CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Cyber Industrial Policy in an Era of Strategic Competition

VINOD K. AGGARWAL AND ANDREW W. REDDIE

CLTC WHITE PAPER SERIES

Cyber Industrial Policy in an Era of Strategic Competition

VINOD K. AGGARWAL AND ANDREW W. REDDIE

CENTER FOR LONG-TERM CYBERSECURITY

Contents

Executive Summary

Cybersecurity has become a central political and economic challenge for governments and businesses around the world. But while election hacking, malware, and cyber warfare have dominated the public discourse, the academic and policy communities have largely ignored the diverse *industrial policies* that governments can use to bolster their domestic cybersecurity and technology industries.

This paper provides an overview of many of the industrial policy approaches available to policymakers seeking to advance their cybersecurity industries, with an investigation of the consequences of policies for national and international economies as well as global governance frameworks.

Our intent is to help cybersecurity industry leaders and policymakers assess the costs and benefits of a range of possible industrial policy measures in an era of renewed strategic competition. We assess the driving forces of cybersecurity industrial policy, inventory existing industrial policy approaches, and examine what challenges and conflicts are likely to arise from the competitive pursuit of such policies.

This report builds upon a two-year comparative project sponsored by UC Berkeley's Center for Long-Term Cybersecurity (CLTC). Drawing upon the efforts of academics from around the world, the study investigates the role of firms, governments, and other key stakeholders involved in the rise of industrial policies related to cybersecurity in the United States, China, Taiwan, Japan, the EU, UK, France, and Finland. Findings from the study were published in December 2018 in a special issue of the *Journal of Cyber Policy*.

Industrial Policy 101

"Industrial policy" refers to non-market efforts by governments to grow sectors of the economy that are deemed to be strategically important, but in which market dynamics have led to an under-provision of a good or service. Governments generally employ such policies when markets fail or are perceived to be failing to produce a good or service deemed to be of national importance. Originally used to describe governments' efforts to bolster their manufacturing sectors—for example, to maintain the supply of steel needed to build tanks—industrial policy today is applied broadly to sectors of strategic interest, including in emerging technologies.

For decades, companies have framed protectionist efforts by claiming the importance of their industry for national security. In 1959, for example, the U.S. government responded to domestic lobbying by the oil industry by imposing oil quotas, which ironically ended up draining American reserves and contributed to OPEC's ability to raise oil prices in 1973.[1] Such national security claims are sometimes even more 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."[2]

In our view, the cybersecurity industry has a significantly more plausible claim for its critical role in national security. From spearphishing and distributed denial-of-service attacks (DDoS) to advanced persistent threats (APT), cyber-attacks have become increasingly commonplace as internet technology has become ubiquitous. These attacks pose a significant security and economic problem for governments and firms whose day-to-day operations rely upon digital infrastructure. The challenge of coping with such intrusions raises critical questions about the role that governments should play in supporting the domestic provision of cybersecurity products and services.[3]

Industrial Policy Approaches to Cybersecurity

In recent years, in the wake of massive cyberattacks on public- and private-sector targets, governments across the globe have expanded their focus on cybersecurity-related issues. Nations have adopted measures to bolster their cyber defenses, increase the resilience of their internet networks, and protect both their own data and that of their citizens. Governments have proactively sought to advance their domestic cybersecurity industries, fearing the lack of home-grown capabilities and striving to remain at the cutting edge of computer and network security. Given a wide range of options, some countries have taken a more activist approach than others.[4]

The following provides an overview of diverse policy approaches taken by governments to support their respective cybersecurity sectors, based upon a typology of five market interventions:[5]

Market Creation: In many countries, national governments have played a vital role in creating domestic cybersecurity markets simply by becoming customers for cybersecurity-related goods and services. For example, in China, the government is the sole customer for cybersecurity products developed by state-sponsored entities. In France, we see the use of coordinated procurement processes that are focused on building indigenous capabilities. These policies, designed to serve as a "sovereign solution" to the cybersecurity challenge, are enshrined within the *Loi de Programmation Militaire-LPM 2014–2019* (Military Programming Law).[6] Such policies reflect Paris' long tradition of investing substantial public aid to support the French IT market. In the United States, the government and military are major consumers of cybersecurity-related goods and services, and also have government-linked venture capital arms devoted to maintaining the supply of these services (see sidebar on page 8).[7]

Market Facilitation: Market facilitation policies promote or improve the operation of markets by reducing transaction costs, enhancing incentives, or internalizing benefits and costs. In the United States, for example, the National Security Technology Accelerator (NSTXL) provides early-stage funding to help bring to market technologies that are viewed as promising by the military and intelligence communities. The Defense Innovation Unit (formerly DIUx), the DHS Silicon Valley Innovation Program (SVIP), and the National Geospatial Agency's Outpost Valley also enable government agencies to tap into the technology talent and early-stage startups that produce goods and services of strategic interest. In China, Beijing's "indigenous innovation

Market Failures

Governments around the world have pointed to a variety of failures in the cybersecurity market that have catalyzed policy responses. 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 identified five primary market failures that have led to the shaping of industrial policies for cybersecurity:

IMPERFECT MARKETS: Characterized by the presence of monopolies, oligopolies, or collusive anticompetitive behavior, imperfect markets frequently serve as a rationale for state intervention in an industry. In China, for example, 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 and has negative effects upon the provision of cybersecurity. In the United States, on the other hand, there are a plethora of companies marketing cybersecurity programs, but more general market forces have encouraged interoperability across IT systems and have led to cybersecurity vulnerabilities for the firms, users, and government agencies that rely upon them.

FACTOR ADJUSTMENT FAILURES: Factor adjustment failures are characterized by shortages of adequately appropriate labor and capital in the marketplace. Markets working properly should adjust to these factors, but in the cybersecurity markets, we have observed intractable labor shortages and capital markets that have hitherto failed to grow boutique firms into mid-size firms. Both the United States and United Kingdom have documented the shortage of programmers and computer scientists working on cybersecurity issues. Multiple factors have caused this shortage, ranging from opportunities to exit to more lucrative sectors of the computer science economy and the length of time associated with training.

AGGLOMERATION EFFECTS: Agglomeration effects—when firms within related industries are located near each other geographically—have been identified as an important factor in industrial success. We have seen efforts in many countries to copy the Silicon Valley model by encouraging linkages between academic, government, and the private sector, including the government-subsidized "Chilecon Valley" in Santiago, Chile and the Silicon Roundabout in London. Such efforts have not always proven successful, however, and even in the United States, analysts have expressed concerns about the growing concentration of markets, particularly as dominant firms have acquired start-ups and as Chinese and other foreign firms have invested in smaller firms to secure technology. These developments have led to calls for both antitrust measures, as well are more careful review of the implications of foreign investment in such technology hubs.

INFORMATION PROBLEMS: A variety of information problems contribute to market failures in the cybersecurity sector. First, firms are often not aware of the vectors of cyber-attacks they face, nor do they 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 recognizing vulnerabilities in their system or share information related to their own breaches given the reputation costs associated with disclosure.

NATIONAL SECURITY: Governments may intervene in markets on the basis of national security, regardless of the efficiency provided by a market. The American, Chinese, Finnish, and French cases each note the national security prerogatives associated with the cybersecurity sector that impact regulatory standard-setting, procurement, and public investment in the cybersecurity market. In France, reliance upon foreign firms is viewed as a problem, and Paris has moved toward policies designed to provide "industrial independence." In the United States, national security priorities have led to various efforts to discriminate against IT products from foreign firms, including ZTE and Huawei, which allegedly have links to the Chinese government.

procurement guidelines" seek to bolster the domestic cybersecurity market in China by creating incentives for government agencies to become key customers of native cybersecurity firms.[8] In Finland, the government allocates investments in research and development and has developed a monitoring and warning system that provides key threat information to be used by those seeking to secure their systems. Japan's "Information Base Strengthening Tax System," on the other hand, uses tax policy to provide a subsidy to cybersecurity firms.

Market Modification: Market modification uses regulations to change the conduct of subjects—or to change the objects, medium, or terms of exchange—to produce outcomes that are different from those the market would otherwise produce. In the United States, the Cybersecurity Information Sharing Act (CISA) and Cybersecurity Intelligence and Sharing Protection Act (CISPA) serve as examples of this type of approach; CISA, for example, allows the sharing of information between federal agencies and technology and manufacturing firms. The NIST Framework for Improving Critical Infrastructure Cybersecurity offers an alternative example of a best-practices approach for developing informal standards that private industry can follow and incorporate into their "organizational risk management processes."[9] Importantly, this "best practices" approach has no enforcement mechanism.

France's Industrial Cyber Plan includes a voluntary information-sharing system (CERT-FR) that provides a reporting mechanism, supports the sharing of best practices among companies, sponsors crisis management exercises involving the private sector (Piranet), and facilitates certification schemes for both firms and individuals to signal subject-matter expertise.[10] Finland's market-modifying mechanisms include statutory requirements, government resolutions, platforms for voluntary cooperation, forums to build shared understanding, and public-private partnerships.[11] At the EU level, the European Commission has developed rules concerning data retention and standardization of cybersecurity guidelines and, similar to France, has undertaken efforts to build a certification scheme for cybersecurity firms.[12]

Many governments have taken measures to promote their own countries' firms while limiting foreign firms' participation in cybersecurity markets, a process we call *indigenization*, in which states seek to create markets where both supply and demand are largely domestic. While some nations, like Japan, have opened their markets to foreign cybersecurity products to compensate for a lack of indigenous capacity, most have been skeptical of relying on foreign firms, preferring instead to create the conditions for national firms to build expertise. This skepticism appears to be growing in the U.S., as evidenced by limits placed on the procurement of technology from China's Huawei and ZTE or the use of products from Kaspersky Labs, a Russian anti-virus firm, amid concerns that these companies may provide undue access to Beijing or Moscow,

Government as Venture Capitalist

In the United States, the federal government has launched initiatives to allocate venture capital to fund projects of importance to national security, including cybersecurity. As an example, Palantir, a data analytics and software firm, was founded in 2003 in part through a $2 million investment from In-Q-Tel, a self-described "strategic investor for the U.S. intelligence and defense communities."

Founded by former CIA director George Tenet in 1998, In-Q-Tel (IQT) has provided hundreds of millions of dollars to over two hundred technology companies while establishing relationships between members of the intelligence community and private firms. In response to the challenge posed by cybersecurity operations, In-Q-Tel has sought to "start providing venture capital funding to [Silicon Valley] startups that can help the Pentagon develop more advanced cybersecurity and intelligence systems to fend off nation states and hackers targeting everything from top-secret military correspondence to public power grids."

Similarly, the CIA has created the Directorate of Digital Innovation (DDI), which focuses on accelerating digital innovation across the intelligence community. DDI is designed to help "prioritize requirements for the venture capital entity" and "identify critical emerging digital issues and capabilities" for the CIA. It will also have "a very close and robust relationship" with the private sector to detect emerging technology trends, accelerate technology application, and create internal conditions for innovation.

respectively. (The national security review processs created by the Committee on Foreign Investment in the United States (CFIUS) statute of the Defense Production Act has only been used to block transactions on three occasions, with Chinese companies involved in all three instances.[13] Currently a major effort is underway to enhance the role of CFIUS (via passage in 2108 of legislation known as the Foreign Investment Risk Review Modernization Act) in evaluating the impact of foreign investments in the United States. This is part of President Trump's focus on China's "Made in 2025" industrial policy efforts.[14])

Market Proscription: Governments can use policy to proscribe how firms can behave in a market. Export controls and procurement rules are the best-known use of market proscribing tools that limit the ability of domestic cybersecurity firms to take part in international markets. The United States, for example, has enshrined export control in the Arms Export Control Act, while the United Kingdom limits exports through the Cyber Security Export Strategy and National Cyber Security Strategy.[15] The European Union has moved 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 each respective government to determine appropriate technology sales (and potentially lose customers abroad to foreign competitors).[16]

Market Substitution: Market-substituting policies involve creating markets where a private market would not otherwise exist. In China, top-down policies have been used to identify "strategic industries" and their associated national champions.[17] Using a less direct approach, Japan transfers investment from government agencies to firms through the provision of services. Through the Bot Removal program and Cyber Clean Center, for example, the Japanese government provides direct services to private industry.[18] In the United States, In-Q-Tel—a government-focused investor focused on investments related to military and intelligence technologies—effectively functions as a venture capital firm, while various human capital-related programs have been established to subsidize cybersecurity education, including the Federal Cybersecurity Workforce Strategy, National Initiative for Cyberspace Education, CyberCorps, and Cybersecurity Education and Training Assistance Programs (CETAP). Finland and the United Kingdom also are working to grow their respective cybersecurity workforces through various initiatives, including master's programs and vocational programs such as Digital Skills for the UK Economy and the Cyber Retraining Academy.

Each of these policies has been built in the shadow of state-society relations in which various government agencies build and implement policies within bureaucratic politics, and with input and challenges from societal actors, including labor, consumers, interest groups, and IT firms. Our research concluded 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.

NIST Guide to Cyber Threat Information Sharing

The National Institute of Standards and Technology (NIST) has developed a guide to sharing information on cyber threats between industry and government. This framework was born from the Burr-Feinstein Bill, Cybersecurity Information Sharing Act (CISA), which included a mandate to build a framework for government-firm cooperation concerning cyber threats. The Cybersecurity Act of 2015, (formerly Cybersecurity Information Sharing Act of 2015), established a voluntary information-sharing regime that sought to eliminate legal barriers and disincentives that would have otherwise discouraged large-scale dissemination of relevant data. As long as information-sharing occurs in accordance with the technical requirements outlined in the bill, private-sector participants are protected from legal liability.

Building the Pipeline

A lack of skilled professionals is one of the most important challenges facing governments seeking to enhance their nation's cybersecurity. The U.S. has launched an array of initiatives to increase the workforce in the cybersecurity marketplace for both public and private actors.

National Initiative for Cybersecurity Education (NICE): Established in 2012 as a joint effort by the federal government, industry, and academia to improve cybersecurity education and workforce development. Operating under NIST's Applied Cybersecurity Division, NICE also runs the Interagency Coordinating Council, which convenes federal agencies to coordinate cybersecurity education and workforce policy.

National Integrated Cyber Education Research Center (NICERC): Exists in partnership with DHS as an education-oriented non-profit subsidiary of the Cyber Innovation Center to provide cybersecurity curricula to elementary, middle, and high school students.

National Cybersecurity Workforce Framework: Developed by the White House, this program helps agencies categorize cybersecurity work and, in doing so, assist with the identification of federal and private workforce needs.

Building a Pipeline for Talent: The initiative is part of a broader federal effort to reach out to K-12 institutions, and, appears to be part of CETAP (Cybersecurity Education and Training Assistance Program), a DHS cybersecurity education program.

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

TechHire: Aims to provide workers with skills to fill vacant positions in the IT sector, and is supported by federal grant funding and public-private partnerships. In the initial announcement, President Obama pledged $100 million in federal grants. In 2016, the Vice President and Secretary of Labor announced an additional $150 million in Department of Labor grants.

U.S. Defense Digital Service: Operates a number of programs—including "Hack the Pentagon," "Hack the Army" and "Defense Travel System Modernization"—that have brought private citizens and companies to the government to build products that address a specific government need.

Key Challenges Related to Industrial Policy for Cybersecurity

The use of industrial policy to bolster national markets might seem to represent an unequivocal good for the firms based in that country, but that is not necessarily the case. A range of challenges can emerge in the wake of industrial policies set by a national government. In China, for example, Beijing's procurement and licensing models have led to significant corruption, degrading the very cybersecurity that the Chinese government is attempting to bolster; human capital programs backed by the Chinese government have failed to produce as many cybersecurity-trained workers as expected;[19] and regulations have been vague, complicating the entry of new firms into the cybersecurity sector.

In this section, we provide an overview of some of the key challenges associated with devising and implementing industrial policies related to cybersecurity:

Firms may be reluctant to share proprietary information: Many governments have established regulations and standards to incentivize the sharing and adoption of best practices in security, and they have encouraged the sharing of breach data to help companies quickly respond to cyber-attacks and keep citizens safe. Yet firms are often reluctant to sign on to information-sharing regimes due to concerns about sharing proprietary information and enabling other firms to operate as "free riders." This has led to significant variation in the binding or non-binding nature of these regimes across countries. In France, for example, government efforts to regulate and bolster the cybersecurity industry have been met with resistance from business associations opposed to the creation of a certification regime that ranks firms on the basis of their performance against cybersecurity metrics.[20]

Import and export rules restrict free trade: The use of export controls to prevent the diffusion of key technologies, and import controls to avoid purchases from competitors for security concerns, have inserted back doors or have potential to undermine domestic firms in the market. Policies that impose barriers on foreign firms' participation often impede knowledge flows and limit the potential for firms to learn from more experienced firms abroad, while also

limiting the pursuit of comparative advantage in the sector.[21] In the United States, government procurement rules limiting acquisitions from foreign firms (Chinese firms, in particular) have led to increased tensions between Beijing and Washington amid a broader trade disagreement. In addition, countries' focus on supporting their domestic industries has potentially slowed the advancement of international engagement and partnerships.

Regulations create opportunities for arbitrage: The development of divergent national regulatory frameworks around cybersecurity has potential to lead to *regulatory arbitrage*, in which businesses choose to operate in the most permissive regulatory environments. In the case of the European Union, for example, regulatory arbitrage has proved a challenge for effective coordination of cyber policy among the EU and its member states. Europe's multi-layered architecture has also contributed to regulatory gaps and disagreement among countries and the EU concerning how cybersecurity ought to be governed.[22]

Actors have diverging interests: While some firms benefit from efforts by governments to regulate the cybersecurity industry by setting standards and promoting the adoption of best practices, others are negatively impacted by export control policies that prevent them from working with private- and public-sector partners abroad. These diverging interests—among firms and within government—are reflected in lobbying and the levels of government intervention. The regulations that are good for large technology firms like Facebook or Amazon may not be good for smaller, cybersecurity firms like FireEye or Darktrace. Most often, large IT firms and other companies have lobbied for "light footprint" approaches to regulation, including voluntary information-sharing regimes and the creation of non-binding best practices.

The private and public sectors have different values and interests: Cooperation on cybersecurity standards depends on strong relations between governments and technology companies. Rifts have emerged in these relationships in recent years around ethical issues. In the U.S., for example, Google's June 2018 withdrawal from the Pentagon's Project Maven illustrates how the government's role in driving innovation and technology-related research and development may face resistance, despite the government's historical role in developing scientific and technological advances such as satellite technology, GPS, and the internet. In China and Russia, where the relationship between the government and industry is much closer, these types of challenges are much less common; indeed, Chinese technology companies often directly reflect the policy prerogatives of the Chinese leadership and government.[23] The lack of disagreement in the policy creation process may represent a comparative advantage for Beijing.

Traditional procurement and licensing processes are slow and burdensome: In the U.S., the procurement process used by the Department of Defense and defense firms[24] has often been described as slow and burdensome, which lowers the potential for small firms to bid for government contracts and has arguably led to the entrenchment of a small number of large firms dominating the space. The process has come under criticism from inside and outside of government given the new threats and risks posed by cybersecurity.[25] Recent efforts to reform this traditional procurement and licensing arrangement are being developed by a number of military services and intelligence agencies with a goal to make it simpler for smaller companies to contract with the government.[26]

Conclusion

From activist states like China, which channels government funds toward cybersecurity firms with direct relationships with the national security establishment, to more passive states like France, Finland, and the United Kingdom, which pursue industrial policy at the margins by encouraging private investment and human capital development, national governments have demonstrated considerable variation in their industrial policy responses to the cybersecurity challenge. These varied approaches appear to be based on the broader political, economic, and security context faced by each government.

Governments' interest in intervening in the cybersecurity sector may grow more urgent as international relationships evolve. For example, the past few years have seen a return to great power competition, as U.S., China, and Russia are vying for strategic advantage in the geo-political sphere. In the U.S., there is growing concern surrounding China's effort to promote advanced technology through its Made in China 2025 policy. At the same time, threats have emanated from other nations, such as North Korea, which has successfully employed techniques of cyber warfare against the United States. These developments have sparked a broader discussion concerning how governments may have to assume a more proactive role in shaping policy to maintain an "edge" in global competition surrounding high technology.

Given the lessons learned over the past decade of addressing cybersecurity across a number of countries, we suggest 1) that programs to promote human capital development remain important but are currently under-funded; 2) the regulatory context within which firms operate remains opaque—particularly with regard to information sharing requirements placed upon firms; and 3) further research is necessary to examine the multinational aspects of the cybersecurity, IT, and adjacent markets.

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 opportunity to watch and learn, as the complicated nature of interactions between the public and private sector are likely to have corollaries in other emerging technologies with potential to be applied for economic and military purposes, including artificial intelligence, quantum computing, and robotics.

About the Authors

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 received his B.A. from the University of Michigan and his M.A. and Ph.D. from Stanford University. His work was partially supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2017S1A3A2067636).

Andrew W. Reddie is a Ph.D. candidate in the Charles and Louise Travers Department of Political Science, University of California, Berkeley. He is an affiliated researcher in the Department of Nuclear Engineering, Goldman School of Public Policy, Center for Long-Term Cybersecurity, Nuclear Science and Security Consortium, and BASC, and he serves as Deputy Director for the Nuclear Policy Working Group. He holds an M.Phil in International Relations from Oxford University and a B.A. (hons.) from the University of California, Berkeley.[27]

Endnotes

1 Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton University Press. Retrieved from: http://www.jstor.org/stable/j.ctt7sq9s.

2 1959 Pastore Senate Committee on Trade. See the discussion in Aggarwal, Vinod K. 1985. *Liberal Protectionism*. Berkeley, CA, USA: UC Press.

3 Weber, Steven. 2017. "Data, Development, and Growth." *Business and Politics* 19 (3): 397–423.

4 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.

5 To organize the typology, we use a previous categorization developed by economists Carman and Harris in 1985.

6 D'Elia, Danilo. 2018. "Industrial Policy: The Holy Grail of French Cybersecurity Strategy?" *Journal of Cyber Policy* 3 (3): 385–406.

7 Aggarwal, Vinod K., and Andrew W. Reddie. 2018. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis." *Journal of Cyber Policy* 3 (3): 291–305.

8 Cheung, Tai Ming. 2018. "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities." *Journal of Cyber Policy* 3 (3): 306–326.

9 National Institute of Standards and Technology. 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

10 D'Elia, Danilo. 2018. "Industrial Policy: The Holy Grail of French Cybersecurity Strategy?" *Journal of Cyber Policy* 3 (3): 385–406.

11 Griffith, Melissa K. 2018. "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity." *Journal of Cyber Policy* 3 (3): 407–429.

12 Timmers, Paul. 2018. "The European Union's Cybersecurity Industrial Policy." *Journal of Cyber Policy* 3 (3): 363–384.

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

14 Aggarwal, Vinod K., and Andrew W. Reddie. 2018. "Comparative Industrial Policy and Cybersecurity: The US Case." *Journal of Cyber Policy* 3 (3): 445–466.

15 Carr, Madeline, and Leonie Maria Tanczer. "UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions." *Journal of Cyber Policy* 3, no. 3 (2018): 430-444.

16 Timmers, Paul. 2018. "The European Union's Cybersecurity Industrial Policy." *Journal of Cyber Policy* 3 (3): 363–384.

17 Cheung, Tai Ming. 2018. "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities." *Journal of Cyber Policy* 3 (3): 306–326.

18 Bartlett, Benjamin. 2018. "Government as Facilitator: How Japan is Building its Cybersecurity Market." *Journal of Cyber Policy* 3 (3): 327–343.

19 Cheung, Tai Ming. 2018. "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities." *Journal of Cyber Policy* 3 (3): 306–326.

20 D'Elia, Danilo. 2018. "Industrial Policy: The Holy Grail of French Cybersecurity Strategy?" *Journal of Cyber Policy* 3 (3): 385–406.

21 Huang, Hsini, and Tien-Shen Li. 2018. "A Centralized Cybersecurity Strategy for Taiwan." *Journal of Cyber Policy* 3 (3): 344–362.

22 Timmers, Paul. 2018. "The European Union's Cybersecurity Industrial Policy." *Journal of Cyber Policy* 3 (3): 363–384.

23 Cheung, Tai Ming. 2018. "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities." *Journal of Cyber Policy* 3 (3): 306–326.

24 Eugene, Gholz, and Harvey M. Sapolsky. "Restructuring the US Defense Industry." *International Security 24*, no. 3 (1999): 5-51.; Lindsay, Jon R. "War upon the map: The politics of military user innovation." (2006). Retrieved from https://dspace.mit.edu/handle/1721.1/33457; Avant, Deborah D. *The Market for Force: The Consequences of Privatizing Security*. Cambridge University Press, 2005; Deutch, John. "Consolidation of the US defense industrial base." *Acquisition Review Quarterly* 8, no. 3 (2001): 137–150. Retrieved from https://www.dau.mil/library/arj/ARJ/arq2001/Deutch.pdf.

25 Gallagher, Sean. 2013. "Why US government IT fails so hard, so often" (10 October). Retrieved from https://arstechnica.com/information-technology/2013/10/why-us-government-it-fails-so-hard-so-often/.

26 Orazem, Geoff, et al. 2017. "Why Startups Don't Bid on Government Contracts (22 August)." Available at https://www.cambridge.org/core/services/aop-file-manager/file/575abb2876fa00070ad0e9a1/ino-ifc.pdf.

27 For research support, both authors would like to thank Tianyu Claire Qiao and Courtney Kantowski.

Cover image: iStock/MarsYu

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley