BASC WORKING PAPER SERIES

COMPARATIVE INDUSTRIAL POLICY AND CYBERSECURITY: A FRAMEWORK FOR ANALYSIS

Vinod K. Aggarwal
Andrew W. Reddie

Working Paper 2018-01

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. This project has been supported by the Institute of East Asian Studies, UC Berkeley's Center for Long-Term Cybersecurity, Social Science Matrix, and the Berkeley's APEC Study Center. For research support, the authors are grateful to Anastasia Pyrinis and Yujie Shen.

Comparative Industrial Policy and Cybersecurity: A Framework For Analysis
Vinod K. Aggarwal and Andrew W. Reddie
BASC Working Paper No. 2018-01

Abstract

This comparative project evaluates the role of firms, governments, and other key stakeholders in the rise of industrial policy in important states in the cybersecurity industry. In particular, we focus on the U.S., China, Taiwan, Japan, the EU and other key European states. Our goals are as follows: 1) to examine the motivation for government promotion of the cybersecurity industry; 2) to inventory existing measures employed by these countries; 3) to understand the driving forces of cybersecurity industrial policy in these countries; and 4) to examine the likely conflicts that will arise from the competitive pursuit of such industrial policies and how they might possibly be resolved through international cooperation. To this end, we suggest an analytical framework to serve as the comparative structure for this project, drawing on a variety of approaches to understand industrial policy.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked." –Richard C. Clarke

Vinod Aggarwal[1]
University of California, Berkeley
Department of Political Science
210 Barrows Hall
Berkeley, CA 94720
vinod@berkeley.edu

Andrew W. Reddie[2]
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.

1. Introduction

Cyber attacks of varying severity, ranging from email hacking to Distributed Denial of Service attacks (DDoS) to advanced persistent threats (APT) are commonplace throughout the globe. Yet at the same time, with the economy being increasingly data-based, these attacks pose both a significant security and economic problem. The issue of how to cope with such intrusions raises critical questions about the role that governments around the world should play in regulating the data economy.[3] While few would doubt the importance of maintaining secure data, whether the government should go beyond sharing best practices for data security and implement more aggressive industrial polices to secure data remains hotly contested.[4]

Tracing how businesses, governments, and other actors interact is crucial for understanding how cybersecurity policy has evolved. Firms' efforts to secure government protection of a sector critical to national security are hardly new. In the 1950s, the U.S. Government responded to concerns about the national security implications of the oil industry, then seen as the lifeblood of the industrial economy, by imposing oil quotas in 1959—a policy that lasted until 1973. One could argue that this policy undermined—rather than enhanced national security—by leading to a policy of "drain America first," as restrictions on the use of foreign oil increased extraction of American oil. In Japan, similarly, firms have often argued that rice production is essential for national security. Similar claims about a particular industry's essential role in national security are commonplace. In fact, claims about a given sector being critical to national security have often been abused. In the 1950s, the wool industry argued for the protection of domestic production by claiming that "there is a need for 150 million to 200 million woolen blankets to ensure survival in case of an atomic war."[5]

While many industries make improbable claims concerning the importance of their industries for national security to secure favorable government intervention, the cybersecurity industry has a significantly more plausible claim for its critical role. At the same time, government agencies have also specifically sought to promote the cybersecurity industry, fearing a lack of national home-grown capabilities, as well as concerns about being at the cutting edge of computer and network security. Thus, the dynamics of business-government relations in this sector are of particular significance. As we demonstrate in this project, the cybersecurity industry in a number of countries is not always in favor of government involvement, as the government's participation can mean greater regulation, restrictions on a global strategy, and the diversion of their efforts from potentially far more lucrative civilian markets.

In this light, this project's central goal is to explore the role of firms, governments, and other key stakeholders in the rise of industrial policy toward the cybersecurity industry in several important states. Given the "cybersecurity industrial complex" worth billions of dollars and the growing market for IT security products, this topic is in need of significant academic attention.[6] Given the observed variation in patterns of industrial policy in the cybersecurity sector, a comparative

[3] Weber (2017).

[4] Abelson et al. (2015).

[5] 1959 Pastore Senate Committee on Trade. See the discussion in Aggarwal (1985).

[6] Brangetto et al. (2014)

analysis also represents a useful method to address questions surrounding how states respond to and seek to drive innovation. Specifically, this comparative industrial policy project focuses on the U.S., China, Russia, Taiwan, Japan, the European Union as well as key European states including France and the United Kingdom. Our goals are as follows: 1) to identify market failures of various types that lead to calls for government intervention (whether top down or bottom up); 2) to inventory existing measures employed by these countries using literature on measures that governments might use; 3) to analyze the driving forces of cybersecurity industrial policy in these countries 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. To that end, this chapter proceeds by providing a theoretical framework used consistently across each of the cases examined in this volume while briefly summarizing the arguments made in each of the subsequent chapters.

1.1. Outline of Case Studies

Each of the papers in this volume considers the importance of the country as a model for state intervention in the cybersecurity sector. In the process, each case study chapter considers the following:

- What are the real or perceived *market failures* in the cybersecurity sector?
- What is the *state response* to these market failures?
- What are the effects of *industrial policy* upon national cybersecurity markets?

In each of the chapters, there is considerable variation in terms of how governments have sought to encourage investment in the private cybersecurity sector in terms of human capital, regulation, and response to business lobbying. In the United States, for example, the government has sought to integrate public appropriations into the private market via a series of venture capital efforts.[7] Tai Ming Cheung, on the other hand, points out that China's cybersecurity market is, to all intents and purposes, driven by government prerogatives.[8]

1.2. A Framework for Analysis

To engage with the question noted above, this paper provides a framework for analyzing these questions. Section 2 of this paper provides an analytical overview of potential market failures.[9] We then turn to an analysis of the cybersecurity and allied industries that raise important questions about data security and the possible market failures that government actors have identified. In Section 3, we turn to an inventory of the types of responses that governments might engage in, drawing on work on industrial policy.[10] Section 4 considers the literature on state-society relations with an eye to understanding the dynamics of intervention in cybersecurity

[7] Cite US Chapter in special issue.

[8] Cite China Chapter in special issue.

[9] Harris and Carman (1983).

[10] For this task we draw on Harris and Carman (1984) and the work on trade protection by Aggarwal and Evenett (2014).

industry and the perceptions of both government and industry. Section 5 concludes with some thoughts concerning possible the domestic problems and international conflicts that arise as a result of the pursuit of industrial policy in this sector.

2. Market Failure and the Global Cybersecurity Industry

This section proceeds as follows. We begin by looking at the types of market failures that might occur in any sector of the economy and serve as the rationale for industrial policy.[11] Next, we consider the characteristics of the global cybersecurity industry, based on our definition of the nature of the industry.

2.1. The Analytics of Market Failure: Theory

Past industrial policy efforts, particularly broad-scale import substitution industrialization in developing industries during the post-WW II era, led most economists to be highly critical of policies that are seen as attempts to pick winners and losers. For them, the government's role is to cultivate a macroeconomic environment based on sound monetary, fiscal, trade, and exchange rate policy. Yet a few economists—and many political economists—point to a host of reasons for more significant government intervention in the economy. In general, intervention options have been divided into so-called horizontal and vertical industrial policies. Horizontal policies include human capital development and tax credits, among others, to promote industries such as manufacturing or services.[12] In this volume, Madeline Carr notes the various programs developed by the United Kingdom to increase its cybersecurity workforce and its apparent focus upon human capital development.[13] By contrast, vertical sectoral policies are explicitly targeted to bolster a specific industry. They seek to help firms conform to a state's comparative advantage or encourage firms to move away from a state's static comparative advantage. What might be the logic of more direct intervention?

The standard rationale for state intervention that has been generally agreed upon concerns *imperfect markets*. As economists generally claim, any deviation from a competitive market is likely to lead to market inefficiencies.[14] Thus, state intervention is often seen as legitimate to address monopolies or oligopolies or collusive anticompetitive behavior. Yet different schools of thought on what constitutes a concentrated market have led to debate between the so-called structural, Chicago School, and IO models of antitrust policy. In light of these competing

[11] Harris and Carman (1983) provide a typology of market failures, based on the traditional literature. These include imperfect competition, excessive competition, imperfect information, side effects, public good, merit/demerit goods, and income maldistribution. Aggarwal and Aggarwal (2013) focus on political and economic reasons, aside from many of the elements that Harris and Carman point to, and add some more recent concerns. Here, we select from both to focus on cybersecurity relevant issues.

[12] Of course, such broad-based policies may have a differential impact on industries. See Gruber, Harald. "Innovation, skills and investment: a digital industrial policy for Europe." *Economia e politica industriale*44, no. 3 (2017): 327-343.

[13] Carr (2018). See also: Stoddart, Kristan. "UK cyber security and critical national infrastructure protection." *International Affairs* 92, no. 5 (2016): 1079-1105.

[14] See Glykou and Pitelis (2011) for a discussion of industrial policy and imperfect competition.

models, while deviations from a competitive market may be identifiable, what to do about them is contested both in the U.S. and in other countries.

Carman and Harris focus on markets wherein excessive competition might take place, leading to market failures.[15] These include cases where there is too much entry at some times and not enough at others. The aggressive competition in software markets with lots of failures and exit and a few major hyper-successful companies has often occurred in Silicon Valley, leading to a highly dynamic but unstable market.

Factor adjustment failures may occur with respect to both asset specific labor and capital. Thus, while in theory markets should adjust with respect to these factors, as Williamson and others have noted,[16] asset specific investments may mean that factors are less mobile than one might anticipate. Moreover, markets may also not correctly signal to firms and workers the attractiveness of particular industries. Another important focus on a potential rationale for intervention focuses on dynamic scale economies and capital market failures. This line of thinking, harkening back in part to import substitution arguments, claims that given time, firms can lower production costs given the presence of scale economies (for example, in commercial aircraft production). Thus, some industries may lack static competitive advantage but with government support of various types could be successful in the long run. The capital market connection is that financiers should be able to recognize such dynamic arguments, but may be unwilling to do so, in part because of incomplete information (as discussed below).[17]

Paul Krugman, on the other hand, focuses on *agglomeration effects*,[18] pointing to the importance of clusters, be they urban or regional, as a key element in driving industrial success. Analysts such as Fan and Scott draw on some of these claims to argue that clusters can produce dense local labor markets, knowledge spillovers, and various forms of business organization and culture that can enhance competitive advantage.[19] They focus on the importance of geographical proximity in increasing efficiency and productivity.

Arguments about the need to promote nascent industries as in cybersecurity are tied to the impact of this industry on a host of allied industries. The concern is that firms may not capture the benefits of innovation, which may diffuse to others.[20] This applies in particular to technologically focused products that may suffer from a lack of investment. In addition, concerns about coordination failures focus on the difficulty of upstream and downstream industries to coordinate their investments. While it may be individually unprofitable to produce computers or software, if private firms in these two sectors invest somewhat simultaneously, both will benefit. But because there is informational uncertainty about the growth of complementary industries, there may be underinvestment, leading to market failure.

---

[15] Carmen and Harris (1983).

[16] Williamson (1975).

[17] See a summary of the arguments in Rodrik (2013).

[18] See Haggard (2004), p. 66-7 for a discussion.

[19] Fan and Scott (2003), p. 297.

[20] For more on informationa externalities, see Pack and Saggi (2006). Hausmann and Rodrik 2003 and Hausmann and Rodrik 2008 also note the need for experimentation in the marketplace.

The importance of being part of *global supply chains* developed by multinational corporations is an important theme in Gereffi's work.[21] He notes countries might be able to foster industrial upgrading when involved in a global value chain in order to follow their comparative advantage. Yet whether governments can successfully promote supply chains depends on a host of other factors as noted by Morrison, Pietrobelli and Rabellotti on global value chains. They note that participation in supply chains must be combined with "local technological capabilities" to be successful.[22]

Aside from market failure, even free market economists accept that governments might need to protect industries for reasons of national security.[23] As noted, these arguments are often abused, and assessing which industries are truly important for security and also potentially subject to export controls is a complex question. The American, Chinese, and Finnish cases included in this volume note the security externalities associated with cybersecurity—both of the government and of consumers.

Finally, firms may also lobby the government to secure benefits that may have little to do with market failures or security considerations and avoid competition. In the cybersecurity industry, given the obvious concerns about security, the temptation to engage in rent seeking behavior is particularly high.[24]

2.2. The Characteristics of Cybersecurity Firms

As noted above, the cybersecurity market is growing rapidly. Between 2016 and 2021, it is expected that the global cybersecurity market will grow with a compound annual interest rate (CAGR) of 10.16%. By 2021, the global market for cyber security is projected to be over $200 billion. The projected areas of growth in the industry include security analytics (10%+), threat intelligence (10%+), mobile security (18%+), and cloud security (50%+).[25] The cybersecurity industry itself also has network effects upon the industries to which it is adjacent. As a result, it is useful to broadly define what we mean by the cybersecurity industry and where it fits in relationship to other sectors that are influenced by data security issues.

For our purposes, we identify three critical sectors 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.

---

[21] Gereffi (1999).

[22] Morrison and Rabellotti (2008). See also: Pietrobelli, Carlo, and Fernanda Puppato. "Technology foresight and industrial strategy." *Technological Forecasting and Social Change* 110 (2016): 117-125.

[23] See the discussion by Mastanduno (1991) who examines arguments about national security and industrial policy in the context of responding to Japan's economic policies.

[24] https://www.washingtonpost.com/business/capitalbusiness/lobbying-on-data-cybersecurity-has-tripled/2014/05/11/fad0fe12-d6e9-11e3-8a78-8fe50322a72c_story.html

[25] https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#3150df4f10c3

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 this type of firm in the U.S. include FireEye, Palantir, Qadium, and Kasperky Lab. In-Q-Tel's founding investment (CIA) in Palantir Technologies in 2003 serves as an example of the close relationship between these firms and government. In terms of market failure, it is also worth pointing out that these firms have an incentive to contribute to misinformation—theorized by Harris and Carmen—due to the perception of the challenge posed by cybersecurity driving their business outcomes.

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. We consider firms working in the "Internet of Things (IoT)" space such as General Electric, Tesla, and PG&E as examples of these types of firms. The recent NHTSA guidelines for autonomous cars offer a recent example of government business-relations.

2.3. The Cybersecurity Industry and Market Failure

Having outlined the types of firms that are the subject of study, we now turn to looking at market failure and other motivations for government intervention in this sector. Put simply, the reality of various cyber attacks on government and commercial actors poses the question: Why isn't there more investment in cybersecurity?

In a perfect market, we should expect commercial firms to provide a service demanded by customers. But in the cybersecurity sector of the economy, there are a number of network failures that result in what are often described as market failures.[26] As Anderson and Moore note, "people have realized that security failure is caused at least as often by bad incentives as by bad design."[27] Moreover, for many IT firms, security is not the first priority. Efficiency, a simple user interface, getting a product to market, establishing a monopoly position in the market for a product and dumping risk are all competing business goals for businesses shipping IT.[28] Below, we consider the question: What are some of the market failures in the cybersecurity industry?

First, there are obvious *externalities* associated with the IT infrastructure with deleterious effects for cybersecurity. We point to three externalities, in particular, that increase cyber insecurity.

[26] Friedman (2011); Brangetto et al. (2014).

[27] Anderson and Moore (2006).

[28] Safa, Nader Sohrabi, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations." *Computers & Security* 56 (2016): 70-82.

One, the *network effects* of IT and user behavior tend toward "winner takes all" monocultures.[29] Indeed, companies such as Apple, Amazon, Facebook, Google, Microsoft, and Adobe have built platforms and product environments that have won out in their various sectors—becoming "natural monopolies."[30] These effective monopolies have two effects. First, there is no competition on security itself and subsequently security does not improve. Second, all users are at risk to vulnerabilities emanating from each specific product. Two, we consider interoperability. *Interoperability* is a primary guiding principle of the Internet. Because all platforms must be able to communicate with all others, however, there is a significant risk of contagion across the network with little to no barriers to stop the spread of malware, viruses, worms, and other malevolent programs.[31] Three, we point to the importance of *complementarity* as a profit-maximizing tool among companies building IT platforms. Facebook, Apple, and Google all profit from partner companies building on their platform. If they were to increase the security requirements to access their platforms, they run the risk of losing this source of revenue and also increasing costs to these subsidiary businesses.[32] As a result, the grafting of new applications and software onto existing operating systems or "app stores" drives "insecurity by design." As a consequence, the cybersecurity industry suffers from Hardin's "tragedy of the commons."[33] Cybersecurity is nominally a collectively held good with network effects that reward good ("secure") behavior and that punish bad ("insecure") behavior.[34] As a result of these network effects, there is little to no incentive to be a first mover with a more secure product as even those that spend more on secure products remain at the whim of their more insecure colleagues and competitors on the network.[35]

Second, we consider *information problems*. The clearest example of an information problem in the cybersecurity sector stems from the unwillingness and lack of incentive for individual firms to disclose breaches due to the reputational costs of doing so. It is also difficult to determine whether defensive measures employed by government agencies or commercial firms are, in fact, successful.

Third, failures related to *moral hazard* among IT firms are significant as platforms such as Facebook or YouTube rarely bear the cost of data breach, fraud, and privacy on their network.[36] Instead, responsibility is passed down to the user to patch the system or bear the cost of a data breach.[37] Moreover, government is increasingly blamed for the fragility of the IT architecture

---

[29] Friedman (2011)

[30] https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html

[31] For example, the Stuxnet virus has been repeatedly discovered "in the wild."

[32] Fixing this problem might also prove problematic given that increasing costs for subsidiary businesses reinforces the monopoly of platform companies and increases the barrier of entry for new firms entering the market.

[33] Hardin (1968).

[34] It is worth noting that there is a substantial debate with regard to whether cybersecurity represents a public or a privately held good that is beyond the scope of our discussion here.

[35] We may also focus on the issue of *adverse selection* that leads to the crowding out of secure, expensive (in terms of time and money) products in favor of those of a lower quality but that are cheaper. This concept draws upon Akerlof's "lemon" theory.

[36] YouTube, for example, takes no responsibility for the material posted on the platform.

[37] Lindsay (2015).

rather than firms.[38] This moral hazard is also linked to *liability dumping*. Liability dumping, in which platform and application providers abdicate responsibility for the use or misuse of an application and security risks to the user, is exacerbated by short-time scales related to program delivery in which companies face considerable to push code quickly.[39] An example of this problem was made clear in a 2009 GAO report which concluded that the of federal agencies had failed to "fully or effectively implement information security programs" due to "inattentive/untrained employees," "equipment failures," and a failure to stay current with software upgrades.[40]

3. Types of Market Intervention

Identifying potential market failures in the cybersecurity industry provides a first step in understanding potential real and perceived reasons to intervene in the industry. The next issue is: what measures might make sense to address such market failures? Clearly, even if governments identify similar market failures, it is quite possible that they would use different measures to address them, and provide a centrally important research question for this project that speaks to the issue of convergence in policymaking.

The number of measures that countries have used to intervene in the market is long, and analysts have attempted to characterize them in various ways. The theoretical work of Harris and Carman[41] speaks directly to this issue and the empirical work of Global Trade Alert, led by Simon Evenett, also considers intervention measures with an eye to understanding their consequences on the inter international economy.[42]

3.1. Introducing Intervention Measures:

Having outlined the classification scheme above, we now consider the effects of various industrial policies using Carman and Harris's framework. Specifically, we consider the market creating, market facilitating, market modifying, market substituting, and market proscribing consequences of government policies on the cybersecurity market.

Market Creating involves public policies designed to create markets, by establishing rights, incentives and opportunities for exchange; e.g., creating a market for air pollution "rights."

Market Facilitating involves policies that promote or improve the operation of markets by reducing transactions costs, enhancing incentives, or internalizing benefits and costs; e.g., public investment in transportation to expand the geographic scope of markets by reducing transport costs. In the U.S. case, the National Security Technology Accelerator (NSTXL) serves as an example of a market facilitating mechanism.

---

[38] Moore, Tyler. "The economics of cybersecurity: Principles and policy options." *International Journal of Critical Infrastructure Protection* 3, no. 3-4 (2010): 103-117.
[39] Brangetto et al. (2014).
[40] GAO Report (2009).
[41] Harris and Carman (1984).
[42] Globaltradealert.org

Market Modifying involves the creation of regulations that attempt to change the conduct of subjects, the objects, medium or terms of exchange, in order to produce outcomes different from those the market would otherwise produce; e.g., agricultural marketing orders. In the United States case, the Cybersecurity Information Sharing Act (CISA) and Cybersecurity Intelligence and Sharing Protection Act (CISPA) perform this role.

Market Substituting involves policies that create substitutes for markets, in which instruments of political authority are used to allocate or distribute resources or control conduct of individuals or organization's outcomes are achieved. In the U.S. case, In-Q-Tel substituting for venture capital firms and various human capital related programs that subsidize cybersecurity education such as the Federal Cybersecurity Workforce Strategy, National Initiative for Cyberspace Education, CyberCorps, and Cybersecurity Education and Training Assistance Programs (CETAP) each play this role.

Market Proscribing involves policies that attempt to prohibit exchanges by particular subjects or of particular objects, with no attempt to use authority as a substitute method for achieving a given outcome; rather, authority is used in an effort to prevent that outcome from occurring; e.g., laws prohibiting the sale of dangerous drugs. In the U.S. case, various arms control regimes governing cyber tools such as Wassenaar and the Arms Export Control Act play a clear role here.

3.2. Measuring Effects: Intensity

The project also considers the *intensity* of the effect of each state's policy tools upon cybersecurity markets. Indeed, the number of interventions in the market alone does not reflect the impact of industrial policy. Thus, each country expert for the case study chapters is tasked with making a determination concerning the intensity of the intervention by the state in the market by considering the amount of investment in the intervention, the engagement of elite policy-makers, and location of intervention in the bureaucracy among alternative measures.

3.3. Measuring Effects: Discriminating

The final step of each chapter's analysis involves considering whether the intervention *discriminates* among domestic or foreign cybersecurity firms. This allows for a determination of how the policies aimed at national markets might have international consequences.

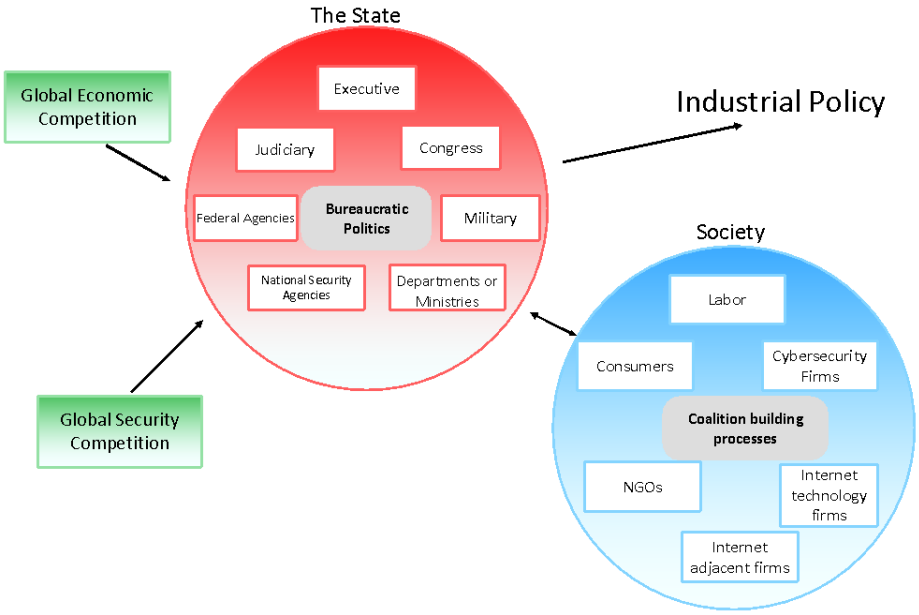
4. What are the Drivers of the Constellation of Intervention Measures

The political economy literature on industrial policy provides a variety of rich explanations of forces that drive variation in governments' industrial policy choices.[43] Tai Ming Chueng notes in his analysis of China, for example, that Beijing uses a model of deliberate state-led

[43] See the literature review and discussion in Aggarwal and Evenett (2014).

capitalism.[44] Ben Bartlett, on the other hand, notes that Japan promotes private sector-led development of the cybersecurity market.[45] Even among Western-capitalist states, it is evident in the chapters to follow that there is considerable variation with regard to the manner in how countries pursue and implement policies.[46] In terms of driving forces, Figure 2 illustrates the relationship between State and Society.[47]

Figure 2: State-Society Interaction in Policymaking



State actors include different branches of government, the military, and a variety of agencies or ministries. The relationship among them may be more or less fragmented depending on the specific organization of the state structure. Thus we may see more or less bureaucratic politics in different states. In addition to policy outputs (industrial policy, in this case) emerging from interaction among these actors, states also face systemic pressure in the form of global economic and security competition. Societal actors include labor, NGOs, firms, consumers and other such actors. Again, the relationship of these actors varies depending on specific rules, regulations, and norms. For example, in Germany labor plays a much more active role on corporate boards than in the United States.

The key question that emerges from Figure 2 is the issue of convergence or divergence in industrial policy. Will systemic international pressures, in view of the unique importance of cybersecurity, drive all states to pursue similar policies over time? Or is national variation the key explanatory factor that will continue to drive differences in cybersecurity policy?

---

[44] Cheung (2018). See also: Ernst, Dieter. "From Catching Up to Forging Ahead? China's New Role in the Semiconductor Industry." (2016) and Chen, Ling, and Barry Naughton. "An institutionalized policy-making mechanism: China's return to techno-industrial policy." *Research Policy* 45, no. 10 (2016): 2138-2152.

[45] Bartlett (2018).

[46] Peter A. Hall and David Soskice (2001). In this volume, see Tai Ming Cheung's (2018) article.

[47] This literature, going back decades, has often pointed to the difference as being one of strong and weak states, and also strong and weak societies. See Peter J. Katzenstein (1977).

In terms of thinking about industrial policy with respect to the national security sector, Linda Weiss argues that geopolitics and the perception of threat have led to a top-down relationship between a "national security state" and commercial firms working in the technology sector.[48] This relationship, she contends, explains the foundations of the high-tech commercial sector, in general, and the technological innovations that we use on a daily basis, despite 'anti-statism' among firms and individuals that has led to the complex public-private partnerships that exist today. This specific "national security state" institutional milieu, Weiss argues, explains the variation observed between the United States and other advanced democracies. Aggarwal and Reddie in the examination of the United States point to the various firm-state relations that exemplify the close linkages between the intelligence agencies, well-establish defense firms, and Silicon Valley.[49] Griffith, too, examines the cybersecurity market in Finland against the backdrop of geopolitical concerns.[50]

By contrast, Fred Block and Matthew Keller suggest that the rationale for government intervention to foster innovation "normalizes" state activity and contributes to the expansion of the "hidden developmental state" that takes on significant industrial policy functions.[51] Specifically, they suggest that the state's role "can be divided into four distinct but overlapping tasks—targeted resourcing, opening windows, brokering, and facilitation."[52] Interestingly, rather than viewing the role of the state in driving innovations in the business economy as being unique to the United States as Weiss contends, Block suggests that it represents a convergence in industrial policy-making at the technological frontier among advanced democracies.

Like Weiss, Block, and Keller, we point to a puzzling gap in the literature with regard to the role the state has played in driving investment in the high-tech industry, but with a specific focus on the cybersecurity sector. But while current work overwhelmingly focuses on the top-down nature of the relationship between the state and firms, we conceptualize industrial policy as dependent upon the interaction between both state- and firm-level preferences and subsequently ask different questions: What does the relationship between states and firms look like? Under what conditions is the relationship likely to enhance cybersecurity? How do firms acquiesce or push back against state preferences?

Paul Timmers, in his analysis of EU cybersecurity policy, notes the role that the private sector plays in policy-making in a challenging regional context.[53]

---

[48] Weiss (2014).

[49] Aggarwal and Reddie (2018).

[50] Griffith (2018)

[51] Block and Keller (2009).

[52] Block (2008).

[53] Timmers (2018). See also: Olesen, Nina. "European Public-Private Partnerships on Cybersecurity-An Instrument to Support the Fight Against Cybercrime and Cyberterrorism." In *Combatting Cybercrime and Cyberterrorism*, pp. 259-278. Springer, Cham, 2016; Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62; and Carrapico, Helena, and André Barrinha. "The EU as a coherent (cyber) security actor?" *JCMS: Journal of Common Market Studies* 55, no. 6 (2017): 1254-1272; Ruohonen, Jukka, Sami Hyrynsalmi, and Ville Leppänen. "An outlook on the institutional evolution of the European Union cyber security apparatus." *Government Information Quarterly*33, no. 4 (2016): 746-756; and Bures, Oldrich.

5. The Consequences of State Intervention

In the final section of each paper, each author examines the challenges associated with government intervention in the market to address market failures. Specifically, the papers examine the consequences of market failure, whether regulatory shortcomings stem from design or implementation. They also consider alternate regulatory frameworks as well as the time horizons of regulatory frameworks.

5.1. The Domestic Consequences of Intervention

Using the concept of regulatory failure, the case study papers consider the effects of regulation on the cybersecurity sector in each of the respective countries. Specifically, we are concerned with the criteria used by governments to create and enact public policy, the potential design failures of industrial policy, and the challenges associated with the implementation of industrial policy. In the sections below, we consider the criteria through which to evaluate the potential failures of industrial policy. Given that industrial policy represents an inherently political process in which actors win and lose, it is necessary to consider the criteria for successful industrial policies in the cybersecurity sector.

The first of these is a fair process for participation in the construction of an end result. This involves the freedom of individuals to take part in the policy-making process as "process rights."[54] The second criteria involves the consideration of the economic distributive consequences of an industrial policy. A third criteria is concerned with the efficiency of an industrial policy: "the best possible use of scarce resources to fulfill human needs and wants."[55] An evaluation of the efficiency of industrial policy necessarily involves as consideration of the costs of compliance on the part of economic actors and the cost of enforcement for government actors. Finally, each of the cases considers the effects of industrial policies upon economic stability and overall economic growth. For states seeking to grow the cybersecurity sector, for example, they face the challenge of applying industrial policies that do not stymie growth in the broader economy via stringent cybersecurity regulations and standards that make data and activity on the Internet more secure.

5.2. Design Failures

Having outlined the criteria through which industrial policies might be evaluated, we turn now to a discussion of the design failures associated with industrial policy. There are a variety of causes of design failure. First, the scope of the market failure may not be appropriately assessed. In the U.S. cybersecurity market, for example, the human capital needs of the market are so significant that existing policies designed to address the shortfall are inadequate.[56] Second, the policy may have unforeseen consequences or unintended side effects. Third, a miscalculation in the predictions of the costs and benefits of an industrial policy may occur. Indeed, there are varying

---

"Contributions of private businesses to the provision of security in the EU: beyond public-private partnerships." In *Security Privatization*, pp. 23-49. Springer, Cham, 2018.

[54] Carmen and Harris (1986), 53.

[55] Carmen and Harris (1986), 53-54.

[56] Aggarwal and Reddie (2018).

distributions of costs and benefits of industrial policy across different types of economic actors. Moreover, there are costs of compliance and costs of enforcement to be taken into account. And finally, the failure to adequately design a regulatory response to a market failure may be critical. There are several examples that fall into this last category. For example, increased access to information via information sharing mechanisms is limited by the ability to consumers to process the information. In another example, uniform standards that seek to minimize the costs of enforcement fail to take into account the variation of actors that are subject to the policy. Relatedly, the public provision of a good means that the provider does not face a market test and subsequently can lead to inefficiencies on the part of the producer.

5.3. Implementation Failures

The implementation of industrial policy emanates from two processes. In this section, we consider the public choice of a specific policy and subsequently the challenges facing the implementer. In their analysis of intervention, Carmen and Harris point to a variety of potential regulatory failures: electoral failures, bureaucratic failures, legislative failures, and judicial failures. Each of these failures involves the inability for a segment of society to support industrial policy that would address a market failure. In each of the institutions charged with implementing industrial policy there are four issues that must be overcome. The first are information failures in which one actor in an economic exchange might have asymmetrical access to information and subsequently exploit a partner. The second are transaction costs incurred in the economic transaction. The third are free riders that seek to avoid incurring the expenses associated with a regulation such as the costs of compliance by that benefit from it nonetheless. And finally, principal-agent problems occur when an agent (a regulatory agency, for example), ostensibly acting on the behalf of a principal such as a government, crafts an inefficient or inequitable regulation either due to regulatory capture or the incentives of bureaucrats.

These domestic challenges are made more complicated in the cybersecurity sector given the global market place of Internet technology.

5.4. The International Consequences of Intervention

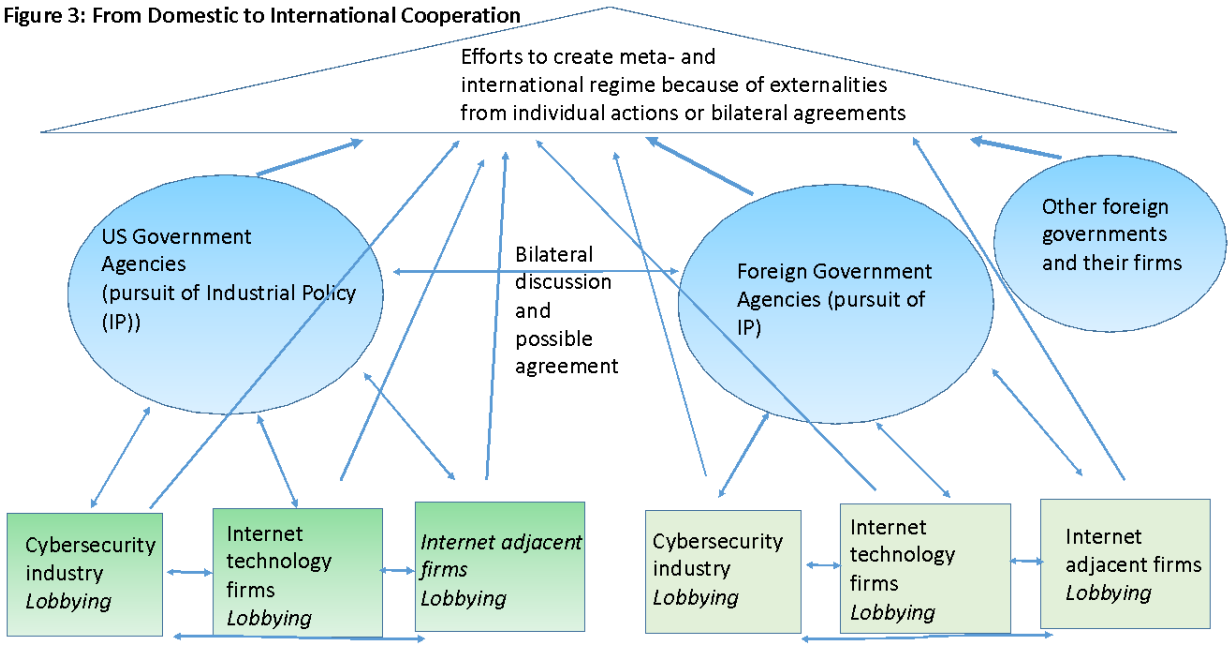
As countries pursue industrial policy in cybersecurity, conflict is nearly inevitable among firms and governments over access to markets.[57] Indeed, cybersecurity policies can be seen as an example *par excellence* of "behind the border" issues—unlike tariffs and quotas, these barriers are measures that are fundamentally part of the regulatory apparatus of the states. Given the sharp variation in how states appear to be dealing with such issues as well as their differing political structures, the likelihood of convergence is still uncertain. The GATT was somewhat successful in managing some behind the border conflicts, such as in the aircraft industry involving Boeing and Airbus, but dispute resolution in this sector has neither been easy nor even permanently resolved. By contrast, the WTO has encountered difficulties with addressing many of these issues, as evident by the long-standing Doha Round that began in 2001 fell apart in December 2015. In response, states have tried to resolve behind the border barriers through the

[57] There has been considerable discussion about cybersecurity cooperation (frameworks dealing with preventing attacks on critical infrastructure, etc.) but here we are focused on the creation of an international regime that focuses on preventing conflict with respect to competitive cybersecurity industrial policies through the WTO or mega-FTAs.

TPP (Trans Pacific Partnership) and the TTIP (Trans Atlantic Trade and Investment Partnership).[58] However, as these mega-FTAs have become hotly debated in U.S. and the EU, it is by no means a foregone conclusion that these agreements will ever come into effect. Indeed the US has pulled out of TPP and other countries have gone ahead with the creation of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Alternative arrangements to deal with such issues have come about through sectoral agreements such as the Information Technology Agreement (ITA), Basic Telecom Agreement (developed in the late 1990s), and ITA II, which was signed in 2015. Thus, at least in principle, there is a potential avenue for cooperation over the management of cybersecurity industrial policies at the international level.

If cooperation emerges in the cybersecurity sector, what will it look like? One way to conceptualize this is to think about how countries attempt to cope with the externalities of domestic policies, be they state or firm driven. These include industry-related domestic restrictions or bilateral agreements, which may create conflict as firms are excluded from markets or damaged by foreign industrial policies. This may lead to calls for creating international principles and norms (meta-regime) or rule procedures (international regime) to address the externalities of industrial policies in cybersecurity. Figure 3 shows this process graphically.

Figure 3: From Domestic to International Cooperation



Source: Adapted from Vinod K. Aggarwal, ed., *Institutional Designs for a Complex World*, Ithaca: Cornell University Press, 1998.

[58] Azmeh and Foster (2016).

6. Conclusion

This project evaluates the role of firms, governments, and other key stakeholders in the rise of industrial policy in important countries in the growing, multi-billion-dollar global cybersecurity industry. Above, we outlined the theoretical market failures in the cybersecurity industry. Then, we examined the types of market intervention (market creating, facilitating, modifying, substituting, and proscribing) employed by the governments in response to these market failures and considered by the authors of each case study chapter. The chapter then compares a variety of theories with regard to the drivers of the constellation of intervention measures taken in the cybersecurity sector. Finally, the chapter considers the existing theoretical work concerning potential problems of intervention.

In the case studies that follow, each author draws conclusions concerning the type and intensity of state intervention in national cybersecurity markets for their specific case. In our concluding article, we use these cases to consider the variation in the types of measures employed by states to influence (or not) their respective cybersecurity markets. Such an analysis allows us to consider the divergence and convergence in state efforts to bolster their cybersecurity markets and to compare the state intervention in the cybersecurity sector in comparison to other sectors of the economy more often studied by political economists.

7. References

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore et al. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." *Journal of Cybersecurity* 1, no. 1 (2015): 69-79.

Ackerman, Robert K. 2016. “The CIA Accelerates Innovation.” *Signal*, 70:10, pp. 25-28. June.

Aggarwal, Sonia and Vinod K. Aggarwal 2013. “Industrial Policy: Theory and Practice,

Prepared for the World Bank.

Aggarwal, Vinod K. 1985. *Liberal Protectionism.* Berkeley: UC Press, USA.

Aggarwal, Vinod K., and Simon J. Evenett. 2014. "Do WTO rules preclude industrial policy? Evidence from the global economic crisis," *Business and Politics*, 16: 4, pp. 481-509.
Anderson, Ross., and Tyler Moore. 2006. "The Economics of Information Security". *Science*, 314: 99, pp. 610-613

Avant, Deborah D. 2005. *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

Azmeh, Shamel, and Christopher Foster. *The TPP and the digital trade agenda: digital industrial policy and Silicon Valley's influence on new trade agreements*. No. 16-175. Working Paper Series, 2016.

Block, Fred, and Matthew R. Keller. 2009. "Where Do Innovations Come from? Transformations in the US Economy, 1970-2006." *Socio-Economic Review*, 7, pp. 459-483.

Block, Fred. 2008. "Swimming Against the Current: The Rise of a Hidden Developmental State in the United States," *Politics and Society*, 36:2, p. 172.

Brangetto, P., Markus Maybaum, and Jan Stinissen. 2014. "2014 6th International Conference on Cyber Conflict," NATO CCD COE Publications.

Budiansky, Stephen. 2016. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union.* New York. Alfred A. Knopf.

Clapper, James R., Marcel Lettre, and Michael S. Rogers. 2017. "Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States."
Cybersecurity Ventures. 2017. "Cybersecurity 500." *Cybersecurity Ventures*.

Deutch, John. 2001. "Consolidation of the U.S. Defense Industrial Base," *Acquisition Review Quarterly*, pp. 137-150. Fall.

Fan, C. Cindy and Allen J. Scott. 2003. Industrial Agglomeration and Development: A Survey of Spatial Economic Issues in East Asia and a Statistical Analysis of Chinese Regions. Economic Geography 79 (3):295-319.

Friedman, Allan. 2011. "Economic and Policy Frameworks for Cybersecurity Risks," Center for Technology Innovation at Brookings. July 21.

Gereffi, Gary. 1999. International trade and industrial upgrading in the apparel commodity chain. *Journal of International Economics* 48:37-70.

Gholz, E., and Harvey M. Sapolsky. 1999. “Restructuring the U.S. Defense Industry.” *International Security*, 24:3, pp. 5-51. Winter.

Glykou, Ioanna and Christos N. Pitelis. 2011. “On the Political Economy of the State, the Public-Private Nexus and Industrial Policy,” *Policy Studies*, 32:4, 461-478.

Gompers, Paul, and Josh Lerner. 2001. “The Venture Capital Revolution.” *The Journal of Economic Perspectives*, 15:2, pp. 145-168. Spring.

Haggard, Stephen. 2004. “Institutions and Growth in East Asia,” *Studies in Comparative International Development,* 36:4, pp. 53-81. Winter.

Hall, Peter A., and David Soskice. 2001. *Varieties of capitalism: The institutional foundations of comparative advantage*. (ed.). Oxford: Oxford University Press.

Hardin, Garrett. 1968. “The Tragedy of the Commons,” *Science,* 162: 3859, pp. 1243-1248.

Harris, Robert G., and James M. Carman. 1983. “Public Regulation of Marketing Activity: Part I: Institutional Typologies of Market Failure,” *Journal of Macromarketing*. 3:1, June, pp. 49-58.
Harris, Robert G., and James M. Carman. 1984. “Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures,” *Journal of Macromarketing*. 4:1, June, pp. 41-52.
IQT. n.d. “About IQT.”

Jones, Sam. 2015. “GCHQ Chief to Say Free Market Failing on Cyber Security.” *Financial Times*, November 9.

Katzenstein, Peter J. 1977. *Between Power and Plenty: Foreign economic policies of advanced industrial states*. (ed.). Madison: University of Wisconsin Press.

Lerner, Josh. 1996. “The Government as Venture Capitalist: The Long-Run Effects of the SBIR Program,” NBER Working Series (No. 5753), September.

Lindsay, Jon R. 2006. “War Upon the Map: The Politics of Military User Innovation,” Program on Emerging Technologies Working Papers, MIT, July 18.

Lindsay, Jon R. 2015. “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack”. Oxford University Press, September 28.

Mastanduno, Michael. 1991. “Do Relative Gains Matter? America's Response to Japanese Industrial Policy,” *International Security*, 16:1, pp. 73-113. Summer.

Morgan, Steve. 2015. “Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020,” *Forbes*, December 20.

Morrison, Andrea, Carlo Pietrobelli and Roberta Rabellotti. 2008. Global value chains and technological capabilities: a framework to study learning and innovation in developing countries. *Oxford development studies*, *36*(1), 39-58.

National Geospatial-Intelligence Agency. 2017. "NGA's CIBORG Initiative Enables $4.4M Contract with VRICON for 3D Modeling."

National Institute of Standard and Technology. 2014. "Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0)."

National Security Technology Accelerator. n.d. "About."

Obama, Barack. 2016. "Protecting U.S. Innovation From Cyberthreats." *The Wall Street Journal*, February 9.

Rodrik, Dani. 2013. "The Right Green Industrial Policies," *Project Syndicate*. August 7.

Sender, Henry. 2016. "US Defence: Losing Its Edge in Technology?" *Financial Times*, September 4.
Somerville, Heather. 2015. "Defense Department's Tech Investing Signals Silicon Valley's Importance in Cyberwarfare." *The Mercury News*, May 13.

Taplin, Jonathan. 2017. "Is It Time to Break Up Google?" *The New York Times*, April 22.

The White House Office of the Press Secretary. 2016. "Fact Sheet: Cybersecurity National Action Plan."

The White House. (date?). "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure."

The White House. 2008. "Cybersecurity Policy (U)," NSPD-54/HSPD-23.

The White House. 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World."

The White House. 2011. "Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security."

United States Department of Commerce National Institute of Standards and Technology. 2016. "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150.

United States Department of Defense. 2011. "Department of Defense Strategy for Operating in Cyberspace."

United States Department of Defense. 2015. "The Department of Defense Cyber Strategy."

United States Department of Homeland Security. 2003. “Critical Infrastructure Identification, Prioritization, and Protection,” HSPD-7.

United States Department of Homeland Security. 2011. “Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise.”

United States Department of State Export Control and Related Border Security Program. n.d. “Overview of U.S. Export Control System.”

USG 2010. “National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy (Draft).”

United States Government Accountability Office. 2009. “CYBERSECURITY Continued Efforts Are Needed to Protect Information Systems from Evolving Threats,” GAO-10-230T.

United States Government Accountability Office. 2017. “CYBERSECURITY Actions Needed to Strengthen U.S. Capabilities” GAO-17-440T.
United States Government Publishing Office. 2014. “Federal Information Security Modernization Act of 2014,” PUBLIC LAW 133-238—DEC. 18, 2014.

United States National Security Agency Center for Strategic and International Studies. 2010. “CSIS Cybersecurity Policy DebateSeries: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM.” (Debate transcript)

Weber, Steven. "Data, development, and growth." *Business and Politics* 19, no. 3 (2017): 397-423.

Weiss, Linda. 2014. *America, Inc.* Ithaca: Cornell University Press.