Testimony of Dr. Charles Clancy

Professor of Electrical and Computer Engineering, Virginia Tech

before the House Energy and Commerce Committee, Subcommittee on Communications and Technology, Hearing on Telecommunications, Global Competitiveness, and National Security

May 16, 2018

Chairman Blackburn, Ranking Member Doyle, and Subcommittee Members:

My name is Charles Clancy and I am a professor of electrical and computer engineering at Virginia Tech, where I direct the Hume Center for National Security and Technology. In these roles, I lead major university programs in security, resilience, and autonomy. I am an internationally-recognized expert in wireless security and have held leadership roles within international standards and technology organizations including the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE). My current research sits at the intersection of 5G wireless, the Internet of Things, and cybersecurity.

I am co-author to over 200 peer-reviewed academic publications, to include five books on digital communications; am co-inventor to over 20 patents; and am co-founder of four venture-back startup companies all focused in the wireless and security sectors.

Prior to joining Virginia Tech in 2010, I served as research leader for emerging mobile technologies the National Security Agency.

It is my distinct pleasure to address this committee again on topics of critical national importance.

Background

Over the past 20 years, major forces have reshaped the telecommunications industry in the United States and globally. As the industry has moved from delivering phone calls to delivering the Internet, American titans of the 20th century like Motorola and Lucent have faded and given rise to innovators of the 21st century like Apple and Cisco. These shifts have given birth to a global marketplace, which in turn has resulted in a global supply chain.

Supply chains for telecommunications are complex. They include development of intellectual property and standards; fabrication of components and chips; assembly and test of devices; development of software and firmware; acquisition, installation, and management of devices in operational networks;

and the data and services that operate over those networks. Competing in a global marketplace drives where and how each portion of this supply chain is executed.

An example of the modern supply chain is that of the Apple iPhone. Over 700 suppliers from 30 countries provide components. Component technologies come from all over the world and are assembled in China – cameras from Japan, displays from Korea, and computer processors from Taiwan. Only 7% of the suppliers are US companies, including wireless chips from Qualcomm and Intel, that are actually fabricated Korea and Taiwan. Note that generally with respect to chip fabrication, Taiwan leads with over 45% of global capacity, and China is number two at 20%. The United States only accounts for 8%.

Another interesting statistic to consider is contribution to the standards process. As someone who has participated heavily in international standards, I personally saw Chinese participation increase from zero in 2005 to a commanding presence by 2010. Huawei in particular leveraged a bounty system of bonuses to recruit away many of the most prolific contributors. In 2017, Huawei authored 21% of standards within the Internet Engineering Task Force, and was nearly tied with Cisco for the #1 filer of intellectual property claims. If the current trends hold, Huawei will be the world's top contributor to Internet Standards within five years, and the leading developer of associated intellectual property. Huawei accomplished this position not through buying American companies, but rather through buying American innovators, and therefore was invisible to the Committee on Foreign Investment in the United States (CFIUS).

While several Chinese companies have clearly taken shortcuts, from theft of intellectual property to revenue from product sales to embargoed countries, China is undeniably part of the global telecommunications marketplace and supply chain.

Securing the Supply Chain

Given this reality, questions of national security are critical. The cyber threat facing the United States is real and tangible, and supply chain operations are among the most pernicious and difficult to detect. The best approach for tackling this challenge is through thorough supply chain risk management.

In the telecommunications sector, there are varying degrees of criticality associated with core networking equipment, cell tower equipment, and individual smartphones. While recently there has been significant media emphasis on Huawei phones, Huawei also offers a complete line of core networking devices and cell tower equipment. In most every telecommunications subsector, Huawei's market share is in the top three, if not #1.

Consider the risks associated with latent malware on a core Internet router sharing bogus routing information with its peers – incidents in the past have demonstrated that accidental misconfigurations on a single router can take down significant segments of the Internet for extended periods of time. Imagine the impact if many routers acted in a coordinated fashion. This isn't about cell phones; it's about the survivability of the Internet itself.

As stated, it all comes down to risk management. Telecommunications companies need to consider the criticality of each component in their network, and the entire supply chain for each product they acquire and provision in their network. It is financially impossible to eliminate all risk, but supply chain risk needs to be assessed and quantified before it can be effectively managed. The overall trend in cybersecurity away from compliance-based security in favor of risk-based methodologies needs to be extended to supply chain, and the NIST Cybersecurity Framework is a great starting point for formulating such a strategy. Specifically, compliance-based approaches that ban specific vendors or products may offer near-term results but will not be durable approaches long term.

Recommendations

Looking forward, I encourage this subcommittee to consider the following.

First, supply chains for critical infrastructure are not well understood. There should be recurring assessments performed collaboratively between government and industry that examine each layer of the supply chain, from research and development through operations. Areas of risk should be identified and prioritized. Specific concerns about particular products or vendors should be shared with relevant industries. Those industries should, in turn, develop and implement risk management plans to address concerns.

Second, in areas where risk cannot be effectively managed unilaterally by industry, the US government should take actions to help foster the competitiveness of domestic industry to fill the gap. For example, these assessments can help inform the CFIUS process to promote more consistent and informed decisions regarding foreign acquisition of US companies. Other tools can be leveraged to help foster American innovation in gap areas to expand the pool of supply chain options.

Lastly, it is important that any actions taken to foster US industry in gap areas consider the global marketplace for telecommunications. Protectionist measures may help promote a domestic market, but in the long term companies will only be viable if they can compete internationally as the US is only around 20% of the global telecommunications market.

Thank you for the opportunity to address the subcommittee today and I look forward to questions.