

BASC WORKING PAPER SERIES

COMPARATIVE INDUSTRIAL POLICY AND CYBERSECURITY:
THE U.S. CASE

Vinod K. Aggarwal
Andrew W. Reddie

Working Paper 2018-02
<https://basc.berkeley.edu/working-papers/WP2018-02>

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project “Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications,” organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. For funding support, both authors would like to thank the Center for Long-Term Cybersecurity, the Institute of East Asian Studies, the Social Science Matrix and the Berkeley APEC Study Center (BASC). For research support, we are grateful to Mahshad Badii, Prashant Desai, Somi Yi, Anastasia Pyrinis, and Yujie Shen. We are also grateful to Phil Stupak, Michael Adams, Steve Weber, and Stephan Haggard for helpful comments during the drafting of the manuscript.

BASC working papers are circulated for discussion and comment. They have not been peer-reviewed.

© 2018 by Vinod K. Aggarwal and Andrew W. Reddie. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

Abstract

This paper evaluates the role of firms, governments, and other key stakeholders in the rise of industrial policy in the United States toward the cybersecurity sector. Our goals are as follows: 1) to examine the motivation for government promotion of the cybersecurity industry in the United States; 2) to inventory existing measures employed by the U.S. government; 3) to understand the driving forces of cybersecurity industrial policy in the United States; and 4) to examine the likely conflicts that will arise from the competitive pursuit of these industrial policies and to consider how they might possibly be resolved through international cooperation. To this end, we use a “market failure”-based analytical framework to serve as the structure for this project, drawing on a variety of approaches to understand industrial policy in the United States as well as the variety of intervention strategies and instruments used by the U.S. government.

Vinod K. Aggarwal¹
University of California, Berkeley
Department of Political Science
210 Barrows Hall
Berkeley, CA 94720
vinod@berkeley.edu

Andrew W. Reddie²
University of California, Berkeley
Department of Political Science
210 Barrows Hall
Berkeley, CA 94720
areddie@berkeley.edu

¹ Vinod K. Aggarwal is Travers Family Senior Faculty Fellow and Professor at the University of California at Berkeley, with appointments in the Travers Department of Political Science and the Haas School of Business. He serves as Director of the Berkeley Asia Pacific Economic Cooperation Study Center (BASC), Editor-in-Chief of the journal *Business and Politics*, and Co-Chair of the U.S. Consortium of APEC Study Centers. Dr. Aggarwal received his B.A. from the University of Michigan and his M.A. and Ph.D. from Stanford University.

² Andrew Reddie is a Ph.D. candidate in the Charles and Louise Travers Department of Political Science, University of California, Berkeley. He currently serves as a researcher for the Nuclear Policy Working Group, Complexity Science and Nuclear Security Group, Department of Nuclear Engineering, and Goldman School of Public Policy at UC Berkeley. He is also an affiliated researcher at the Center for Long-Term Cybersecurity at the UC Berkeley Information School and the Nuclear Science and Security Consortium and a researcher at the Center for Global Security Research at Lawrence Livermore National Lab. He holds an MPhil in International Relations from Oxford University as well as an M.A. and a B.A. (hons.) from the University of California, Berkeley.

Introduction

The United States government has a long history of taking advantage of, reacting to, and taking steps to support technological innovation. In the past two decades, the opportunities and risks afforded by the Internet have been steadily increasing. As Deputy Secretary of Defense George England pointed out during his tenure under the Bush administration:

...technology is an integral part of the solution to emerging challenges... but things have fundamentally changed. Technology is more widely available than ever before. Adversaries have ready access to leading-edge science and technology... it's out there, on the Internet... with detailed application instructions in multiple languages. But while some things have changed... some haven't. Just as it was in 1958, the answer is still to always stay ahead of everyone else in technology.³

Most recently, and following a series of cyber attacks on U.S. government and U.S. private sector targets, Internet technology and cybersecurity have become the technology *de jour* receiving the primary focus of U.S. policy-makers.⁴

This article examines the various efforts taken and policies used by the United States government “to stay ahead of everyone else” in cybersecurity. Specifically, we focus on the patterns of interaction between government and the private sector. To do this, we frame this research project in the context of political economy theories concerning market failure—in which the private sector fails to adequately provide the goods and services called for by public actors—and apply existing theories related to industrial policy to this new realm of government activity.

While the lessons from the international political economy literature have yet to be applied to cybersecurity, these conversations have already taken place in the public sector. Indeed, Deputy Secretary William Lynn asks:

“how do we [the U.S. government] partner with industry? Neither government nor the private sector can solve our cybersecurity challenges alone. Government needs industry, which owns and operates most of the nation's information infrastructure. The private sector needs government -- the government to establish coherent, effective and transparent laws and regulations.”⁵

Given the unique challenges afforded by the cyber domain, how firms and government interact will likely be of central importance. This article—and the broader project of which it is a part—offers a first effort to analytically examine the patterns of interaction between the public and private sector.

On a more practical level, this paper also engages with the questions of why and how the United States government is engaging with the expertise of engineers and computer scientists from Sili-

³ England, G. (2008, April 10). *DARPA 50th Anniversary Dinner*. Retrieved from speech delivered by Deputy Secretary of Defense Gordon R. England in Washington D.C. on technology.

⁴ Fonseca, Brian, and Jonathan D. Rosen. (2017). "Cybersecurity in the US: Major Trends and Challenges." In *The New US Security Agenda*, pp. 87-106. Palgrave Macmillan.

⁵ Lynn, W (2009, June 15). *Center for Strategic and International Studies*. Retrieved from speech delivered by Deputy Secretary of Defense William J. Lynn in Washington D.C. on cyber security.

con Valley to address security challenges, in general, and in cybersecurity, specifically. During the Obama administration, Secretary Ash Carter sought to strengthen ties between the San Francisco Bay Area and Washington: “through successes and strains, our ties have broadly endured...but I believe we must renew the bonds of trust and rebuild the bridge between the Pentagon and Silicon Valley.”⁶ He goes on to note the broad cooperation necessary to address emerging security threats:

We want to partner with businesses on everything from autonomy to robotics to biomedical engineering; from power, energy, and propulsion to distributed systems, data science, and the Internet of things. Because if we’re going to leverage these technologies to defend our country and help make a better world, the Department of Defense cannot do everything in all these areas alone. We have to work with those outside. And the same is true, finally, with cybersecurity – we’re going to have to work together on this one.⁷

Increasingly, this cooperation involves far more than lip service and has been reflected in U.S. government policies that have sought to strengthen the cybersecurity industry—both to provide the public sector with necessary talent and to contribute to the strength of the economy itself. The growth of this relationship between Washington and Silicon Valley has not been without its procedural challenges.⁸ The recent controversy surrounding Google’s role in Project Maven—an artificial intelligence stood up by the military—and the petitioning of Google employees against the continued relationship between Google and DoD serves as the most recent examples of the dissent that is coupled with government involvement in the data economy.⁹

To examine these policies, our goals are as follows: 1) to identify real and perceived market failures of various types that lead to calls for government intervention (whether top down or bottom up) in the United States; 2) to inventory existing measures employed by the United States using the existing literature from international political economy concerning industrial policy; 3) to analyze the driving forces of cybersecurity industrial policy in the United States based on the political economy of state-society relations; and 4) to examine the likely conflicts that arise from the competitive pursuit of such industrial policies and how they might possibly be resolved through institutional cooperation.

⁶ Carter, A. (2015, April 23). Drell Lecture: “Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity” (Stanford University). Retrieved from <https://www.defense.gov/News/Speeches/Speech-View/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber/>

⁷ *ibid.*

⁸ Schulman, Loren DeJonge, Alexandra Sandra and Madeline Christian. (2017, July 18). “The Rocky Relationship Between Washington and Silicon Valley: Clearing the Path to Improved Collaboration.” *Center for New American Security*. Retrieved from <https://copia.is/wp-content/uploads/2017/07/COPIA-CNAS-Rocky-Relationship-Between-Washington-And-Silicon-Valley.pdf>

⁹ Shane, Scott, Cade Metz and Daisuke Wakabayashi. (2018, May 30). “How a Pentagon Contract Became an Identity Crisis for Google.” *The New York Times*. Retrieved from <https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html>; Wakabayashi, Daisuke and Scott Shane. (2018, June 1). “Google Will Not Renew Pentagon Contract that Upset Employees.” *The New York Times*. Retrieved from <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>; Wakabayashi, Daisuke and Cade Metz. (2018, June 7). “Google Promises Its A.I. Will Not Be Used for Weapons.” *The New York Times*. Retrieved from <https://www.nytimes.com/2018/06/07/technology/google-artificial-intelligence-weapons.html>

2. Market Failure and the U.S. Cybersecurity Industry

Concerns related to cybersecurity from the U.S. government stem from a broader fear among engineers that applications and products reliant upon Internet technology suffer from various security-related vulnerabilities. In this section, we detail the units of analysis with which this study is concerned and discuss the conceptualization of market failure.

2.1 Units of Analysis

For the purposes of this study, we identify three critical sets of actors with which the government interacts in our analysis. There are: “cybersecurity firms,” “Internet technology firms,” and “Internet-adjacent” firms. Understanding each type of industry player is integral to conceptualizing the interests they bring to the issue-space as well as considering how government actors may view them.

The first category involves cybersecurity firms that work directly on cybersecurity-related challenges for a variety of commercial and/or government clients. Their role runs the gamut from creating cybersecurity-related products to protecting networks, consulting on cybersecurity literacy for employees, performing threat assessments, and tracing cyber attacks and hacks. Examples of these types of firms in the U.S. include FireEye, Palantir, and Qadium. In-Q-Tel, a CIA funded venture capital firm provided a foundational investment in Palantir Technologies in 2003, and serves as an example of the close relationship between these firms and government.

Second, we point to Internet technology (IT) firms that rely on cybersecurity to protect their operations and products—but that are not involved in the cybersecurity space *per se*. Examples of this type of firm include those that work in what is often called the “big data” space such as Alphabet, Facebook, and IBM, which require cybersecurity to carry out their business and interact with customers.

Finally, there are Internet-adjacent firms whose products have Internet-based components but that are outside of the technology sector. These types of firms include those working in the “Internet of Things (IoT)” space such as General Electric, Tesla, and PG&E as well as firms such as the *New York Times* and *Washington Post* that rely upon the Internet for consumption of their products. The recent NHTSA guidelines for autonomous cars offer an example of government-business relations in a space where Internet technology is used for a kinetic, real-world application.

Interestingly, the first category of firms exists to address the cybersecurity concerns of IT and Internet-adjacent firms. The government, too, has increasingly faced security threats emanating from cyberspace—as the hack of the Office of Personnel Management makes clear—and has also started to play a role in attempts to mitigate the cybersecurity threats faced by firms. Already, there has been a significant amount of economic activity related to cybersecurity and the industry has grown substantially in recent years. In the section to follow, we detail the state of the industry in the United States.

2.2 U.S. Cybersecurity Industry

Over half of global spending on cybersecurity occurs in the North American market and is primarily driven by the United States.¹⁰ Microsoft, for example, intends to invest \$1 billion each year on cybersecurity in coming years. This investment occurs in the context of an information technology industry worth \$909.2 billion measured in terms of real value added to the U.S. economy in 2016.¹¹

To protect this industry in 2017, the U.S. government spent \$19 billion on cybersecurity, an increase from the \$14 billion it spent in 2016. According to the Obama Administration, this investment was necessary given the potential of cyber threats that “could lead to widespread vulnerabilities in civilian infrastructure and U.S. government systems.”¹² By 2022, it is projected that the U.S. federal government will be spending \$22 billion on cybersecurity each year. Beyond government spending, new market-making is also occurring in the United States with about 90% of all cyber insurance policies purchased by U.S. firms.

In terms of companies working in the cybersecurity sector, the United States is also a leader. Of Cybersecurity Venture’s Cybersecurity 500 list (a list of the 500 largest and most innovative cybersecurity companies), 350 were from the United States, Israel was second with 36 companies, and Canada was third with 13.¹³

The United States also remains a common target of cyber attacks. The number of incidents reported by federal agencies to the U.S. Computer Emergency Response Team (US-CERT) and the U.S. Office for Management and Budget (OMB) steadily increased from 2006 to 2016.¹⁴

2.3 U.S. Cybersecurity Market Failures

Given the obvious reliance upon the Internet in the U.S. economy, the substantial security vulnerabilities online represent a significant policy challenge. To think about these security vulnerabilities, we borrow from existing theoretical work in political economy to consider the insecurity in existing Internet architecture in terms of a market failure. Specifically, we suggest that framing cyber insecurity reflects the existing incentive structure in the current IT market in which innovation, attempts by firms to get to market as quickly as possible, and the emphasis on consumer-friendly user interfaces lead to security being a secondary or tertiary concern. As a result, the market fails to reward actors that privilege security. Cyber insecurity subsequently contributes to

¹⁰ Editors at Cybersecurity Ventures. (2016). “Cybersecurity Market Report”. Cybersecurity Ventures. Retrieved from: <https://cybersecurityventures.com/cybersecurity-market-report-test/>

¹¹ (2016). “Industry Data.” Bureau of Economy Analysis, U.S. Department of Commerce. Retrieved from: <https://www.bea.gov/iTable/iTable.cfm?ReqID=51&step=1#reqid=51&step=51&isuri=1&5114=a&5102=10>

¹² Clapper, James. (2016, February). Remarks of United States National Intelligence Director James Clapper to Congress. Retrieved from <http://www.npr.org/sections/thetwo-way/2016/02/09/466139494/key-moments-from-the-u-s-spy-chiefs-annual-litany-of-doom>

¹³ Kovacs, E (2014, August 25). “Global Cybersecurity Spending to Reach \$76.9 Billion in 2015. SecurityWeek. Retrieved from <http://cybersecurityventures.com/cybersecurity-500/>

¹⁴ (2016). “Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices.” *Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2016*. Retrieved from <https://www.gao.gov/assets/690/687461.pdf>

the vulnerability of companies and government actors and has contributed to the increasing role of government to address cybersecurity challenges.

Indeed, in an op-ed to the *Wall Street Journal* on February 9, 2016, President Barack Obama noted the inability of the market to protect government and companies from “criminals and lone actors who are targeting our computer networks, stealing trade secrets from American companies and violating the privacy of American people.”¹⁵ In the piece, he makes clear the importance of collaboration between the government and the private sector to address these challenges. Secretary Penny Pritzker also noted in her remarks to the Commission on Enhancing National Cybersecurity, “today, our cybersecurity posture is failing to keep pace with the incredible innovations our time.” These failures, she suggests, are driven by a lack of coordination and collaboration between industry and government as well as a chronic lack of human capital.

Gen. Keith Alexander, former head of the NSA, detailed these same fears during his speech at CSIS calling the risks “compromised by carelessness, poor design.”¹⁶ James Clapper (DNI), Marcel Lettre (DoD), and Adm. Michael Rogers (CYBERCOM), also detailed these challenges in a Joint Statement to the Senate Armed Services Committee on January 5, 2015. In their remarks, they point out that adversaries are increasingly likely to “exploit our nation’s public and private sectors in the pursuit of policy and military insights, sensitive research, intellectual property, trade secrets, and personally identifiable information.”¹⁷

Among U.S. allies, too, there are concerns that the free market has failed to adequately address cyber insecurity. In November 2015, Robert Hannigan, Director of GCHQ in the UK, told senior business figures that the free market is failing: “Standards are not yet as high as they need to be... the global cyber security market is not developing as it needs to: demand is patchy and it is not yet generating supply. That much is clear. The normal drivers of change, from regulation and incentivization through to insurance cover and legal liability, are still immature.”¹⁸

2.4 The U.S. Rationale for Government Intervention

Reflecting the arguments above, there are several rationales for U.S. government intervention in the cybersecurity sector. In this section, we outline several challenges facing the United States cybersecurity market before outlining the foundational documents that hitherto represent the U.S. response.

¹⁵ Obama, B. (2016, February 9). “Protecting U.S. Innovation from Cyberthreats”. The Wall Street Journal. Retrieved from <https://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003>

¹⁶ Alexander, K. (2016, May 3). “Center for Strategic and International Studies – Cybersecurity Policy Debate Series”. National Security Agency. Retrieved from <https://www.nsa.gov/news-features/speeches-testimonies/speeches/100603-alexander-transcript.shtml>

¹⁷ Clapper et al. (2017, January 5): Joint Statement for the Record. Senate Armed Services Committee on Foreign Cyber Threats to the United States. Retrieved from https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf

¹⁸ Jones, S. (2015, November 9). “GCHQ chief to say free market failing on cyber security”. Financial Times. Retrieved from <https://www.ft.com/content/4ec3e438-8708-11e5-90de-f44762bf9896>

First, there are two types of negative externalities that have served as the rationale for government intervention: economic externalities and security concerns. First, the economic costs incurred by cybercrime and cyber insecurity represent a drag on the U.S. economy. Addressing these challenges represent a public good for market participants. Second, the threat posed by cyber espionage and the international security consequence of cyber attacks and related fears concerning cyberwarfare have increasingly played a role in U.S. strategic decision-making, as evident in the National Security Strategy and 2018 Nuclear Posture Review that explicitly note the dangers posed by cyber weapons to the United States.¹⁹ The latter security rationale focused on three areas: the vulnerability of U.S. federal agencies to cyber attacks, the vulnerability of national critical infrastructure to cyber attacks, and the threat to the continuing competitiveness of the U.S. military vis-à-vis other great powers.

To address these externalities, there are two series of problems that market participants and policy-makers face: information problems and coordination problems. The information problems facing firms are considerable. Indeed, both firms in the IT sector and in other business sectors have been slow to address cybersecurity challenges. This could be due to cybersecurity falling outside the core of their business and the coordination problems associated with addressing them. With regard to specific types of malware and viruses, there is also an acute information problem given that information-sharing networks are in their nascent phase.²⁰ When threats are recognized, there are also coordination problems associated with creating the appropriate response architecture as well as challenges associated with enforcement of these responses. These coordination problems are particularly problematic given 1) the downstream consequences of cybersecurity breaches and 2) that any vulnerability is “networked.” The combination of these negative externalities, coordination, and information problems have led a number of scholars to suggest that the cybersecurity market represents a venue for the provision of public goods.²¹

Reflecting these economic and security concerns, we point to three foundational documents that have underpinned policy-making prerogatives in the cybersecurity sector over the past decade. The first is the Comprehensive National Cybersecurity Initiative (CNCI) born from the 2009 recommendations of the Cyberspace Policy Review that drove American policy-making around cybersecurity.²² It is worth noting that this Review and Initiative took place during a period of growing concern with regard to the use of cyber tools in warfare—particularly by Russia in Estonia and Georgia—and calls from members of the previous administration—most notably by

¹⁹ The fourth potential motivation is politically motivated. Policy-makers and politicians might seek to “do something” in the cybersecurity sector in lieu of doing nothing; U.S. National Security Strategy 2017; U.S. Nuclear Posture Review 2018.

²⁰ Indeed, a number of company representatives have noted the importance of ad hoc information sharing relationships with other firms, government agencies, and law enforcement.

²¹ Carr, Madeline. (2016) “Public-private partnerships in national cyber-security strategies.” *International Affairs* 92, no. 1: 43-62; Nye Jr, Joseph S. (2010) *Cyber power*. Harvard University Press.

²² (2009). “The Comprehensive National Cybersecurity Initiative”. The White House. Retrieved from <https://obamawhitehouse.archives.gov/node/233086>. Other important government documents include the DHS Blueprint for a Secure Cyber Future, the White House Cyberspace Policy Review, the President’s International Strategy for Cyberspace, the President’s Strategy to Combat Transnational Organized Crime, HSPD-7, NSPD 54, FISMA, the National Strategy for Trusted Identities in Cyberspace, and the DoD Strategy for Operating in Cyberspace.

William J. Lynn's in a *Foreign Affairs* article, "Defending a New Domain," and Richard C. Clark's book *Cyber War: The Next Threat to National Security and What to do About It*.

The Initiative itself had a tripartite structure calling for the establishment of "a frontline of defense against today's imminent threats," with the goal of "increasing the security of the supply chain for key information technologies" and "strengthening the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government." The latter two goals involve industrial policy processes toward cybersecurity outcomes. Initiative #8, for example, calls for a national strategy to meet the challenging of develop cybersecurity training and personnel development programs. These initiatives represent market creating and market modifying roles taken by the U.S. government.

The second foundational document is the 2015 DoD Cyber Security Strategy.²³ Included within the Strategy were various measures to address factor market failures including the importance of "building career paths" in the cybersecurity sector via institutions such as the nascent Defense Digital Service, "civilian recruitment" via public-private exchange programs, and the National Initiative for Cyberspace Education to address a shortfall of approximately 6,200 jobs in the cybersecurity sector.²⁴ Taken together, the strategy seeks to overcome the existing obstacles for government-private sector interaction such as the cumbersome clearance process, risk-averse project managers on the public sector side, bureaucratic decision-making apparatus, aging infrastructure, and antiquated human resources policies to contribute to the creation of a robust cybersecurity labor market and government consumption of cybersecurity products.

The third foundational document is the 2016 Cybersecurity National Action Plan to address the "need [for a] bold reassessment of how we approach security in the digital age."²⁵ This Plan includes a variety of initiatives including a proposed \$3.1 billion modernization of government IT, establishing a Commission on Enhancing National Cybersecurity comprised of academics and industry actors to issue recommendations on potential public and private sector initiatives intended to strengthen cybersecurity, updating the 2014 BuySecure Initiative, establishing a National Center for Cybersecurity Resilience, and allocating \$19 billion from the 2017 budget to various programs for small businesses and cybersecurity firms. The Plan also launched the National Cybersecurity Awareness Campaign to educate consumers about best practices for protect-

²³ Carter et al. (2015, April). "The DOD Cyber Strategy". Department of Defense. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

²⁴ (2016, April). "National Initiative for Cybersecurity Education (NICE) Strategic Plan". National Initiative for Cybersecurity Education. Retrieved from <https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan>. For more on education programs related to cybersecurity, see the Cyber Workforce Strategy and the nascent Cyber Workforce Incubator announced by UC Berkeley's CLTC. See also: the BNKR_75 Fellowship Program.

²⁵ Office of the Press Secretary. (2016, February 9). "FACT SHEET: Cybersecurity National Action Plan". The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>; Daniel, M., Scott, T., and Felten, E. (2016, February 9). "The President's National Cybersecurity Plan: What You Need to Know". The White House. Retrieved from <https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know>; Office of the Press Secretary. (2016, February 9). "Executive Order – Commission on Enhancing National Cybersecurity". The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity>

ing personal information through industry partnerships with leading tech and financial services firms. The campaign also supports the Federal Cybersecurity Workforce Strategy, which includes the CyberCorps scholarship program and the National Centers for Academic Excellence.

To deal with the problems facing the cybersecurity industry, the U.S. government, we argue, has a substantial number of industrial policy tools at its disposal—as already evidenced by the frameworks and initiatives noted throughout this paper. Below, we discuss the theory and empirical examples of these interventions.

3. U.S. Market Intervention

In this section, we systematically examine the variation associated with the patterns of intervention that the U.S. government has employed to address the market failures noted above.

3.1 Patterns of Intervention

To examine the patterns of interaction between Washington and firms in the past decade, we propose five typologies to describe these relationships by drawing on various industrial policy measures. These models draw from the variety of intervention measures that states might theoretically use but packages them into coherent strategic models. These five models combine some form of three ideal types of industrial policy: market making, market modifying, and market substituting, and we provide examples of each one.

3.1.1 Traditional Procurement and Licensing

The first pattern of U.S. government intervention in the cybersecurity market involves the government as a participant in the cybersecurity marketplace. There, it has significant market making, market modifying, and market substituting roles. The first represents the traditional pattern of government-private sector interaction practiced by the Department of Defense and defense firms.²⁶ Amid the postwar downsizing following WWII, Op-20-G (a naval intelligence agency) alumnae spun off Engineering Research Associates (ERA) to continue the development of early computational machines on government contracts without an official bidding process in what was the first example of this process.²⁷ This relationship between private contractors with close ties to government continued to grow over the course of the Cold War era. However, the procurement process has often been described as slow and burdensome—removing the potential for small firms to bid for government contracts—and has come under criticism given the new threats

²⁶ Gholz, E. and Sapolsky, H. (1999). “Restructuring the U.S. Defense Industry”. *International Security*. Retrieved from <http://www.mitpressjournals.org/doi/pdf/10.1162/016228899560220>;

Lindsay, J. (2006, July 18). “War Upon the Map: The Politics of Military User Innovation. Retrieved from <https://dspace.mit.edu/handle/1721.1/33457>; Avant, D. (2005). *The Market for Force: The Consequences of Privatizing Security*. Cambridge University Press. Retrieved from <https://books.google.com/books?hl=en&lr=&id=TJ3CzP2MiZUC&oi=fnd&pg=PP1&ots=5vMwzv7v&sig=tdfTCmIqKWuanNMkLEI41gyuWcA#v=onepage&q&f=false>;

Deutch (2001): Retrieved from

http://isites.harvard.edu/fs/docs/icb.topic706688.files/Consolidation_of_the_US_Defense_Industrial_Base.pdf

²⁷ Budiansky S. (2016) *Code Warriors*. Toronto, Canada: Alfred A. Knopf, psg. 99

and risks posed by cybersecurity. This has arguably led to the entrenchment of a small number of large firms dominating the space. Examples of company-government relationships that fall under this first model include those between the U.S. government and Lockheed Martin, Raytheon, SAIC, and others that operate primarily out of northern Virginia.

Recent efforts to reform this traditional procurement and licensing arrangement are being developed to make it simpler for smaller companies to contract with the government. CIBORG (the Commercial Initiative to Buy Operationally Responsive GEOINT) represents an example from the National Geospatial Intelligence Agency and the National Reconnaissance Office to speed up the process of buying data, hiring analysts, and contracting with companies. In March of 2017, for example, the CIBORG initiative led to a \$4.4M contract with VRICON for various data modeling and data packages.²⁸

In this model, the government might also supply seed funds to companies that are making strategically useful technologies that can be employed in an intelligence or military context. Following the much older DARPA-based model that provided seed funding to companies involved in early computing and network building, more recent instances government and private industry interaction involves the government providing direct investment to technologies with strategic value. An example of such an arrangement can be seen in how DARPA recently provided funding to Boston Dynamics to design and produce BigDog—a quadruped robot designed for the U.S. military—and DI-Guy—a software tool used in computer simulations by the military for troop training. There are also numerous instances of seed funding for specific technology firms that cultivate sponsorship from single government agencies. Such instances include Apple’s Siri virtual personal assistant tool developed by Stanford Research Institute (SRI) with seed funding from the Department of Defense and Google’s partnership with the NGA to provide a suite of data visualization tools.²⁹

3.1.2 Government as Venture Capitalist

The second model, in this case, market substituting, accounts for patterns of interaction between government and the private sector that uses an increasingly prominent investment vehicle—venture capital—to fund projects of importance to national security—including cybersecurity.³⁰ The founding of Palantir in 2003 with \$2 million in venture capital funding from In-Q-Tel—by a

²⁸ (2017, March 6). “NGA’s CIBORG initiative enables \$4.4M contract with VRICON for 3D modeling”. National Geospatial-Intelligence Agency. Retrieved from [https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA's-CIBORG-initiative-enables-\\$4-4M-contract-with-VRICON-for-3D-modeling.aspx](https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA's-CIBORG-initiative-enables-$4-4M-contract-with-VRICON-for-3D-modeling.aspx)

²⁹ Google Earth has similar origins (GPS through the Massive Digital Data Systems (MDDS) program).

³⁰ Lerner, J. (1996, September). “The Government as Venture Capitalist: The Long-Run Effects of the SBIR Program”. The National Bureau of Economic Research. Retrieved from <http://www.nber.org/papers/w5753>
See also: Brander, J., Du, Q., and Hellmann, T. (2014, March 17). “The Effects of Government-Sponsored Venture Capital: International Evidence”. *Review of Finance*. Retrieved from <https://academic.oup.com/rof/article/19/2/571/1581912/The-Effects-of-Government-Sponsored-Venture>; Gompers, P. and Lerner, J. (2001). “The Venture Capital Revolution”. *The Journal of Economic Perspectives*. Retrieved from http://www.jstor.org/stable/2696596?seq=1#page_scan_tab_contents;
Lerner, J. (2002, February). “When Bureaucrats Meet Entrepreneurs: The Design of Effective ‘Public Venture Capital’ Programmes”. *The Economic Journal*. Retrieved from <http://onlinelibrary.wiley.com/doi/10.1111/1468-0297.00684/full>

group of former CIA officials—along with a \$30 million investment from Peter Thiel serves as the prototypical example of this pattern of interaction. Palantir’s mission is to use big data and software to provide federal agencies of the U.S. intelligence community with a means of counter-ing the growing threat of terrorism. Its product, Palantir Gotham, does just that and is used throughout the intelligence and law enforcement community in the United States.

In-Q-Tel (IQT) itself, founded by former CIA director George Tenet in 1998, has provided hun-dreds of millions of dollars to over two hundred technology companies and has built relation-ships between members of the intelligence community and these firms. It describes itself as a “non-profit strategic investor that accelerates the development and delivery of cutting-edge tech-nologies for U.S. government agencies that keep our nation safe.”³¹ IQT’s mission is to “identify startups with the potential for high impact on national security” and the company works with private venture capital firms to provide funding for startups. In the process, it partners with the Central Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agen-cy, Office of the Secretary of Defense/Joint Chiefs of Staff, Defense Intelligence Agency, Feder-al Bureau of Investigation, National Reconnaissance Office, and Department of Homeland Secu-rity and has provided funding to Basis Technology, Oculis Labs, Sonitus Medical, D-Wave Sys-tems, Forterra Systems Inc., and CyPhy Works among others. In response to the challenge posed by cybersecurity operations, In-Q-Tel has sought to “start providing venture capital funding to valley startups that can help the Pentagon develop more advanced cybersecurity and intelligence systems to fend off nation states and hackers targeting everything from top-secret military corre-spondence to public power grids.”³²

More recently, the CIA has created its own Directorate of Digital Innovation (DDI) as its newest directorate. The DDI focuses on accelerating digital innovation across the intelligence communi-ty. In its operation “DDI has a close partnership with In-Q-Tel” and will help strengthen CIA’s relationship with IQT. DDI is designed to help “prioritize requirements for the venture capital entity”, and identify critical emerging digital issues and capabilities” for the CIA. It will also have “a very close and robust relationship” with the private sector to detect emerging technology trends, accelerate technology application and create internal conditions for innovation.³³

3.1.3 Government in the Valley

The third model stems from the 2015 DoD Cyber Strategy document put forward during Secre-tary of Defense Ashton Carter’s tenure and is primarily market facilitating. This model involves government agencies creating offices and cultivating relationships directly in Silicon Valley. During the Defense One Tech Summit June 2016, Carter noted, “I am committed to building and rebuilding the bridges between our national security endeavors at the Pentagon and innovators

³¹ In-Q-Tel, Inc. Retrieved from <https://www.iqt.org/about-iqt/>

³² Somerville, H. (2015, May 13). “Defense Department’s Tech investing signals Silicon Valley’s importance in cyberwarfare”. *The Mercury News*. Retrieved from <http://www.mercurynews.com/2015/05/13/defense-departments-tech-investing-signals-silicon-valleys-importance-in-cyberwarfare/>

³³ Ackerman, R. (2016, June). “The CIA Accelerates Innovation”. The Central Intelligence Agency. Retrieved from <http://eds.b.ebscohost.com/eds/detail/detail?vid=2&sid=c6f31930-46f0-4f2a-920f-5134a8e005f4%40sessionmgr102&hid=122&bdata=JnNpdGU9ZWZLRzLWxpdmU%3d#AN=117142112&db=edb>

throughout the nation from the tech entrepreneurs in Silicon Valley.”³⁴ Of course, the link between Silicon Valley and DoD has a long history with Dave Packard, co-founder of Hewlett-Packard, serving as Deputy Secretary of Defense during the Nixon administration.

Currently, both DHS and DoD have opened offices specifically meant to engage with Silicon Valley firms directly. The DHS Innovation Program and DHS Science and Technology Directorate have offices in the Bay Area while DoD, via the Defense Innovation Unit Experimental (DIUx) seeks to “strengthen existing relationships and build new ones; help scout for new technologies; and help function as a local interface for the department.”³⁵ The NGA, too, via the NGA Outpost Valley with Peter Highnam, former IARPA director, at the helm has opened a lab in Silicon Valley “to investigate emerging research challenges, operate permanent analyst cells, and leverage emergent capabilities to deliver results to the National Security Enterprise across all security domains.”³⁶ Finally, the National Security Technology Accelerator (NSTXL) operates a not-for-profit consortium to connect, advise, and fund early start-ups to facilitate a contract relationship between the U.S. Department of Defense and the firm.³⁷ Each of these efforts attempt to overcome challenges facing the existing procurement pipelines that are viewed by many as being inefficient and difficult for emerging companies to maneuver through. DIUx, in particular, serves as an important example of the emerging OT (“other transactions”) procurement process within the contemporary Federal Acquisition Regulations (FAR).

3.1.4 Bringing the Valley to DC/NoVa

The fourth model operates similarly to the model above but combines all three ideal types in reverse. Here, government actors seek to acquire technological talent and bring it to Washington, DC and northern Virginia for the purposes of greater integration with military and intelligence agencies. The U.S. Digital Service serves as the best example of this approach with the Department of Defense creating its own U.S. Defense Digital Service (DDS) under the auspices of the Service.³⁸ As part of this effort, DDS operates a number of programs including “Hack the Pentagon,” “Hack the Army” and “Defense Travel System Modernization.”

There are also a variety of programs designed to increase technology-focused human capital in the government workforce. There are a large number of these initiatives so we focus on a few here. The first example is the National Initiative for Cybersecurity Education (NICE) established

³⁴ Sender, H. (2016, Septmeber 4). “US defence: Losing its edge in technology?”. *Financial Times*. Retrieved from <https://www.ft.com/content/a7203ec2-6ea4-11e6-9ac1-1055824ca907>

³⁵ Defense Innovation Unit Experimental. Retrieved from <https://www.dinux.mil> Tadjdeh, Yasmin. (2015, August 13). “Army Reserve Pursuing Partnerships with Silicon Valley.” *National Defense Magazine*. Retrieved from <http://www.nationaldefensemagazine.org/articles/2015/8/13/army-reserve-pursuing-partnerships-with-silicon-valley-updated>

³⁶ National Geospatial-Intelligence Agency Mission Statement. National Geospatial-Intelligence Agency Retrieved from www.nga.mil

³⁷ “Overview”. National Security Technology Accelerator. Retrieved from <http://www.nstxl.org/about.php#overview>

³⁸ Department of Defense: Defense Digital Service. Retrieved from <https://www.dds.mil>

in 2012.³⁹ NICE is a joint effort by the federal government, industry, and academia that aims to improve cybersecurity education and workforce development operating under NIST's Applied Cybersecurity Division. NICE also runs the Interagency Coordinating Council, which convenes federal agencies to coordinate cybersecurity education and workforce policy. It also developed the National Cybersecurity Workforce Framework, which helps agencies categorize cybersecurity work and, in doing so, assist with the identification of federal and private workforce needs.⁴⁰

Second, the National Integrated Cyber Education Research Center (NICERC) exists in partnership with DHS as an education-oriented non-profit subsidiary of the Cyber Innovation Center to provide cybersecurity curricula to elementary, middle, and high school students.⁴¹ The initiative is part of a broader federal effort to reach out to K-12 institutions, and, specifically, appears to be part of CETAP ("Cybersecurity Education and Training Assistance Program"), a DHS cybersecurity education program.

Third, the CyberCorps Scholarship for Service Program⁴² represents a joint initiative by the NSF and DHS that provides scholarships to undergraduate/graduate students at NSA/DHS designated Centers of Academic Excellence in information assurance.⁴³ After the completion of their degree, students commit to serving federal, state, local, or tribal governments for as long as they received the scholarship.

Finally, the government also supports the broader TechHire program announced by President Obama in March of 2015. Its goal is to create a national campaign to build "tech talent pipelines" across the United States for both the private and public sectors.⁴⁴ The initiative aims to provide workers with the skills to fill vacant positions in the IT sector, and is supported by federal grant funding and public private partnerships. In the initial announcement, the President pledged \$100 million in federal grants. In 2016, the Vice-President and Secretary of Labor announced an additional \$150 million in Department of Labor grants. Each of these programs represents an industrial policy seeking to increase the workforce in the cybersecurity marketplace for both public and private actors.

³⁹ Cobert, B. (2017, July 12). "Strengthening the Federal Cybersecurity Workforce". United States Office of Personnel Management. Retrieved from <https://www.opm.gov/blogs/Director/2016/7/12/Strengthening-the-Federal-Cybersecurity-Workforce/>

⁴⁰ "NICE Cybersecurity Workforce Framework". National Initiative for Cybersecurity Education (NICE). National Institute of Standards and Technology. Retrieved from <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

⁴¹ (2016, September 20). "Cybersecurity Education and Career Development". Department of Homeland Security. Retrieved from <https://www.dhs.gov/topic/cybersecurity-education-career-development>

⁴² See Title III of the Cybersecurity Enhancement Act of 2014

⁴³ "CyberCrops: Scholarship for Service". U.S. Office of Personnel Management. Retrieved from <https://www.sfs.opm.gov/StudFAQ.aspx>; <http://www.sait.fsu.edu/resources/SFSToolkit.pdf>

⁴⁴ "TechHire Initiative" The White House. Retrieved from <https://obamawhitehouse.archives.gov/issues/technology/techhire#section-commitments>; "H-1B Grants for Innovative Approaches to Connect Individuals with Barriers to Good Jobs in Technology and Other In-Demand Fields". Department of Labor. Retrieved from <https://www.dol.gov/sec/media/reports/H-1BTechHireFactSheet.pdf>

Beyond human capital concerns, other venues of government-private sector interaction include the Pentagon Highlands Forum that serves as “an informal, cross-disciplinary network sponsored by Federal Government with a common interest in information, science, and technology.” Second, the National Cyber Security Alliance—including actors from industry and various government agencies—provides a venue for industry focused on cybersecurity challenges to meet with government actors.⁴⁵

3.1.5 Regulatory Power

In this fifth and final model of interaction, the U.S. government provides regulations and standards that condition the American cybersecurity market and proscribe specific activities. Below, we describe an example of “hard” law and penalties surrounding import and export controls before examining the nascent NIST information-sharing framework and the NIST Framework for Improving Critical Infrastructure Cybersecurity as examples of the government regulating and providing standards for the market.

Import and export controls clearly manipulate markets by limiting the market of private companies for their goods and services abroad while also limiting international competition as a form of protection. For an example of import controls, consider Section 516 of the Consolidated and Further Continuing Appropriations Act, 2013 signed into law by President Obama on March 26, 2013. This law prohibits the procurement of any information-technology system subsidized, produced, manufactured, or assembled in China by various government departments including the departments of Commerce & Justice, NASA, or NSF.⁴⁶

Similarly, Section 8048 of the Consolidated and Further Continuing Appropriations Act of 2015 stipulates that the funds made available by the Act cannot be used to purchase any supercomputer manufactured outside of the United States, unless the Secretary of Defense demonstrates to the congressional defense committees that acquisition of a similar supercomputer from a domestic manufacturer would not be possible.⁴⁷

The government also played an active role in managing mergers and acquisitions for companies with subsidiaries in the United States. The “Presidential Order Regarding Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GMBH,” for example, prohibited the acquisition of Aixtron SE by Grand Chip Investment GMBH—invoking the authority

⁴⁵ See also Defense Innovation Advisory Board. Ferdinando, Lisa. (2017, January 9). “Advisory Board Approves 11 DoD Innovation Recommendations.” *Department of Defense*. Retrieved from <https://www.defense.gov/News/Article/Article/1045458/advisory-board-approves-11-dod-innovation-recommendations/>. We are also interested in investigating intermediary institutions that bolster or undermine cybersecurity in future work.

⁴⁶ “American Procurement of Chinese IT Equipment Contingent Upon FBI Certification”. Global Trade Alert. Retrieved from <http://www.globaltradealert.org/measure/united-states-america-procurement-chinese-it-equipment-contingent-fbi-certification>; Pearson, H. (2013, April 12). “Spending Bill’s China Cybersecurity Provision is Unclear”. Law360. Retrieved from <https://www.law360.com/articles/432500/spending-bill-s-china-cybersecurity-provision-is-unclear>

⁴⁷ “United States of America: Buy American provisions in an omnibus spending bill”. Global Trade Alert. Retrieved from <https://www.globaltradealert.org/intervention/19338/public-procurement-localisation/united-states-of-america-buy-american-provisions-in-an-omnibus-spending-bill>

granted to the president by section 721 of the Defense Production Act. The Committee on Foreign Investment in the United States (CFIUS) had previously recommended that the involved parties abandon the deal on account of the potential national security risks it would pose. The deal would have merged Grand Chip Investment's parent companies, GC Investment S.a.r.l. (based in Luxembourg) and Fujian Grand Chip Investment Fund LP (based in China). The national security review process created by the CFIUS statute of the Defense Production Act has only been used to block transactions on three occasions, with Chinese companies involved in all three instances.⁴⁸ Currently a major effort is underway to enhance the role of CFIUS in evaluating the impact of foreign investments in the United States as part of President Trump's focus on China's "Made in 2025" industrial policy efforts.

Another form of this market-proscribing role stems from the U.S. export control system. Under the auspices of this system, three government agencies (the Departments of State, Commerce, and Treasury) are tasked with controlling the export of sensitive equipment, software, and technology. These controls are designed to:

"provide for national security by limiting access to the most sensitive U.S. technologies and weapons; promote regional stability; take into account human rights considerations; prevent proliferation of weapons and technologies, including weapons of mass destruction, to problem end-users and supporters of international terrorism; [and] comply with international commitments, i.e. nonproliferation regimes and UN Security Council sanctions and UNSC resolution 1540."⁴⁹

Of these latter international commitments, the Missile Technology Control Regime (MTCR) and Wassenaar Agreement (WA) include Internet technology on their control lists. The vehicle for export controls within the United States is the Arms Export Control Act (AECA) implemented by the Department of State via the International Traffic in Arms Regulations (ITAR). These regulations require companies to register with the U.S. government and also provide licenses and authorizations for the "specific exports of defense articles and services."⁵⁰ DHS and U.S. Customs enforce these controls with criminal and civil penalties for export control violations to ensure compliance.

While the export control regime noted above emphasizes coercion, there are less coercive regulatory standard-setting measures that the U.S. government is engaged in with the private sector. The NIST guide to sharing information on cyber threats between industry and government pro-

⁴⁸ "United States of America: Presidential order blocking a Chinese-German acquisition of a US semiconductor firm". Global Trade Alert. Retrieved from <https://www.globaltradealert.org/intervention/9636/fdi-entry-and-ownership-rule/united-states-of-america-presidential-order-blocking-a-chinese-german-acquisition-of-a-u-s-semiconductor-firm>; Office of the Press Secretary. (2016, December 2). "Presidential Order – Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GMHB". The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/presidential-order-regarding-proposed-acquisition-controlling-interest>

⁴⁹ "Overview of U.S. Export Control System". A Resource on Strategic Trade Management and Export Controls. U.S. Department of State. Retrieved from <https://www.state.gov/strategictrade/overview/>

⁵⁰ m ibid.

vide an example of such a framework.⁵¹ This framework was born from the mandate of the Burr-Feinstein Bill, Cybersecurity Information Sharing Act (CISA) to build a framework for government-firm cooperation concerning cyber threats. The Cybersecurity Act of 2015, formerly “Cybersecurity Information Sharing Act of 2015”, established a voluntary information sharing regime that sought to eliminate legal barriers and disincentives which would have otherwise discouraged large-scale dissemination of relevant data. The act vested responsibility for information sharing between the private sector and federal government in the civilian-run National Cybersecurity and Communications Integration Center in the DHS. As long as information-sharing occurs in accordance with the technical requirements outlined in the bill, private-sector participants are protected from legal liability.

Due to the privacy concerns voiced by legislators, the final bill included a requirement that companies remove any “information that identifies a specific person not directly related to a cybersecurity threat, prior to sharing [a cybersecurity threat] indicator.” Unlike the export control example, above, this framework seeks to solve a firm-level challenge emanating from U.S. law: the sharing of personal data and meta-data both among industry players and with government in the event of a network intrusion. Indeed, this framework is specifically designed to overcome the information problems associated with market failure. This information is designed to “help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents.”⁵²

The NIST Framework for Improving Critical Infrastructure Cybersecurity offers an alternative example of a best practices approach to creating informal standards for private industry to follow and incorporate into their “organizational risk management processes.”⁵³ Importantly, this best practices approach has no enforcement mechanism.

As demonstrated above, there are a variety of patterns of interaction between the U.S. government and private firms in the cybersecurity market. To investigate this variation, the following section considers the drivers of these intervention measures.

4. Drivers of the Constellation of Intervention Measures

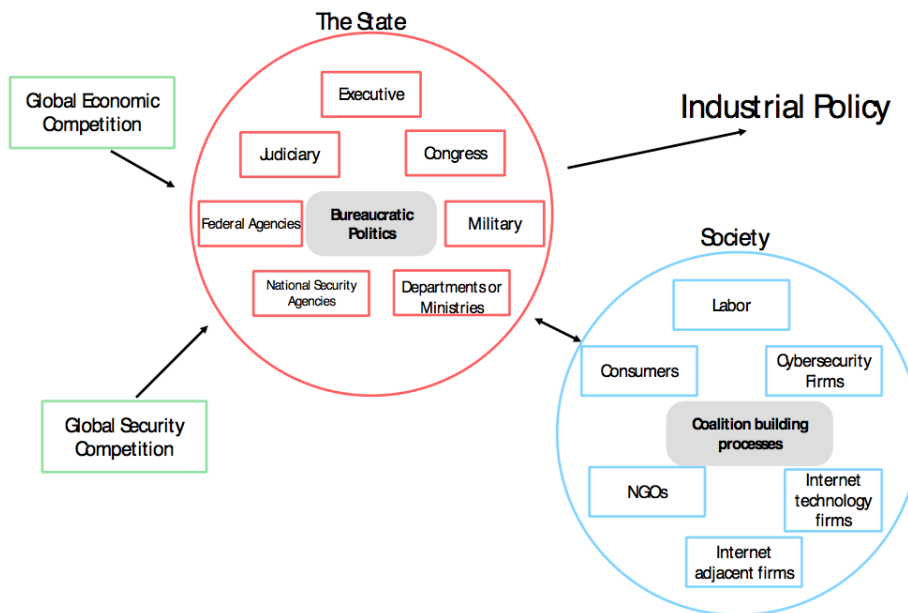
To examine the intervention measures taken by the U.S. government, we examine three sets of variables that broadly reflect state-society interactions in policy-making. These interactions are summarized in figure 2, below.

⁵¹ Johnson et al. “Guide to Cyber Threat Information Sharing”. NIST Special Publication 800-150. National Institute of Standards and Technology. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

⁵² Johnson et al. *ibid.*

⁵³ (2014, February 12). “Framework for Improving Critical Infrastructure Cybersecurity”. National Institute of Standard and Technology. Retrieved from <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

Figure 2: State-Society Interaction in Policymaking



First, we consider the geopolitical context in which the U.S. government makes decision to intervene in its domestic market. Second, we consider the state-level preferences and bureaucratic incentives that drive market intervention. Third, we consider the society-level preferences and how they interact with the industrial policy-making process via lobbying.⁵⁴

4.1 Geopolitical Context

Structural determinants of state behavior have long been suggested as the motivating factor for state decision-making.⁵⁵ In the context of market intervention, recent work has also pointed to the importance of geopolitics to industrial policy.⁵⁶ This context may be further split to reflect global security competition and global economic competition. Indeed, the use of import and export controls, alongside efforts to build an indigenous cyber workforce to decrease the vulnerabilities of IT firms and Internet-adjacent industry as part of the U.S. government's industrial policy to address cybersecurity market failures reflects in part the global security competition. Moreover, since cybersecurity threats from abroad stem from great power competitors—China and Russia—as well as non-great power competitors—North Korea, it is perhaps unsurprising to see geopolitical realities used as a justification for U.S. government intervention in the market.

With regard to global economic competition, efforts to bolster cybersecurity are often hedged in language related to protecting intellectual property from foreign governments and firms follow-

⁵⁴ Given the short time horizons associated with the cybersecurity marketplace and lack of variation in cybersecurity industrial policy and the potential drivers, we do not seek to make a causal argument of U.S. industrial policy concerning cybersecurity.

⁵⁵ Waltz, K. (1979) *Theory of International Politics*. New York.

⁵⁶ Griffith, Melissa, Richard Steinberg, and John Zysman. 2017. "From great power politics to a strategic vacuum: Origins and Consequences of the TPP and TTIP." *Business and Politics* 19(4):

ing the hacks on various U.S. defense contractors ostensibly to steal the design specifications of weapons systems.

4.2 State-Level Preferences

At the State level, we consider a variety of bureaucratic incentives that culminate in state-level preferences that influence U.S. industrial policy. As noted above, there are a variety of U.S. government agencies that have been responsible for agenda-setting, designing, funding, and implementing various cybersecurity programs including a number of branches within the military, a number of intelligence agencies from the Central Intelligence Agency to the National Geospatial Agency, various government departments including the Department of Defense, the Department of Commerce, and the Department of the Treasury as well as the White House and Congress. In the section, below, we outline a number of representative initiatives undertaken by the Executive and Congress to address the national cybersecurity marketplace.

4.2.1 Domestic Strengthening

The legislative and executive branches at the federal level are largely responsible for government action and agenda-setting when it comes to cybersecurity and the cyber-industrial complex in the United States as it allocates funds to specific projects. There are two mechanisms, an executive order or the setting of standards/rules whereby the executive implements cybersecurity policy. President Obama's Executive order to promote public-private cybersecurity collaborations serves as example of such an approach.⁵⁷ Congress, on the other hand, operates through budgeting and appropriations procedures as well as bringing forth further conversation regarding these topics in hearings before committees such the House Committee on Science, Space, and Technology.

H.R. 2774: "Hack DHS Act" introduced by Rep. Ted Lieu (D-CA) serves as an example of this agenda-setting role.⁵⁸ The bill itself proposes the establishment of a "bug bounty program," a "program under which an approved computer security specialist or security research is temporarily authorized to identify and report vulnerabilities within the information system of the" DHS in exchange for monetary payment to allow for DHS and other government agencies to address existing vulnerabilities and prepare against potential attacks. The program itself calls for the use of \$250,000 of government funds during FY 2018 to carry out the program. Similarly, H.R.3359: "Cybersecurity and Infrastructure Security Agency Act of 2017" authorizes the establishment of the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security in an attempt to strengthen government institutions from attack.

Most recently and in response to the 'WannaCry' cyberattack in May of 2017 (a ransomware attack), President Trump and the White House issued Executive Order 13800 that mandates all federal systems under the executive branch implement a NIST framework for their computer systems, a highly acclaimed framework known for its cybersecurity.

⁵⁷ Office of the Press Secretary. (2015, February 13). "Executive Order - Promoting Private Sector Cybersecurity Information Sharing." The White House. Retrived from <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>

⁵⁸ H.R.2774 - Hack DHS Act. Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/2774?q=%7B%22search%22%3A%5B%222774%22%5D%7D&r=1>

4.2.2 Domestic Standards

Another example of government agenda-setting stems from recent updates to programs addressing the cybersecurity standards of small businesses that amends the “National Institute of Standards and Technology Act to require the National Institute of Standards and Technology (NIST) to consider small businesses when it facilitates and supports the development of voluntary, consensus-based, industry-led guidelines and procedures to cost-effectively reduce cyber risks to critical infrastructure.”⁵⁹ It calls on NIST to provide the resources that are

“1) technology-neutral, (2) based on international standards to the extent possible, (3) able to vary with the nature and size of the implementing small business and the sensitivity of the data collected or stored on the information systems, (4) capable of promoting awareness of third-party stakeholder relationships to assist small businesses in mitigating common cybersecurity risks, and (5) consistent with the national cybersecurity awareness and education program under the Cybersecurity Enhancement Act of 2014.”⁶⁰

This effort was followed up in S. 1428: “Small Business Cyber Training Act of 2017” that allocates \$350,000 to establish a “cyber counseling program.”⁶¹

4.2.3 Regulating Commerce

The U.S. government has also had a role in regulating access and collaboration among extraterritorial actors in regards to cybersecurity. Perhaps most controversially, the United States government ceased its partnership with Kaspersky Labs because of alleged links to the Russian government.⁶² In contrast, the United States also uses cooperation on issues of cybersecurity as a venue for cooperation with cooperation frameworks with a variety of countries including Israel and Ukraine.⁶³

4.3 Society-Level Preferences

Actors at the society-level are not only the subject of industrial policy but also play a role in creating it. In this section, we consider a number of players that are involved in the creation of soci-

⁵⁹ H.R.2105 - NIST Small Business Cybersecurity Act. Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/2105?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=11>

⁶⁰ *ibid.*

⁶¹ S.1428 - Small Business Cyber Training Act of 2017. Retrieved from <https://www.congress.gov/bill/115th-congress/senate-bill/1428?q=%7B%22search%22%3A%5B%22cyber%22%5D%7D&r=5>

⁶² (2017, September 14) “About Kaspersky Labs, the Russian-based company Trump is expelling from the US government.” *FOX Business*. Retrieved from <http://www.foxbusiness.com/politics/2017/09/14/about-kaspersky-labs-russian-based-company-trump-is-expelling-from-us-government.html>

⁶³ S. 719 - United States-Israel Cybersecurity Cooperation Enhancement Act of 2017. This bill requires the Department of Homeland Security (DHS) to establish a grant program to support cybersecurity research and development, and the demonstration and commercialization of cybersecurity technology, in accordance with the Agreement between the Government of the United States of America and the Government of the State of Israel on Cooperation in Science and Technology for Homeland Security Matters, done at Jerusalem, dated May 29, 2008, or a successor agreement: <https://www.congress.gov/bill/115th-congress/senate-bill/719?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=13>

ety-level players. These players include cybersecurity firms, IT firms, Internet adjacent firms, consumers, labor, and NGOs such as advocacy organizations Electronic Frontier Foundation or industry groups. Each one of these players has specific interests that are reflected in their policy priorities. We consider their role below.

4.3.1 Agenda-Setting

In the private sector, public-private cooperation on cybersecurity has thus far been characterized by a lack of enforcement mechanisms. A number of firms view proposed requirements to develop cybersecurity measures as an additional government “invasion” into the market, preferring instead to adhere to laissez-faire business principles.⁶⁴ The Business Software Alliance (BSA), a Microsoft-led trade group that operates as the leading advocate for nearly 100 of the world’s largest software makers, including Apple, Adobe, McAfee, and Intel, noted in their 2012-2013 Action Plan: “[We advocate] supporting policies that strengthen cybersecurity capabilities, without putting undue regulatory burdens on industry...and ensuring cybersecurity policies protect our members’ ability to innovate, especially in new fields such as mobile and the cloud.”⁶⁵ In the 2017 plan, BSA note their support for “public-private partnerships, strengthening cybersecurity workforce capabilities, implementing effective information sharing frameworks, policies that support the development of cutting-edge cybersecurity technologies.”⁶⁶ However, this agenda appears particularly vague given that other parts of the agenda relating to government access to data notes that BSA specifically supports the modernization of the Electronic Communications Privacy Act and the a reauthorization of section 702 of the Foreign Intelligence Surveillance Act. Similarly, the U.S. Chamber of Commerce, a prominent business-oriented lobbyist group, released a February 06, 2017 memo on the State of American Cybersecurity that notes, “Government policy and decisions shouldn’t get in the way of the private sector.”⁶⁷

These prerogatives are also reflected in various war-making scenarios. In April 2015, RAND Corporation conducted “360° Discovery Games” in both Washington D.C. and Silicon Valley in which key stakeholders in the government, journalism, academia, and tech industry (including IT producers and IT security) worked together in groups to solve theoretical cybersecurity-threat scenarios.⁶⁸ While groups were mixed in both locations, because of convenience, more members of the public sector were present in D.C. and more of the private in Silicon Valley. In Washington, the majority of working groups concluded that a major barrier to IoT security was user failure to install patches and upgrades. While groups argued over which government agency should impose regulations, a market-based solution was ultimately chosen as the most realistic one, in which insurance companies could offer lower premiums to devices equipped with patch-

⁶⁴ Etzioni, Amitai. (2014) “The Private Sector: A Reluctant Partner in Cybersecurity.” *Georgetown Journal of International Affairs*, pp. 69–78. Retrieved from www.jstor.org/stable/43773650.

⁶⁵ “Strategic Plan 2013-2015.” *BSA The Software Alliance*. Retrieved from http://www.bsa.org/~media/files/general/bsa_strategicplan_final.pdf

⁶⁶ “2017 US Policy Agenda.” *BSA The Software Alliance*. Retrieved from http://www.bsa.org/~media/Files/Policy/BSA_2017USPolicyAgenda.pdf

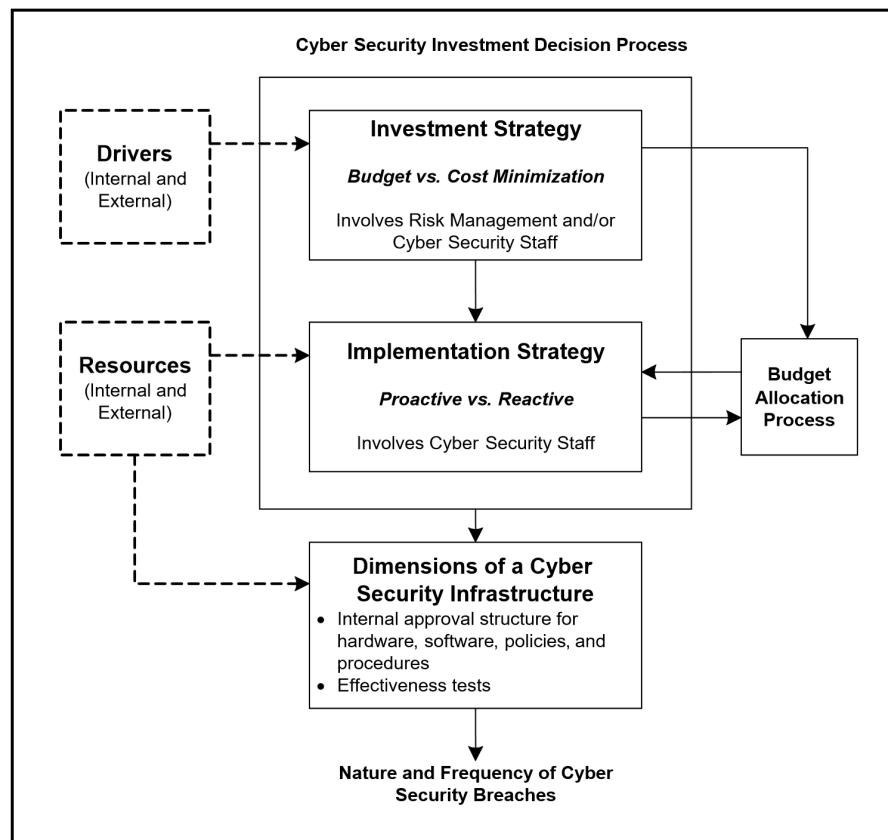
⁶⁷ Beauschesne, Ann M. (2017, February 6) “The State of American Cybersecurity”. *US Chamber of Commerce*. Retrieved from <https://www.uschamber.com/above-the-fold/the-state-american-cybersecurity>

⁶⁸ (2016) “Exploring Cybersecurity Policy Options.” RAND. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf

es/upgrades, and competition would lead to greater security. The question of what would incentivize the market, however, remained unanswered.⁶⁹ In Silicon Valley's scenario, again, players considered a market solution. In their ideal structured model, the "security of the ecosystem" would be balanced with private-sector goals of profit and efficiency.⁷⁰ Specifically, the players noted that there are dangers to prescribing a one-size-fits-all solution, as different devices and systems have data of varying levels of sensitivity.

While associations that bridge private and public sectors have been established to attempt to promote greater investment in cybersecurity, a "lack of economic incentives to participate and share" via the free-rider problem results in limited success for such organizations.

Figure 1. Diagram of Cyber Security Investment Decisions Inputs and Outputs



71

⁶⁹ Ibid

⁷⁰ Ibid.

⁷¹ Rowe, Brent R. and Michael P. Gallaher. (2006, March). "Private Sector Cyber Security Investment Strategies: An Empirical Analysis." WEIS. Retrieved from <https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf>

Table 1. Categorization of Relevant Drivers and Information Resources

Internal	External Public	External Private
DRIVERS		
Business Process needs (i.e., strong business reliance on network)	Regulations	Client demands
Major past breach		Supplier demands
INFORMATION RESOURCES		
Internal audits	NIST best practices	Customer suggestions/ requirements
Staff experience/training	ISO guidelines	Vendor suggestions/advice
Internally collected/calculated data (e.g., number of compromises, cost estimates)	American National Standards Institute (ANSI) guidelines	Conferences or trade publications
CEO/CTO/COO/etc. suggestions	Security impact estimated (e.g., CSI/FBI survey)	Outside consultants
	CERTS, SANS, etc.	Other organizations
		External audits

72

Table 2. Drivers Affecting Organizations Cyber Security Investment Strategy

Categories	Average Percentage across Organizations
Regulation driven	30.1%
Network history/IT staff knowledge	18.9%
Client driven	16.2%
Result of internal or external audit	12.4%
Response to current events (e.g., media attention)	8.2%
Response to internal security compromise	7.3%
Externally managed/determined	5.0%
Other	1.7%

73

Cybersecurity efforts could also be hindered in that employees are vulnerable to even basic cybersecurity breaches made possible through such things as phishing scams.⁷⁴ According to the Pew Researcher Center, conducted a study that found that employee error caused around 35 percent of cyber breaches overall. Additionally, of the participants in the study, the average score on a test that included “fairly standard cybersecurity questions” was about 50 percent.⁷⁵ Given these risks, it is perhaps unsurprising that businesses seek to avoid responsibility for cyber insecurity related to their products.

Business responses to the proposed 2015 Cybersecurity Information Sharing Act (CISA) that would have required the Department of Homeland Security to establish a cybersecurity information-sharing system with the private sector have also been lukewarm. In a statement released

⁷² *ibid.*

⁷³ Rowe, *ibid.*

⁷⁴ Hite, Collin. (2017, April 11). “Your employees are the weak link in your cybersecurity program.” *Virginia Business*. Retrieved from <http://www.virginiabusiness.com/opinion/article/your-employees-are-the-weak-link-in-your-cybersecurity-program>

⁷⁵ *ibid.*

to *The Washington Post*, Apple notes, “We don't support the current CISA proposal. The trust of our customers means everything to us and we don't believe security should come at the expense of their privacy.”⁷⁶ Dropbox's head of global public policy and government affairs similarly emphasized the need for greater privacy protection in CISA stating that, “While it's important for the public and private sector to share relevant data about emerging threats, that type of collaboration should not come at the expense of users' privacy.” Other industry giants including Yelp, Reddit, Twitter, and Wikipedia had all previously affirmed their own opposition to the bill, as well. More recently, Google, Facebook, Dropbox, and other technology companies have been collaborating with the President's Commission on Enhancing National Cybersecurity but rather than pass laws, the firms have asked government to issue “recommendations on transparency, threat sharing, and privacy for consumer data.”⁷⁷

Between businesses and the advocacy groups that represent them, there is a clear inclination toward avoiding government regulation. Why is this the case? The simplest answer is that IT and Internet-adjacent firms rely on the Internet to connect with customers or sell products to customers. These Customers may lose faith in a business that has been hacked, and thus the urge to deny the existence of cyber attacks is significant. One year after their 2012 massive security breach, for example, Target disclosed the company had received alerts from FireEye—a cybersecurity company—of potential malware in advance of the attack, but failed to take action.⁷⁸ Ultimately, Target's security flub resulted in \$18 million in lost revenue—largely an impact of negative publicity—and is indicative of a harmful feedback loop: firms fear admitting cybersecurity weaknesses will decrease consumer confidence, firms are hacked, and firms scramble to recover, yet fear among consumers linger.⁷⁹ Indeed, ambivalence and idleness are not unique to Target's case. A three year-study conducted by Verizon Enterprise Solutions also found that while companies discover breaches in advance only 31% of the time, for retailers it's only 5%.⁸⁰ One of the key limitations of investment in cybersecurity on the side of the private sector is the “efficiency of the investment and ... its marginal cost and... its marginal benefit.”⁸¹

Target's vulnerability can be captured by the greater phenomenon of IT and Internet-adjacent firms weighing short-term goals and costs over long-term ones, with cybersecurity threats being mentally checked off by CEOs as a minor risk far into the future. Indeed, for these companies,

⁷⁶ Fung, Brian. (2015, October 20). “Apple and Dropbox say they don't support a key cybersecurity bill, days before a crucial vote” *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/apple-says-its-against-a-key-cybersecurity-bill-days-before-a-crucial-vote/?utm_term=.f549286f9cd6

⁷⁷ Daniel, Michael, Ed Felton and Tony Scott. (2016, April 16). “Announcing the President's Commission on Enhancing National Cybersecurity.” *The White House*. Retrieved from <https://obamawhitehouse.archives.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity>

⁷⁸ Finkle, Jim and Susan Heavy. (2014, March 13). “Target says it declined to act on early alert of cyber breach.” Reuters. Retrieved from <http://www.reuters.com/article/us-target-breach/target-says-it-declined-to-act-on-early-alert-of-cyber-breach-idUSBREA2C14F20140313>

⁷⁹ Etzioni, *ibid.*.s9.R

⁸⁰ Riley, Michael, Ben Elgin, Dune Lawrence and Carol Matlack. (2014, March 17). “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It.” Bloomberg. Retrieved from <https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data>

⁸¹ Rowe, *ibid.*

cybersecurity is an externality. That is, if companies suffer incursions at the hands of cybercriminals, much of the harm will fall on third parties, such as the Target credit-card holders whose identities were released.⁸² The marginal benefit of cybersecurity investment largely depends of factors

related to organizational and performance characteristics such as an organization's existing information technology (IT) characteristics, the compatibility of available cybersecurity technologies with the current technologies, the security needs of the products and services the organization provides, and the preferences/perceptions of its customers.⁸³

4.3.2 Design and Implementation

Costs to reputation and skepticism concerning the role of government among firms has led to lobbying efforts that emphasize a free public sector. In a 2012 letter to the US Senate, BSA called for bipartisan legislation to match the evolving threat landscape while also avoiding over-regulation. Their priorities included eliminating legal barriers to cyber threat information sharing both between private firms and with the public sector, establishing a trust-based environment, and creating an incentive-based system to encourage international cooperation on fighting cyber-crime due to its borderless nature. Indeed, the Chamber of Commerce lobbied Senate Republicans to sink a 2010 cybersecurity bill that would have regulated privately-owned infrastructure (e.g. electric utilities) to prevent major cyber attacks.⁸⁴

While cybersecurity and IT firms have eschewed government regulation and legal solutions, they have focused on cybersecurity education and strengthening their own networks. In a 2017 keynote address at the Black Hat USA conference, Facebook CSO Alex Stamos announced \$1 million in funding for cybersecurity research in addition to investment in education programs, and hackathons/competitions.⁸⁵ In a partnership with CodePath, the tech giant is creating a new, free, 12-week cybersecurity course to students interested in tech at the following institutions: The City College of New York, Merritt College, Mississippi State University, California State University San Bernardino, and Virginia Tech.⁸⁶

Beyond society-state relations involving business and government, the gap between public and private sector goals in cybersecurity is often bridged by NGOs such as the Electronic Frontier Foundation (EFF), the SANS Institute, and the Anti-Phishing Working Group (APWG). As noted in the RAND Discovery Games, much of the cybersecurity threat is rooted in consumer ignorance and failure to upload appropriate protection such as patches and upgrades to devices. While industry and government struggle over regulatory issues, NGOs often attempt bring cybersecurity education and advocacy directly to consumers. In an effort to connect with consumers, EFF works to increase awareness of its collaborative projects such as HTTPS Everywhere

⁸² Sales, Nathan Alexander. (2013) "Regulating Cyber-Security" *Northwestern University Law Review*, Vol. 107(4). Retrieved from <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1040&context=nulr>

⁸³ Rowe, *ibid*.

⁸⁴ Dilanian, Ken. (2012, August 3). "U.S. Chamber of Commerce leads defeat of cyber-security bill." *Los Angeles Times*. Retrieved from <http://articles.latimes.com/2012/aug/03/nation/la-na-cyber-security-20120803>

⁸⁵ Stamos, Alex. (2017, July 26). "Preparing for the future of security requires focusing on defense and diversity." *Facebook*. Retrieved from <https://www.facebook.com/notes/facebook-security/preparing-for-the-future-of-security-requires-focusing-on-defense-and-diversity/10154629522900766/>

⁸⁶ Codepath*org. Retrieved from <https://codepath.org/classes>

and Certbot.⁸⁷ NGOs don't just work on consumer education in their own independent sphere. The gap between public and private sector goals in cybersecurity fortification is being bridged by NGO collaboration on consumer engagement. As noted above, the National Cyber Security Alliance, a 501c nonprofit and the United States's leading public-private partnership, has worked in conjunction with DHS to create National Cyber Security Awareness month each October. NCSAM has been championed by hundreds of other tech companies, including security-giant Kaspersky Lab North America, colleges and universities, and other nonprofits.⁸⁸

5. The Negative Externalities of Intervention

Thus far, we have outlined the patterns of intervention by the U.S. government in the cybersecurity market and considered the drivers of the constellation of intervention measures emanating from state-society relations. In this section, we move to a discussion of the domestic consequences, public policy criteria, design failures, and implementation failures associated with U.S. industrial policy toward its domestic cybersecurity market.

5.1 A Balancing Act

There is a delicate balance to be negotiated with regards to ensuring that corporations that have not been affected by cybersecurity breaches still be proactive with their cybersecurity while being careful to not stifle innovation. The Heritage Foundation, for example, argues that a mandate for certain cybersecurity regulations "would be more like an anchor holding back U.S. entities while not providing additional security."⁸⁹ Thus, the government is faced with the various challenges including creating an effective and useable information sharing regime, fostering a duty of care toward cybersecurity by private actors, overseeing the nascent cyber insurance system, devoting resources to cybersecurity education, and engaging with the transnational aspects of cybersecurity.

5.2 Governance Failures and Rising Uncertainty

This balance occurs against the backdrop of the government's previous failures to pass reform bills related to cybersecurity. The 112th Congress was unsuccessful in passing several bills on cybersecurity, including the Cyber Intelligence and Sharing Protection Act (CISPA). To bypass this failure, President Obama issued an executive order on "Improving Critical Infrastructure Cybersecurity" in 2013 that was similar to a bill that failed to pass in the Senate.

Within government, agencies such as the NSA and DHS have also been involved in disputes over which agency is better suited to be leading the initiative for cybersecurity and which has

⁸⁷ EFF. Retrieved from <https://www.eff.org/issues/security>

⁸⁸ Stay Safe Online. Retrieved from <https://staysafeonline.org/ncsam/ncsam-champions/>

⁸⁹ Rosenzweig, Paul, Steven Bucci and David Inserra. (2013, April 1). "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace." *The Heritage Foundation*. Retrieved from <http://www.heritage.org/defense/report/congressional-guide-seven-steps-us-security-prosperity-and-freedom-cyberspace>; Wilshusen, Gregory C. (2012, July 17). "Cybersecurity: Challenges in Securing the Electricity Grid." *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/600/592508.pdf>

jurisdiction of doing so. This battle creates redundancy between the agencies and mixed messages being sent to the private sector over which agency to collaborate with, further convoluting an already difficult process for the private sector.⁹⁰ There has also been a lack of a White House Cybersecurity Plan. As noted by the Government Accountability Office (GAO), the lack of leadership in the White House (both Trump and Obama administration) with regard to establishing a cybersecurity policy has left federal departments and agencies unaccountable with regard to improving their cybersecurity.⁹¹

5.3 Increasing Government Vulnerability

The government also faces an increasing cyber related vulnerability.⁹² Most obviously, the Department of Defense's reliance on civilian systems and products mean that DoD is vulnerable to attacks on commercially available software. Companies that the United States government contracts with often use foreign subcontractors. As a consequence, scholars have pointed out the danger of this resulting in an offshore "programmer...secretly" inserting "a Trojan Horse or other malicious code into a new commercial software product."⁹³

6. Conclusion

With respect to industrial policy in cybersecurity, the U.S. has a distinctive approach. Although the mainstream consensus has been that industrial policy doesn't work, cybersecurity provides an important exception. As noted, the Defense Department and the intelligence community recognize that much of the innovation in cybersecurity has come from the private sector. In light of the need to maintain both a security and economic edge over competitors, the U.S. government has identified a number of distinct market failures and sought solutions to address both real and perceived gaps. At the same time, given market players view of the government as "don't stand too close to me," the pursuit of industrial policy is by no means a simple matter.

In terms of market failures, we noted how policymakers expressed both economic and security concerns. From an economics perspective, the costs of cyberattacks have been increasing, posing a challenge to the highly data-focused U.S. economy. From a security perspective, several reports have pointed to the ongoing vulnerability of federal agencies and critical infrastructure to cyber attacks, and noted the danger of maintain cybersecurity for the military with respect to other countries. The general consensus has been that neither the government nor industry working on their own have been able to address these issues, most if which are tied to the labor market in regards to lack of training, career paths, and other problems such as a failure to upgrade infrastructure.

⁹⁰ Rosenzweig, *ibid.*

⁹¹ (2013, February). "National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/660/652170.pdf>

⁹² Wilson, Clay. (2007). "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues in Congress." *Focus on Terrorism, Volume 9*. Retrieved from <https://books.google.com/books?hl=en&lr=&id=wI-Ds42YMDIC&oi=fnd&pg=PA1&dq=domestic+consequences+of+cyber+industrial+policy&ots=dRdrijLq7f&sig=nA8bY2tWnnl4yjXt4TI0yIJMWa4#v=onepage&q&f=false>

⁹³ *ibid.*

With respect to efforts to address market failures, we identified five ideal type government intervention patterns that draw from efforts to engage in market making, market modifying, and market substituting that we have seen over the last few years. These include traditional procurement and licensing, the government as a venture capitalist, direct government presence in Silicon Valley, efforts to involve the Valley in the D.C area, and regulatory efforts. Some examples include the creation of the VC firm In-Q-Tel, the use of export controls to prevent the diffusion of key technology, and import controls to avoid purchases from competitors who might either have inserted back doors or more prosaically, undermine U.S. firms in the market through old-fashioned protectionism.

The drivers of industrial policy include the geopolitical context of both great power competitors and other countries such as North Korea who have successfully employed cyber warfare. More recently, concern about the Chinese effort to promote advanced technology through its Made in China 2025 policy has taken a larger role in policy debates about how to address global competition in high technology.

At the level of state-society relations, the democratic and fragmented nature of U.S. policymaking has raised important challenges in creating and implementing successful industrial policy. Government agencies often appear to be in competition with one another with respect to policy initiatives, including in Silicon Valley. Private firms for their part are wary of government intervention, particularly of regulation, that they see as raising their costs and diminishing their autonomy. Moreover, NGOs are also part of the societal mix of interests, and their concerns often conflict with government initiatives.

In sum, the practice of industrial policy in the cybersecurity marketplace remains in its infancy. While it is too early to tell whether existing policies and plans have been successful, the cybersecurity marketplace offers an important venue for scholars to study the intersection of geopolitical security concerns and their impact on domestic markets, private firms, and the bureaucratic apparatus charged with dealing with public policy challenges.

References

- (2009). "The Comprehensive National Cybersecurity Initiative". The White House. Retrieved from <https://obamawhitehouse.archives.gov/node/233086>
- (2013, February). "National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/660/652170.pdf>

(2014, February 12). “Framework for Improving Critical Infrastructure Cybersecurity”. National Institute of Standard and Technology. Retrieved from <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

(2016) “Exploring Cybersecurity Policy Options.” RAND. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf

(2016). “Industry Data.” Bureau of Economy Analysis, U.S. Department of Commerce. Retrieved from: <https://www.bea.gov/iTable/iTable.cfm?ReqID=51&step=1#reqid=51&step=51&isuri=1&5114=a&5102=10>

(2016). “Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices.” *Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2016*. Retrieved from <https://www.gao.gov/assets/690/687461.pdf>

(2016, April). “National Initiative for Cybersecurity Education (NICE) Strategic Plan”. National Initiative for Cybersecurity Education. Retrieved from <https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan>.

(2016, September 20). “Cybersecurity Education and Career Development”. Department of Homeland Security. Retrieved from <https://www.dhs.gov/topic/cybersecurity-education-career-development>

(2017, March 6). “NGA’s CIBORD initiative enables \$4.4M contract with VRICON for 3D modeling”. National Geospatial-Intelligence Agency. Press released from the NGA concerning the VRICON contract retrieved from [https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA's-CIBORG-initiative-enables-\\$4-4M-contract-with-VRICON-for-3D-modeling.aspx](https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA's-CIBORG-initiative-enables-$4-4M-contract-with-VRICON-for-3D-modeling.aspx)

(2017, September 14) “About Kaspersky Labs, the Russian-based company Trump is expelling from the US government.” *FOX Business*. Retrieved from <http://www.foxbusiness.com/politics/2017/09/14/about-kaspersky-labs-russian-based-company-trump-is-expelling-from-us-government.html>

“2017 US Policy Agenda.” *BSA The Software Alliance*. Retrieved from http://www.bsa.org/~media/Files/Policy/BSA_2017USPolicyAgenda.pdf

“United States of America: Buy American provisions in an omnibus spending bill”. Global Trade Alert. Retrieved from <https://www.globaltradealert.org/intervention/19338/public-procurement-localisation/united-states-of-america-buy-american-provisions-in-an-omnibus-spending-bill>

“United States of America: Presidential order blocking a Chinese-German acquisition of a US semiconductor firm”. Global Trade Alert. Retrieved from

<https://www.globaltradealert.org/intervention/9636/fdi-entry-and-ownership-rule/united-states-of-america-presidential-order-blocking-a-chinese-german-acquisition-of-a-u-s-semiconductor-firm>

“American Procurement of Chinese IT Equipment Contingent Upon FBI Certification”. Global Trade Alert. Retrieved from <http://www.globaltradealert.org/measure/united-states-america-procurement-chinese-it-equipment-contingent-fbi-certification>

“CyberCrops: Scholarship for Service”. U.S. Office of Personnel Management. Retrieved from <https://www.sfs.opm.gov/StudFAQ.aspx>; <http://www.sait.fsu.edu/resources/SFSToolkit.pdf>

“H-1B Grants for Innovative Approaches to Connect Individuals with Barriers to Good Jobs in Technology and Other In-Demand Fields”. Department of Labor. Retrieved from https://www.dol.gov/_sec/media/reports/H-1BTechHireFactSheet.pdf

“Over of U.S. Export Control System”. A Resource on Strategic Trade Management and Export Controls. U.S. Department of State. Retrieved from <https://www.state.gov/strategictrade/overview/>

“Overview”. National Security Technology Accelerator. Retrieved from <http://www.nstxl.org/about.php#overview>

“Strategic Plan 2013-2015.” *BSA The Software Alliance*. Retrieved from http://www.bsa.org/~media/files/general/bsa_strategicplan_final.pdf

“TechHire Initiative” The White House. Retrieved from <https://obamawhitehouse.archives.gov/issues/technology/techhire#section-commitmentsm>

”NICE Cybersecurity Workforce Framework”. National Initiative for Cybersecurity Education (NICE). National Institute of Standards and Technology. Retrieved from <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

Ackerman, R. (2016, June). “The CIA Accelerates Innovation”. The Central Intelligence Agency. Retrieved from <http://eds.b.ebscohost.com/eds/detail/detail?vid=2&sid=c6f31930-46f0-4f2a-920f-5134a8e005f4%40sessionmgr102&hid=122&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=117142112&db=edb>

Alexander, K. (2016, May 3). “Center for Strategic and International Studies – Cybersecurity Policy Debate Series”. National Security Agency. Retrieved from <https://www.nsa.gov/news-features/speeches-testimonies/speeches/100603-alexander-transcript.shtml>

Avant, D. (2005). *The Market for Force: The Consequences of Privatizing Security*. Cambridge University Press. Retrieved from

<https://books.google.com/books?hl=en&lr=&id=TJ3CzP2MiZUC&oi=fnd&pg=PP1&ots=5vMwzvJg7v&sig=tdfTCmlqKWuanNMkLEI41gyuWcA#v=onepage&q&f=false>

Beauschesne, Ann M. (2017, February 6) "The State of American Cybersecurity". *US Chamber of Commerce*. Retrieved from <https://www.uschamber.com/above-the-fold/the-state-american-cybersecurity>

Brander, J., Du, Q., and Hellmann, T. (2014, March 17). "The Effects of Government-Sponsored Venture Capital: International Evidence". *Review of Finance*. Retrieved from <https://academic.oup.com/rof/article/19/2/571/1581912/The-Effects-of-Government-Sponsored-Venture>

Budiansky S. (2016) *Code Warriors*. Toronto, Canada: Alfred A. Knopf.

Carr, Madeline. (2016) "Public-private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1: 43-62.

Carter, A. (2015, April 23). Drell Lecture: "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity" (Stanford University). Retrieved from <https://www.defense.gov/News/Speeches/Speech-View/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber/>

Carter et al. (2015, April). "The DOD Cyber Strategy". Department of Defense. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Clapper et al. (2017, January 5): Joint Statement for the Record. Senate Armed Services Committee on Foreign Cyber Threats to the United States. Retrieved from https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf

Clapper, James. (2016, February). Remarks of United States National Intelligence Director James Clapper to Congress. Retrieved from <http://www.npr.org/sections/thetwo-way/2016/02/09/466139494/key-moments-from-the-u-s-spy-chiefs-annual-litany-of-doom>

Cobert, B. (2017, July 12). "Strengthening the Federal Cybersecurity Workforce". United States Office of Personnel Management. Retrieved from <https://www.opm.gov/blogs/Director/2016/7/12/Strengthening-the-Federal-Cybersecurity-Workforce/>

Codepath*.org. Retrieved from <https://codepath.org/classes>

Daniel, Michael, Ed Felton and Tony Scott. (2016, April 16). "Announcing the President's Commission on Enhancing National Cybersecurity." *The White House*. Retrieved from <https://obamawhitehouse.archives.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity>

Daniel, M., Scott, T., and Felten, E. (2016, February 9). "The President's National Cybersecurity Plan: What You Need to Know". The White House. Retrieved from <https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know>

Defense Innovation Unit Experimental. Retrieved from <https://www.diux.mil>
Department of Defense: Defense Digital Service. Retrieved from <https://www.dds.mil>

Deutch (2001): Retrieved from http://isites.harvard.edu/fs/docs/icb.topic706688.files/Consolidation_of_the_US_Defense_Industrial_Base.pdf

Dilanian, Ken. (2012, August 3). "U.S. Chamber of Commerce leads defeat of cyber-security bill." *Los Angeles Times*. Retrieve from <http://articles.latimes.com/2012/aug/03/nation/la-na-cyber-security-20120803>

Editors at Cybersecurity Ventures. (2016). "Cybersecurity Market Report". Cybersecurity Ventures. Retrieved from: <https://cybersecurityventures.com/cybersecurity-market-report-test/>

EFF. Retrieved from <https://www.eff.org/issues/security>

England, G. (2008, April 10). *DARPA 50th Anniversary Dinner*. Retrieved from speech delivered by Deputy Secretary of Defense Gordon R. England in Washington D.C. on technology.

Etzioni, Amitai. (2014) "The Private Sector: A Reluctant Partner in Cybersecurity." *Georgetown Journal of International Affairs*, pp. 69–78. Retrieved from www.jstor.org/stable/43773650.

Ferdinando, Lisa. (2017, January 9). "Advisory Board Approves 11 DoD Innovation Recommendations." *Department of Defense*. Retrieved from <https://www.defense.gov/News/Article/Article/1045458/advisory-board-approves-11-dod-innovation-recommendations/>.

Finkle, Jim and Susan Heavy. (2014, March 13). "Target says it declined to act on early alert of cyber breach." Reuters. Retrieved from <http://www.reuters.com/article/us-target-breach/target-says-it-declined-to-act-on-early-alert-of-cyber-breach-idUSBREA2C14F20140313>

Fung, Brian. (2015, October 20). "Apple and Dropbox say they don't support a key cybersecurity bill, days before a crucial vote" *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/apple-says-its-against-a-key-cybersecurity-bill-days-before-a-crucial-vote/?utm_term=.f549286f9cd6

Gholz, E. and Sapolsky, H. (1999). "Restructuring the U.S. Defense Industry". *International Security*. Retrieved from <http://www.mitpressjournals.org/doi/pdf/10.1162/016228899560220>

Gompers, P. and Lerner, J. (2001). "The Venture Capital Revolution". *The Journal of Economic Perspectives*. Retrieved from http://www.jstor.org/stable/2696596?seq=1#page_scan_tab_contents

Griffith, Melissa, Richard Steinberg, and John Zysman. 2017. "From great power politics to a strategic vacuum: Origins and Consequences of the TPP and TTIP." *Business and Politics* 19(4).

Hite, Collin. (2017, April 11). "Your employees are the weak link in your cybersecurity program." *Virginia Business*. Retrieved from <http://www.virginiabusiness.com/opinion/article/your-employees-are-the-weak-link-in-your-cybersecurity-program>

H.R.2105 - NIST Small Business Cybersecurity Act. Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/2105?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=11>

H.R.2774 - Hack DHS Act. Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/2774?q=%7B%22search%22%3A%5B%222774%22%5D%7D&r=1>

In-Q-Tel, Inc. Retrieved from <https://www.iqt.org/about-iqt/>

Johnson et al. "Guide to Cyber Threat Information Sharing". NIST Special Publication 800-150. National Institute of Standards and Technology. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

Jones, S. (2015, November 9). "GCHQ chief to say free market failing on cyber security". Financial Times. Retrieved from <https://www.ft.com/content/4ec3e438-8708-11e5-90de-f44762bf9896>

Kovacs, E (2014, August 25). "Global Cybersecurity Spending to Reach \$76.9 Billion in 2015. SecurityWeek. Retrieved from <http://cybersecurityventures.com/cybersecurity-500/>

Lerner, J. (1996, September). "The Government as Venture Capitalist: The Long-Run Effects of the SBIR Program". The National Bureau of Economic Research. Retrieved from <http://www.nber.org/papers/w5753>

Lerner, J. (2002, February). "When Bureaucrats Meet Entrepreneurs: The Design of Effective 'Public Venture Capital' Programmes": *The Economic Journal*. Retrieved from <http://onlinelibrary.wiley.com/doi/10.1111/1468-0297.00684/full>

Lindsay, J. (2006, July 18). "War Upon the Map: The Politics of Military User Innovation. Retrieved from <https://dspace.mit.edu/handle/1721.1/33457>

Lynn, W (2009, June 15). *Center for Strategic and International Studies*. Retrieved from speech delivered by Deputy Secretary of Defense William J. Lynn in Washington D.C. on cyber security.

National Geospatial-Intelligence Agency Mission Statement. National Geospatial-Intelligence Agency Retrieved from www.nga.mil

Nye Jr, Joseph S. (2010) *Cyber power*. Harvard University Press.

Obama, B. (2016, February 9). “Protecting U.S. Innovation from Cyberthreats”. The Wall Street Journal. Retrieved from <https://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003>

Office of the Press Secretary. (2015, February 13). “Executive Order - Promoting Private Sector Cybersecurity Information Sharing.” The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>

Office of the Press Secretary. (2016, December 2). “Presidential Order – Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GMHB”. The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/presidential-order-regarding-proposed-acquisition-controlling-interest>

Office of the Press Secretary. (2016, February 9). “Executive Order – Commission on Enhancing National Cybersecurity”. The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity>

Office of the Press Secretary. (2016, February 9). “FACT SHEET: Cybersecurity National Action Plan”. The White House. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

Pearson, H. (2013, April 12). “Spending Bill’s China Cybersecurity Provision is Unclear”. Law360. Retrieved from <https://www.law360.com/articles/432500/spending-bill-s-china-cybersecurity-provision-is-unclear>

Riley, Michael, Ben Elgin, Dune Lawrence and Carol Matlack. (2014, March 17). “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It.” Bloomberg. Retrieved from <https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data>

Rosenzweig, Paul, Steven Bucci and David Inserra. (2013, April 1). “A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace.” *The Heritage Foundation*. Retrieved from <http://www.heritage.org/defense/report/congressional-guide-seven-steps-us-security-prosperity-and-freedom-cyberspace>

Rowe, Brent R. and Michael P. Gallaher. (2006, March). "Private Sector Cyber Security Investment Strategies: An Empirical Analysis." WEIS. Retrieved from <https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf>

S.1428 - Small Business Cyber Training Act of 2017. Retrieved from <https://www.congress.gov/bill/115th-congress/senate-bill/1428?q=%7B%22search%22%3A%5B%22cyber%22%5D%7D&r=5>

Sales, Nathan Alexander. (2013) "Regulating Cyber-Security" *Northwestern University Law Review*, Vol. 107(4). Retrieved from <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1040&context=nulr>

Schulman, Loren DeJonge, Alexandra Sandra and Madeline Christian. (2017, July 18). "The Rocky Relationship Between Washington and Silicon Valley: Clearing the Path to Improved Collaboration." *Center for New American Security*. Retrieved from <https://copia.is/wp-content/uploads/2017/07/COPIA-CNAS-Rocky-Relationship-Between-Washington-And-Silicon-Valley.pdf>

Sender, H. (2016, Septmeber 4). "US defence: Losing its edge in technology?". *Financial Times*. Retrieved from <https://www.ft.com/content/a7203ec2-6ea4-11e6-9ac1-1055824ca907>

Somerville, H. (2015, May 13). "Defense Department's Tech investing signals Silicon Valley's importance in cyberwarfare". *The Mercury News*. Retrieved from <http://www.mercurynews.com/2015/05/13/defense-departments-tech-investing-signals-silicon-valleys-importance-in-cyberwarfare/>

Shane, Scott, Cade Metz and Daisuke Wakabyashi. (2018, May 30). "How a Pentagon Contract Became an Identity Crisis for Google." *The New York Times*. Retrieved from <https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html>

Stamos, Alex. (2017, July 26). "Preparing for the future of security requires focusing on defense and diversity." *Facebook*. Retrieved from <https://www.facebook.com/notes/facebook-security/preparing-for-the-future-of-security-requires-focusing-on-defense-and-diversity/10154629522900766/>

Stay Safe Online. Retrieved from <https://staysafeonline.org/ncsam/ncsam-champions/>

Tadjdeh, Yasmin. (2015, August 13). "Army Reserve Pursuing Partnerships with Silicon Valley." *National Defense Magazine*. Retrieved from <http://www.nationaldefensemagazine.org/articles/2015/8/13/army-reserve-pursuing-partnerships-with-silicon-valley-updated>

Wakabayashi, Daisuke and Cade Metz. (2018, June 7). "Google Promises Its A.I. Will Not Be Used for Weapons." *The New York Times*. Retrieved from <https://www.nytimes.com/2018/06/07/technology/google-artificial-intelligence-weapons.html>

Wakabayashi, Daisuke and Scott Shane. (2018, June 1). "Google Will Not Renew Pentagon Contract that Upset Employees." *The New York Times*. Retrieved from <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>

Waltz, K. *Theory of International Politics*. New York. 1979.

Wilshusen, Gregory C. (2012, July 17). "Cybersecurity: Challenges in Securing the Electricity Grid." *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/600/592508.pdf>

Wilson, Clay. (2007). "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues in Congress." *Focus on Terrorism, Volume 9*. Retrieved from <https://books.google.com/books?hl=en&lr=&id=w1-Ds42YMDIC&oi=fnd&pg=PA1&dq=domestic+consequences+of+cyber+industrial+policy&ots=dRdrijLq7f&sig=nA8bY2tWnnl4yjXt4TI0ylJMWa4#v=onepage&q&f=false>