Department of Justice

STATEMENT OF

ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"DANGEROUS PARTNERS: BIG TECH AND BEIJING"

PRESENTED

MARCH 4, 2020

STATEMENT OF
ADAM S. HICKEY
DEPUTY ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"DANGEROUS PARTNERS: BIG TECH AND BEIJING"

PRESENTED
MARCH 4, 2020

Good afternoon Chairman Hawley, Ranking Member Whitehouse, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the Department of Justice regarding the threats that foreign adversaries pose to our information security, the vulnerabilities that can arise from doing business in those nations or with companies they can control, and the national security implications of an increasingly integrated internet.

The Department's leadership has identified these issues as priorities. Attorney General Barr has emphasized the importance of cybersecurity, having spoken publicly about the risks our telecommunications sector faces, especially from China, and personally announced charges against Chinese military hackers. Prior to that, in February 2018, then-Attorney General Sessions established a Cyber-Digital Task Force to canvass how the Department combats the global cyber threat and to identify how law enforcement can more effectively accomplish its mission in this area. The Task Force's July 2018 report[1] did just that, and I will draw from it in my testimony today.

Below I will outline some of the threats we have identified, particularly from foreign nation-states, and how we have responded through our investigations and other operational work, before going on to describe some of the legislative changes that, we believe, would help us better confront them.

[1] U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE (2018), https://www.justice.gov/ag/page/file/1076696/download [hereinafter *Report*].

I. Cyber Threats from Foreign Nation States

A. State-Sponsored Intrusions

Beginning in 2012, the Department's National Security Division shifted our approach to malicious cyber activity sponsored by foreign nation states. Applying the rationale that all tools of government power should be brought to bear on national security threats, we began opening criminal investigations of state-sponsored computer intrusions and attacks, with the intention of identifying, charging, arresting, prosecuting, and otherwise disrupting those responsible according to the same Principles of Federal Prosecution that apply in other, purely criminal contexts. We took this approach based on lessons learned from the counter-terrorism and counter-espionage contexts, where our objectives include a mix of intelligence collection and detection, disruption of illegal activity, and deterrence, and law enforcement has proven effective at those ends, especially when combined with other Executive Branch efforts. Since then, our investigations have exposed a number of disturbing trends.

First, China, in particular, has for years sponsored computer intrusions to steal trade secrets and other confidential business information from American companies (among others) for the apparent benefit of its own industries, to give them a competitive advantage or to advance its military:

- In 2014, for example, a grand jury in Pittsburgh, Pa., indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries. According to the indictment, the defendants conspired to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs), including trade secrets, communications about business strategy, cost and pricing information, and litigation strategy.[2]
- Later that year, Su Bin, a Chinese engineer, was arrested in Canada at the Department's request, on charges that he conspired with Chinese military officers to target U.S. defense contractors in order to steal military technical data related to aircraft. Su used his expertise to advise the military officers which companies to target, what files to steal, and why it was significant. (He was ultimately sent to federal court in Los Angeles, Cal., where he pled guilty and was sentenced to prison.)[3]
- In October 2018, a San Diego, Cal., grand jury indicted Chinese intelligence officers, among others, on charges of conspiring to steal turbofan technology used in U.S. and

[2] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[3] Press Release, U.S. Dep't of Justice, Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison (July 13, 2016), https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

European commercial airliners. According to the charges in that case, the defendants relied on computer hackers to infiltrate company networks, but they were assisted by employees of a victim company who were working in China and who are accused of facilitating the computer intrusions.[4]

- And in December 2018, the Department unsealed charges in Manhattan, N.Y., against two Chinese nationals accused of working in association with a Chinese intelligence service (the Ministry of State Security) in a global campaign of computer intrusions targeting managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world. According to the charges, the conspiracy targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production.[5] That activity violated China's 2015 commitment to stop stealing trade secrets and other confidential business information through computer hacking "with the intent of providing competitive advantages to companies or commercial sectors."[6]

As we have spoken about in other forums, breaches like these (as well as trade secret thefts committed by company insiders) leach hard-earned intellectual property from American firms, unjustly enrich Chinese firms, and, at scale, threaten our economic security.[7]

Second, China has also targeted large stores of personally identifiable information (PII), personal health information (PHI), and the like. In February, an Atlanta, Ga., grand jury indicted four Chinese military hackers on charges of hacking into the computer systems of the credit

---

[4] Press Release, U.S. Dep't of Justice, Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years (Oct. 30, 2018), https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal.

[5] Press Release, U.S. Dep't of Justice, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018), https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[6] Deputy Attorney General Rod J. Rosenstein, U.S. Dep't of Justice, Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers (Dec. 20, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers.

[7] *China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses Before the S. Comm. on the Judiciary*, 115th Cong. 2 (2018) (statement of John C. Demers, Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Justice), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/ 2018/12/18/12-05-2018_john_c._demers_testimony_re_china_non-traditional_espionage_against_the_united_states_the_threat_and_potential_policy_responses.pdf.

reporting agency Equifax in 2017, where, according to the indictment, they stole names, addresses, birthdates, and social security numbers belonging to nearly half of all American citizens (and driver's license numbers belonging to millions).[8] As the Attorney General said in announcing the charges, this data breach was "of a piece with other Chinese illegal acquisitions of sensitive personal data," including the theft of personnel records from the U.S. Office of Personnel Management.[9] Bulk thefts of sensitive personal data like these can support China's development of artificial intelligence tools as well as aid their intelligence services in targeting U.S. government employees and those they work with.

The Department has been increasingly concerned about the national security consequences of sensitive personal data falling into our adversaries' hands. For a few reasons, the theft of PII, PHI, locational data, electronic communications, and the like is more than an inconvenience and can present more than a risk of criminal identity theft or embarrassment to an individual victim. First, there is vastly more information about us and our habits stored online than there ever was before, and with the proliferation of connected devices, the volume of that information will continue to increase exponentially.[10] Second, while any individual piece of consumer data is probably not a national security secret, a mosaic of personal information can enable computer hackers and intelligence officers alike to better target us, by guessing our passwords, tricking us into responding to a phishing request, or, more darkly, exploiting our weaknesses, fears, or ambitions. Third, the extent to which we are connected to each other (online and otherwise) means that information about people who do not themselves know national security or corporate secrets (perhaps our friends and relatives) can be exploited to target those of us who do. And, fourth, as recent studies have shown,[11] even masked or purely transactional information, when collected in bulk, can be very revealing when mined and analyzed.[12]

---

[8] Press Release, U.S. Dep't of Justice, Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

[9] Attorney General Barr, U.S. Dep't of Justice, Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

[10] According to an annual report released in February 2019, overall global internet traffic was 2,000 gigabytes (GB) per second in 2007, 46,600 GB per second in 2017, and is projected to be 150,700 GB per second in 2022. Cisco, Visual Networking Index: Forecast and Trends, 2017-2022 5 (2019), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf.

[11] *See, e.g.*, Stuart A. Thompson & Charlie Warzel, *One Nation, Tracked: An Investigation into the Smartphone Tracking Industry from Times Opinion*, N.Y. TIMES, Dec. 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; Yves-Alexandre de Montijoye, *et al.*, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, SCIENCE, Jan. 30, 2015, at 536-39, https://science.sciencemag.org/content/347/6221/536/tab-pdf.

[12] Accordingly, the Department was pleased to support Congress's recent expansion of authority of the Committee on Foreign Investment in the United States (CFIUS), by the Foreign Investment Risk Review and Modernization Act of 2018 (FIRRMA), to consider investments in U.S. businesses that maintain or collect sensitive

All too often, privacy is spoken about as if it is a value opposed to law enforcement. But, in fact, our prosecutions vindicate the right to privacy, whether it is the right of a company to control who has access to its trade secrets; or the expectation of privacy we have in our e-mail communications and medical records. When a company faces retaliation through exposure of its internal communications, a political campaign's e-mails are hacked and dumped, or an Olympic athlete's medical records are exposed online, we will respond to these violations of privacy, both by investigating and charging those responsible (as we have in all of those situations) and by working to mitigate the harm (such as by working with providers and foreign law enforcement in countries where the stolen information is hosted to facilitate takedown requests).

It is troubling, however, that our efforts to hold nation states and ordinary criminals alike accountable for their violations of privacy (among other crimes) are increasingly stymied by providers that seem determined to frustrate law enforcement access, not just to prevent unauthorized intrusions by bad actors. To be sure, the increasing prevalence of encryption has raised the baseline of protection and privacy we all enjoy, and it has been a net social benefit. As the Attorney General has observed, encryption "provides enormous benefits to society by enabling secure communications, data storage, and on-line transactions," and "[b]ecause of advances in encryption, we can now better protect our personal information; more securely engage in e-commerce and internet communications; obtain secure software updates; and limit access to sensitive computers, devices, and networks."[13] But encryption, like other decisions requiring tradeoffs between functionality and security, is not an all-or-nothing proposition. In the Department of Justice's opinion, in some circumstances, companies have gone well past the point of ensuring, to a high degree of confidence, that unauthorized outsiders cannot compromise the security of your communications, choosing instead to blind both themselves and law enforcement officials attempting to execute court-authorized warrants to the malicious activity occurring on their platforms. In the United States, that decision might qualify as a marketing opportunity. Yet, some of these same companies willingly accommodate the demands of authoritarian regimes by relocating data centers to enable warrantless, bulk surveillance; disabling features and applications used by pro-democracy advocates; and otherwise catering to

---

personal data of United States citizens that may be exploited in a manner that threatens national security. In regulations implementing this authority, CFIUS defined "sensitive personal data" for purposes of its jurisdiction by describing categories of identifiable data that could potentially implicate national security, including financial data that could be used to analyze or determine an individual's distress or hardship, consumer report information, insurance applications, health information, non-public electronic communications, geolocation data, biometric data, government identification information, security clearance status, government employment applications, and genetic tests. 85 Fed. Reg. 3112, 3132 (Jan. 17, 2020) (to be codified at 31 C.F.R. pt. 800.241(a)(1)(ii)). These categories reflect some of the most sensitive types of data that could be used to target individuals in ways that threaten national security. We look forward to working with other members of CFIUS to review qualifying foreign investments with an eye towards protecting national security by safeguarding Americans' sensitive personal data.

[13] Attorney General William P. Barr, U.S. Dep't of Justice, Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security (July 23, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

the whims of the politically powerful, where doing so is a pre-requisite for market access.[14] Their systems design, in other words, reflects a business decision, not an immutable principle. As the Attorney General has said about engaging with the private sector on this issue, it is well past time for the tech community to "abandon the indefensible posture that a technical solution is not worth exploring, and instead turn their considerable talent and ingenuity to developing products that will reconcile good cybersecurity to the imperative of public safety and national security."[15]

B. The Rule of Law

China is not limited to using intelligence and military officers and their proxies to hack U.S. systems. The legal environment in China—the authorities the Communist Party can bring to bear on Chinese companies and individuals to cooperate, combined with the government's failure to honor its commitments or to respect the rule of law and legal process more generally—has grave implications for trusting Chinese companies beholden to that political party for success.

Starting in 2014, the Chinese Communist Party began enacting an interrelated package of national security, cyberspace, and law enforcement legislation. They include the 2014 Counterespionage Law, the 2015 National/State Security Law, the 2015 Counterterrorism Law, the 2016 Foreign Non-Governmental Organization Law, the 2017 Cybersecurity Law, and the 2017 National Intelligence Law, and most recently, the 2019 Cryptography Law. Together, these laws reflect President Xi Jinping's effort to transform Chinese national and state security in accordance with his vision of the "China Model."[16] While some of the provisions of these laws could support legitimate, defensive national security activities, the 2017 Cybersecurity Law and the 2017 National Intelligence Law, in particular, impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for Beijing's intelligence gathering activities. Other provisions, such as those contained in the 2019 Cryptography Law, impose requirements that will expose commercial encryption used within China to testing and certification by the Chinese government, potentially facilitating those same intelligence activities.

---

[14] *See, e.g., Apple Stores Russian Users' Personal Data Locally, Filing Shows*, BLOOMBERG, Feb. 5, 2019, https://www.themoscowtimes.com/2019/02/05/apple-stores-russian-users-personal-data-locally-filing-shows-a64395; Paul Moser et al., *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES, July 12, 2017, https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html; Olga Razumovskaya, *Google Moves Some Servers to Russian Data Centers*, WALL ST. J., Apr. 10, 2015, https://www.wsj.com/articles/google-moves-some-servers-to-russian-data-centers-1428680491.

[15] Attorney General William P. Barr, U.S. Dep't of Justice, Attorney General William P. Barr Delivers Remarks at the Lawful Access Summit (Oct. 4, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit.

[16] Remarks, Dr. Christopher Ashely Ford, Assistant Secretary, Department of State, *Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications,* (Sept. 11, 2019), https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/.

Article 28 of the 2017 Cybersecurity Law states, "[n]etwork operators *shall* provide technical support and assistance to public security organs and national security organs that are safe guarding national security and investigating criminal activities in accordance with the law."[17] Article 7 of the 2017 National Intelligence Law states explicitly, "[a]ny organization and citizen *shall* support, assist, and cooperate with the state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work."[18] Article 26 of the 2019 Cryptography Law requires any "[c]ommercial cryptography products that involve national security, the national welfare and the people's livelihood, or the societal public interest" to be tested and certified by Chinese government authorities, pursuant to the relevant provisions of the 2017 Cybersecurity Law.[19] None of these laws provide much, if any, detail about legal procedures or judicial oversight available to challenge Chinese government demands. These laws are not merely defensive in nature: they enable the Chinese government to make affirmative demands on its people and entities to advance the Communist Party's interest.

While it demands obedience to the law from its firms – as well as foreign firms that choose to operate within its borders – on the one hand, the Chinese government has demonstrated a willingness to break its commitments and disregard *our laws*, on the other. In 2015, China and the United States agreed to cooperate with requests to investigate computer crime, collect electronic evidence, and mitigate malicious cyber activity emanating from their respective territories. Yet in 2017, when the Department invoked that commitment to request assistance in connection with an investigation of a purported Internet security firm for trade secret theft, we received no meaningful response.

Since 2001, the United States and China have had a Mutual Legal Assistance Agreement (MLAA). The Agreement creates an obligation, after one country makes a request to the other, to share evidence and provide other assistance "in investigations, in prosecutions, and in proceedings related to criminal matters." Over the past 10 years, however, China has rarely produced bank records or similar business transactional records pursuant to the United States' MLAA requests. In the few cases where China produced records, they were incomplete, untimely, or inadmissible.[20] On the other hand, when we exercise our authorities as federal prosecutors to compel businesses located here to produce records, the Chinese government threatens them not to comply, on pain of sanctions under their laws.[21] And when a foreign government cooperates with the United States, in our effort to vindicate our laws and protect our

[17] Keynote Remarks, William Evanina, Director, National Counterintelligence and Security Center, International Legal Technology Association (ILTA) LegalSEC Summit 2019, June 4, 2019, https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf.

[18] *Id.*

[19] *See* Economics and Trade Bulletin (U.S.-China Econ. and Sec. Review Comm'n) Nov. 5, 2019, at 13, https://www.uscc.gov/sites/default/files/2019-11/November%202019%20Trade%20Bulletin.pdf. For an unofficial English-language translation, *see, e.g.,* China Law Translate, Cryptography Law of the P.R.C. (2019), https://www.chinalawtranslate.com/en/cryptography-law/ (accessed Feb. 20, 2020).

[20] As the U.S. District Court in Washington, D.C., recently observed in litigation seeking to compel the production of bank records from three Chinese banks, "based on past practice, China's preferred MLAA procedure would likely be futile." *In re Sealed Case*, 932 F.3d 915, 921 (D.C. Cir. 2019) (summarizing district court's findings).

[21] *Id.* at 933.

people, that government may face threats and reprisals from China, such as economic pressure or even the detention of its nationals on trumped-up charges.

For these reasons, among others, the Department has been sounding the alarm about Chinese providers that are ultimately subject to direction or control by the Communist Party. All too often we talk about the security of a product or service in a simplistic way: whether there is proof that a company has already conducted illicit surveillance, for example. But if we wait for a smoking gun in this context, we might get shot.

Whether a company has a culture that promotes theft, dishonesty, or obstruction of justice is just as relevant, because it tells you how the company will behave when it suits its interests. And that is all the more true if the company operates in a legal environment, like China's, where success depends on cooperation with the authorities, no matter how sweeping or illegal their requests. As the Attorney General wrote to FCC Chairman Ajit Pai late last year, urging the FCC to designate Huawei and ZTE as threats to the telecommunications supply chain that are ineligible for FCC programs, "Surely a willingness to break U.S. law combined with a determination to avoid the consequences by obstructing justice argues against the reliability of a provider."[22]

Our cases show that the Chinese government will use the employees of Chinese companies doing business here, and Chinese employees of foreign companies in China, to engage in illegal activity. Last year, for example, a former airline ticket counter agent pleaded guilty to acting as an agent of the Chinese government, without notification to the Attorney General, by working at the direction and control of military officers assigned to China's Mission to the United Nations. During her employment at JFK airport in New York for a Chinese Air Carrier, she accepted packages from PRC military officers, and placed those packages aboard flights to China as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. She encouraged her coworkers to assist the military officers, telling them that, because the Air Carrier was a Chinese company, their primary loyalty should be to China. But covertly doing the Chinese military's bidding on U.S. soil is a crime, and the defendant and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight, violating TSA regulations.[23]

This record—of intent, capability, and practice of exploiting access to U.S. systems; and of violating our laws and refusing to honor commitments—has led this Administration to take unprecedented steps to protect our critical infrastructure. In July 2018, for example, the Executive Branch recommended that the FCC deny an application for a license to offer

---

[22] Letter from Att'y Gen. William Barr to the Hon. Ajit Pai, Chairman, Fed. Commc'ns Comm'n (Nov. 13, 2019) https://ecfsapi.fcc.gov/file/11130351518674/Attorney%20General%20Letter%20FCC%20Docket%2018-89.pdf.

[23] Press Release, U.S. Dep't of Justice, Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government (Apr. 17, 2019), https://www.justice.gov/opa/pr/former-manager-international-airline-pleads-guilty-acting-agent-chinese-government.

international telecommunications services in the United States. The applicant was a subsidiary of China Mobile Communications Corporation (a Chinese state-owned enterprise and the world's largest mobile carrier). The Justice Department led the national security and law enforcement review of the application, and the Executive Branch's recommendation highlights the risks of granting a Chinese SOE common carrier status and, with it, access to trusted, peering relationships with American carriers.[24]

We considered a number of factors, including whether the applicant's planned operations would provide opportunities

- to disrupt our communications infrastructure;
- to enable economic espionage; or
- to undermine authorized law enforcement or national security missions.

Because China Mobile is subject to exploitation, influence, and control by the Chinese government, we advised the FCC that granting China Mobile's application would pose unacceptable national security and law enforcement risks. And we were gratified when the FCC accepted that recommendation and denied the application, in May 2019.

Cases like China Mobile have brought home to the Department how important our foreign investment review work is to protecting our equities in law enforcement, counterintelligence, and telecom security.

- That is why, during the first two years of this Administration, we co-led more CFIUS reviews than in the five years before that, combined.
- That is why we have renamed the staff that conducts these reviews to be a "Section," and reorganized its management structure, to match other operational components of NSD.
- And that is why the President's FY2020 budget for the Department significantly increased the staff and other resources devoted to this work; an increase, fortunately, that Congress approved.

To be clear, China is not the only country whose political and legal environment presents a challenge. As we found during an investigation of a software company that performed contract work for the Defense Department, even an American firm can present risks, depending on where it performs critical functions. In that case, the vendor used a Russian back office to code software intended for a classified network. But under a legal regime known as the Russian System of Operative-Investigative Measures ("SORM"), that software was subject to collection by Russia's Federal Security Service (the "FSB"), raising a risk that the FSB could gather

[24] The Department was also pleased to support the President's Executive Order, *Securing the Information and Communications Technology and Services Supply Chain*, No. 13873 (May 15, 2019), and looks forward to working with the Department of Commerce to implement it.

information about our defense networks.[25] Similarly, the Department of Homeland Security barred federal agencies from using Kaspersky anti-virus software, because it was concerned about the ties between Kaspersky officials and Russian intelligence, and because Russian law allows Russian intelligence agencies to request or compel assistance from Kaspersky, and to intercept communications on Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicated U.S. national security.[26]

II. New Ideas to Combat Cyber Threats

In the face of these disturbing and ever-increasing threats, I know the Subcommittee has on its mind a key question: How can Congress help, today? The good news is that, as the Attorney General's Cyber-Digital Task Force concluded, there are several key changes to Federal law that would greatly aid our work to combat threats online.

A. Data Breach Notification

In 2018, the White House's Council of Economic Advisors observed that most data breaches are not reported to the U.S. government.[27] This reluctance may be driven by a fear of regulatory action, of reputational harm, or of an interruption to business operations. The reluctance of organizations and businesses to disclose that they have been attacked constitutes a major challenge for the U.S. government in its battle against cybercrime. Law enforcement cannot be effective without the cooperation of crime victims. A lack of cooperation may not only prevent discovery of evidence that could lead to identifying and holding the threat actors accountable, but also creates barriers to fully understanding the threat environment.

---

[25] Press Release, U.S. Dep't of Justice, National Security Division Announces Agreement with Netcracker for Enhanced Security Protocols in Software Development (Dec. 11, 2017), https://www.justice.gov/opa/pr/national-security-division-announces-agreement-netcracker-enhanced-security-protocols. As a result of our investigation, which we resolved without criminal charges, the vendor (Netcracker Technology Corp. (NTC)) agreed to implement an Enhanced Security Plan to increase information security by regulating remote access by Netcracker to its clients' U.S. networks and transfers of sensitive data therefrom. We believe the Enhanced Security Plan (which can be accessed through the above link) is a model of good security practices: it requires Netcracker to use U.S.-based infrastructure to provide certain services to U.S.-based clients; obtain prior, written consent from U.S.-based clients before remotely accessing their networks; and avoid transferring certain categories of sensitive client data outside the U.S. without taking certain precautions. In addition, Netcracker was required to engage an auditor to ensure compliance with the Enhanced Security Plan. Based on our direct engagement with the company as well as external information and analysis to-date, we believe Netcracker has so far complied with its obligations under the agreement.

[26] Press Release, U.S. Dep't of Homeland Sec., DHS Statement on the Issuance of Binding Operational Directive 17-01 (Sept. 13, 2017), https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

[27] "The Cost of Malicious Cyber Activity to the U.S. Economy," COUNCIL OF ECON. ADVISORS, EXEC. OFFICE OF THE PRESIDENT, at 33 (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

The Department has been actively evaluating statutory data breach notification requirements. Currently, there is no federal reporting requirement or standard. All 50 States have enacted separate notification laws setting standards governing notification by private entities when a data breach occurs, and companies must navigate and comply with the varying requirements in multiple jurisdictions. In the wake of recent high-profile data breaches exposing Americans' personal information, there is revived interest in national notification requirements.

As you and your colleagues consider a national data breach standard, we would urge you to follow the model of many State statutes and include a requirement to promptly notify law enforcement in addition to, and in advance of, notification of impacted consumers. Government notification would increase Federal law enforcement's ability to pursue hackers and prevent data breaches. The Administration is actively working on proposed legislation, and we look forward to working with Congress on this important issue.

B. Deterring Insider Threats

I would like to spend the balance of my time today focusing on areas of concern in the Computer Fraud and Abuse Act ("CFAA") and related statutes that currently hamper our work to combat threats online. The CFAA is the primary Federal law against hacking. It protects the public against criminals who intrude into computers to steal information, install malicious software, and delete files. It was also intended to criminalize malicious conduct by insiders who abuse their right of access to computer systems and networks to commit online crime. The CFAA, in short, reflects our baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The CFAA was enacted in 1986, at a time when the problem of online crime was still in its infancy. Over the years, Congress has enacted a series of measured, modest changes to the CFAA to encompass new technologies and to equip law enforcement to respond to changing threats. The CFAA has not been amended since 2008, however, and the intervening years have again witnessed the need for the enactment of modest, incremental changes. The CFAA needs to be updated to make sure that it continues to appropriately deter violations of Americans' privacy and security.

At its core, the CFAA is a privacy statute, because it deters criminals from stealing peoples' information. Yet, the CFAA's privacy protections now contain a significant gap. The statute was meant to apply both to hackers who gain access to victim computers without authorization from halfway around the world, and to so-called "insiders" who have some authorization to access a computer — like company employees entitled to access a sensitive database for specified work purposes — but who intentionally abuse that access. The part of the CFAA that covers the conduct of those who have some authorization to access a computer is the tool that Department prosecutors have used to charge, for example, police officers who misuse their access to confidential criminal records databases in order to look up sensitive information about a boyfriend or girlfriend, who sell access to private records to others, or who provide

confidential law enforcement information to a charged drug trafficker. As a recent survey of 472 cybersecurity professionals indicated, 90% percent of organizations feel vulnerable to insider attacks, and 53% have confirmed insider attacks against their organization in the previous 12 months. The survey also found that the type of data most vulnerable to insider attacks is confidential business information, and that a plurality of those surveyed estimated that the potential cost/loss of an insider attack was between $100,000 and $500,000.[28]

Unfortunately, recent judicial decisions have limited the Government's ability to prosecute such cases. As a result, in circuits covered by these decisions, insiders cannot be charged under the CFAA — even where the insider has intentionally exceeded the bounds of his legitimate access to confidential information and has caused significant harm to his employer and to the people, often everyday Americans, whose data he has improperly accessed.

The insider threat is relevant to voting security. Currently, for example, if a foreign hacker accessed a State's voter registration database over the Internet, that could be charged under the CFAA as an access "without authorization." But if an insider, such as a State government employee, used his privileges to access the same information, that insider could not be prosecuted under the CFAA, at least as several courts have interpreted the statute.

The narrow judicial interpretation of the term "exceeds authorized access" in the CFAA stems from concerns that the statute potentially makes relatively trivial conduct a Federal crime. We understand the concerns of the courts, and I would like to reiterate that the Department of Justice has no interest in prosecuting harmless violations, to the extent that the statute could be construed to cover them.

However, by essentially barring CFAA prosecutions of insiders in certain circuits, these court decisions have constrained our ability to bring certain cybercriminals to justice. Over the last several years, numerous Department of Justice officials have called on Congress to address this issue in a manner that would maintain the law's key privacy-protecting function, while providing further reassurance that trivial violations of things like a website's terms of service will not be prosecuted as Federal crimes.

The Department supports efforts that would accomplish this task. This can be done by reaffirming that the definition of "exceeds authorized access" includes the situation where the person accesses the computer for a purpose that he knows is not authorized by the computer owner. Such an amendment is necessary to ensure the nationwide ability to prosecute, for example, a law enforcement officer who is permitted access to criminal records databases, but only for official business purposes. At the same time, a legislative fix could add further limitations that reflect the statute's focus. For example, a limitation could be put into the CFAA making clear that in order to constitute a crime under the new insider provision, not only must an offender access a protected computer in excess of authorization and obtain information, but the information must be worth $5,000 or more, the access must be in furtherance of a separate felony

[28] CROWD RESEARCH PARTNERS, INSIDER THREAT REPORT (2018), http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf.

offense, or the information must be stored on a government computer.

We strongly believe that the insider threat problem in the CFAA can be fixed in a way that empowers the Department to prosecute and deter significant threats to privacy and security and further assures that prosecutions will remain focused on such crimes. Of all of the reforms to the CFAA under consideration by this Subcommittee, addressing this problem would have the most immediate, significant impact in improving our ability to punish and deter cybercriminals. We would like to work closely with Congress and, specifically, this Subcommittee, to find a way forward on this pressing issue.

C. Certain Malicious Activities as RICO Predicates

We support the efforts to update the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make CFAA offenses and certain Wiretap Act offenses subject to RICO as was proposed in the International Cybercrime Prevention Act ("ICPA"), which was sponsored by Senator Graham and the Ranking Member in the last Congress. As computer technology has evolved, it has become a key tool of organized crime. Criminal organizations operating around the world hack into public and private computer systems, including systems key to America's national security and defense. They hijack computers to steal Americans' identity and financial information; they extort American businesses with threats to disrupt computers; and they commit a range of other online crimes.

Accordingly, much of the fight against transnational organized crime has moved online. Federal prosecutors have used RICO for over forty years to prosecute organized criminals ranging from mob bosses to Hells Angels to members of MS-13. Just as RICO has proven to be an effective tool to prosecute the leaders of these organizations who may not have been directly involved in committing the underlying crimes, it should be a tool to fight criminal organizations that use computer intrusions and other CFAA violations to further their schemes. These changes, as proposed in ICPA, would simply make clear that all types of CFAA violations should be considered criminal activities under the RICO statute, with the associated heavy penalties.

D. Protecting Election Computers from Attack

Protecting election infrastructure from attack is another important goal. Yet, as the Department's recent Cyber-Digital Task Force report noted, "should hacking of a voting machine occur, the government would not, in many conceivable circumstances, be able to use the CFAA to prosecute the hackers."[29] The CFAA's current definition of "protected computer" includes computers "affecting interstate or foreign commerce," a definition that attempts to encompass the breadth of congressional power under the Commerce Clause. We are concerned that courts might conclude that the Commerce Clause power, alone, does not reach voting machine computers that are not used in a commercial setting, are not used in interstate communication, and are typically never connected to the Internet or to any other network.

[29] *Report*, *supra* note 1.

The Department and each of its components has consistently recognized the primacy of State and local jurisdictions in the administration and policing of electoral processes under Article I, Section 4, of the Constitution. Accordingly, the Department remains committed to its longstanding policy in criminal law enforcement against operations, actions, or public statements that would interfere with State and local election administration, or appear to do so. Nevertheless, the Constitution in that same Section also provides for a federal role in regulating elections that include federal candidates on the ballot, and we believe that this provision provides additional support for an amendment that would cover election-related hacking.

Expanding the definition of a protected computer to include electronic voting machines will strengthen confidence in the integrity of our electoral system and ensure that any attempts to manipulate the results of an election can be prosecuted to the fullest extent under Federal law. We therefore applaud the Senate's passage of the Defending the Integrity of Voting Systems Act last year, which would accomplish this important goal.

E. Botnets

Another striking example of online crime that victimizes Americans is the threat from botnets — networks of victim computers surreptitiously infected with malicious software, or "malware." Once a computer is infected with malware, it can be controlled remotely from another computer with a so-called "command and control" server. Using that control, criminals (including nation-state actors) can steal usernames, passwords, and other personal and financial information from the computer user, or hold computers and computer systems for ransom. Criminals can also use armies of infected computers to commit other crimes, such as DDoS attacks, or to conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation.

The scale and sophistication of the threat posed by botnets is increasing every day. Individual hackers and organized criminal groups are using state-of-the-art techniques to infect hundreds of thousands — sometimes millions — of computers and cause massive financial losses, all while becoming increasingly difficult to detect. If we want security to keep pace with criminals' technological innovations, we need to ensure that we have a variety of effective tools to combat rapidly evolving cyber threats like these.

One powerful tool that the Department has used to disrupt botnets and free victim computers from criminal malware is the civil injunction process. Current law gives Federal courts the authority to issue injunctions to stop the ongoing commission of certain crimes by authorizing actions that prevent a continuing and substantial injury. This authority played a critical role in the Department's successful disruption of the Coreflood botnet in 2011 and of the Gameover Zeus botnet in 2014. (The Gameover Zeus botnet, which infected computers worldwide, inflicted over $100 million in losses on American victims alone, many of them small- and medium-sized businesses.) Because the criminals behind these particular botnets used them to commit fraud against banks and bank customers, existing law allowed the

Department to obtain court authority to disrupt the botnets by taking actions such as disabling communications between infected computers and the command and control servers.

The problem is that current law permits courts to consider injunctions only for limited categories of crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity. They can be used to steal sensitive corporate information, to harvest email account addresses, to hack other computers, or to execute denial of service attacks against websites or other computers. Yet — depending on the facts of any given case — these crimes may not constitute fraud or illegal wiretapping. In those cases, courts may lack the statutory authority to consider an application by prosecutors for an injunction to disrupt the botnets in the same way that injunctions were successfully used to incapacitate the Coreflood and Gameover Zeus botnets.

Thus, we support the provision in ICPA that would add activities like the operation of a malicious botnet to the list of offenses eligible for injunctive relief. ICPA would allow the Department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked. This numerical threshold focuses the injunctive authority on enjoining the creation, maintenance, operation, or use of a malicious botnet, as well as other widespread attacks on computers using malicious software (such as ransomware).

The same legal safeguards that currently apply to obtaining civil injunctions, and that applied to the injunctions obtained by the Department in the Coreflood and Gameover Zeus cases, would also apply under the ICPA proposal. Before an injunction is issued, the Government must civilly sue the defendant and demonstrate to a court that it is likely to succeed on the merits of its lawsuit and that the public interest favors an injunction; the defendants and enjoined parties have the right to notice and to have a hearing before a permanent injunction is issued; and the defendants and enjoined parties may move to quash or modify any injunctions that the court issues.

I would now like to turn to the criminal statutes that prohibit the creation and use of botnets. Unfortunately, these statutes also contain shortcomings. We find that criminals continue to find new ways to make money illegally through botnets. Law enforcement officers now frequently observe that creators and operators of botnets not only use botnets for their own illicit purposes, but also sell or even rent access to the infected computers to other criminals.

Current criminal law prohibits the *creation* of a malicious botnet because it prohibits hacking into computers without authorization. It also prohibits the *use* of botnets to commit other crimes. But it is not similarly clear that the law prohibits the *sale* or *renting* of a botnet. In one case, for example, undercover officers discovered that a criminal was offering to sell a botnet consisting of thousands of victim computers. The officers accordingly "bought" the botnet from the criminal and notified the victims that their computers were infected. The operation, however, did not result in a prosecutable U.S. offense because there was no evidence that the seller himself had created the botnet in question. While trafficking in botnets is sometimes chargeable under other subsections of the CFAA, this problem has resulted in, and

will increasingly result in, the inability to prosecute individuals selling or renting access to thousands of hacked computers.

We believe that it should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already clearly illegal to sell or transfer computer passwords. That is why we support the provision in ICPA to prohibit the sale or transfer not only of "password[s] and similar information" (the wording of the existing statute) but also of "means of access," which would include the ability to access computers that were previously hacked and are now part of a botnet. In addition, we recommend replacing the current requirement that the Government prove that the offender had an "intent to defraud" with a requirement to prove that the offender not only knew his conduct is "wrongful," but also that he knew or should have known that the means of access would be used to hack or damage a computer. This last change is necessary because, as noted above, criminals do not use botnets only to commit fraud — they also use them to commit a variety of other crimes.

Some commentators have raised the concern that this proposal would chill the activities of legitimate security researchers, academics, and system administrators. The Department takes this concern seriously. We have no interest in prosecuting such individuals, and our proposal would not prohibit legitimate activity. That is because the Government should have the burden to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be wrongful. The Government should similarly have to prove that the individual knew or had reason to know that the means of access would be used to commit a crime by hacking someone else's computer without authorization.

ICPA's approach makes clear that ordinary conduct by legitimate security researchers and others is not a crime. We believe that ICPA's botnet injunction provision strikes the proper balance in prohibiting the pernicious conduct I have described without chilling the activities of those who are trying to improve cybersecurity for us all.

F. Enhanced Penalties for Malicious Activity Directed at Critical Infrastructure

The Department also supports the efforts in ICPA to strengthen the criminal code to better deter malicious activities directed at computers and networks that control our critical infrastructures. As I have discussed, America's open and technologically complex society includes, as a part of its critical infrastructure, numerous vulnerable targets. While the CFAA's maximum penalties apply to malicious efforts to harm the computers and networks that run our critical infrastructure, the statute does not currently require any enhanced penalties for such conduct. While it is reasonable to believe that judges would impose appropriate prison terms if malicious activity severely debilitates a critical infrastructure system, it is possible that courts may not impose adequate penalties for activities that cause less disruption — and they could conceivably impose no penalty at all in the case of an attempt that is thwarted before it is completed.

In light of the grave risk posed by those who might compromise our critical infrastructure, the Department believes that the enhanced penalties for such malicious activity called for in ICPA not only will appropriately punish offenders, but also will more effectively deter others who would engage in misconduct that puts public safety and national security at risk. Criminals and other malicious actors should know that any attempt to damage a vital national resource will result in serious consequences.

G. Updated Tools for Investigators and Prosecutors

We have long had concerns about the text of the "Pen Register and Trap and Trace" ("PRTT") statute that is used, among other things, to support criminal investigations and the security of government networks. The PRTT statute's exceptions — which, for example, permit a provider, but not a user, of wire or electronic communications services to monitor their own network — are subtly and inexplicably different than the Wiretap Act's exceptions. The existing language in the PRTT statute has been difficult to apply, resulting in complex legal analyses for services as simple as Caller ID. The Wiretap Act's rules appropriately protect the content of communications; they are more than adequate to protect non-content information, which is much less sensitive. Importing the Wiretap Act's exceptions into the PRTT statute would remedy these problems and result in a more logical framework for applying these two related statutes that regulate the real-time collection of communications. There is no reason why a user of a PRTT device, whether a private or governmental entity, should be precluded from logging his or her own communications. We have proposed language under which the PRTT statute would continue to protect user privacy, but it would no longer inappropriately limit private entities' or the Government's ability to use PRTT devices on their own computer networks.

Finally, we support several amendments to the CFAA, which are reflected in the ICPA. Key amongst these changes would be amendments to 18 U.S.C. § 2513, which would bring the forfeiture provisions of the CFAA in line with other Federal criminal statutes, providing concrete procedures for the forfeiture of property used to commit or facilitate a violation of this statute as well as the proceeds of such violation. These amendments support consistent application of the law, while maintaining the Government's ability to dismantle and disrupt criminal operations and deter future violations, both when prosecutors are able to reach violators and when those violators are located overseas beyond the judicial reach of our courts. The amendments in ICPA are a measured and sensible addition that will help assure that criminal hackers do not profit from their crimes.

We also support the change in ICPA that would make the sale or advertising of a surreptitious interception device under 18 U.S.C. § 2512 a predicate offense under the Federal money laundering statutes. Section 2512, which is part of the Wiretap Act, has proven to be a valuable tool for protecting the privacy of innocent Americans by criminalizing the manufacture, distribution, possession, and advertising of devices, such as spyware, that unlawfully collect private communications. Section 2512 is not a predicate offense under 18 U.S.C. §§ 1956 and 1957, however, which impedes the Government's ability to punish and deter certain offenders

who conceal and spend their ill-gotten gains by selling and advertising spyware and other illegal interception devices.

H. Assuring Jurisdiction of Thefts of U.S. Companies' Trade Secrets

The Economic Espionage Act recognizes that trade secret theft frequently involves an international component (and section 1831 of Title 18 specifically criminalizes trade secret theft committed for the benefit of foreign instrumentalities). However, since the statute came into force in 1996, manufacturing, research, and development have become increasingly dispersed geographically. Just as manufacturing supply chains often cross borders, U.S. firms conduct research and development across international borders, with collaboration between facilities in multiple countries. With this trend, U.S. companies face increasing risk that their trade secrets may be stolen from facilities they own or operate outside U.S. borders.

Under the current EEA, the Department can prosecute trade secret thefts occurring abroad, but only where either (1) the defendant(s) are U.S. persons or organizations, or (2) an act in furtherance of the offense is committed in the United States. 18 U.S.C. § 1837. One illustration of the EEA's extraterritorial reach is the Department's ongoing prosecution of United Microelectronics Corporation (UMC) and Fujian Jinhua Integrated Circuit Co., and three Taiwan nationals for theft of trade secrets belonging to Micron Technologies. In that case, the defendants are charged with stealing trade secrets from a Micron facility in Taiwan, but acts in furtherance of the theft were committed within the U.S. However, it is easy to imagine future cases in which trade secrets owned by a U.S. company may be stolen by foreign nationals from facilities outside the U.S., which would fall outside the extraterritorial reach of the current statute. To address this scenario, Congress could amend Section 1837 to permit jurisdiction over extraterritorial conduct, at least in criminal cases, where "the trade secret owner injured as a result of the offense conduct is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof."

III. Conclusion

I want to thank the Subcommittee again for providing me this opportunity to discuss these important issues on behalf of the Department of Justice. We look forward to continuing to work with Congress to improve the Government's ability to counter threats posed by our foreign adversaries in cyberspace. I am happy to answer any questions you may have.