



Comparative industrial policy and cybersecurity: a framework for analysis

Vinod K. Aggarwal & Andrew W. Reddie

To cite this article: Vinod K. Aggarwal & Andrew W. Reddie (2018) Comparative industrial policy and cybersecurity: a framework for analysis, Journal of Cyber Policy, 3:3, 452-466, DOI: [10.1080/23738871.2018.1553989](https://doi.org/10.1080/23738871.2018.1553989)

To link to this article: <https://doi.org/10.1080/23738871.2018.1553989>



Published online: 13 Dec 2018.



[Submit your article to this journal](#)



Article views: 20





[View Crossmark data](#)



Citing articles: 4 [View citing articles](#)



Comparative industrial policy and cybersecurity: a framework for analysis

Vinod K. Aggarwal  and Andrew W. Reddie 

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

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 US, China, Taiwan, Japan, the EU and 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 provide an analytical framework to serve as the structure for this project by drawing on a variety of theoretical approaches to understand industrial policy.

ARTICLE HISTORY

Received 27 August 2018
Revised 5 November 2018
Accepted 11 November 2018

KEYWORDS

Industrial policy; comparative political economy; international political economy; cybersecurity

Introduction

From spear phishing and distributed denial-of-service attacks (DDoS), to advanced persistent threats (APT), cyberattacks have become increasingly commonplace as internet technology (IT) has become ubiquitous. These attacks pose a significant security and economic problem for both governments and firms whose day-to-day operations increasingly rely upon digital infrastructure. The challenge of coping with such intrusions raises critical questions about the role that governments should play in regulating the data economy (Weber 2017). Few doubt the importance of maintaining secure data, but the question of whether the government should go beyond sharing best practices, to implementing more aggressive industrial policies, remains hotly contested. Given the range of options, some nations have taken a more activist approach than others (Abelson et al. 2015).

Tracing how businesses, governments, and other actors interact is crucial in understanding how cybersecurity policy has evolved. For decades, companies have worked to secure government protection for economic sectors deemed critical to national security. In 1959, the US government responded to concerns about the national security implications of the oil industry, then viewed as the lifeblood of the industrial economy, by imposing oil quotas, a policy that lasted until 1973.¹ Such national security claims sometimes seem far-fetched: in the 1950s, the American 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’ (Aggarwal 1985).

Today, the cybersecurity industry has a significantly more plausible claim for its critical role in national security. Indeed, government agencies around the world have proactively sought to bolster the cybersecurity industry, fearing a lack of homegrown capabilities and striving to remain at the cutting edge of computer and network security. At the same time, firms in the cybersecurity industry in many countries are not always in favour of government involvement, as the government's participation can mean increased regulation, export controls, and the diversion of their efforts toward military and government customers from more lucrative civilian markets. Thus, the dynamics of business-government relations in this sector are of great significance.

In this special issue, scholars from the disciplines of political science, political economy, computer science and diplomacy examine how national governments in the United States, China, France, the United Kingdom, Finland, Japan, and Taiwan have developed industrial policies to address cyber insecurity. These cases demonstrate the variety of industrial policies employed by states to bolster their respective cybersecurity sectors and reflect their diversity in terms of geography, regime type, and market composition. We also include a case study examining how a supranational institution – in this case the European Union – is attempting to develop policies in the cybersecurity sector at the intersection of economic and security policy.

Each case study 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* on national cybersecurity markets?

In each of the articles, there is considerable variation in 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 (Aggarwal and Reddie 2018). Tai Ming Cheung, on the other hand, points out that China's cybersecurity market is, to all intents and purposes, driven by government prerogatives (Cheung 2018).

The goals of the project 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 article identifies the types of firms included in the study, providing a theoretical framework, used consistently across each of the cases examined in this volume, and briefly summarising the arguments made in each of the subsequent articles vis-à-vis market failures and industrial policies employed by their respective governments.

Actors in cyberspace

Cybersecurity markets are growing rapidly. Between 2016 and 2021, it is expected that the global cybersecurity market will grow with a compound annual interest rate of 10.16%. By

2021, the global market for cybersecurity is projected to be worth 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%) (Morgan 2015). The cybersecurity industry itself also interacts with other types of firms in the industries to which it is adjacent. As a result, it is useful to 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 types of firms in our analysis: 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-space as well as considering how government actors may view them. It is also useful for considering which types of actors might be able to leverage lobbying power in relation to demands for state intervention.

The first category involves firms that work directly on cybersecurity-related challenges for 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 cyberattacks and hacks. Examples of this type of firm include Darktrace, FireEye, Palantir, Qadium, and Kaspersky Lab.

Second, we point to internet technology (IT) firms that rely on cybersecurity (provided by external firms and by in-house teams) 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 Yahoo, to sell products as well as hardware manufacturers, such as Intel, Qualcomm, Microsoft, Apple, and IBM, that require protection from breaches related to their most recent research and development projects and to keep their products safe from cyberattacks.

Finally, there are internet-adjacent firms whose products have internet-based components but that have core business interests outside of the technology sector. We consider firms working in the ‘Internet of Things (IoT)’ space such as General Electric, Kenmore, and PG&E as well as ‘big-box’ stores that rely on the internet to sell ‘real-world’ goods, such as Walmart, Tesco, and Target as examples of these types of firms. Increasingly, most firms besides the two other categories we have identified, are becoming internet-adjacent as they increasingly rely on the internet as a marketplace to meet customers, carry out logistics, and track consumer data.

All of these firms across industries and countries engage with the challenges posed by cyber insecurity and the apparent under-provision of cybersecurity in the market. Each type of firm also engages with government in different ways, from petitioning for protection, to lobbying against regulation.

Market failures

To identify these challenges, we begin by looking at the types of market failures that serve as the rationale for industrial policy (Harris and Carman 1983). We then apply these concepts to the cybersecurity sector. While analysts and policymakers have differed on the extent to which these problems are ‘real’ market failures that require government intervention, some worry that the ‘cure’ of government intervention may be worse than the disease. Our analysis, described in detail below, identified five primary market failures:

concerns about imperfect markets, factor adjustment failures, agglomeration effects, information problems, and national security prerogatives that lead to suboptimal outcomes (Aggarwal and Aggarwal 2016). Below, we detail the distribution of these market failures across the globe.

Imperfect markets

Imperfect markets, characterised by the presence of monopolies, oligopolies, or collusive anticompetitive behaviour, most typically serve as a rationale for state intervention in an industry. As economists generally claim, any deviation from a competitive market is likely to lead to market inefficiencies (Glykou and Pitelis 2011). Yet different schools of thought on what constitutes a deviation from the market have led to debate between the so-called structural, Chicago School, and IO models of antitrust policy. In light of these competing models, while deviations from a competitive market may be identifiable, what to do about them is contested both in the US and in other countries. Harris and Carman (1984), for example, focus on markets wherein excessive competition might take place. These include cases where there is too much entry into the market at some times, and not enough at others. Arguably, the cybersecurity market is representative of the latter phenomenon.

Across the cases explored in this special issue, we point to various examples of imperfect markets. In China, the cybersecurity market is dominated by large monopolies with links to the national security apparatus. As a consequence, there are few firms in the Chinese cybersecurity marketplace. This, some have argued, decreases competition with negative effects upon the provision of cybersecurity (Cheung 2018). In Japan, the historical reliance upon large firms with ties to the Ministry of International Trade and Industry (MITI) and its successor, the Ministry of Economy, Trade, and Ministry (METI), as well as a long-established practice of top-down policymaking have also contributed to the slow speed of growth in the cybersecurity sector (Bartlett 2018). In the United States, on the other hand, there is a plethora of companies marketing their cybersecurity programmes'. At the same time, however, market forces have encouraged interoperability across IT platforms and have led to cybersecurity vulnerabilities for the firms and users, as well as the government agencies that rely upon them (Aggarwal and Reddie 2018).

Factor adjustment failures

Factor adjustment failures are characterised by shortages of appropriate labour and capital in the marketplace. Markets working properly should adjust to these factors, but in the cybersecurity markets, we have hitherto observed intractable labour shortages and capital markets that have failed to grow boutique firms into mid-size firms. While in theory markets should adjust with respect to these factors, as Williamson and others have noted, 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 resulting in a human capital deficit.

On the human capital side, both the United States and United Kingdom have documented the shortage of programmers and computer scientists working on cybersecurity issues (Aggarwal and Reddie 2018; Carr and Tanczer 2018). Multiple factors have caused this

shortage, ranging from opportunities to exit to more lucrative sectors of the computer science economy to the length of time associated with training (Carr and Tanczer 2018).

As well as human capital shortages, there are also capital concerns. In Finland and Taiwan, for example, there are significant scaling issues for cybersecurity firms due to a lack of 'patient capital' – that is, venture capital willing to wait for returns on investment in the cybersecurity sector (Bartlett 2018; Huang and Li 2018). Indeed, cybersecurity firms are considerably less attractive to investors than firms focused on innovation where potential returns are significantly larger. The lack of available capital has also led to 'hollow' cybersecurity markets. In France, for example, there are a large number of small firms and a few large firms providing cybersecurity services, with few mid-size companies between them (D'Elia 2018). At the EU level, too, there has been a documented lack of access to capital markets for investment in the cybersecurity sector (Timmers 2018).

Agglomeration effects

Agglomeration effects – when firms from within related industries are located near each other geographically – have been identified as an important aspect driving industrial success and technological innovation (Haggard 2004, 66–67). Analysts such as Fan and Scott (2003) draw on some of these claims to argue that clusters can produce dense local labour markets, knowledge spillovers, and various forms of business organisation and culture that can enhance competitive advantage.

The ability to achieve these effects, however, has proven difficult and, in some ways, driven the very industrial policies that the market is supposed to make sure are unnecessary. In the IT sector, we have seen efforts in many countries to copy the Silicon Valley model of linkages between academic, government and the private sector, including the government-subsidized 'Chilecon Valley' in Santiago, Chile and the Silicon Roundabout in London. In the cybersecurity sector, there are similar efforts to drive innovation in urban centre and regional hubs. These developments that represent an attempt to 'indigenize' IT and cybersecurity provision have led to calls from domestic industry for antitrust measures and protectionist policies. Policymakers have also increasingly paid attention to the impact of foreign investment in these clusters given concerns surrounding technology transfer.

Information problems

A variety of information problems contribute to market failures in the cybersecurity sector. First, firms – whether in the IT sector or not – are often unaware of the types of vectors of cyberattacks they face, and do not fully understand the vulnerabilities in their software and hardware architecture. Second, even when firms know their vulnerabilities, there is an incentive to engage in 'liability dumping', in which companies attempt to avoid recognising vulnerabilities in their system or share information related to their own breaches, given the reputation costs associated with disclosing them, and pass the liability to their customers.

In the United States, these reputational concerns have impacted nascent information-sharing regimes. Thus far, there has been a reliance upon informal, private information sharing networks, on the basis of secrecy, that include only a small number of large

internet technology firms – despite the creation of a non-binding NIST framework for information sharing specifically designed for the purpose of sharing vulnerabilities in 2014 (Aggarwal and Reddie 2018). In Europe, firms must also navigate complex, multi-jurisdictional governance systems. This multi-layered architecture has also contributed to regulatory gaps and disagreement among countries and the EU concerning how cybersecurity ought to be governed (Timmers 2018).

National security

Finally, governments may intervene in markets on the basis of national security – regardless of the efficiency provided by a market. Indeed, even free market economists accept that governments might need to protect industries for reasons of national security (Mastanduno 1991).

The American, Chinese, Finnish, and French articles in this special issue each note the national security prerogatives associated with the cybersecurity sector that impact regulatory standard setting, procurement, and public investment in the cybersecurity market (Aggarwal and Reddie 2018; Cheung 2018; D’Elia 2018; Griffith 2018). In France, reliance upon foreign firms is viewed as a problem, and the government has moved toward policies designed to provide ‘industrial independence.’ In the United States, national security priorities have led to analysis of the supply chain and various efforts to discriminate against foreign IT products including ZTE and Huawei, given their alleged links to the Chinese government that have led to bans on their procurement by various government agencies. And while the analysis in this special issue does not focus on the geopolitics of cybersecurity – instead focusing on the domestic politics of industrial policymaking – it is worth noting that state preferences are conditioned by global structural dynamics, in general, and a return to an era of strategic competition between the United States, China, and Russia, in particular.

Broadly, governments around the world have pointed to a variety of failures in the cybersecurity market that have catalysed policy responses. In the following section, we outline the variety of market-creating, market-facilitating, market-modifying, market-proscribing, and market-substituting industrial policies in order to provide a typology of market interventions by the government in the cybersecurity sector.

Industrial policies

Governments around the world have responded to market failures in their domestic cybersecurity industries in diverse ways. In the following section, we outline the types of industrial policies.

Market creation

Industrial policy for market creation involves using public policies to create markets by establishing rights, incentives, and opportunities for exchange that would otherwise not exist (Harris and Carman 1984).

In many countries, governments play a significant role in creating domestic cybersecurity markets by becoming key (and, occasionally, primary) customers for cybersecurity-related goods and services. In China, the government is the sole customer for

cybersecurity products created by state-sponsored entities (Cheung 2018). In France, we see the use of coordinated procurement processes focused on building indigenous capabilities – conceived of as a ‘sovereign solution’ to the cybersecurity challenges. These are enshrined within the *Loi de Programmation Militaire-LPM 2014–2019* (Military Programming Law) (D’Elia 2018). These policies reflect the French government’s long tradition of substantial public aid in the development of its IT market. In the United States, the government and military are major (though not the only) consumers of cybersecurity-related goods and services and have government-linked venture capital arms devoted to maintaining the supply of these services by providing capital for continued development (Aggarwal and Reddie 2018).

Market facilitation

Market facilitating measures involve policies that promote or improve the operation of markets by reducing transaction costs, enhancing incentives, or internalising benefits and costs.

In the United States, the National Security Technology Accelerator (NSTXL), designed to provide early-stage funding to technologies viewed by the military and intelligence community as holding promise, serves as an example of a market-facilitating mechanism designed to bring IT to market more quickly. Beijing’s ‘indigenous innovation procurement guidelines’ similarly sought to bolster the domestic cybersecurity market in China by creating incentives for government agencies to become key customers of native cybersecurity firms (Cheung 2018). In Finland, Griffith (2018) observed the provision of a monitoring and warning system that provides key threat information to be used by those seeking to secure their own systems, as well as investments in research and development. Japan, on the other hand, has used its tax policy via the ‘Information Base Strengthening Tax System’ to provide a subsidy to cybersecurity firms (Bartlett 2018).

Market modification

Market-modifying industrial policy uses regulations to change the conduct of subjects, the objects, the medium, or the terms of exchange to produce outcomes that are different from those the market would otherwise produce.

In the United States case, efforts to regulate industry and consumers via the Cybersecurity Information Sharing Act (CISA) and Cybersecurity Intelligence and Sharing Protection Act (CISPA) serve as examples of this type of approach. In France, examples include the Industrial Cyber Plan and the creation of a voluntary information-sharing (CERT-FR) that provides a reporting mechanism and shares best practices among companies, government sponsorship of crisis management exercises (Piragnet) involving the private sector, and public certification schemes for both firms and individuals to signal subject matter expertise (D’Elia 2018). Finland’s own market-modifying mechanisms include statutory requirements, government resolutions, platforms for voluntary cooperation, forums to build shared understanding, and public-private partnerships (Griffith 2018). At the EU level, the European Commission has developed rules concerning data retention and standardisation of cybersecurity guidelines and, similar to France, has undertaken efforts to build a certification scheme for cybersecurity firms (Timmers 2018).

Market proscription

Industrial policy proscribing specific behaviour in a market involves government measures that attempt to prohibit specific behaviours.

Export controls and procurement rules are perhaps the most obvious use of market proscribing tools that limit the ability of domestic cybersecurity firms to take part in international markets. The United States, for example, enshrines export control in the Arms Export Control Act, International Traffic in Arms Regulations, and Export Administration Regulations, while the United Kingdom does the same as part of its Cyber Security Export Strategy and National Cyber Security Strategy. The European Union also continues to move forward with plans to institute export controls on technologies related to cyber-surveillance, much to the chagrin of BAE Systems and other private firms in the cyber sector that must liaise with the respective government to determine appropriate technology sales and potentially lose customers abroad to foreign competitors (Timmers 2018).

Market substitution

Market-substituting policies involve the government creating markets where a private market would not otherwise exist.

In China, we have seen top-down policies involving the identification of ‘strategic industries’ and their associated national champions (Cheung 2018). Using a less direct approach, Japan provides direct investment from government agencies to firms via the direct provision of services as a public service to firms such as the Bot Removal Program and Cyber Clean Center offer two examples of this approach in which the Japanese government provide direct services to private industry (Bartlett 2018).

In the United States, In-Q-Tel – a government-focused investor concentrating on investments related to military and intelligence technologies – substitutes for venture capital firms, while various human capital-related programmes subsidise cybersecurity education, including the Federal Cybersecurity Workforce Strategy, National Initiative for Cyberspace Education, CyberCorps, and Cybersecurity Education and Training Assistance Programs (CETAP) (Aggarwal and Reddie 2018). Finland and the United Kingdom also work to grow their respective cybersecurity workforces through various initiatives, including Master’s programmes and vocational programmes such as Digital Skills for the UK Economy and the Cyber Retraining Academy (Carr and Tanczer 2018; Griffith 2018).

Each of these industrial policies has been built in the shadow of state-society relations in which various government agencies build and implement policies within bureaucratic politics, with input and challenges from societal actors including labour, consumers, interest groups, and IT firms. Indeed, each of the articles in this special issue concludes that the variation in the types of industrial policy employed by different governments reflects, to some degree, the distinctive state-society relations within each country.

Industrial policy implementation

Having outlined both the market failures and a number of responses to these market failures across each case, we now turn briefly to the implementation of these industrial policies. While it is too soon to conclude definitively which policies have worked and which have not, it is worth considering the consequences of intervention in the IT sector.

The domestic consequences of intervention

Using the concept of market failure, the case studies consider the effects of regulation on the cybersecurity sector in different 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 section below, we consider the criteria through which the authors evaluate the consequences 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. An evaluation of the efficiency of industrial policy necessarily involves a 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. States seeking to grow the cybersecurity sector 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.

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 (Harris and Carman 1984). There are a variety of causes of design failure. First, the scope of the market failure may not be appropriately assessed. In the US cybersecurity market, for example, the human capital needs of the market are so significant that existing policies designed to address the shortfall are inadequate (Aggarwal and Reddie 2018). 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 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 design adequately a regulatory response to a market failure may be critical. There are several examples that fall into this last category. Information-sharing regimes that firms are reluctant to sign onto, and often lobby against, serve as a prototypical example of the design challenges facing government regulators as they straddle the requirements of building a collaborative response to specific cyberattacks from firm to firm, while minimising freeriding and sharing of proprietary information. Across countries, this has led to significant variation in the binding or non-binding nature of these regimes. As our analysis points out, information sharing in both Japan and the United States remains a central problem of cybersecurity, despite regulatory efforts to address it.

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, Harris and Carman (1984) point to a variety of potential regulatory failures: electoral failures, bureaucratic failures, legislative failures,

and judicial failures. Each of these failures involves the inability of a segment of society to support industrial policy that would address market failure.

In China, for example, Beijing's procurement and licensing models have led to significant amounts of corruption and the government's vulnerability to cyberattack, degrading the very cybersecurity that the Chinese government is attempting to bolster. At the same time, human capital programmes backed by the government have failed to produce as many cybersecurity-trained workers as expected (Cheung 2018). Regulations created by the Chinese government have also been vague, complicating the entry of new firms into the cybersecurity sector. In France, government efforts to regulate and bolster the cybersecurity industry have been met with resistance from business associations, as many are opposed to the creation of a certification regime that ranks firms on the basis of their performance against cybersecurity metrics (D'Elia 2018). At the EU level, coordination between the EU and its member states represents a continuing problem for implementation of cyber policy given the dangers of regulatory arbitrage – in which businesses pursue the most permissive regulatory environment.

State-society relations

Having outlined market failures, the industrial policies created to address them, and challenges associated with implementation, we turn now to the state-society relations that frame their creation.

The political economy literature on industrial policy provides a variety of rich explanations of forces that drive variation in governments' industrial policy choices (Aggarwal and Evenett 2014). Tai Ming Cheung notes in his analysis of China, for example, that Beijing uses a model of deliberate state-led capitalism (Cheung 2018). Ben Bartlett, on the other hand, notes that Japan promotes private sector-led development of the cybersecurity market (Bartlett 2018). Even among Western capitalist states, it is evident in the articles in this issue that there is considerable variation with regard to the manner in which countries pursue and implement policies that reflect their regime type, bureaucratic politics, geopolitics, and location on the ladder of development.

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 organisation 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 labour, 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, labour plays a much more active role on corporate boards than in the United States.

The key question that emerges from Figure 1 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?

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 (Weiss 2014). 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 (2018) in their examination of the United States point to the various firm-state relations that exemplify the close linkages between the intelligence agencies, well-established defence firms, and Silicon Valley. Griffith (2018), too, examines the cybersecurity market in Finland against the backdrop of broader geopolitical concerns.

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 (Block and Keller 2009). In earlier work, Block (2008) suggests that the state’s role ‘can be divided into four distinct but overlapping tasks – targeted resourcing, opening windows, brokering, and facilitation.’ 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 policymaking at the technological frontier among advanced democracies.

Like Weiss, Block, and Keller, this project to examine the industrial policies of government around the world from a comparative perspective points 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

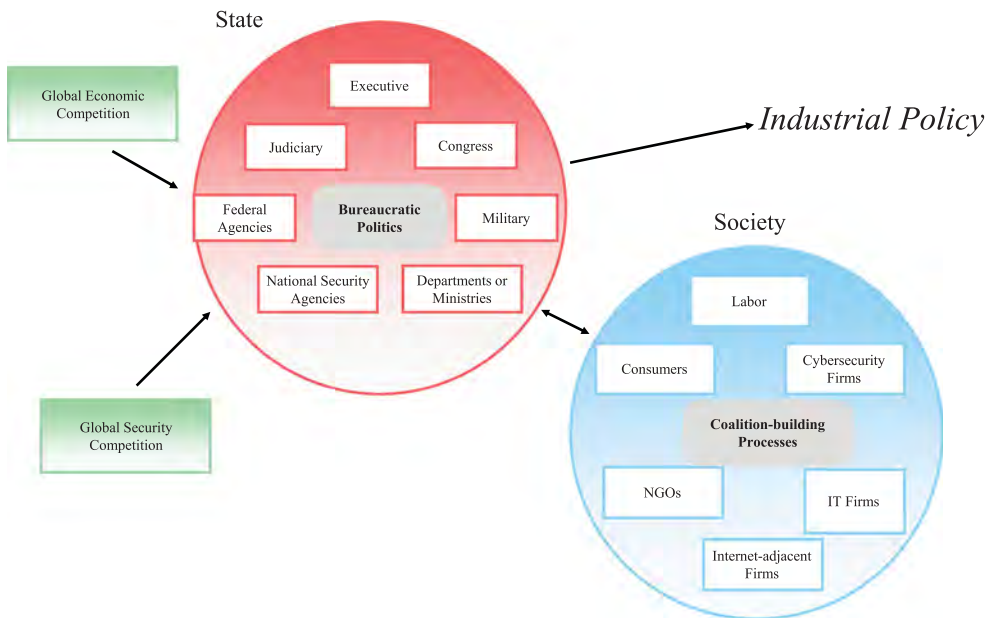


Figure 1. Explaining variation in state-society interaction in policymaking.

state and firms, we conceptualise 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 to, or push back against, state preferences?

The international consequences of intervention

As countries pursue industrial policy in cybersecurity, conflict is nearly inevitable among firms and governments over access to markets.² 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 evidenced by the long-standing Doha Round that began in 2001 and fell apart in December 2015. In response, states have tried to resolve behind-the-border barriers through the TPP (Trans Pacific Partnership) and the TTIP (Transatlantic Trade and Investment Partnership) (Azmeah and Foster 2016). However, as these mega-FTAs have become hotly debated in the US 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 conceptualise 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.

Thus far, efforts to create international engagement and partnerships centred on cybersecurity have largely failed. Barriers to foreign firms have also impeded knowledge flows and arrested the potential for firms to learn from more experienced firms abroad, while also limiting the pursuit of comparative advantage in the sector. In the United States, for example, government procurement rules limiting acquisitions from foreign firms (Chinese firms, in particular) have increased tensions between Beijing and Washington amid broader disagreement surrounding their respective terms of trade flows, deficits, and tariff barriers.

Conclusion

With respect to industrial policy in cybersecurity, each country examined in this study has followed a distinctive approach. Although the conventional wisdom has been that industrial policy does not work and that a reliance on market-based processes to allocate capital and labour remains appropriate, the cybersecurity market appears to provide an important exception – particularly from a government perspective. At the same time, however, firms often appear to reflect the maxim of ‘don’t stand too close to me’. As a consequence, the pursuit of industrial policy in each state is by no means a simple matter.

In terms of market failures, we noted how policymakers expressed both economic and security concerns while promoting cybersecurity policies. From an economic perspective, the costs of cyberattacks have been increasing, posing a challenge to the increasingly data-centric US economy as well as economies around the world. From a security perspective, several reports have pointed to the ongoing vulnerability of federal agencies and critical infrastructure to cyberattacks. The White House Council of Economic Advisors has also recently noted the substantial cost – estimated to be between \$57 billion and \$109 billion in 2016 – to the economy from malicious cyber activity. The general consensus has been that neither the government, nor industry working on their own, have been able to address these issues, most of which are tied to issues in the labour market, such as lack of training and career paths, as well as other problems, such as a failure to upgrade infrastructure.

The drivers of these industrial policies include the increasingly troubling geopolitical context described in recent US policy documents as a return to strategic competition as well as the widespread use of the internet as a venue for cybercrime. With regard to the former, there is an increasing concern surrounding the Chinese effort to promote advanced technology via its Made in China 2025 policy as part of a broader discussion concerning how governments may have to take a more proactive role in policy debates concerning how to address and maintain an ‘edge’ in global competition surrounding high technology (Sender 2016).

In sum, the practice of industrial policy in the cybersecurity marketplace remains in its infancy. While it is too early to tell whether existing policies and plans have been successful, the cybersecurity marketplace offers an important venue for scholars to study the influence of industrial policy upon domestic markets, private firms, and the bureaucratic apparatus charged with dealing with public policy and security-related challenges in a rapidly changing geopolitical context.

Notes

1. 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.
2. There has been considerable discussion concerning international cybersecurity cooperation (frameworks dealing with preventing attacks on critical infrastructure, etc.) but here we have focused on the creation of an international regime designed to preventing conflict with respect to competitive cybersecurity industrial policies through the WTO or mega-FTAs.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by National Research Foundation of Korea [grant number NRF-2017S1A3A2067636].

Notes on contributors

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 Center (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.

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 Center 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.

ORCID

Vinod K. Aggarwal  <http://orcid.org/0000-0002-8572-6323>

Andrew W. Reddie  <http://orcid.org/0000-0003-3231-8307>

References

- Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. 2015. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications." *Journal of Cybersecurity* 1 (1): 69–79.
- Aggarwal, Vinod K. 1985. *Liberal Protectionism*. Berkeley, CA, USA: UC Press.
- Aggarwal, Sonia, and Vinod K. Aggarwal. 2016. "The Political Economy of Industrial Policy." BASC Working Paper 16-1, University of California, Berkeley.
- 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): 481–509.
- Aggarwal, Vinod K., and Andrew W. Reddie. 2018. "Comparative Industrial Policy and Cybersecurity: The US Case." *Journal of Cyber Policy* 3 (3). doi:10.1080/23738871.2018.1551910.
- Azmeh, Shamel, and Christopher Foster. 2016. "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.
- Bartlett, Benjamin. 2018. "Government as Facilitator: How Japan is Building its Cybersecurity Market." *Journal of Cyber Policy* 3 (3). doi:10.1080/23738871.2018.1550522.
- Block, Fred. 2008. "Swimming Against the Current: The Rise of a Hidden Developmental State in the United States." *Politics and Society* 36 (2): 169–206.
- Block, Fred, and Matthew R. Keller. 2009. "Where Do Innovations Come From? Transformations in the US Economy, 1970–2006." *Socio-Economic Review* 7 (3): 459–483.
- Carr, Madeline, and Leonie Tanczer. 2018. "UK Cyber Security Industrial Policy: The Socio-technical Factors." *Journal of Cyber Policy* 3 (3). doi:10.1080/23738871.2018.1550523.

- 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). doi:10.1080/23738871.2018.1556720.
- D'Elia, Danilo. 2018. "Industrial Policy: The Holy Grail of French Cybersecurity Strategy?" *Journal of Cyber Policy* 3 (3). doi:10.1080/23738871.2018.1553988.
- 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.
- 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.
- Griffith, Melissa. 2018. "A Comprehensive Security Approach: Bolstering Cybersecurity Capacity Through Industrial Policy." *Journal of Cyber Policy* 3 (3).
- Haggard, Stephan. 2004. "Institutions and Growth in East Asia." *Studies in Comparative International Development* 38 (4): 53–81.
- 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): 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): 41–52.
- Huang, Hsini, and Tien-Shen Li. 2018. "A Centralized Cybersecurity Strategy for Taiwan." *Journal of Cyber Policy* 3 (3). doi:10.1080/23738871.2018.1553987.
- Mastanduno, Michael. 1991. "Do Relative Gains Matter? America's Response to Japanese Industrial Policy." *International Security* 16 (1), Summer: 73–113. doi:10.2307/2539052.
- Morgan, Steve. 2015. "Cybersecurity Market Reaches \$75 Billion In 2015; Expected To Reach \$170 Billion By 2020." *Forbes*, December 20.
- Sender, Henry. 2016. "US Defence: Losing Its Edge in Technology?" *Financial Times*, September 4. <https://www.ft.com/content/a7203ec2-6ea4-11e6-9ac1-1055824ca907>.
- Timmers, Paul. 2018. "European Union Cybersecurity Industrial Policy." *Journal of Cyber Policy* 3 (3).
- Weber, Steven. 2017. "Data, Development, and Growth." *Business and Politics* 19 (3): 397–423.
- Weiss, Linda. 2014. *America, Inc.?* Ithaca: Cornell University Press.