Cyber Update
5 February 2019
By Michael Kans

Senate Intelligence Hearing on Worldwide Threats

On January 29, the Senate Intelligence Committee held a hearing entitled: "Worldwide Threats." The witnesses appearing before the committee were:

- Director of National Intelligence Daniel Coats
- Federal Bureau of Investigation Director Christopher Wray
- Central Intelligence Agency Director Gina Haspel
- Defense Intelligence Agency Director General Robert Ashley
- National Security Agency Director General Paul Nakasone
- National Geospatial-Intelligence Agency Director Robert Cardillo

Chairman Richard Burr (R-NC) stated that the U.S. has entered a new age characterized by hybrid warfare and weaponized disinformation in a world "producing more data than mankind has ever seen." He said that "[t]omorrow its going to be deep fakes, artificial intelligence, 5G enabled Internet of Things with billions of internet connections on consumer devices." Burr said he wan ted to know from the Intelligence Community (IC) how well equipped it is to take on the new generation of technological threats. He said he envisioned a world with greater information sharing between government and the private sector while still protecting the sources and methods of the IC. Burr said the enemies of the U.S. will try to harm the nation through technology and said that when American democracy was threatened in 2016, it was through social media accounts.

Ranking Member Mark Warner (D-VA) remarked on the multiplicity of threats the U.S. faces, from new threats like cyber and online influence to old ones like terrorism, extremism, and rogue actors. He asserted the U.S. must face the myriad of threats with its allies. Warner highlighted his concerns about Russia's use of social media to amplify divisions in U.S. society and to influence our democratic process. He noted that at the 2018 hearing on worldwide threats, there was ample discussion that Russia would try to influence the 2018 elections. Warner said there was evidence of Russian attempts to use social media and hackers probing critical cyber infrastructure. He commended Nakasone and said the U.S. did a much better job. Warner asked how the IC will help address these types of threats for 2020 and how the government can build upon public-private partnerships with social media companies. He also expressed concern about threats from China in the technology field, particularly

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

China's whole-of-society approach to catching the U.S., which often entails criminal activity and espionage.

In concert with the hearing, an unclassified version of the Intelligence Community's Worldwide Threat Assessment was released a week after the Director of National Intelligence (DNI) released the "National Intelligence Strategy" (NIS), and DNI Dan Coats warned that adversarial nation states and others are using current technologies in ways that posed threats to the U.S. and that new technologies will likely lead to additional ways for the U.S. to be challenged.

Key excerpts from the Worldwide Threat Assessment include:

Cybersecurity

> *Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners.* China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.
> *At present, China and Russia pose the greatest espionage and cyber attack threats, but we anticipate that all our adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence US policies and advance their own national security interests.* In the last decade, our adversaries and strategic competitors have developed and experimented with a growing capability to shape and alter the information and systems on which we rely. For years, they have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk. They are now becoming more adept at using social media to alter how we think, behave, and decide. As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information.

Elections/Influence Campaigns

> *Our adversaries and strategic competitors probably already are looking to the 2020 US elections as an opportunity to advance their interests. More broadly, US adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States*

and elsewhere. We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences, suggesting the threat landscape could look very different in 2020 and future elections.

Emerging and Disruptive Threats

For 2019 and beyond, the innovations that drive military and economic competitiveness will increasingly originate outside the United States, as the overall US lead in science and technology (S&T) shrinks; the capability gap between commercial and military technologies evaporates; and foreign actors increase their efforts to acquire top talent, companies, data, and intellectual property via licit and illicit means. Many foreign leaders, including Chinese President Xi Jinping and Russian President Vladimir Putin, view strong indigenous science and technology capabilities as key to their country's sovereignty, economic outlook, and national power.

The global race to develop artificial intelligence (AI)—systems that imitate aspects of human cognition—is likely to accelerate the development of highly capable, application-specific AI systems with national security implications. As academia, major companies, and large government programs continue to develop and deploy AI capabilities, AI-enhanced systems are likely to be trusted with increasing levels of autonomy and decisionmaking, presenting the world with a host of economic, military, ethical, and privacy challenges. Furthermore, interactions between multiple advanced AI systems could lead to unexpected outcomes that increase the risk of economic miscalculation or battlefield surprise.

Foreign production and adoption of advanced communication technologies, such as fifth-generation (5G) wireless networks, most likely will challenge US competitiveness and data security, while advances in quantum computing foreshadow challenges to current methods of protecting data and transactions. US data will increasingly flow across foreign-produced equipment and foreign-controlled networks, raising the risk of foreign access and denial of service. Foreign deployment of a large-scale quantum computer, even 10 or more years in the future, would put sensitive information encrypted with today's most widely used algorithms at greatly increased risk of decryption.

DOJ Indicts Huawei

This week, the Department of Justice (DOJ) announced a grand in jury indictment against "Huawei Device Co., Ltd. and Huawei Device Co. USA with theft of trade

secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice." This ten-count indictment was unsealed in the Western District of Washington State and focuses on alleged crimes against T-Mobile.

DOJ explained in their press release that

> [I]n 2012 Huawei began a concerted effort to steal information on a T-Mobile phone-testing robot dubbed "Tappy." In an effort to build their own robot to test phones before they were shipped to T-Mobile and other wireless carriers, Huawei engineers violated confidentiality and non-disclosure agreements with T-Mobile by secretly taking photos of "Tappy," taking measurements of parts of the robot, and in one instance, stealing a piece of the robot so that the Huawei engineers in China could try to replicate it. After T-Mobile discovered and interrupted these criminal activities, and then threatened to sue, Huawei produced a report falsely claiming that the theft was the work of rogue actors within the company and not a concerted effort by Huawei corporate entities in the United States and China. As emails obtained in the course of the investigation reveal, the conspiracy to steal secrets from T-Mobile was a company-wide effort involving many engineers and employees within the two charged companies.

The DOJ also unsealed a 13-count indictment against "Huawei and two Huawei affiliates — Huawei Device USA Inc. (Huawei USA) and Skycom Tech Co. Ltd. (Skycom) — as well as Huawei's Chief Financial Officer (CFO) Wanzhou Meng (Meng)" as detailed in their press release. The DOJ stated that "[t]he charges in this case relate to a long-running scheme by Huawei, its CFO, and other employees to deceive numerous global financial institutions and the U.S. government regarding Huawei's business activities in Iran."The DOJ noted Meng is being held in Canada, pending a U.S. effort to extradite her to face charges in the U.S.

DOJ explained that

> The defendants Huawei and Skycom are charged with bank fraud and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA, and conspiracy to commit money laundering. Huawei and Huawei USA are charged with conspiracy to obstruct justice related to the grand jury investigation in the Eastern District of New York. Meng is charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud.

Krach Nominated As Ombudsperson

Last week, the Administration nominated former DocuSign CEO Keith Krach to a number of posts, including Under Secretary of State (Economic Growth, Energy, and the Environment), which, if confirmed, would make him the ombudsperson overseeing allegations from European Union or Swiss citizens regarding possible United States' law enforcement agency access to the personnel data of EU citizens transferred under the EU-U.S. Privacy Shield. The lack of an Ombudsperson has been a source of tension between the EU and U.S. regarding the implementation of Privacy Shield and larger issues arising from U.S. surveillance activities the EU claims violates the rights of its citizens.

In a press release from mid-January, the Trump Administration provided a brief biography of Krach:

> Mr. Krach is Chairman and former CEO of DocuSign, and was also the co-founder, Chairman, and CEO of Ariba. Prior to that, Mr. Krach was Chief Operating Officer of Rasna Corporation and served as the first Entrepreneur and CEO-in-Residence for Benchmark Capital. Mr. Krach began his career at General Motors. Mr. Krach served as Chairman of Purdue University's Board of Trustees, Chairman of Angie's List, and is Chairman of the DocuSign Impact Foundation. He received his B.S. and Honorary Doctorate in Engineering from Purdue University and an M.B.A. from Harvard University.

The EU's Data Protection Supervisor Giovanni Buttarelli said that an Ombudsperson is "a prerequisite for the functioning of the Privacy Shield" and the nomination was made "later than expected." He added that there are "some missing points in the U.S. implementation" of Privacy Shield and there are "areas for improvement." Buttarelli also expressed misgivings that an Ombudsperson would not be politically independent. He remarked "[w]e understand that due to the US constitutional framework, no person in such a role could be fully independent by default."

While the EU has not threatened to suspend the Privacy Shield, in December 2018, the European Commission set a deadline of February 28, 2019 by which the U.S. must have an Ombudsperson nominated but not confirmed. The European Commission stated that "If this does not take place by that date, the Commission will then consider taking appropriate measures, in accordance with the General Data Protection Regulation."

Other Hearings and Events

"China and Russia" –Senate Armed Services
"Department of Defense Enterprise-wide Cybersecurity Policies and Architecture"–Senate Armed Services/Cybersecurity
"H.R. 1, the 'For the People Act of 2019'"–House Judiciary

Further Reading

The Cybersecurity 202: This is the Senate Homeland Security Committee's top cyber priority this year – Washington Post
EU considers proposals to exclude Chinese firms from 5G networks – Reuters
The Shutdown's Impact on Cybersecurity Talent – Nextgov
UAE Used Cyber Super-Weapon To Spy On iPhones Of Foes – Reuters
Citing cyber risk, Pentagon watchdog wants to pause JRSS – FCW
Feds lead industry in DMARC adoption – FCW

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans