Department of Justice

STATEMENT OF
CLYDE E. WALLACE
DEPUTY ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

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
CLYDE E. WALLACE
DEPUTY ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

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

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

PRESENTED
MARCH 4, 2020

Chairman, Ranking Member, and members of the committee, thank you for the opportunity to appear before you today to discuss the current threats to the United States homeland. Our nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists ("HVEs") to cyber criminals to hostile foreign intelligence services and operatives. Keeping pace with these threats is a significant challenge for the FBI. Our adversaries — terrorists, foreign intelligence services, and criminals — take advantage of modern technology to hide their communications; recruit followers; and plan and encourage espionage, cyber-attacks, or terrorism to disperse information on different methods to attack the U.S. homeland, and to facilitate other illegal activities.

Cyber Threats

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, these actors seek to steal our state secrets, our trade secrets, our technology, and our ideas — things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to hold our critical infrastructure at risk and to harm our economy.

The FBI is investigating a wider-than-ever range of threat actors, from transnational organized cybercrime to nation-state adversaries to terrorists using social medial for recruiting and radicalization purposes. The scale, scope, speed and impact of cyber threats is constantly evolving, which may explain why we are also seeing a blending of threats, such as nation state adversaries using criminal actors as proxies to mask their activities.

The frequency and severity of malicious cyber activity on our nation's networks have increased dramatically in the past decade when measured by the amount of corporate data stolen or deleted, the volume of personally identifiable information compromised, or the remediation costs incurred by U.S. victims. Companies that hold large amounts of Personally Identifiable Information ("PII") are susceptible to loss of American's personal data to criminal organizations, terrorists, and nation-state cyber actors. Hotel chains, airlines, healthcare companies, credit bureaus, government agencies, and cleared defense contractors have previously been victims of PII theft.

Cyber Criminal Trends

Cyber threats are not only increasing in size and scope, but are also becoming increasingly difficult and resource-intensive to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that lower the barrier to entry for aspiring criminals and that can be used to facilitate malicious cyber activity. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient to disruption than ever. In addition, whether located at home or abroad, many cyber actors are obfuscating their identities and obscuring their activity by using combinations of leased and compromised infrastructure in domestic and foreign jurisdictions. Such tactics make coordination with all of our partners, including international law enforcement partners, essential.

Increasingly sophisticated obfuscation techniques are also enabling actors to stealthily obtain data from victims or repurpose victim computers into cryptocurrency-mining botnets. Botnets used by cyber criminals have been responsible for billions of dollars in damages over the past several years. The widespread availability of malicious software ("malware") that can create botnets allows individuals to leverage the combined bandwidth of thousands, if not millions, of compromised computers, servers, or network-ready devices to disrupt the day-to-day activities of governments, businesses, and individual Americans.

Cyber threat actors are conducting ransomware attacks against U.S. systems, encrypting data and rendering systems unusable — thereby victimizing individuals, businesses, and even emergency service and public health providers. Our threat reporting has demonstrated that ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of ransomware attacks is holding steady or declining. Since early 2018, the incidence of broad, indiscriminate ransomware campaigns has sharply declined, while losses from ransomware attacks have increased significantly. Allow me to restate that for emphasis: while the number of reported attacks has gone down, the effects and impacts of the attacks are going up. Meanwhile, state and local governments have been particularly visible targets for ransomware attacks. However, ransomware campaigns have also heavily impacted health care organizations, industrial companies, and the transportation sector.

Business Email Compromise ("BEC") remains a pervasive threat due to its low barrier of entry and maturing social engineering techniques, and cyber criminals almost certainly will continue to use BEC to target industries indiscriminately. BEC threat actors have widened their money laundering networks, including domestic transfers prior to laundering the money overseas, which presents challenges and opportunities for countering this type of fraud. Readily available online personal and business information enhances the reconnaissance capability of actors, providing BEC threat actors with more credible social engineering lures. Spoofed domains are seen in the majority of BEC attempts, and likely will remain a technique used by cyber actors. BEC attacks combining social engineering with network intrusions demonstrate an increase in attack sophistication that can use keyloggers or other malware to identify potential targets, such as business vendors, as well as sell access to or further exploit compromised systems.

Actors have learned that BEC is effective and are adapting lures to target human resources departments for PII, such as W-2 tax forms to commit stolen identity return fraud, rather than requesting wire transfers. Additionally, industry partners have observed BEC actors increasingly instruct victims to send automated clearing house transfers to prepaid cards in the initial laundering phase.

Nation State Activities: China

While several nation-states pose a cyber threat to U.S. interests, no other country presents a broader and more comprehensive threat to our ideas, innovation, and economic security than the People's Republic of China ("PRC") under the leadership of the Chinese Communist Party ("CCP"). The threat takes many different forms. Beijing employs a whole-of-government approach to its intelligence collection strategy. While cyber network operations remain a primary and possibly increasing collection tool, the CCP also relies on techniques such as intellectual property theft, purchases of U.S. corporations, and physical and property theft to acquire U.S. data.

For example, less than a month ago, on February 10, 2020, the Department of Justice ("DOJ"), in coordination with the FBI, publicly unsealed an indictment against four Chinese cyber actors who allegedly acted as agents of the People's Republic of China's People's Liberation Army ("PLA"). All four actors are currently located in China. The alleged crimes occurred between May 13, 2017 and July 30, 2017. The actors targeted a software vulnerability to gain unauthorized access to Equifax's network and ultimately obtain PII for 145 million American citizens as well as the intellectual property of the U.S. company.

The indictment alleges the four individuals named therein reside in Beijing, China and are members of the 54th Research Institute. The 54th Research Institute is a component of the People's Liberation Army. The indicted individuals gained unauthorized access, via a software vulnerability, to Equifax's internal network where they allegedly ran approximately 9,000 queries on Equifax's systems and obtained the names, birth dates, and social security numbers for approximately half of all adult American citizens. The defendants also took deliberate steps to evade detection in the system, including routing traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location, using encrypted channels in order to blend in normal traffic within Equifax's network, and wiping log files on a daily basis to try to eliminate records of their activity.

DOJ, the FBI, and our partners will continue to work tirelessly to combat this threat posed by the Chinese government against our nation. Although the PRC continues to modify the ways in which it conducts nefarious cyber activity, including through working with criminal hackers, the cases prosecuted by the DOJ in partnership with the FBI reflect an increasingly sophisticated ability to attribute criminal conduct to the individuals and nation states involved. We will be relentless in our pursuit of such malicious activity against our citizens and our industry.

There are other risks. Chinese companies are increasingly acquiring or launching social media applications not housed in mainland China for the global consumer market. These applications generate big data and collect PII such as biometric information, contact lists, location data, log data, communication metadata, content (text and photographic), bank and credit card details, and financial transactions of U.S. persons. The associated user agreements and privacy policies typically obfuscate the companies' data handling responsibilities or directly state any and all data can be transferred to other locations and associated entities to include the Chinese parent company. These data handling policies create a risk for U.S. big data and PII to be targeted and exploited by PRC actors. More broadly, consumers should be aware of the privacy implications of any application they install, especially applications from foreign countries with weak data protection laws.

In June 2017, the PRC introduced a new national cyber security law that requires foreign firms to store data locally and submit to data surveillance measures. Although implementing regulations are still being drafted, Beijing could likely use these authorities and policies to compel access to U.S. commercial and sensitive personal data, including sensitive information stored or transmitted through Chinese systems. U.S.-based subsidiaries of Chinese corporations and entities, or organizations in the U.S. partnering on cooperative research and development efforts, are among the entities affected by this law. The law has raised fears by those concerned with Beijing's control of sensitive company information and increased opportunity to steal intellectual property.

Threats Exposing Vulnerabilities on Critical Infrastructure Networks and the Public

Virtually all companies collect and maintain sensitive data either of their own employees or customer information. The overall trend of digitizing data for ease of use or access makes many different industries vulnerable to data breaches. For instance, over recent years the healthcare industry has moved to centralizing patient data and using Internet-connected devices, which has increased the sector's potential attack surface. Cyber actors benefit from this targetrich environment as the passage of patient data between healthcare departments and networks is critical to their care, but often levels of cybersecurity vary. Ransomware, denial of service attacks, and data breaches can all impede the ability to provide basic patient care and privacy for protected health information ("PHI"). Electronic medical records typically contain PII, which, combined with medical record information, is known as PHI.

It is also highly likely cyber actors target the IT Sector to access their customers' data and networks. IT sector entities manage and store valuable customer data and have unique, privileged access to client networks. These vital services create an environment where IT sector networks are compromised as a means for malicious cyber actors to reach a final target for fraud, hacktivism, and counterintelligence purposes.

Entertainment and media companies use Internet-enabled systems for marketing, merchandising, ticketing, and reservations. As a result, owners and operators manage and protect databases of customer and employee data, including personal, financial, and credit card information. Since at least 2015, nation-state and criminal cyber actors have conducted computer network exploitation against the subsector likely to gain unauthorized access to non-public information, although the extent of the access in each case remains unclear.

Efforts Used to Combat, Prevent, and Investigate Hacking or the Misuse of this Data

In order to combat cyber threats, the FBI has taken a whole-of-society approach. We actively engage with our private sector partners through the National Cyber-Forensics and Training Alliance ("NCFTA"), which is a non-profit partnership between private industry, government and academia all working together to identify and disrupt cyber-crime. We recently hosted a ransomware-focused summit, with incident response companies, representatives from the legal and insurance industries as well as other government entities, where we discussed collaborative efforts to address the threats.

The FBI also partners with the National Defense Cyber Alliance ("NDCA"), which is a non-profit organization bringing together the U.S. Intelligence Community and Cleared Defense Contractor community to improve the security of their networks. Similar to how the NCFTA supports the financial/retail sector against criminal threats, the NDCA is designed to support the Defense Industrial Base against national security threats.

Through undercover operations and confidential human sources, we are targeting and shutting down dark-net and Clearnet criminal forums where identities are sold and where cyber-criminals gather to plan their next attack. We are actively engaging with our international partners through our Cyber Assistant Legal Attaché ("ALAT") program, through our annual FBI-sponsored International Task Force and through our participation in the FBI-led International Cyber Crime Operations Summit ("ICCOS") as well as the Five Eyes Law Enforcement Group ("FELEG") Cyber Crime Working Group.

The FBI understands the importance of stressing cybersecurity with individuals, not just with organizations. To do so, we hold a series of events aimed at educating and speaking with individuals about these issues. The FBI regularly takes part in Public Awareness Campaigns, where we coordinate with other agencies on initiatives for engagement with the private sector to prevent threats to critical infrastructure, educate entities on serious cyber threats, and ultimately close intelligence gaps. Additionally, we disseminate Private Industry Notifications ("PINs"), FBI Liaison Alert System ("FLASH") reports, and Public Service Announcements ("PSAs") to share cyber threat information with the private sector and the general public.

Conclusion

The FBI is engaged in myriad efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of the government, to developing and retaining new talent, to examining the way we operate to disrupt and defeat these threats. FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques — such as sources, court-authorized electronic surveillance, physical surveillance, and forensics — to counter these threats.