The Risks of Huawei To The 5G Ecosystem

By Craig Spiezle
Managing Director, Agelight Advisory & Research Group

As the world continued to grapple with the impact of the Coronavirus and the cyber threats to the global supply chain are mounting with fears of state sponsored actions and backdoors. The security and trustworthiness of the 5G ecosystem is being questioned with leading to the balkanization of one of the most promising technologies.

At the 2020 RSA Conference in San Francisco, (RSAC) I moderated a keynote panel discussing the potential security risks of Huawei products in the telecommunications supply chain. When I proposed the topic and recruited speakers, my goal was to provide a forum for a 360-degree view of the issues. The all-star panel included Katie Arrington, Cyber Information Security Officer of Acquisitions for the U.S. Department of Defense, Andy Purdy, CSO for Huawei Technologies USA, Bruce Schneier, Security Technologist and Kathryn Waldron, Fellow at R Street Institute. Watch the RSA panel discussion.

Solving a Problem, But Not Solving THE Problem

The buzz at RSAC centered on the promise of 5G along with the inherent risks, especially from foreign actors and in particular China. A key question presented to the panel was whether the banning of Huawei was grounded on security and/or trade issues. Second, a fundamental question debated was what a ban would achieve. Bruce Schneier stated, "blocking Huawei may address one problem, but it does not solve THE problem." This point was in reference to the complexity and associated risks of the ecosystem.

Globally, there is no consensus on the security threat posed by Huawei. While the United States' position is entrenched, the EU, UK, France and other countries have come to different conclusions, reportedly based on the intelligence dataset that was the foundation of the U.S.'s ban.[1] This is not surprising, as decision makers must balance supply chain risks against their overall risk appetite and ultimately whether they can mitigate or "buy down their risk" to an acceptable level or adopt a "zero trust model".

The panel discussed the reality that all networks and ecosystems have multiple points of potential failure as well as the inherent insecurity of some of the 5G protocols themselves.[2] In addition to the physical infrastructure and equipment, the 5G ecosystem assumes operators and carriers are worthy of

[1] EU outlines 5G rules https://www.theregister.co.uk/2020/01/29/eu_snubs_us_to_permit_huawei_5g_gear/
[2] 5G Standards Insecure https://www.informationsecuritybuzz.com/articles/the-future-of-5g-may-be-bright-but-is-it-secure/ and https://www.wired.com/story/5g-more-secure-4g-except-when-not/

trust. As the FCC earlier this year fined ATT, T-Mobile, Verizon and others $200 million for sharing user location data, their ability to be stewards of consumer data is in question.[3]

Historically industry has been able to build reliable networks with unreliable components. Given today's state of technology and geo-political landscape, the ability to build a trustworthy network from untrustworthy components may be impossible. Threats from sophisticated and malicious actors can compromise most any system or supply chain. These risks run the gamut from the design, manufacture and assembly to the shipping and delivery of any product, service or software update.

Is This the Pot Calling the Kettle Black?

While Apple and Microsoft have successfully gone to the courts to prevent being forced to turn over data or create backdoors for the government, the U.S. government has found other creative methods to insert control.[4] The NSA had reportedly compromised RSA encryption protocols,[5] intercepted devices implanting back doors and covertly purchased encryption companies to provide access.[6] While the U.S. rightfully has concerns on actions that could be taken by the Chinese government through Huawei, it is important to recognize the U.S. has a checkered past itself, and knows first-hand what is possible.

Is This a Trade Issue?

Allegations of Huawei's IP theft and reverse engineering efforts have been asserted for years. Some critics believe it is rooted in Chinese culture that promotes the theft of trade secrets. As reported by the Wall Street Journal (WSJ), "Huawei's rise is littered with accusations of theft and dubious ethics."[7] For many, this alone may be justification that Huawei should be banned from the U.S. Arrington stated, "adversaries have stolen 70 years of naval technologies, and Huawei has a checkered past." She alluded to Huawei's alleged unfair business practices, including efforts to "wipe out competition through dumping, IP theft and racketeering." [8, 9]

Competitors and Huawei's detractors have claimed that Huawei and other Chinese technology providers have an unfair advantage due to the funding they receive from their government. The reality is the U.S. lost its leadership in telecom years ago. This was not a result of IP theft alone but due to the confluence

---

[3] FCC Fines carriers $200 Million for sale of location data https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf

[4] Microsoft wins privacy case over DOJ https://searchsecurity.techtarget.com/news/450411743/Microsoft-defeats-DOJ-appeal-in-cloud-data-privacy-case

[5] NSA infiltrated RSA protocols https://www.reuters.com/article/us-usa-security-nsa-rsa/exclusive-nsa-infiltrated-rsa-security-more-deeply-than-thought-study-idUSBREA2U0TY20140331

[6] CIA rigged spy devices https://www.washingtonpost.com/outlook/the-cia-rigged-foreign-spy-devices-for-years-what-secrets-should-it-share-now/2020/02/28/b570a4ea-58ce-11ea-9000-f3cffee23036_story.html

[7] WSJ; Huawei's Accusation of Theft & Dubious Ethics https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858

[8] DOJ charges Huawei with fraud, IP theft https://www.nationalreview.com/news/doj-charges-huawei-fraud-intellectual-property-theft/

[9] 1 in 5 corporations say China has stolen their IP https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html

of several issues, including inadequate investments. One of the largest factors was deregulation and lack of national standards, which resulted in U.S. carrier networks competing over TDMA, CDMA and GSM. As a result, Lucent - who at the time was a telecom leader - had to support all of these unique platforms and failed to achieve economies of scale. Its subsequent merger with Alcatel wasn't successful, and it was ultimately acquired by Nokia.[10, 11]

Huawei's Purdy offered up an interesting solution to help spur U.S. innovation. He reiterated Huawei's Chairman's offer to license Huawei's 5G technology and patents. According to Purdy, they have yet to receive a response. During the panel, Arrington disparaged the skill set and competencies of Huawei's developers, stating, "they are 25 years behind those of Microsoft developers." While this might have been the case in the past, the reality is Chinese developers are on par or in cases better than U.S. developers. A 2016 study by HackerRank disputes Arrington's statement, saying China and Russia have some of the best software developers, with U.S. developers ranking 28th.[12]

Backdoors – Who Can Be Trusted?

There is a broad consensus that no country should have backdoors, as the risk for abuse is too high. Schneier stated "the U.S. wants to have it both ways; prevent others, yet have access themselves." Backdoors could provide a "kill switch," resulting in an interruption or degradation of services or hidden functionality. He added "unlike the ability to test for known vulnerabilities, the reliable detection of backdoors is significantly more difficult, if not impossible". Just as concerning is the fact that backdoors can introduce significant risks to civil liberties and potential abuse by law enforcement.

It is an accepted fact that over a product's lifecycle, nearly every software and hardware product will have a vulnerability. Huawei and telecom equipment providers are no exception. At the same time, it is important to recognize that the presence of a vulnerability or weakness does not suggest it has been exploited or that an attack targeting the vulnerability has occurred. While I have argued Huawei's vulnerability disclosure practices, patching cadence and bounty programs have room for improvement, to date, no maliciously inserted backdoors have been discovered. To this point, Arrington stated that the "risk of waking up and banks and traffic not working, Huawei is just too risky."

Country of Origin

Focusing where a company is domiciled as a primary risk factor, while "green lighting" companies from countries deemed safe, can lure one into a false sense of security. Responding to a question about her past writings, Waldron of R Street stated that country of origin is certainly an important contributing factor to consider when it comes to supply chain security, but "narrowly focusing on that alone can create a false narrative and lead you to make hasty, needlessly economically damaging conclusions."

To this point, many leading technology providers, including Nokia, Ericsson, Cisco and others, have large R & D and/or manufacturing presences in China. Wisdom suggests any organization or government who is fearful of the Chinese should apply the same rigor and monitoring to these companies as well.

---

[10] How US went from telecom leader to also-ran https://www.scmp.com/tech/enterprises/article/3004325/how-us-went-telecoms-leader-5g-also-ran-without-challenger-chinas

[11] Why Alcatel-Lucent failed https://research-methodology.net/alcatel-lucent-merger-failure-a-critical-analysis/

[12] Developer Skills - https://www.cnet.com/news/which-country-has-the-best-programmers-hint-its-not-the-us/

The panel agreed that increased vulnerability disclosures by technology providers and transparent testing processes are needed. Such testing, complemented with certification programs, can be beneficial for both the public and private sectors. Availability of fact-based reports can enable customers to make informed risk-based purchasing decisions depending on their operating environment. Equally as important, vendors can apply the test results to help address product vulnerabilities before they become zero-day threats. Unfortunately, such testing and evaluation criteria being used by the U.S. government is not publicly available today. A positive effort cited by Arrington is the Department of Defense's Cyber Security Maturity Model Certification, (CMMC) focusing on data security.[13] When I asked why not apply the same testing criteria against Huawei, Arrington responded it was a silly question, stating it is against the law, so there is no reason to test Huawei. Schneier responded it is not a silly question, it is a good and fair question and most importantly what is needed.

The Road Ahead

Securing a complex ecosystem takes a holistic approach and multi-stakeholder collaboration. While citing Huawei as a security threat may be justified (assuming it is not based on a false narrative), it is essential we apply the same objective criteria and rigor to every supplier and determine if the identified risks can be mitigated. So, what is needed?

1. Increase transparency of the threats. Doing so will enable all nations to make an informed decision, delineating the political and trade issues from security threats.
2. Convene technology leaders and competitors, including Huawei, to develop best practices and share threat data.
3. Develop testing and certification programs to help prevent, detect, and remediate threats.
4. Shift from a trust but verify model to a zero-trust mindset
5. Take up Huawei's offer to license their technology to help energize U.S. innovation.

Now is the time to put aside the political arguments and focus on driving public-private collaboration to increase the reliability and resilience of the 5G ecosystem and cyberspace. We are faced with a global threat that requires a response to help society to realize the full potential of a connected world.

---

[13] U.S. DOD CMMC - https://www.acq.osd.mil/cmmc/