



Comparative industrial policy and cybersecurity: the US case

Vinod K. Aggarwal & Andrew W. Reddie

To cite this article: Vinod K. Aggarwal & Andrew W. Reddie (2018) Comparative industrial policy and cybersecurity: the US case, *Journal of Cyber Policy*, 3:3, 291-312, DOI: [10.1080/23738871.2018.1551910](https://doi.org/10.1080/23738871.2018.1551910)

To link to this article: <https://doi.org/10.1080/23738871.2018.1551910>



Published online: 12 Dec 2018.



[Submit your article to this journal](#)



Article views: 31



[View Crossmark data](#)



Citing articles: 2 [View citing articles](#)



Comparative industrial policy and cybersecurity: the US case

Vinod K. Aggarwal  and Andrew W. Reddie 

Berkeley APEC Study Centre, University of California, Berkeley, CA, USA

ABSTRACT

This paper investigates the relationship between the US government and its domestic cybersecurity sector drawing on the special issue framework. We show how there has been, and argue that we will likely continue to see, substantial public investment in the sector by the US government via industrial policy to address cybersecurity market failures. This analysis is particularly important given that both the market failures associated with the provision of cybersecurity and the government role in addressing this challenge remain under-explored in the existing academic and policy literature. The paper proceeds in three parts. First, it outlines the unique categories of three types of firms – those in the cybersecurity sector, large technology companies and internet-adjacent firms – involved in the under-provision of cybersecurity and examines possible market failures. Second, we inventory existing measures employed by the US government to engage with each type of firm to address real and perceived market failures in these different sectors. Finally, we examine how state-society relations have conditioned US government intervention approaches in this sector and argue that well-established IT firms now have a privileged lobbying role related to state-society relations in the United States.

ARTICLE HISTORY

Received 26 August 2018
Revised 30 October 2018
Accepted 31 October 2018

KEYWORDS


Cybersecurity; industrial policy; governance; regulation

1. Introduction

The US government has a long history of taking advantage of, reacting to and taking steps to support technological innovation by providing both direct and indirect support to firms – despite perceptions that the US government takes a *laissez-faire* approach. In the information economy over the past two decades, this has been no different.

As Deputy Secretary of Defense Gordon 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 ... (England 2008)

CONTACT Andrew W. Reddie  areddie@berkeley.edu

This article has been republished with minor changes. These changes do not impact the academic content of the article.

© 2018 Chatham House

Most recently, and following a series of cyberattacks on US government and US private sector targets, internet technology and cybersecurity have become the technology *du jour* receiving the focus of US policymakers.

As part of a broader project that investigates the industrial policies and cybersecurity across geographies, this article uses a political economy lens to examine the various efforts taken and policies used by the US government ‘to stay ahead of everyone else’ in cybersecurity. Specifically, we focus on the patterns of interaction between government and firms in 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 or is perceived to inadequately 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 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 US 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. (Lynn 2009)

Given the unique challenges afforded by the cyber domain, and in light of concerns surrounding private and public supply chains, how multinational firms and government interact will likely be of central importance.

On a more practical level, this paper also engages with the questions of why and how the US government is engaging with the expertise of engineers and computer scientists from Silicon Valley to address broader security challenges in general and in cybersecurity specifically. During the Obama administration, Secretary of Defense 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’ (Carter 2015). He goes on to note that broad cooperation is 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. (Carter 2015)

Increasingly, this cooperation involves far more than lip service and has been reflected in US government policies that have sought to strengthen the cybersecurity industry – both to provide the public sector with necessary talent by developing human capital 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 challenges (Schulman, Sander, and Christian 2017). The recent controversy surrounding Google’s role in Project Maven – an artificial intelligence project led by the military and involving private sector partners – and the petitioning of Google employees against the continued relationship

between the company and the US Department of Defense serves as the most recent examples of the dissent that follows government involvement in the data economy (Shane, Metz, and Wakabayashi 2018; Wakabayashi and Metz 2018; Wakabayashi and Shane 2018).

To examine these policies, our paper identifies both 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. We then inventory existing measures employed by the US government to address challenges facing cybersecurity firms, IT firms and firms that rely on internet technology that we term internet-adjacent firms. Finally, we analyse the driving forces of cybersecurity industrial policy in the United States based on the political economy of state-society relations and note the increasingly prominent role of well-established IT firms lobbying for specific market facilitating and regulatory interventions from Washington.

Given the relative youth of industrial policy to address cyber insecurity, this paper seeks to inventory steps taken by the government to address cyber insecurity in the private sector rather than provide an in-depth assessment of the successes or failures of those measures.

2. The variety of firms in the cybersecurity market and market failures

US government concerns related to cybersecurity stem from a broader fear among policymakers and engineers that applications and products reliant upon internet technology suffer from a variety of security-related vulnerabilities that both state and non-state actors can take advantage of. Indeed, over half of global spending on cybersecurity occurs in the North American market and is primarily driven by the United States (Cybersecurity Ventures 2018).

In 2017, the US 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 cyberthreats that 'could lead to widespread vulnerabilities in civilian infrastructure and US government systems' (Clapper 2016). By 2022, it is projected that the US 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 per cent of all cyber insurance policies purchased by US firms.

In this section, we categorise the firms affected by cyber insecurity before discussing the conceptualisation of market failure through which these firms and the government interact in section 3.

For the purposes of this study, we identify three categories of firms that frame our analysis. These are: 'cybersecurity firms,' 'internet technology firms,' and 'internet-adjacent' firms. Understanding each type of industry player is integral to conceptualising the interests they bring to the issue as well as considering how they interact with Washington.

The first category involves cybersecurity firms that work directly on cybersecurity-related challenges and provide a suite of cybersecurity-related products and services for a variety of commercial and/or government clients. They run the gamut from creating cybersecurity-related products to protecting networks, consulting on cybersecurity literacy for employees, performing threat assessments, penetration testing, and tracing cyberattacks and hacks. Examples of these types of firms in the United States include

Mandiant, Darktrace, Symantec, FireEye, Palantir and Qadium. In-Q-Tel, a CIA-funded venture capital firm that provides a foundational investment in a number of IT firms including Palantir Technologies, serves as an example of the close relationship between these firms and government. 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, 36 from Israel and 13 from Canada (Kovacs 2014). Despite the dramatic American lead, concerns about the rapid rise of competitors in this space, particularly of China, has led to fears that this lead will not persist.

Second, we have internet technology (IT) firms that rely on cybersecurity to protect their own operations and products – but that do not provide cybersecurity goods and services beyond their own company. Examples of this type of firm include those that work in what is often called the 'big data' space, such as Alphabet, Facebook, Microsoft, Apple and IBM. These companies require cybersecurity to carry out their business operations and interact with customers, but cybersecurity is not a core part of their business. Microsoft, for example, intends to invest \$1 billion each year on cybersecurity in the 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 US economy in 2016 (US Department of Commerce 2016). Concerns from this sector arose from the 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 of secondary or tertiary concern. As a consequence, the existing market incentives fail to reward actors that privilege security.

Finally, there are internet-adjacent firms whose products have internet-based components but that have a large proportion of their operation outside the technology sector. These types of firms include those working in the 'Internet of Things' (IoT) space such as General Electric, Kenmore and Tesla, as well as retail firms like Target and Walmart, and media companies such as the *New York Times* and *Washington Post* that rely upon the internet for the consumption of their products. Other firms, including those in the defence industrial base such as Northrop Grumman and Lockheed Martin rely upon networked infrastructure to collaborate with government partners. Firms that provide critical national infrastructure such as energy utilities, power stations and dams such as Pacific Gas and Electric and smaller utilities such as East Bay Municipal Utility District in the Bay Area are also included in this category given their use of networked systems to control the provision of water and power, respectively. For these companies, the regulations and standards proposed and, occasionally, imposed by the government relating to data privacy, data protection and cybersecurity standards have consequences for these firms' operations. These consequences have led to calls for a 'light footprint' approach to regulation exemplified by the NIST-sponsored Framework for Improving Critical Infrastructure Cybersecurity. The framework provides a voluntary mechanism for states to act upon public-private guidelines and best practices.

From the perspective of firms, each has their own distinct interests concerning government action in the cybersecurity sector – whether related to the type of talent that they are interested in developing or the type of regulation and standard-setting that they deem most appropriate. From a government perspective, security threats emanating from cyberspace are extremely damaging – as the hack of the Office of Personnel Management in

June 2015 made clear. This has led to the US government taking on an active role addressing its own vulnerabilities and attempting to mitigate the cybersecurity threats faced by private 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. Market failures in a cybersecurity context

Given the obvious reliance upon internet technology in the US economy, the substantial online security vulnerabilities represent a significant policy challenge. To think about these security vulnerabilities, we draw on the theoretical framework of this special issue to consider the insecurity in the existing internet architecture in terms of market failure. In particular, we focus on some general concerns about coordination, information problems, moral hazard and externalities before turning to specifics for each market sector noted in section 2.1.

Firms face trade-offs between innovation and security in product design. Indeed, a number of firms have evidenced a proclivity for ‘publish and patch’ applications. This is particularly problematic given the downstream consequences of cybersecurity breaches and that any vulnerability is ‘networked’ into interoperable systems controlled by a wide variety of companies. This *coordination* problem means that individual firms have the incentive to attempt to free-ride on the ‘security’ of the whole system and to dump liability on the platforms upon which their application runs or to otherwise assume that the user assumes liability for the negative consequences of interacting with the internet – whether in e-commerce or social media.

These coordination problems are also related to the *information* problems facing both firms and government. Firms in both the IT sector and in other business sectors have been slow to address cybersecurity challenges. This is due in part 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 and that hacks are occasionally difficult to detect.¹

Market failures relating to *moral hazard* among IT firms are also significant as platforms such as Facebook or YouTube rarely bear the cost of data breaches, fraud and intellectual property theft on their network.² Instead, responsibility is passed down to the user to patch the system or to bear the cost of a data breach. Moreover, government is increasingly blamed for the fragility of the IT architecture rather than firms (Moore 2010). This moral hazard is also linked to *liability dumping*, in which platform and application providers abdicate responsibility for the use or misuse of an application and security risks to the user – whether individual consumers or subsidiary companies.

Interlinked security and economic externalities are also critical in this sector. First, the economic costs incurred by cybercrime and cyber insecurity represent a drag on the US economy. Addressing these challenges represents a public good for market participants. Second, the threat posed by cyber espionage and the international security consequence of cyberattacks and related fears concerning cyberwarfare have increasingly played a role in US strategic decision-making, as evident in the National Security Strategy and 2018 Nuclear Posture Review that explicitly note the dangers posed by cyberweapons to the

United States.³ The latter security rationale focused on three areas: the vulnerability of US federal agencies to cyberattacks, the vulnerability of national critical infrastructure to cyber-attacks, and the threat to the continuing competitiveness of the US military vis-à-vis other great powers. Gen. Keith Alexander, former head of the NSA, detailed these fears during his speech at CSIS calling cybersecurity ‘compromised by carelessness, poor design’ (Alexander 2016).

The government response to this reality has been variously described as inadequate. In an op-ed in the *Wall Street Journal* on 9 February 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’ (Obama 2016). In the article, 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 of our time’ (Pritzker 2016). 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.

To deal with the challenges facing the cybersecurity industry, the US government has pursued a substantial number of industrial policy initiatives in the cybersecurity market.

3. US market intervention: patterns of intervention

In this section, we draw on the concepts outlined in the theory article in this volume to examine the interactions between the US government and cybersecurity firms, internet technology firms, and internet-adjacent firms (Aggarwal and Reddie 2018). In our discussion, we point to concerns about market failure and then examine government responses in each subsection.

3.1. Washington and cybersecurity firms

The challenges faced by both government and the private sector in relation to cybersecurity firms are relatively new and have become increasingly pronounced over the past decade. The market failures facing the US government include the under-supply of cybersecurity goods and services, the inefficiency of the existing procurement architecture, lack of human capital and reliance upon global supply chains.

3.1.1. The under-supply of cybersecurity goods and services

Government agencies have often played the role of primary customer to firms in the cybersecurity sector. Indeed, much of the innovation with respect to cybersecurity tools comes from the private sector rather than the intelligence agencies. Although the US market dominates the provision of cybersecurity tools, there remains the fear that these tools are inadequate to address the challenges posed by emerging adversaries – both state and non-state.

To address these perceived failures, the US government has played a *market substitution* role as a provider of investment to create firms to meet its security needs. Indeed, Washington uses an increasingly prominent investment vehicle – venture

capital – to provide government support to projects of importance to national security, including cybersecurity (Lerner 1996; Brander, Du, and Hellmann 2015). The founding of Palantir in 2003 with \$2 million in venture capital funding from In-Q-Tel – led by a group of former CIA officials – serves as the prototypical example of this pattern of interaction.

In-Q-Tel (IQT) itself, founded by former CIA director George Tenet in 1998 and described as ‘a non-profit strategic investor that accelerates the development and delivery of cutting-edge technologies for US government agencies that keep our nation safe,’ has provided hundreds of millions of dollars to over two hundred technology companies and has built relationships between members of the intelligence community and these firms (In-Q-Tel, Inc. n.d.). 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 start-ups. In the process, it partners with the Central Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, Office of the Secretary of Defense/Joint Chiefs of Staff, Defense Intelligence Agency, Federal Bureau of Investigation, National Reconnaissance Office and Department of Homeland Security.⁴ 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 correspondence to public power grids’ (Somerville 2015).

More recently, the CIA has created its own Directorate of Digital Innovation (DDI). The DDI focuses on accelerating digital innovation across the intelligence community. In its operation, ‘DDI has a close partnership with In-Q-Tel’ and will help strengthen the 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 related to cybersecurity – including artificial intelligence and quantum computing tools (Ackerman 2016).

This type of interaction between government and industry that is focused on a particular area of demand reflects a historical pattern. Indeed, amid 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 practice (Budiansky 2016). This relationship between private contractors with close ties to government continued to grow over the course of the Cold War era.

3.1.2. An inefficient procurement process

The traditional procurement processes through which emerging technologies move from the private sector to public agencies have often been described by both academic and policymakers as slow and burdensome – removing the potential for small firms to bid for government contracts – and has come under criticism given the new threats and risks posed by cybersecurity. Given the innovative nature of small firms in creating critical security tools, the need to bolster such firms is evident.

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.⁵

3.1.3. A lack of human capital

Government concerns about the failure to develop adequate human capital for the intelligence services and fear that the best talent will migrate to Silicon Valley has led to increased efforts to promote cybersecurity education and exchange. These human capital concerns impact the public and private sectors across countries – as discussed in greater detail in Carr and Tanczer’s paper focused on the United Kingdom and Benjamin Bartlett’s paper on Tokyo’s industrial policy in this special issue (Bartlett 2018; Carr and Tanczer 2018).

As a result, there are a variety of government-led programmes ostensibly designed to address this challenge. These programmes are designed to increase technology-focused human capital in the government and private sector workforce. There are a large number of these initiatives so we inventory just a few here. The first example is the National Initiative for Cybersecurity Education (NICE) established in 2012 (Cobert 2017). NICE is a joint effort by the US 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 US federal agencies to coordinate cybersecurity education and workforce policy. It also developed the National Cybersecurity Workforce Framework, which helps agencies categorise cybersecurity work and, in doing so, assists with the identification of US federal and private workforce needs (NICE 2018).

Second, the National Integrated Cyber Education Research Centre (NICERC) exists in partnership with the DHS as an education-oriented non-profit subsidiary of the Cyber Innovation Centre to provide cybersecurity curricula to elementary, middle and high school students (US Department of Homeland Security 2016). The initiative is part of a broader US federal effort to reach out to all schools, and, specifically, appears to be part of CETAP (‘Cybersecurity Education and Training Assistance Program’), a DHS cybersecurity education programme.

Third, the CyberCorps Scholarship for Service Programme⁶ represents a joint initiative by the NSF and the DHS that provides scholarships to undergraduate/graduate students at NSA/DHS-designated Centres of Academic Excellence in information assurance (US Office of Personnel Management 2018). After the completion of their degree, students commit to serving federal, state, local or tribal governments for as long as they received the scholarship.

There are also a variety of human capital development pipelines designed to integrate trained individuals in Washington, DC and northern Virginia with military and intelligence agencies. The US Digital Service serves as the best example of this approach with the Department of Defense creating its own US Defense Digital Service (DDS) under the auspices of the Service (US Department of Defense: Defense Digital Service n.d.). As part of this

effort, DDS also operates a number of programmes including ‘Hack the Pentagon’ and ‘Hack the Army.’

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.’ Another, the National Cyber Security Alliance – including actors from industry and various government agencies – provides a venue for cybersecurity firms to liaise with government actors.⁷

3.1.4. Reliance upon global supply chains

The US high-tech and cybersecurity markets are also reliant upon *global supply chains*. James Clapper (DNI), Marcel Lettre (DoD) and Adm. Michael Rogers (CYBERCOM) detailed the challenges of this integration in a Joint Statement to the Senate Armed Services Committee on 5 January 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’ (Clapper et al. 2017). This has led to fears that adversaries might use their own ‘national champion’ companies in the cybersecurity sector to infiltrate private and public sector networks in the United States.

To address these vulnerabilities, Washington has increasingly relied upon its *regulatory* role. Domestic cybersecurity firms in the United States benefit from this regulatory role, particularly the procurement rules that limits external competition available to cybersecurity firms. These rules proscribe international suppliers and place limits on international components from entering the United States for technologies of strategic importance. Perhaps most controversially, the US government ceased its partnership with Kaspersky Labs because of alleged links to the Russian government. In the past two years, oversight of foreign investment in industries deemed to be strategically important by an increasingly activist Committee on Foreign Investment in the United States (CFIUS) has become routine and culminated in the Foreign Investment Risk Review Act of 2018 (FIRRMA).

3.2. Washington and internet technology firms

Beyond the challenges faced in the cybersecurity market specifically, there are broader market failures afflicting the IT sector related to network effects and global vulnerabilities that have led to the US government becoming increasingly engaged with the tech sector.

Cyber insecurity increases as IT systems scale and companies build products that work on the platforms of another. Indeed, interoperability offers a paradox as increased efficiency contributes to cyber insecurity. For example, Facebook has developed an application for its service that runs on the Google Android OS used by Samsung in its Galaxy handsets. While interoperability offers a boon to consumers, it has attendant risks as vulnerabilities increase across platforms and spread across the internet. Put another way, there are network effects that drive vulnerability in the private sector. Increasingly, these vulnerabilities also travel to the public sector and have contributed to the increasing role of government to address cybersecurity challenges.

To address these challenges and to bring the interests of government to Silicon Valley and the private sector, Washington has sought to play a *market facilitation* role with the broader internet technology sector to encourage cooperation. This role is encapsulated by Secretary of Defense Ash Carter's insistence that government agencies build offices and cultivate relationships directly in Silicon Valley. During the Defense One Tech Summit in June 2016, Carter noted, 'I am committed to building and rebuilding the bridges between our national security endeavors at the Pentagon and innovators throughout the nation from the tech entrepreneurs in Silicon Valley' (Carter 2016).

Currently, both the DHS and the DoD have opened offices specifically meant to engage with Silicon Valley firms directly. The DHS Innovation Programme and DHS Science and Technology Directorate have offices in the Bay Area while the DoD – via the Defense Innovation Unit (formerly 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' (Tadjdeh 2015). 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' (National Geospatial-Intelligence Agency n.d.). 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 US Department of Defense and each firm (National Security Technology Accelerator, n.d.). Each of these efforts attempts to overcome challenges facing the existing procurement pipelines that are viewed by many as being inefficient and difficult for emerging companies to manoeuvre through. The DIU, in particular, serves as an important example of the emerging OT ('other transactions') procurement process within the contemporary Federal Acquisition Regulations (FAR).

More recently, these types of relationships have led to close collaboration between the private and public sector related to emerging technologies such as artificial intelligence as well as the widespread use of private sector tools – particularly cloud services – by US government agencies.

This collaboration has been more fraught in areas related to *regulation*. Efforts to bolster information-sharing regimes, for example, have been the subject of consternation with disclosure of breaches via private information-sharing regimes preferred over public clearing houses – even when these voluntary arrangements release firms from legal liability. With regards to standards, a legally-binding set of standards has also proved elusive with the non-binding NIST Framework for Improving Critical Infrastructure Cybersecurity offering a 'best practices' approach to creating informal standards for private industry to follow and incorporate into their 'organizational risk management processes' (NIST 2014).

3.3. Washington and the internet-adjacent industry

In the broader marketplace, the US government has also taken on a significant *regulatory* role while also playing the role of *facilitator* for firms struggling to adapt to cyber insecurity.

3.3.1. Collateral damage

As noted above, a number of firms from outside the IT sector have become increasingly reliant upon the internet to run their businesses – particularly related to payment

processing and customer relationship management. These firms have increasingly found themselves at risk of cyberattacks and represent the collateral damage of informatization that reduces transaction costs but increases a firm's vulnerability.

To address these concerns, the US government has employed a mix of market facilitating and regulatory roles designed to communicate best practices to firms and to increase cybersecurity standards across the entirety of the market as described in greater detail below. In contrast to their allies in Tokyo, Washington has not provided services directly to the private sector (market substitution).

3.3.2. Import and export controls

Import and export controls offer the most obvious example in which Washington manipulates 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 domestic industry. Section 516 of the Consolidated and Further Continuing Appropriations Act 2013, signed into law by President Obama on 26 March 2013, offers an example of an import control with impacts upon IT-adjacent US companies. This law prohibits the procurement of any information technology system subsidised, produced, manufactured or assembled in China by various government departments including the departments of Commerce and Justice, NASA and NSF (Global Trade Alert 2013; Pearson 2013). 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 the United States, unless the Secretary of Defense demonstrates to the congressional defence committees that acquisition of a similar supercomputer from a domestic manufacturer would not be possible (Global Trade Alert 2014).

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) (US Department of State n.d.).

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 US government and also provide licences and authorizations for the 'specific exports of defense articles and services' (US Department of State n.d.) DHS and US Customs enforce these controls with criminal and civil penalties for export control violations to ensure compliance.

The government also plays 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 granted to the president by Section 721 of the Defense Production Act. 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 (Global Trade Alert 2013; Global Trade Alert 2014; Global Trade Alert 2016). A major effort is currently 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.

3.3.3. Information-sharing regimes and sharing best practices

While the export control regime noted above emphasises the coercive aspects of compliance, internet-adjacent firms are also impacted by the less coercive regulatory standard-setting measures. The NIST Framework for sharing information related to cyberthreats between industry and government applies to these firms, too (Johnson et al. 2016). This framework, born from the mandate of the Burr-Feinstein Bill and Cybersecurity Information Sharing Act of 2015, establishes a voluntary information-sharing regime and attempts to eliminate legal barriers and disincentives which would have otherwise discouraged large-scale dissemination of relevant data. As part of this process, the National Institute of Standards and Technology is mandated 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' (Johnson et al. 2016). 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](#) (National Institute of Standards and Technology, n.d.).

This effort was followed up in Section 1428: 'Small [Business Cyber Training Act of 2017](#)' that allocates \$350,000 to establish a 'cyber counseling program.'

3.3.4. Human capital development

Internet-adjacent firms also benefit from US government efforts to improve the IT talent pipeline such as the TechHire programme announced by President Obama in March 2015. TechHire's goal is to create a national campaign to build 'tech talent pipelines' across the United States for both the private and public sectors (White House, n.d.). The initiative aims to provide workers with the skills to perform IT roles that are too often left vacant.

As demonstrated above, there are a variety of patterns of interaction between the US government and private firms in the cybersecurity market. These interactions, however, are the result of sustained push and pull interaction between private and public actors.

4. State-society relations in the United States

How have US state-society relations affected industrial policy in the cybersecurity market? Traditionally, scholars of American politics have developed pluralist interpretations of US policymaking. For these scholars, interest groups form to address issues relevant to them, they create alliances amongst themselves as necessary, and then the government simply implements policy based on the power of the dominant coalition. But as work by Steve Krasner (1978) argues, it may make more sense to view policymaking in terms of state-society relations whereby the state has its own goals. In the case of the US, as Krasner argues, while the state may be weak, it is conceptually misleading to believe that the state does not have goals of its own. Indeed, as we have noted, the US government has clearly sought to influence the cybersecurity market, driven by broad strategic concerns. Here we look at this strategic interaction between state and society in the formulation of industrial policies, focusing on the variation in power among firms in different segments of the cybersecurity market. Specifically, we note the relative power of entrenched internet technology firms in the lobbying process compared to the nascent cybersecurity sector and the broader marketplace with its divergent interests.

4.1. Lobbying from the cybersecurity sector is under-developed

As noted above, efforts by the cybersecurity industry to promote cybersecurity awareness in government has largely been successful – particularly in the aftermath of several hacks of government agencies. As a consequence, the US government has created several institutional mechanisms that allow for government-cybersecurity sector collaboration. The H.R. 2774: ‘Hack DHS Act’ introduced by Representative Ted Lieu (D-CA), for example, proposes the establishment of a ‘bug bounty 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 the DHS and other US government agencies to address existing vulnerabilities and prepare against potential attacks. The programme itself calls for the use of \$250,000 of government funds during the 2018 fiscal year to carry out the programme. Similarly, H.R. 3359: ‘Cybersecurity and Infrastructure Security Agency Act of 2017’ authorises the establishment of the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security in an attempt to strengthen US government institutions from cyberattack.

The relationship between firms in the cybersecurity sector and US government agencies, however, tend towards being functional and, perhaps as a result of their relative youth, the lobbying capacity of cybersecurity firms has been considerably less apparent in debates surrounding data localisation, privacy, information sharing and security standards than their much larger cousins in the IT sector.

4.2. IT firms and entrenched lobbying power

As has been well-documented, the tech sector has substantially increased its lobbying capacity over the past decade (Sullivan 2018). This has had a significant impact upon the *regulatory* role of the US government.

As noted above, public-private cooperation on cybersecurity has thus far been characterised 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 (Etzioni 2014). 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' (BSA The Software Alliance 2013). 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' (BSA The Software Alliance 2017). 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 modernisation of the Electronic Communications Privacy Act and the reauthorization of section 702 of the Foreign Intelligence Surveillance Act. Similarly, the US Chamber of Commerce, a prominent business-oriented lobbyist group, released a 6 February 2017 memo on the state of American cybersecurity that notes, 'Government policy and decisions shouldn't get in the way of the private sector' (Beauchesne 2017). The Information Technology Industry Council (ITI) and USTelecom also announced, upon the creation of their shared Council to Secure the Digital Economy, 'we're all in agreement ... that regulatory and compliance regime[s] won't really address threats that are evolving in the long term' (Breland 2018).

These prerogatives are also reflected in various war-making scenarios. In April 2015, RAND Corporation conducted '360° Discovery Games' in both Washington DC and Silicon Valley in which key stakeholders in the government, journalism, academia and the tech industry (including IT producers and IT security) worked together in groups to solve theoretical cybersecurity-threat scenarios (RAND 2016). 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 patches/upgrades, and competition would lead to greater security. The question of what would incentivize the market, however, remained unanswered (RAND 2016). 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 (RAND 2016). 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. Another argument often put forward by industry suggests that a static regulatory framework may have unintended and negative consequences upon a company's ability to respond to evolving cyberthreats.

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 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’ (Fung 2015). Dropbox has similarly emphasised 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 passing laws, the firms have asked government to issue ‘recommendations on transparency, threat sharing, and privacy for consumer data’ (Daniel, Felton, and Scott 2016).

Costs to reputation and scepticism concerning the role of government among firms has led to lobbying efforts that emphasise 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 overregulation. Their priorities included eliminating legal barriers to cyberthreat information-sharing both between private firms and within the public sector, establishing a trust-based environment and creating an incentive-based system to encourage international cooperation on fighting cybercrime 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 cyberattacks (Dilanian 2012).

4.3. Internet-adjacency and liability dumping

Beyond the IT sector, 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 cyberattacks 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 (Finkle and Heavey 2014). Ultimately, Target’s security breach resulted in \$18 million in lost revenue – largely an impact of negative publicity – and is indicative of a harmful feedback loop: firms fear that admitting cybersecurity weaknesses will decrease consumer confidence, firms are hacked, firms scramble to recover, yet fear among consumers lingers (Etzioni 2014). 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 per cent of the time, for retailers it amounts to only 5 per cent (Riley et al. 2014). 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’ (Rowe and Gallaher 2006).

Target’s vulnerability exemplifies 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, 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 (Sales 2013). In political economy terms, the liability for the breach is dumped on the consumer. Indeed, the marginal benefit of cybersecurity investment largely depends on 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. (Rowe and Gallaher 2006)

Yet other companies, at the insistence of cybersecurity firms like FireEye, view cyberattacks and subsequent breaches as an inevitability. As a consequence, it is perhaps unsurprising that internet adjacent firms do not spend their marginal dollar on cybersecurity but on their core business.

4.4. NGOs

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 to bring cybersecurity education and advocacy directly to consumers. In an effort to connect with consumers, the EFF works to increase awareness of its collaborative projects such as HTTPS Everywhere and Certbot (EFF n.d.). 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, the United States' leading nonprofit public-private partnership, has worked in conjunction with the 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 (Stay Safe Online n.d.).

5. Conclusion

Although the mainstream consensus has been that industrial policy does not work, the US government has actively pursued a large number of industrial policy initiatives in the cybersecurity market to address market failures. Both the Department of Defense and the intelligence community recognise that much of the innovation in cybersecurity has come from the private sector. At the same time, a large number of cybersecurity risks are also linked with the private sector. In light of the need to maintain both a security and economic edge over competitors, we have inventoried industrial policy initiatives enacted by Washington over the past decade. At the same time, the pursuit of industrial policy is by no means a simple matter – as evidenced by the variety of programmes inventoried in this paper.

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 US economy. From a security perspective, several reports have pointed to the ongoing vulnerability of federal agencies and critical infrastructure to cyberattacks, and noted the cybersecurity vulnerabilities for the military with respect to other countries. This vulnerability stems from a geopolitical context of great power competitors and in which recalcitrant states like North Korea and non-state actors have successfully employed cyberattacks.

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. Similarly, Washington faces challenges related to its own operations (Wilson 2007). For example, the Department of Defense's reliance on civilian systems and products – some of which are developed and manufactured abroad – mean that the DoD is vulnerable to attacks on commercially available software. Companies that the US government contracts with also 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' (Wilson 2007). The general consensus has been that neither the US government nor industry working on their own have been able to address these issues, most of which are tied to the labour market in regards to lack of training, career paths and other problems such as a failure to upgrade infrastructure.

That said, there is a delicate balance to be negotiated with regards to ensuring that corporations are proactive in their consideration of cybersecurity when designing products while at the same time 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 US entities while not providing additional security' (Rosenzweig, Bucci, and Inserra 2013). Thus, the US government is faced with a delicate balancing task to create an effective and useable information-sharing regime, foster a duty of care toward cybersecurity by private actors, oversee the nascent cyber insurance system, devote public resources to cybersecurity education, and engage with the transnational aspects of cybersecurity. Indeed, our analysis that accounts for three types of firms notes the variation in how the government engages with each.

While cyberattacks that take advantage of cyber vulnerabilities continue to come from abroad, there are understandable incentives to undertake a programme of indigenisation in terms of both human capital and equipment reminiscent of China's approach outlined in Cheung's paper in this special issue (Cheung 2018). At the same time, protectionist policies – even those that are justified on the basis of national security – have consequences for the international economic regime and the global supply chains upon which a large number of American corporations and consumers rely. The industrial policies favoured by Washington also likely to reflect existing power dynamics in the US domestic marketplace. Indeed, we already see that the current 'winners' in the internet marketplace – IT firms themselves – appear to have significant lobbying advantages with attendant consequences upon the US government's market facilitation and regulatory roles.

While the practice of industrial policy in the cybersecurity marketplace remains in its infancy and it remains 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 geopolitics, government policies to craft domestic markets, and their impact upon various types of actors in the private sector.

Notes

1. Indeed, a number of company representatives have noted the importance of ad hoc information sharing relationships with other firms, government agencies and law enforcement.
2. YouTube, for example, takes no responsibility for the material posted on the platform.
3. The fourth potential motivation is politically motivated. Policymakers and politicians might seek to 'do something' in the cybersecurity sector in lieu of doing nothing; US National Security Strategy 2017; US Nuclear Posture Review 2018.
4. IQT has provided funding to Basis Technology, Oculis Labs, Sonitus Medical, D-Wave Systems, Forterra Systems Inc. and CyPhy Works among others.
5. In March 2017, for example, the CIBORG initiative led to a \$4.4M contract with VRICON for various data modeling and data packages: (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)
6. See Title III of the Cybersecurity Enhancement Act of 2014
7. See also Defense Innovation Advisory Board. Ferdinando, Lisa. (2017, January 9). "Advisory Board Approves 11 DoD Innovation Recommendations." *Department of Defense News*. 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.

Acknowledgements

For research support, we are grateful to Mahshad Badii, Prashant Desai, Somi Yi, Anastasia Pyrinis, Claire Tianyu Qiao and Yujie Shen. We are also grateful to Phil Stupak, Michael Adams, Steve Weber, Stephan Haggard, the editorial staff at the *Journal of Cyber Policy* and two anonymous reviewers for helpful comments during the drafting of this manuscript.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

For funding support, both authors would like to thank the Center for Long-Term Cybersecurity and the Hewlett Foundation, the Institute of East Asian Studies, the Social Science Matrix and the Berkeley APEC Study Centre (BASC). Aggarwal's work was also partially supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea [grant number NRF-2017S1A3A2067636].

Notes on contributors

Andrew W. Reddie is a PhD candidate in the Charles and Louise Travers Department of Political Science at the University of California, Berkeley. He also serves as Managing Editor of *Business and Politics* and as a research associate at the Centre for Global Security Research at Lawrence Livermore National Lab. Reddie received an MPhil in International Relations from Oxford University as well as an MA and a BA (hons) from the University of California, Berkeley.

Vinod K. Aggarwal is Travers Family Senior Faculty Fellow and Professor in the Travers Department of Political Science, Affiliated Professor at the Haas School of Business, and Director of the Berkeley Asia Pacific Economic Cooperation Study Centre (BASC) at the University of California, Berkeley. He is also Editor-in-Chief of the journal *Business and Politics*. He is the author of 21 books and over 120 articles. His most recent book is *Responding to the Rise of China*. Dr. Aggarwal received his BA from the University of Michigan and his MA and PhD from Stanford University.

ORCID

Vinod K. Aggarwal  <http://orcid.org/0000-0002-8572-6323>
 Andrew W. Reddie  <http://orcid.org/0000-0003-3231-8307>

References

- Ackerman, R. 2016. "The CIA Accelerates Innovation." *SIGNAL*, June 1. <https://www.afcea.org/content/Article-cia-accelerates-innovation>.
- Aggarwal, Vinod, and Andrew W. Reddie. 2018. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis." *Journal of Cyber Policy* 3 (3): 452–466.
- Alexander, K. 2016. "Center for Strategic and International Studies – Cybersecurity Policy Debate Series." *CSIS*, May 3. <https://www.csis.org/events/cybersecurity-discussion-general-keith-b-alexander-director-nsa-commander-us-cyber-command>.
- Bartlett, Benjamin. 2018. "Government as Facilitator: How Japan is Building its Cybersecurity Market." *Journal of Cyber Policy* 3 (3): 334–350.
- Beauchesne, Ann M. 2017. "The State of American Cybersecurity." *US Chamber of Commerce*, February 6. <https://www.uschamber.com/above-the-fold/the-state-american-cybersecurity>.
- Brander, James A., Qianqian Du, and Thomas Hellmann. 2015. "The Effects of Government-Sponsored Venture Capital: International Evidence." *Review of Finance* 19 (2): 571–618.
- Breland, A. 2018. "Tech and Telecom Lobbying Groups Announce Joint Cybersecurity Initiative." *The Hill*, February 23. <https://thehill.com/policy/technology/375287-lobbying-groups-for-tech-and-telecom-announce-joint-cybersecurity>.
- BSA The Software Alliance. 2013. "Strategic Plan 2013–2015." *BSA The Software Alliance*. http://www.bsa.org/~media/files/general/bsa_strategicplan_final.pdf.
- BSA The Software Alliance. 2017. "2017 US Policy Agenda." *BSA The Software Alliance*. http://www.bsa.org/~media/Files/Policy/BSA_2017USPolicyAgenda.pdf.
- Budiansky, Stephen. 2016. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union*. Toronto, Canada: Alfred A. Knopf.
- Carr, Madeline, and Leonie Tanczer. 2018. "UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures, and Interventions." *Journal of Cyber Policy* 3 (3): 437–451.
- Carter, A. 2015. "Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity." (*Stanford University*), April 23. <https://www.defense.gov/News/Speeches/Speech-View/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber/>.
- Carter, Ashton. 2016. "Remarks by Secretary Carter at the Defense One Tech Summit." *U.S. Department of Defense*, June 10. <https://dod.defense.gov/News/Transcripts/Transcript-View/Article/797129/remarks-by-secretary-carter-at-the-defense-one-tech-summit/>.
- Cheung, Tai Ming. 2018. "The Rise of China as a Cybersecurity Industrial Power: Balancing Between National Security, geo-Political, and Development Priorities." *Journal of Cyber Policy* 3 (3): 313–333.
- Clapper, James. 2016. "Remarks of United States National Intelligence Director James Clapper to Congress." February 9. https://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf.
- Clapper, James R., Marcel Lettre, and Michael S. Rogers. 2017. "Joint Statement for the Record. Senate Armed Services Committee on Foreign Cyber Threats to the United States." January 5. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Letter-Rogers_01-05-16.pdf.

- Cobert, B. 2017. "Strengthening the Federal Cybersecurity Workforce." *United States Office of Personnel Management*, July 12. <https://www.opm.gov/blogs/Director/2016/7/12/Strengthening-the-Federal-Cybersecurity-Workforce/>.
- Cybersecurity Ventures. 2018. "2018 Cybersecurity Market Report." *Cybersecurity Ventures*. <https://cybersecurityventures.com/cybersecurity-market-report/>.
- Daniel, Michael, Ed Felton, and Tony Scott. 2016. "Announcing the President's Commission on Enhancing National Cybersecurity." *The White House*, April 16. <https://obamawhitehouse.archives.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity>.
- Dilanian, Ken. 2012. "U.S. Chamber of Commerce leads defeat of cyber-security bill." *Los Angeles Times*, August 3. <http://articles.latimes.com/2012/aug/03/nation/la-na-cyber-security-20120803>.
- Electronic Frontier Foundation (EFF). n.d. "Security." *EFF*. <https://www.eff.org/issues/security>.
- England, G. 2008. *DARPA 50th Anniversary Dinner*, April 10. Retrieved from speech delivered by Deputy Secretary of Defense Gordon R. England in Washington DC on technology.
- Etzioni, Amitai. 2014. "The Private Sector: A Reluctant Partner in Cybersecurity." *Georgetown Journal of International Affairs* 15: 69–78.
- Finkle, Jim, and Susan Heavey. 2014. "Target says it Declined to Act on Early Alert of Cyber Breach." *Reuters*, March 13. <http://www.reuters.com/article/us-target-breach/target-says-it-declined-to-act-on-early-alert-of-cyber-breach-idUSBREA2C14F20140313>.
- Fung, Brian. 2015. "Apple and Dropbox say they don't Support a Key Cybersecurity Bill, Days before a Crucial Vote." *The Washington Post*, October 20. 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.
- Global Trade Alert. 2013. "American Procurement of Chinese IT Equipment Contingent Upon FBI Certification." *Global Trade Alert*. <https://www.globaltradealert.org/state-act/4340/united-states-of-america-procurement-of-chinese-it-equipment-contingent-on-fbi-certification>.
- Global Trade Alert. 2014. "United States of America: Buy American provisions in an Omnibus Spending Bill." *Global Trade Alert*. <https://www.globaltradealert.org/intervention/19338/public-procurement-localisation/united-states-of-america-buy-american-provisions-in-an-omnibus-spending-bill>.
- Global Trade Alert. 2016. "United States of America: Presidential Order Blocking a Chinese-German acquisition of a US semiconductor firm." *Global Trade Alert*. <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>.
- In-Q-Tel, Inc. n.d. ABOUT IQT. <https://www.iqt.org/about-iqt/>.
- Johnson, Chris, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. "Guide to Cyber Threat Information Sharing." NIST Special Publication 800–150. National Institute of Standards and Technology. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.
- Kovacs, E. 2014. "Global Cybersecurity Spending to Reach \$76.9 Billion in 2015." *SecurityWeek*, August 25. <https://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner>.
- Krasner, Stephen. 1978. *Defending the National Interest*. Princeton, NJ: Princeton University Press.
- Lerner, J. 1996. "The Government as Venture Capitalist: The Long-Run Effects of the SBIR Program." *The National Bureau of Economic Research*, September. <http://www.nber.org/papers/w5753>.
- Lynn, W. 2009. *Center for Strategic and International Studies*, June 15. Retrieved from speech delivered by Deputy Secretary of Defense William J. Lynn in Washington DC on cyber security.
- Moore, Tyler. 2010. "The Economics of Cybersecurity: Principles and Policy Options." *International Journal of Critical Infrastructure Protection* 3: 103–117.
- National Geospatial-Intelligence Agency. n.d. "Mission." *National Geospatial-Intelligence Agency*. <https://www.nga.mil/ProductsServices/Pages/default.aspx>.
- National Institute of Standards and Technology. 2014. "Framework for Improving Critical Infrastructure Cybersecurity." *National Institute of Standards and Technology*, February 12. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

- National Security Technology Accelerator. n.d. "Our Approach." *National Security Technology Accelerator*. <https://nstxl.org/#>.
- NICE (National Initiative for Cybersecurity Education). 2018. "NICE Cybersecurity Workforce Framework." *National Institute of Standards and Technology*. <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>.
- Obama, B. 2016. "Protecting U.S. Innovation from Cyberthreats." *Wall Street Journal*, February 9. <https://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003>.
- Pearson, H. 2013. "Spending Bill's China Cybersecurity Provision is Unclear." *Law360*, April 12. <https://www.law360.com/articles/432500/spending-bill-s-china-cybersecurity-provision-is-unclear>.
- Pritzker, Penny. 2016. "U.S. Secretary of Commerce Penny Pritzker Details Cybersecurity Challenges Faced by Cabinet Secretaries in Speech to Commission on Enhancing National Cybersecurity." U.S. Department of Commerce.
- RAND Corporation. 2016. "A Framework for Exploring Cybersecurity Policy Options." RAND corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf.
- Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. 2014. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *Bloomberg*. <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. "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace." *The Heritage Foundation*, April 1. <http://www.heritage.org/defense/report/congressional-guide-seven-steps-us-security-prosperity-and-freedom-cyberspace>.
- Rowe, Brent R., and Michael P. Gallaher. 2006. "Private Sector Cyber Security Investment Strategies: An Empirical Analysis." *WEIS*, March. <https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf>.
- Sales, Nathan A. 2013. "Regulating Cyber-Security." *Northwestern University Law Review* 107 (4): 1503–1568.
- Schulman, Loren DeJonge, Alexandra Sander, and Madeline Christian. 2017. "The Rocky Relationship Between Washington and Silicon Valley: Clearing the Path to Improved Collaboration." *Center for New American Security*, July 18. <https://copia.is/wp-content/uploads/2017/07/COPIA-CNAS-Rocky-Relationship-Between-Washington-And-Silicon-Valley.pdf>.
- Shane, Scott, Cade Metz, and Daisuke Wakabayashi. 2018. "How a Pentagon Contract Became an Identity Crisis for Google." *New York Times*, May 30. <https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html>.
- Somerville, H. 2015. "Defense Department's Tech Investing Signals Silicon Valley's Importance in Cyberwarfare." *Mercury News*, May 13. <http://www.mercurynews.com/2015/05/13/defense-departments-tech-investing-signals-silicon-valleys-importance-in-cyberwarfare/>.
- Stay Safe Online. n.d. <https://staysafeonline.org/ncsam/ncsam-champions/>.
- Sullivan, Mark. 2018. "Big Tech lobbying spree: Here's how much Apple, Amazon, and others gave DC in 2017." *Fast Company*, January 23. <https://www.fastcompany.com/40520529/big-tech-lobbying-sprees-heres-how-much-apple-amazon-and-others-gave-d-c-in-2017>.
- Tadjdeh, Yasmin. 2015. "Army Reserve Pursuing Partnerships with Silicon Valley." *National Defense Magazine*, August 13. <http://www.nationaldefensemagazine.org/articles/2015/8/13/army-reserve-pursuing-partnerships-with-silicon-valley-updated>.
- US Congress. "H.R.2105 – NIST Small Business Cybersecurity Act." <https://www.congress.gov/bill/115th-congress/house-bill/2105?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=11>.
- US Congress. "S.1428 - Small Business Cyber Training Act of 2017." <https://www.congress.gov/bill/115th-congress/senate-bill/1428?q=%7B%22search%22%3A%5B%22cyber%22%5D%7D&r=5>.
- US Department of Commerce. 2016. "Industry Data." Bureau of Economy Analysis, U.S. Department of Commerce. <https://www.bea.gov/iTable/iTable.cfm?ReqID=51&step=1#reqid=51&step=51&isuri=1&5114=a&5102=10>.
- US Department of Defense: Defense Digital Service. n.d. "Transforming Technology within the Department of Defense." <https://www.dds.mil>.

- US Department of Homeland Security. 2016. "Cybersecurity Education and Career Development". *Department of Homeland Security*, September 20. <https://www.dhs.gov/topic/cybersecurity-education-career-development>.
- US Department of State. n.d. "Overview of U.S. Export Control System." A Resource on Strategic Trade Management and Export Controls. U.S. Department of State. <https://www.state.gov/strategictrade/overview/>.
- US Office of Personnel Management. 2018. "CyberCorps: Scholarship for Service". <https://www.sfs.opm.gov/default.aspx>.
- Wakabayashi, Daisuke, and Cade Metz. 2018. "Google Promises Its A.I. Will Not Be Used for Weapons." *New York Times*, June 7. <https://www.nytimes.com/2018/06/07/technology/google-artificial-intelligence-weapons.html>.
- Wakabayashi, Daisuke, and Scott Shane. 2018. "Google Will Not Renew Pentagon Contract that Upset Employees." *New York Times*, June 1. <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>.
- The White House. n.d. "TechHire Initiative." *The White House*. <https://obamawhitehouse.archives.gov/issues/technology/techhire#section-commitmentsm>.
- Wilson, Clay. 2007. "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." *Focus on Terrorism* 9: 1–42.