Defense One

The US Needs an Industrial Policy for Cybersecurity

By Vinod K. Aggarwal and Andrew W. Reddie

June 5, 2019

President Trump's recent Executive Order restricting the use of Huawei's telecommunications equipment was hardly the first time the U.S. government has intervened in the private sector for purposes of national security. During World War II, for example, the U.S. government pumped investment into the American steel industry to ensure the military had a sufficient supply to build tanks, ships, and other armaments.

In the ensuing decades, however, other industries made more far-fetched claims for intervention. The American wool industry argued in the 1950s for government protection of domestic production by claiming that up to 200 million woolen blankets could help the population survive an atomic war. Oil industry lobbying in the 1950s led the government to impose oil quotas, which ended up draining American reserves and contributing to the oil spike of 1973. Just last year, Trump's tariffs on steel made by U.S. allies, levied in the name of national security, drew protests from the American defense industry.

The 2018 tariffs notwithstanding, industrial policy—actions taken 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—has largely fallen out of favor. But in recent years, the steady barrage of attacks on the digital infrastructure of U.S.-based companies and government agencies suggests that one key sector has a far more plausible claim to make for government intervention: the cybersecurity industry.

Related: The People of Baltimore Are Beginning Their Fifth Week Under Electronic Siege
Related: Trump Signs Executive Order to Boost Federal Cyber Workforce
Related: The US Needs a Cybersecurity Civilian Corps

Industrial policies are appropriate when market failures have led to the underprovision of a good or service. The cybersecurity industry's growth has been held back for several reasons, including intractable labor shortages. Both the United States and United Kingdom suffer from a documented shortage of skilled programmers and computer scientists working on cybersecurity issues, and the U.S. alone is projected to have a shortage of 1.2 million professionals by 2022, according to the Center for Strategic and International Studies. The market has also been hindered by so-called "information problems," as firms are often not aware of their own vulnerabilities and avoid sharing information about data breaches given the reputation costs associated with disclosure.

So what can the government do about it? The White House's move to restrict Huawei's telecommunications equipment offers one approach for reducing the reliance on foreign IT components and expertise. What most analyses of this approach miss, however, is that there are a large number of alternative mechanisms that states can use to bolster domestic industry.

With support from the University of California, Berkeley's Center for Long-Term Cybersecurity, we recently published a report that assesses the costs and benefits of various industrial policy measures, based on an analysis of industrial cybersecurity policies in the United States, China, Taiwan, Japan, the EU, Britain, France, and Finland.

Our analysis found that, while the federal government has taken an array of approaches—ranging from direct procurement of services from U.S.-based firms to the creation of government-linked venture capital arms, such as In-Q-Tel, a self-described "strategic investor for the U.S. intelligence and defense communities"—much more could be done. Given the scope and complexity of the challenge, policymakers should be thinking more broadly about an industrial policy framework that better supports cybersecurity products and services. It's time for the U.S. federal government to take the lead and bolster cybersecurity spending, providing more funding for research and training and creating a more transparent regulatory context, particularly around information sharing.

Implementing effective industrial policy for cybersecurity won't be easy. Firms may be reluctant to share

proprietary information, import and export rules can impede knowledge flows and limit the potential for firms to learn from more experienced firms abroad, and such regulations can limit the pursuit of comparative advantage. Divergent national regulatory frameworks globally can lead to regulatory arbitrage, in which businesses operate in the most permissive regulatory environments and eschew business from countries with more regulations. Different players in the private and public sectors may hold different values and interests, which presents another obstacle to developing one-size-fits-all policy and regulatory solutions.

Despite these challenges, building an effective framework for intervention should be a priority, particularly as the complicated nature of interactions between the public and private sector in cybersecurity markets could affect other emerging technologies, including artificial intelligence, quantum computing, and robotics. The government's role will only grow more important as digital technologies expand and the need to create a robust cybersecurity sector and workforce grows more urgent.

By Vinod K. Aggarwal and Andrew W. Reddie // 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. // 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.

June 5, 2019

https://www.defenseone.com/ideas/2019/06/us-needs-industrial-policy-cybersecurity/157501/