate prior art, not including source code implementation, and being vague and broadly worded).

277 *See infra* Section II.A. and Section IV.B.

C. *The Potential Benefits with Public Finance Initiatives for National Cybersecurity Innovation*

Approaches other than patents provide inducements mechanisms for promoting national cybersecurity innovation. Government should consider funding of mechanisms and endeavors that subsidizes national cybersecurity innovation, which should not be subjected to exclusive rights.[278] In this regard, a public finance strategy that is funded from general tax revenues would promote national cybersecurity and would reduce the deadweight losses associated with the patent system.[279] In so doing, public finance initiatives that are promoted by the government should justify national cybersecurity innovation and would enable knowledge spillovers to foster further future technological advancements that would otherwise not happen with the patent system.[280]

National cybersecurity innovation should be subsidized by public funds, and government should directly fund either prizes or contribute to public and private mechanisms that foster it. Public funding through government-sponsored innovation mechanisms for national cybersecurity innovation is more aligned with the modern critical infrastructure, whereas the patent system's alignment with the market may have a negative impact. The alignment of government-sponsored innovation mechanisms with an expansive, modern critical infrastructure is demonstrated with a graphical representation in *Figure 4*.[281] Government-sponsored mechanisms will have a comparative advantage relative to markets and the private sector for national cybersecurity innovation, for which its value is not reflected in market prices. Although public finance of government-sponsored mechanisms is subject to deficiencies from biases and

---

278 *See supra* Section IV.A.

279 Camilla A. Hrdy, *Patent Nationally, Innovate Locally*, 31 BERKELEY TECH. L.J. 1301, 1304–07, 1325–27 (2016).

280 *See generally* Hrdy, *supra* note 246.

281 The government-sponsored innovation mechanisms as shown in *Figure 4* reflect this Article's prescriptions of prizes and CRADAs, which are shown as a rectangle to reflect the ability to span both public and private sectors. Thus, while the figure demonstrates that prizes and CRADAs, unlike the traditional patent system's reliance on the market, is based on public finance mechanisms. As such, while prizes and CRADAs have private sector elements, which are necessary to align with the mostly private sector ownership of critical infrastructure, the emphasis on the public sector is shown to demonstrate the alignment with the expansive connection of data and devices of the modern, expansive critical infrastructure (for which greater aspects of it are considered public goods). Furthermore, it should be noted that prizes and CRADAs can incentivize innovation in the cyber domain more appropriately than the traditional view of the patent system; as such, the figure shows that prizes and CRADAs can be structured to incentivize in the cyber domain (as well as the physical domain) through dotted, vertical arrows (for viewability, the box representing prizes and CRADAs is drawn in a thin fashion, but the dotted, vertical arrows attached demonstrate that it is conceptually "taller" than actually shown in the figure).

political interests,[282] the government-driven sphere is in many ways better situated than the market to define technological innovation priorities in national cybersecurity.[283]

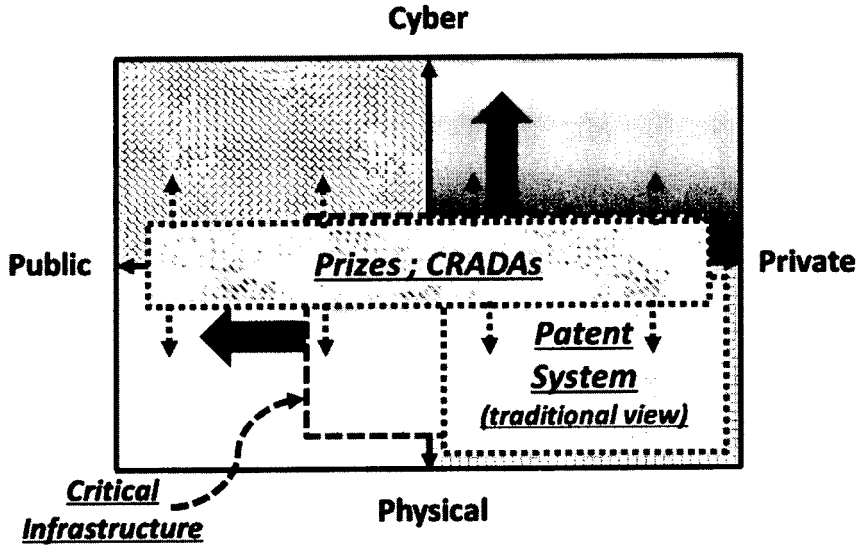

Figure 4: Graphical representation of greater alignment of public funding (government-sponsored) innovation mechanisms with an expansive, modern critical infrastructure

The prescriptions profiled here have several benefits. Government-run support of national cybersecurity can generate additional financial support from the private section, and in so doing, amplify, the impact of taxpayer assistance.[284] Additionally, delegating some of the involvement in the decision making process to the private in such government-run mechanisms would offer advantages relative to purely centralized decision making.

There are some limitations to public funding of government-driven mechanisms for national cybersecurity innovation that are based on public choice theory. Contrary to the pricing and information distribution efficiencies of market-based mechanisms, public funding is susceptible to bias and political interest that favors parties at the expense of efficiency and creation of bureaucracy.[285] Public choice theory suggests that public funding promotes

---

282 Rochelle Cooper Dreyfuss, *Does IP Need IP? Accommodating Intellectual Production Outside the Intellectual Property Paradigm*, 31 CARDOZO L. REV. 1437, 1440 (2010).

283 *See infra* Section IV.A.

284 Sichelman, *supra* note 241, at 286.

285 Gary M. Lucas Jr. & Slavisa Tasic, *Behavioral Public Choice and the Law*, 118 W. VA. L. REV. 199, 225–37 (2015).

patronage when a centralized authority is given authority to make broad investment decisions with limited information.[286] Nonetheless, some of these biases and information costs can be mitigated with some private sector participation in decision-making. Furthermore, public funding of government-driven innovation mechanisms, while unclear what an optimal amount should be, represents a relatively small portion of other federal funding priorities.[287] In sum, public funding of government-driven mechanisms represents a powerful engine for promoting national cybersecurity innovation, which should not be subject to counterproductive regime of exclusive rights with patents.

1. Prizes

Government-sponsored prizes should have significant potential to promote national cybersecurity innovation. Such prizes encourage innovation by rewarding innovators that make the fruits of their innovation available to the public.[288] Notable examples of prizes in the field of cybersecurity include the Cybersecurity Excellence Awards, CyberSecurity Breakthrough Awards, and the Cyber Defense Awards. Prizes encourage innovators to achieve a certain technological objective and only award funds after a satisfactory technological completion.[289] Such prizes can be designed and administered to achieve a special need for society.[290]

Prizes that are awarded on an ex post basis should promote national cybersecurity innovation by simulating the development of workable technological solutions.[291] The techniques used to win the challenges may address a variety of national cybersecurity needs, such as active defense techniques, industrial control system and SCADA protections to vulnerabilities, and passive defense add-ons to industrial control architectures.[292]

---

286 EAMONN BUTLER, PUBLIC CHOICE—A PRIMER 44 (2012); Craig Allen Nard & Andrew P. Morriss, *Constitutionalizing Patents: From Venice to Philadelphia* (Case Sch. of L., Working Paper No. 04-12, 2004).

287 R. ATKINSON, D. CASTRO, S. ANDES, S. EZELL ET AL., INNOVATION POLICY ON A BUDGET 1 (2010); George H. Pike, *Access to Federally Funded Research Back to Congress*, 26 LEGAL ISSUES 8 (2009).

288 V.V. Chari, Mikhail Golosov & Aleh Tsyvinski, *Prizes and Patents: Using Market Signals To Provide Incentives for Innovation*, J. ECON. THEORY 781, 782 (2012).

289 Michael J. Burstein & Fionna E. Murray, *Innovation Prizes in Practice and Theory*, 29 HARV. J.L. & TECH. 401, 402, 407, 424, 433, 444, 448 (2016).

290 NAT'L SCIENCE FOUND., INNOVATION INDUCEMENT PRIZES (2007).

291 Thomas Kalil, *Prizes for Technological Innovation*, HAMILTON PROJECT (BROOKINGS INST. 2006), https://www.hamiltonproject.org/assets/legacy/files/downloads_and_links/Prizes_for_Technological_Innovation.pdf.

292 Lee, *supra* note 5, at 31–43.

Scholars and policymakers are increasingly enthusiastic about prizes since they have a track record of spurring innovation and solving tough problems.[293] There should be a resurgence of government-sponsored prizes for national cybersecurity innovation. Government-sponsored prizes offer several informational advantages when adequate market incentives do not exist and over traditional grants.[294] Notably, such prizes do not require explanation of how a technological problem is solved nor do they require identification on an ex ante basis who would be the best innovator to solve it.[295] In so doing, they increase access to nonparticipants in innovation with new ideas that may not normally apply for grants or have funds necessary to apply for patents.[296]

Moreover, since government-sponsored prizes require an innovation to complete solving of technological problems, they avoid the detrimental effects of over-promising for grant recipients.[297] Additionally, prizes can simulate additional private sector investment to augment their cash value, and create a multiplier effect for society by encouraging additional parallel effects to provide additional solutions, thereby providing a greater return than the government-sponsored prize.[298]

Government-sponsored prizes have some limitations, however, that can be addressed with appropriate calibration. They require the government sponsoring entity to determine which innovations to pay for and how much to spend for the prize through a nonmarket mechanism.[299] This could cause government decision makers to introduce biases with defining the scope of the technological challenge, in selection of the winner, and the award amount.[300] Additionally, government-sponsored prizes present risk for the participants, who may only invest significant time or overspend in trying to win a prize but not achieve success.[301] Also, government-sponsored prizes may be duplicative of

---

293 B. Zorina Khan, *Inventing Prizes: A Historical Perspective on Innovation Awards and Technology Policy* 3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 21375, 2015).

294 *See generally* Roin, *supra* note 241.

295 Kalil, *supra* note 291, at 6.

296 *Id.* at 7.

297 Liam Brunt, Josh Lerner & Tom Nicholas, *Inducement Prizes and Innovation* (Norwegian Sch. of Econs., Discussion Paper No. 0804-6824, 2011).

298 Jonathan Bays, Tony Goland & Joe Newsum, *Using Prizes To Spur Innovation*, MCKINSEY Q. (2009).

299 LUCIANO KAY, MANAGING INNOVATION PRIZES IN GOVERNMENT (2011), http://www.businessofgovernment.org/sites/default/files/Managing%20Innovation%20Prizes%20in%20Government.pdf.

300 Reto Hofstetter, Z. John Zhang & Andreas Herrmann, *The Hidden Pitfall of Innovation Prizes*, HARV. BUS. REV. (Nov. 27, 2017), https://hbr.org/2017/11/the-hidden-pitfall-of-innovation-prizes.

301 Czerina Patel, *Social Innovation Prizes: Who Really Wins*, INSIDE OUT, http://insideoutpaper.org/social-innovation-prizes-who-really-wins/ (last visited Oct. 11, 2020).

private-sector prizes if not delineated properly, thereby resulting in duplicative and wasteful effects for society.[302] Finally, prizes must be of the right size amount in order to incentivize innovators and be calibrated towards the proper metric.[303]

Thus, prizes are best suited for breakthrough and radical national cybersecurity innovations that take leaps from the current state of the art.[304] It would require calibration of the size of the award to be sufficient to incentivize the innovative activity.[305] As the scholarly literature has suggested, the prize award can be tied to a measurable technological metric to promote the appropriate innovative response.[306] Government-sponsored prizes have seen a resurgence in other technological domains, and national cybersecurity innovation policymakers should pay attention and take action. Such prizes should provide the necessary speed and agility to provide major technological innovations to protect the critical infrastructure and rapidly improve cyber defense.

2. Cooperative Research and Development Agreements (CRADAs)

National cybersecurity innovation can be accelerated by providing public–private sector collaboration, such as for example, CRADAs, which can promote communal public–private interactions that should drive national cybersecurity innovation.[307] Cooperative arrangements between the public and private sector have been helpful in infrastructure development, such as building transportation systems, hospitals, and water and sewer systems, and similarly such interactions can help to develop the critical infrastructure for national cybersecurity. Relationships between government and the private sector, even

---

302 B. Zorina Khan, *Inventing Prizes: A Historical Perspective on Innovation Awards and Technology Policy* 3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 21375, 2015).

303 Heidi Williams, *Innovation Inducement Prizes: Connecting Research to Policy*, 31 J. POL'Y ANALYSIS & MGMT. 767 (2012).

304 *See generally* Mokter Hossain, *Breakthroughs with Competition-Based Innovation: The X Prize Foundation*, J. ORG. DESIGN (2014); Michael Hendrix, *The Power of Prizes: Incentivizing Radical Innovation*, U.S. CHAMBER OF COM. FOUND., https://www.uschamberfoundation.org/power-prizes-incentivizing-radical-innovation-0 (last visited Oct. 11, 2020).

305 Kwasi Mitchell, Nes Parker, Sahil Joshi, Jesse Goldhammer et al., *The Craft of Incentive Prize Design: Lessons from the Public Sector*, DELIOTTE INSIGHTS (June 9, 2014), https://www2.deloitte.com/us/en/insights/topics/social-impact/the-craft-of-incentive-prize-design.html.

306 Lee Davis, *How Effective Are Prizes as Incentives to Innovation? Evidence From Three 20th Century Contests* 5, 7, 18 (May 7, 2004) (unpublished manuscript) (available at https://www.keionline.org/misc-docs/ds2004-1343.pdf).

307 NAT'L INST. OF STANDARDS & TECH., CRITICAL CYBERSECURITY HYGIENE: PATCHING THE ENTERPRISE (Feb. 21, 2019), https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise.

when driven by government, should matter in national cybersecurity innovation, since public–private collaboration can create its knowledge spillovers.[308] Public–private sharing of data and collaboration related to coordinating cyber threats and mitigation issues can be promoted through R&D in CRADAs.

CRADAs are a government initiated mechanism for formalizing interactions and partnerships between federally-funded laboratories and the private industry.[309] As a collaborative means to perform research and development, CRADAs serve as legal contracts that enable federally-funded laboratories to conduct joint research with private firms.[310] As written agreements between private companies and a government agency, CRADAs serve as a mechanism by federal laboratories to engage in collaborative research with non-federal partners for technology transfer to move government-funded research and development into the marketplace.[311] In so doing, they operate as a joint venture between a federal laboratory and the private sector.[312] CRADAs close the interactions between the public and private research and development to promote technology transfer and endogenous knowledge spillovers.[313] Using CRADAs should serve the policy and objectives of Congress in promoting collaboration between commercial and governments concerns by promoting public–private partnerships and unique private sector use of federal lab equipment and transfer of scientific information.[314] Statutes authorize federal agencies to enter into licenses and agreements with their CRADA partners to provide, accept, retain, and use funds, personnel, and service from the collaborating party.[315] As in any government-industry collaboration, contractual questions require negotiation, including development of intellectual property.[316] However, unlike other forms of a federal laboratory sector collaboration,

---

308 James D. Adams, Eric P. Chiang & Jeffrey L. Jensen, *The Influence of Federal Laboratory R&D on Industrial Research* (Nat'l Bureau of Econ. Rsch., Working Paper No. 7612, 2000).

309 152 U.S.C.A. § 3710 (West 2020).

310 Clovia Hamilton, *University Technology Transfer and Economic Development: Proposed Cooperative Economic Development Agreements Under the Bayh-Dole Act*, 36 J. MARSHALL L. REV. 397 (2003).

311 *Non-Standard Navy Cooperative Research and Development Agreement between the Naval Research Laboratory (NRL) and XYZ Corporation (XYZ)*, Sept. 18, 2018, https://www.nrl.navy.mil/techtransfer/sites/www.nrl.navy.mil.techtransfer/files/files/XYZ%20CRADA%20Mar%2012%202019.pdf.

312 Nicholas S. Vonortas, U.S. Policy Towards Research Joint Ventures 7, 21 (Nov. 1999) (unpublished manuscript) (available at https://www.econstor.eu/bitstream/10419/155068/1/NDL2000-014.pdf).

313 Adams et al., *supra* note 308, at 3.

314 Robert Premus, *Moving Technology from Labs to Market: A Policy Perspective*, INT'L J. TECH. TRANSFER & COMMERCIALIZATION, Jan. 2002, at 1, 1.

315 152 U.S.C.A. §§ 3710a(b)(1), (b)(3)(A) (West 2020).

316 Hamilton, *supra* note 310, at 418.

CRADAs require cost sharing and an ongoing commitment that necessitates an intensive interaction.[317]

Not surprisingly, CRADAs often exhibit close relationships among government and the private sector. In addition to taking into account the needs and desires of the government and the private sector when commercializing a technology, CRADAs allow for each to benefit financially.[318] There is flexibility in the CRADA in terms of revenue share, and often, the industry partner can pursue patents on the innovative technology with the federal laboratory sharing in royalties.[319] Under the statute that authorizes CRADAs, 15 U.S.C. § 3710a, allow for formalizing mechanisms and partnerships between the federal government and private industry.[320]

CRADAs have been part of historical development in military technology and for the national security context, and there should be more development in the cybersecurity context. One of the reasons that CRADAs are so important for national cybersecurity innovation is because they involve both the government and the private sectors.[321] This intensive knowledge sharing can vastly accelerate the transfer and development of a new national cybersecurity technology that often requires both government and private sector cooperation.[322] The knowledge for implementing and integrating a national cybersecurity technology resides in government, rather than the private sector, since the government is responsible for maintenance of the critical infrastructure and national cybersecurity should be a public good.[323] In the context of national cybersecurity innovations, for example, the integration of the public and private technological elements of the critical infrastructure further underscores the importance of mechanisms by which innovation can best spread.

---

317 Adams et al., *supra* note 308, at 3.

318 Arnold Reisman & Aldonoa Cytraus, Institutionalized Technology Transfer in USA: A Historic Review 21–22 (Aug. 27, 2004) (unpublished manuscript) (available at https://ssrn.com/abstract=585364).

319 Everett M. Rogers, Elias G. Carayannis, Kazuo Kurihara & Marcel M. Allbritton, *Cooperative Research and Development Agreements (CRADAs) as Technology Transfer Mechanisms*, 28 RSCH. & DEV. MGMT. 79 (1998); *Cooperative Research and Development Agreement*, ACQNOTES (May 7, 2020), http://acqnotes.com/acqnote/tasks/cooperative-research-and-development-agreement.

320 15 U.S.C.A. § 3710(a); *How and When To Use a CRADA*, NAT'L INST. OF MENTAL HEALTH, https://www.nimh.nih.gov/research/research-conducted-at-nimh/collaborations-and-partnerships/cooperative-and-development-research-agreements/how-and-when-to-use-a-crada.shtml#when (last visisted Nov. 12, 2020).

321 U.S. Department of Commerce, Office of Technology Policy, Technology Administration (Feb. 2000) at 13–5.

322 Rogers et al., *supra* note 319.

323 *See supra* Section III.B.1.

More broadly, the unique nature of national cybersecurity innovation requires avenues for integration of public sector infrastructure and private sector elements for their dissemination, particularly compared to the seemingly objectively discrete technologies promoted by the patent system. As discussed earlier, most national cybersecurity is not discrete, physical hardware and software, but instead are embedded devices and Internet of Things that are susceptible to malicious cyber-attacks.[324] Such national cybersecurity technologies require a significant amount of interaction between cyber and physical systems that span both public and private sector infrastructure.[325] Indeed, in some cases, national cybersecurity technologies integrate each of cyber and physical elements, as well as each of public and private sector elements, and the classification is very difficult to distinguish.

Thus, a mix of government and private interactions can play a powerful role in enabling national cybersecurity innovation to develop, deploy, and spread. After all, innovations that necessitate operation on critical infrastructure can benefit substantially from government policy intervention and support. The public infrastructure includes an established network of government-controlled communication systems, dams, electrical grids, and transportation system.[326] Federally funded laboratories can aid in a variety of ways to experiment upon and test national cybersecurity innovations. Additionally, private sector efforts can support and formalize manufacturing and deployment resources to promote integration of national cybersecurity innovations on the critical infrastructure.

In a more concentrated fashion, CRADAs leverage the power of knowledge exchange between federally-funded laboratories and private sector resources to promote national cybersecurity innovation.[327] The connection and exchange that drive government and private sector interactions via CRADAs facilitate rapid dissemination of new knowledge and create knowledge spillovers.[328] CRADAs can provide infrastructure for concentrated collaboration between government and the private sector, which in turn, can promote national cybersecurity innovation.[329] In effect, government-funded and government-promoted CRADAs serve to provide connections between the government and private sector to accelerate national cybersecurity innovation.

---

324 *See supra* Section II.A.1. and Section II.B.

325 *See id.*

326 Haber & Zarsky, *supra* note 87.

327 *NIST and NCCoE Use CRADA To Improve Cybersecurity in Healthcare Sector*, FED. LABS, https://federallabs.org/successes/success-stories/nist-and-nccoe-use-crada-to-improve-cybersecurity-in-healthcare-sector (last visited Oct. 11, 2020).

328 James D. Adams, *Endogenous R&D Spillovers and Industrial Research Productivity*, (Nat'l Bureau of Econ. Rsch., Working Paper No. 7484, 2000); Adams et al., *supra* note 308, at 2–3.

329 ARNOLD REISMAN & ALDONA CYTRAUS, INSTITUTIONALIZED TECHNOLOGY TRANSFER IN USA (2004).

D. Normative Implications and Integration of Prizes and CRADAs

Technological innovation is one of many policy mechanisms for promoting national cybersecurity and responding to cyber-attacks.[330] In sum, the patent system's Invention Secrecy Act and government patent use are ineffective for incentivizing national security; this Article instead proposes that policymakers expand prizes and public–private Cooperative Research and Development Agreements (CRADAs) interactions. This Article has more precisely delineated the boundary of government intervention and market forces to argue that the optimal level of incentives for national cybersecurity can be achieved if: (1) in the short term, the government achieves an exogenously identified national cybersecurity policy goal that sets the amount of an *ex post* prize correctly to incentivize innovators to rapidly develop solutions; and (2) in the long term, government expands the missions of its federal laboratories in CRADAs under 15 U.S.C.A. § 3710a to generate more adequate *ex ante* patent incentives and *ex post* patent licensing.

Beyond an innovation mechanism in isolation, sometimes the best mechanism for promoting innovation is to expand the capabilities of a single mechanism in isolation through a combination. This Article has presented generally two contrasting archetypes for incentivizing national cybersecurity innovation—market-based mechanisms and public finance government-sponsored initiatives. It has presented the virtue of prizes for accelerating national cybersecurity innovation,[331] the virtue of CRADAs in integration public and private interaction to intensify national cybersecurity innovation, and the misfit of exclusive rights with the patent system in thwarting cybersecurity innovation. A central insight is that a combination of CRADAs and prizes can intensify public–private interactions, which can be accelerated further to yield technological solutions.

E. Future Directions

This Article introduces the perspective of innovation policy into cybersecurity law and policy scholarship and observes that greater attention should be given to the role of government and public–private partnerships in fostering technological development. The implicit assumption is that patents are significant in themselves for the technological field of cybersecurity such that

---

330 *See generally* U.S. CYBERSPACE SOLARIUM COMM'N, LEGISLATIVE PROPOSALS (July 2020), https://drive.google.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view (providing legislative proposals to support the implementation of cyber deterrence and legislative recommendations).

331 Patric M. Reinbold, How to Get the Most from Your Host: Risks and Rewards of Intellectual Property Terms in Government Prize Competitions (2020) (unpublished manuscript) (available at https://ssrn.com/abstract=3579679).

society should pay attention to their role and the need for change in promoting innovation to protect the critical infrastructure. As noted, the patent system does not adequately incentivize national cybersecurity innovators, who would be undercompensated by patent rewards for their inventions that protect critical infrastructure.

As this Article has shown, the expanding scope of ICT, increasing number of networked devices, and the interwoven nature of data and physical facilities, has promoted co-mingled public–private elements to the critical infrastructure. This Article has introduced a novel and valuable line of inquiry, which explored the intersection of cybersecurity and patent law to suggest that technological advancement presents unique challenges if the sole focus is the patent system, and instead, has proposed that prizes and CRADAs should have significant beneficial effects on national cybersecurity innovation. While this Article has introduced a new scholarly discussion about technological innovation into cybersecurity law and policy, more attention to parsing government needs versus the private market and also government versus private mechanisms is necessary. These are related areas of study, and this Article calls for further examination to elucidate their effects on national cybersecurity innovation.

Future research can pursue those lines of inquiry, and in so doing, evaluate how to design and deploy optimal prizes and CRADAs. A future research project that assesses why national cybersecurity inventors are undercompensated by the government-run reward system may uncover similar problems that may apply to prizes and CRADAs as well. Future research can assess whether the patent reward system's undercompensation of national cybersecurity inventions is caused by uncertainty with the guarantee of the reward, the size of the reward being too small, or the transaction cost being too great. By analyzing the perspectives and concerns of national cybersecurity inventors, such a future research study could provide broader insights about the evaluation and implementation of prizes and CRADAs aimed at improving national cybersecurity.

While it is important to understand how to size a prize or how to implement a CRADA, it is also important to contextualize these proposals within a broader range of innovation mechanisms for national cybersecurity. Broader research insights into the role of a new government agency, the role of negative prizes, and tradeoffs with the choice of trade secrets specifically applicable to national cybersecurity could spawn new scholarly perspectives on the intersection of cybersecurity and technological innovation. Furthermore, a future research project could question whether government should even have a role in national cybersecurity innovation and also could explore an even more thorough account of the spillover effects of national cybersecurity focused prizes and CRADAs onto corporate cybersecurity and into society.

Along these lines, the theoretical and normative contributions of this Article provide motivation for further examination of the effects of innovation mechanisms on national cybersecurity. In sum, while it is important to

understand the complex ways in which innovation impacts national cybersecurity, it is also important to contextualize these effects within the broader economic policy considerations that protect the critical infrastructure.

V. CONCLUSION

This Article has broken new ground by exploring the underappreciated phenomena of technological innovation mechanisms in national cybersecurity law and policy. U.S. government leaders are increasingly aware that protecting critical infrastructure includes providing innovative national cybersecurity technology.[332] An important question to address is whether government or the private sector, or a combination thereof, is essential to ensure an adequate level of cybersecurity.[333] A challenge in fostering national cybersecurity is that while approximately 85% of the U.S. critical infrastructure is owned by the private sector,[334] the government does not impose significant cybersecurity requirements on the private sector to protect critical infrastructure.[335]

In order to promote technological development that would benefit the critical infrastructure, several theoretical insights concerning unifying characteristics of national cybersecurity technologies and their connections to critical infrastructure are given. Moreover, the USPTO's restriction in patenting of some national cybersecurity technologies suppresses disclosure, whereas the patent system is meant to promote disclosure as part of quid pro quo. As such, secrecy of certain inventions supports this Article's normative position that a patent system is inadequate for incentivizing national cybersecurity, which is better done through prizes and CRADAs. The advancement of national cybersecurity to address critical infrastructure requires a reevaluation of innovation institutions for cybersecurity technologies.

The normative vision rooted in this Article for national cybersecurity is that the current patent system is slow and hampers innovation, whereas prizes rapidly place an invention into the public domain rapidly without deadweight losses and reciprocal public–private R&D interactions can recalibrate the patent bargain. The patent system's inadequacies for national cybersecurity include government suppression of patent disclosure through invention secrecy

---

332 Mary Calam, David Chinn, Jonathan Fantini Porter & John Noble, *Asking the Right Questions To Define Government's Role in Cybersecurity*, MCKINSEY & CO. (Sept. 19, 2018), https://www.mckinsey.com/industries/public-and-social-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity#.

333 *See generally* DAN ASSAF, CRITICAL INFRASTRUCTURE PROTECTION (Eric Goetz & Sujeet Shenoi eds., 2007).

334 Sales, *supra* note 98, at 1506.

335 Chung, *supra* note 199, at 441, 476, 450–51.

restrictions[336] and risk of eventual takings with compulsory licensing under government patent use[337] hampers innovation.

336 35 U.S.C.A. § 181 (West 2020).

337 28 U.S.C.A. § 1498.