Statement before the
U.S.-China Economic and Security Review Commission
"China, the United States, and Next Generation Connectivity,"

A Testimony by:

James Mulvenon, Ph.D.
General Manager, Special Programs Division
SOS International

March 8, 2018

2255 Rayburn House Office Building

Introduction and Main Points

Chairman Cleveland, Vice Chairman Bartholomew, and Commissioners, thank you for inviting me to testify today.

My testimony focuses on the Internet of Things (IoT), 5th generation telecommunications (5G), and the role that these technologies could potentially play in national security and information security issues between the United States and China. The top three concerns are:

- Supply chain challenges and threats posed by China-based production of IoT devices deployed in the United States
- Post-installation maintenance and upgrades of those IoT devices as vectors for malware and exfiltration
- Recent Chinese laws that create the legal basis for extraterritoriality of Chinese telecommunications companies and potential intercept access to U.S. communications infrastructure.

Before dealing with these concerns, let me first address the general issues associated with IoT and 5G in a U.S.-China context.

Internet of Things

The so-called "Internet of Things," or IoT, has quickly become a ubiquitous part of our daily lives. Our homes are increasingly filled with WiFi-connected hubs, garage door openers, lights, doorbells, and security cameras. Unfortunately, information security was an afterthought with many of these devices, and many are not designed to be upgradeable. As a result, IoT objects are increasingly being used for malignant purposes, either as part of botnets[1] or for unwanted surveillance. The fact that many of these devices are being produced in China by foreign or Chinese firms only adds an additional layer of potential concern. For example, the three largest Chinese network camera firms (Dahua, Hikvision, Foscam) have been linked in the last two years to major cyber incidents, primarily because of the low levels of information security in their products:

- A researcher at the SANS Technology Institute identified malware designed to infect security camera recorders and routers and use the devices to attempt to mine Bitcoin virtual currency. The malware is designed to run on ARM infrastructure and was spotted on Hikvision DVRs, which have a simple default root password that users often do not change.[2]

---

[1] Brian Krebs, "Dahua, Hikvision IoT Devices Under Siege," *Krebs on Security*, March 2017, accessed at: https://krebsonsecurity.com/tag/hikvision/.

[2] Eduard Kovacs, "Cybercriminals Abuse Security Camera Recorders and Routers to Mine for Bitcoins," 2 April 2014, *Softpedia.*com, accessed at: http://news.softpedia.com/news/Cybercriminals-Abuse-Security-Camera- Recorders-and-Routers-to-Mine-for-Bitcoins-435427.shtml

- Network cameras manufactured by Chinese company Dahua (dahua.com) were main targets of the Mirai internet worm,[3] which "has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks" in the history of the Internet.[4]
- Many network cameras manufactured by Shenzhen-based Foscam (foscam.com) connect to a peer-to-peer network called the "Kalay Network" run by a Chinese company called ThroughTek, though there is almost no mention of this feature in Foscam manuals and it is very difficult to disable.[5] Moreover, information security experts such as Nicholas Weaver call the embedded P2P feature "an insanely bad idea" because "it opens up all Foscam users not only to attacks on their cameras themselves (which may be very sensitive), but an exploit of the camera also enables further intrusions into the home network."
- Large numbers of network cameras manufactured by Chinese company Hikvision were hacked in early 2017 by exploitation of default login and passwords,[6] though more recent Hikvision releases require the creation of a unique password.[7]

Other Chinese IoT companies have been scrutinized for their potential threat to U.S. national security. In May 2017, the Department of Homeland Security issued a cybersecurity warning saying some of Hikvision's cameras contained a loophole making them easily exploitable by hackers, assigning its worst security rating to that vulnerability.[8] It was later discovered that Hikvision cameras were deployed at Fort Leonard Wood in Missouri and the U.S. Embassy in Kabul, Afghanistan.[9] The cameras were later then removed for security concerns. The General Services Administration, which oversees $66 billion of procurement for the U.S. government, subsequently removed Hikvision from a list of automatically approved suppliers. On 30 January

---

[3] Brian Krebs, "Who Makes the IoT Things Under Attack?" *Krebs on Security*, October 2016, accessed at: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

[4] "Mirai (malware)," *Wikipedia.org*, accessed at: https://en.wikipedia.org/wiki/Mirai_(malware)

[5] Brian Krebs, "This is Why People Fear the 'Internet of Things'," *Krebs on Security*, February 2016, accessed at: https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/

[6] Brian Karas, "Hikvision Defaulted Devices Getting Hacked," *IP Video Market* Info, 2 March 2017, accessed at: https://ipvm.com/reports/hik-default-hack

[7] "IP Cameras Default Passwords Directory," accessed at: https://ipvm.com/reports/ip-cameras-default-passwords-directory

[8] "Advisory (ICSA-17-124-01): Hikvision Cameras," Department of Homeland Security Industrial Control Systems Computer Emergency Response Team, accessed at: https://ics-cert.us-cert.gov/advisories/ICSA-17-124-01.

[9] Dan Strumpf, Natasha Khan, and Charles Rollet, "Surveillance Cameras Made by China Are Hanging All Over the U.S.," *Wall Street Journal*, 12 November 2017, accessed at: https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949; and Dan Strumpf, Army Rips Out Chinese-Made Surveillance Cameras Overlooking U.S. Base," *Wall Street Journal*, 12 January 2018, accessed at: https://www.wsj.com/articles/army-rips-out-chinese-made-surveillance-cameras-overlooking-u-s-base-1515753001.

2018, the House of Representatives Committee on Small Business held a hearing on foreign cyber threats to small businesses, and singled out the threat posed by Hikvision cameras.[10]

5G Telecommunications

The next-generation mobile Internet, known as 5th generation or 5G, is the infrastructure upgrade necessary to facilitate billions of IoT devices communicating with each other, as well as emerging technologies like self-driving cars and immersive networking. 5G networks, now in the testing stage, will rely on denser arrays of small antennas and the cloud to offer data speeds up to 50 or 100 times faster than current 4G networks and serve as critical infrastructure for a range of industries.[11] China is widely regarded as one of the leaders in 5G development, allocating billions in state investment and actively promoting the R&D and commercial activities of Huawei and ZTE. Huawei has signed 25 agreements with telecommunications companies around the world to test its 5G technologies, and China Mobile in 2018 plans the world's largest 5G trial.[12] According to Chinese regulations, Huawei and ZTE are each guaranteed one-third of the Chinese 5G market, leaving foreign firms like Ericsson and Nokia to compete over the remaining one-third sliver.[13] The concerns about Huawei or ZTE 5G equipment in the United States telecommunications infrastructure are two-fold:

- If Huawei or ZTE were to win a contract to supply 5G equipment under market terms, the political and legal environment in China would prevent either company from refusing a subsequent entreaty from either the Chinese intelligence services or military for access to the technology or services.
- The PRC government treats Chinese companies operating abroad as subject to PRC law, and multiple new Chinese laws dictate that telecoms operators must provide the Chinese intelligence services with unfettered access to networks for intercept, which raises concerns about Huawei or ZTE 5G support facilities being used for intelligence operations.

At the same time, the barn door long ago slammed on a "keep Huawei out of the USA" strategy, as several dozen Tier 3 telecommunications providers, primarily in rural areas in the United States, already extensively use Huawei base stations and handsets. It is also likely inevitable that Huawei equipment will be eventually deployed in Tier 1 networks run by AT&T, Verizon, and

---

[10] "Small Business Information Sharing: Combating Foreign Cyber Threats," accessed at: https://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=400565

[11] Eric Auchard, Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, 23 February 2018, accessed at: https://www.reuters.com/article/us-telecoms-5g-china/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idUSKCN1G70MV.

[12] Arjun Kharpal, "China 'Has the Edge' in the War for 5G and the US and Europe Could Fall Behind," cnbc.com, 7 March 2018, accessed at: https://www.cnbc.com/2018/03/07/china-has-the-edge-in-the-war-for-5g-us-and-eu-could-fall-behind.html

[13] Eric Auchard, Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, 23 February 2018, accessed at: https://www.reuters.com/article/us-telecoms-5g-china/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idUSKCN1G70MV.

Sprint. It is imperative, therefore, to adopt a “resilience” strategy, designing a security framework that assumes the presence of Huawei equipment in U.S. networks. While this strategy should include independent review of hardware and software and supply chains, the results of the “front end” inspection must be tempered with the understanding that subsequent maintenance and upgrades of the equipment would be the more likely vector for insertion of malware and exfiltration of data. Thus, the security framework should cover the entire “life cycle” of the equipment and software.