The Heritage Foundation

CONGRESSIONAL TESTIMONY

"Cybersecurity Threats to Corporate and Personal Data"

Testimony before
Senate Committee on the Judiciary

United States House of Representatives

November 5, 2019

Klon Kitchen
Senior Research Fellow, Technology, National Security, and Science Policy
The Heritage Foundation

My name is Klon Kitchen. I lead technology policy at The Heritage Foundation where I am also the Senior Research Fellow for Technology, National Security, and Science Policy. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Thank you, Chairman Joshua Hawley (R–MO) and Ranking Member Sheldon Whitehouse (D–RI) for the opportunity to testify before the subcommittee on this important topic. It is critical that our nation consider the opportunities and the challenges that are created in this emerging environment of ubiquitous data generation and growing data insecurity.

As a former intelligence officer within the United States' Intelligence Community, our mission was to collect, to understand, to predict, and to shape human behavior and events. Those in government call this "intelligence."

Technology companies call this "market research," "data analysis," "audience segmentation," or "service provisioning." But in reality, in the age of the so-called "knowledge economy," we are all in the business of intelligence.

The proliferation of sensors, the deluge of digitized data, and the exponential growth in computational capacity are combining to produced previously unimagined possibilities for human thriving and happiness. But these positive outcomes are not all that is being created. In the background of these real and laudable achievements is an undeniable and a potentially existential challenge: we are innovating faster than we can secure.

General cybersecurity risks are combining with increasingly aggressive, hostile foreign actors to create an environment that few understand and that even fewer are prepared for. Specifically, there are three trends that must be turned around if the U.S. is going to thrive going forward.

1. Cybercrime

First, cybercrime is exploding. By 2021, according to Cybersecurity Ventures, cybercriminals are projected to cost the global economy more than $6 trillion annually, up from $3 trillion in 2015.[1] Perhaps nowhere is this trend more clear than in the business sector.

More than 43 percent of global businesses were the victim of a cybersecurity breach in the past 12 months, according to the 2018 Cyber Security Breaches Survey, and 83 percent of finance companies are hit by at least 50 cyberattacks every month.[2] Even more, once bad guys gain access to these networks, they remain undetected, on average, between six and 12 months—stealing intellectual property, siphoning critical data, and generally causing havoc.[3]

With the average cost of a corporate cybersecurity breach now running between $1.25 million and $8.19 million,[4] the professional cybersecurity industry is booming. But even this is a sign of difficult days ahead.

Total spending on cybersecurity is projected to reach more than $120 billion by the end of 2019,[5] an increase of nearly 13 percent over last year—with companies like Microsoft, Google, and Facebook each spending around $1 billion a year on securing their products and offerings. But here is the rub: Few companies have the resources or the technical talent of these tech titans, and yet, smaller companies face many of the same threats that are trying to take down the Silicon Valley giants—including increasingly aggressive state actors.

2. Cyber-Enabled Economic Warfare

Cyber-enabled economic warfare is the second trend that must be engaged. For decades, countries like China and Russia have pursued a deliberate strategy of using their foreign policy and intelligence communities to copy and to steal American technologies. These strategies are starting to produce meaningful results with several foreign tech companies now legitimately rivaling U.S. tech leaders in both innovation and market capitalization.

If left unaddressed, this could pose a challenge, not only to our economic security, but also our greater national security. In January 2020, for example, a new Chinese cybersecurity law will go into effect and companies operating in the country will have no place left to hide. The new law is part of Beijing's years-long effort to expand its domestic surveillance programs and is rooted in a massive cybersecurity law adopted in 2016.

---

[1]Steve Morgan, "2019 Annual Cybercrime Report," Cybersecurity Ventures, December 2018, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (accessed November 1, 2019).
[2]Government of the United Kingdom, "Cybersecurity Breaches Survey," Department of Digital, Culture, Media, and Sport, April 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf (accessed November 1, 2019).
[3]Jack Foster, "21 Terrifying Cybercrime Statistics," VPN Geeks, 2019, https://dataconnectors.com/technews/21-terrifying-cyber-crime-statistics/ (accessed November 1, 2019).
[4]Chris Brooks, "What's the Cost of a Data Breach in 2019?" July 2019, Data Insider, https://digitalguardian.com/blog/whats-cost-data-breach-2019 (accessed November 1, 2019).
[5]Razvan Muresan, "Companies to Spend $124 Billion in 2019 on Cybersecurity," August 2018, Bitdefender, https://businessinsights.bitdefender.com/companies-spending-2019-cybersecurity-gartner (accessed November 1, 2019).

Next year, all companies—including foreign-owned companies—must arrange and manage their computer networks so that the Chinese government has access to every bit and byte of data that is stored on, transits over, or in any other way touches Chinese information infrastructure. Put simply: the Chinese government will have lawful and technical access to all digital data within its borders and perhaps to large volumes of data beyond its borders.

Companies have long known that their intellectual property (IP), trade secrets, and even their communications are highly sought by market competitors and by the Chinese government. Many of these risks are accepted as the price of doing business in Asia and, those risks that are deemed unacceptable, are mitigated by security technologies and networking strategies that attempt to hide critical information from prying eyes.

All of these technologies and strategies, under the new law, will be illegal. For example, it is currently commonplace for companies operating in China to set up virtual private networks (VPNs) on which their data and communication is stored and sent within an encrypted "pipe" that outsiders cannot crack or intercept.

These VPNs and the underlying encryption – to the degree that they prevet access by the Chinese government – will no longer be allowed. There will be no private or encrypted messages in China. No confidential data. No trade secrets. No exemptions. If a company operates in China, it will be required to operate in such a way as to provide the country's intelligence and law enforcement authorities unfettered digital access.

The days of paying the "IP tax" for access to the world's fastest growing market are over. This access will now cost you everything. And this is precisely the Chinese plan.

In a recent report,[6] former Deputy Secretary of Defense Robert O. Work captures the challenge well when he says, "Chinese technological capabilities are growing as rapidly as its economic power…. Indeed, China is keenly focused on blunting the U.S. military's technological superiority, even as it strives to achieve technological parity, and eventually technological dominance."

Put simply: our long-term economic and national security must account for—and roll back—a sustained campaign of cyber-enabled economic warfare the likes of which will take a giant leap forward in January 2020.

But we need to protect against data theft and loss at home too. This is why the United States must treat China as a national security threat to our domestic critical networks as well. As an adversarial power, China cannot be allowed to use its government-controlled companies to gain a significant foothold in any of the United States' critical government or domestic networks. Such a presence would be a clear national security threat that could decisively compromise American telecommunications and data infrastructure—including the communications integrity of the U.S. military and intelligence community.

China's intentions are clear: Beijing will, if not prevented, use the deployment of equipment,

[6]Robert O. Work and Greg Grant, "Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics," 2019, Center for a New American Security, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-final-B.pdf?mtime=20190531090041 (accessed November 1, 2019).

software, and services from Chinese state-controlled companies to compromise U.S. information networks—networks that carry significant volumes of military and intelligence data.

To that end, the Chinese government is implementing a concerted strategy of civil-military fusion through the sale and deployment of technologies and systems that enable Chinese companies with state support to siphon, store, and exploit data transmitted on these systems, and leverages these same companies as extensions of the government's intelligence and national security apparatus.

This threat demands a response. China has:

- Expedited the two-decades-old effort to meld its private and defense communities, with Chinese President Xi Jingping explaining in early 2018 that "[i]mplementing the strategy of military-civilian integration is a prerequisite for building integrated national strategies and strategic capabilities and for realizing the Party's goal of building a strong military in the new era."[7]
- Used Chinese telecommunications companies, such as Huawei, as the prototype of this civil-military fusion, where the company is not only heavily subsidized by the Chinese government, but it is also broadly accused of espionage by national security leaders in the United States, Australia, Japan, and New Zealand.[8] The United Kingdom and Germany also express grave doubts about the company's trustworthiness.[9]
- Employed aggressive national security laws. All Chinese companies are legally required to "support, assist, and cooperate with national intelligence efforts,"[10] and government intelligence agencies are legally allowed to forcibly gain access to any server or data stored within the nation's borders.[11] This means that, regardless of a company's active complicity in spying, the only safe assumption is that any information collected by Chinese companies and held on Chinese servers will be exploited by the Chinese government.

Industry remains best suited to develop and deploy the nation's information infrastructure. That does not absolve the federal government of its constitutional responsibility to provide for the common defense, protecting the people and the interests of the United States. The nation must forge a path so that these goals can be accomplished in a complementary fashion. There are some actions that the U.S. government can undertake now to start moving in the right direction and send Beijing a strong

[7]Zhou Xin, "Xi Calls for Deepened Military-Civil Integration," March 12, 2013, http://www.xinhuanet.com/english/2018-03/12/c_137034168.htm (accessed November 1, 2019).
(accessed April 8, 2018).
[8]News release, "Chinese Telecommunications Device Manufacturer and Its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice," U.S. Department of Justice, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade (accessed November 1, 2019).
[9]Huawei Cyber Security Evaluation Centre (HSEC) Oversight Board, *Annual Report*, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (accessed November 1, 2019), and Sean Keane, "US Reportedly No Longer Demands Huawei Ban from Germany," Cnet, April 9, 2019, https://www.cnet.com/news/us-reportedly-no-longer-demands-huawei-ban-from-germany/#ftag=CAD590a51e (accessed November 1, 2019).
[10]China Law Translate, "National Intelligence Law of the P.R.C.," June 27, 2017, https://www.chinalawtranslate.com/en/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E6%83%85%E6%8A%A5%E6%B3%95/ (accessed November 1, 2019).
[11]Catalin Cimpanu, "China's Cybersecurity Law Update Lets State Agencies 'Pen-Test' Local Companies," ZDNet, February 9, 2019, https://www.zdnet.com/article/chinas-cybersecurity-law-update-lets-state-agencies-pen-test-local-companies/ (accessed November 1, 2019).

message. Specifically, the Administration should:

- **Share threat information with industry.** U.S. government concerns about Chinese technologies and related services cannot be expressed exclusively in classified or other constrained environments. If the U.S. government wants industry to operate in ways that do not provoke national security concerns or make them worse, the government must share its telecommunications security concerns in a detailed and broadly sharable manner.
- **Determine disqualifying factors.** The U.S. government should clearly communicate with industry and with America's foreign partners and allies, as well as the Chinese, which legal frameworks, activities, and business practices will result in exclusion from U.S. 5G infrastructure, services, and other emerging-technology integrations. Further, the U.S. should encourage other nations to adopt these standards as a way of maintaining pressure on countries and companies working against U.S. and allied interests.
- **Block vulnerabilities.** The U.S. should block any foreign technology from U.S. markets that creates vulnerabilities in critical infrastructure or that provides hostile foreign actors with "backdoors" to U.S. data. Doing this will impose significant pressure on China and others to improve poor security practices and it will spur domestic security research in the U.S. that will incrementally improve the safety of the hardware and software supply chains into the United States. The U.S. should encourage the remaining four Five Eyes countries—Australia, Canada, New Zealand, and the United Kingdom—to implement similar exclusionary measures.
- **Block untrusted companies.** The Committee on Foreign Investment in the United States should block foreign companies from U.S. investments if they have a history of producing hardware or software with known vulnerabilities. This would be especially helpful in mitigating the challenge of Chinese investment in, and purchase of, American start-ups that might embrace poor security practices in return for rapid access to capital.
- **Prepare for "zero-trust" networks.** Currently, Huawei controls approximately 30 percent of the global mobile communications market and could win as much as 50 percent of the global 5G market. Even if the U.S. is able to secure its own wireless networks from foreign spying and interference, the vast majority of networks around the world will be developed and managed by the Chinese. This requires the U.S. defense and intelligence communities to begin mitigating this threat and developing new networking strategies that will allow the U.S. to operate and thrive in a "zero-trust" environment—meaning operating on networks that are owned and managed by China or other hostile actors. While it is too soon to cede 5G to U.S. challengers, it is prudent to begin preparing for worst-case scenarios.

Finally, it is not just companies who are being attacked and it is not just IP that is being stolen.

3. Ransomware Attacks Against Companies and Governments

The third and final cybersecurity trend that must be turned around is the growing use of ransomware against enterprises and governments.

Ransomware is any malicious software that limits or prevents someone from using their computer or accessing their files and, in 2017, this threat went to a whole new level. In the wake of a 4.3 percent growth in ransomware variations—including the WannaCry and NotPetya attacks that went global—

at least 15 percent of business in the top 10 industry sectors were infected and nearly a third of those affected were locked out of their systems for five or more days.

When it was all said and done, global ransomware attacks cost individuals and business $5 billion in 2017, a 400 percent increase from the year before. But now these attacks are taking an unexpected turn towards governments.

In 2019, there have been more than 70 ransomware attacks on state, local, and county governments—including Florida, Georgia, Maryland, and a coordinated attack on 22 Texas cities and towns. Several of these attacks have led to catastrophic loss of data and equipment and all of them have temporarily crippled the provision of critical services. These attacks on governments now constitute more than 60 percent of all U.S. ransomware attacks this year.[12]

These three trends cannot be ignored. Even more, they must be rolled back if the United States wants to thrive in the future.

I thank the committee for the opportunity to testify and I look forward to your questions.

* * * * * * * * * * * * * * * * * * *

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2018, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2018 operating income came from the following sources:

Individuals 67%
Foundations 13%
Corporations 2%
Program revenue and other income 18%

The top five corporate givers provided The Heritage Foundation with 1% of its 2018 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

[12]Andrew G. Simpson, "Putting Municipal Ransomware Attacks – And Cyber Insurance – In Context," Insurance Journal, September 2019, https://www.insurancejournal.com/news/national/2019/09/03/538635.htm (accessed November 1, 2019); Bobby Allyn, "22 Texas Towns Hit with Ransomware Attack in 'New Front' of Cyber Assault," National Public Radio, August 2019, https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault (accessed November 1, 2019); and Joe Panettieri, "Ransomware Attack List: Cities, Municipalities, and Government Agencies," MSSP Alert, July 2019, https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/attack-list-cities-government-agencies/ (accessed November 1, 2019).