Don’t Trust Anyone

The ABCs of Building Resilient Telecommunications Networks

By Andy Purdy, Vladimir M. Yordanov, and Yair Kler

The January issue of Prism carried an article titled “The Worst Possible Day”[1] that included a discussion of the implications for the United States of banning Chinese company Huawei from networks that the United States and its allies rely on for national security-related communications. A supporter of the ban, the author, Thomas Donahue, emphasized the critical importance of using equipment from trusted sources in U.S. telecom infrastructure and that of its allies. He argued that the consequences of not doing so could be catastrophic when the United States needs to project power, or convincingly threaten the use of force, such as during a military conflict. The article concluded that the United States needs to seriously consider how to assure the use of trusted alternatives to Huawei equipment, whether by supporting the development of a U.S.-based manufacturer or consortium, or spending tens of billions of dollars to acquire either or both the manufacturers Nokia and Ericsson, or investing significantly in the two Nordic firms.

We cybersecurity professionals at Huawei Technologies concur that the U.S. military and U.S. allies must have access to telecommunications networks that are available at all times, even in the worst conditions imaginable. But we disagree with Donahue’s message that Huawei must be blocked because it is headquartered in China; that companies headquartered in countries allied with the United States can be considered “trusted;” and that the “risk” from Huawei equipment cannot be mitigated. In our view, the best way to assure reliable telecommunication networks is to have a comprehensive approach to risk and resilience, which includes verifiable conformance and testing protocols. When it comes to managing risks in cyberspace, the best approach is to distrust everyone.

For the past year, as telecommunication service providers in numerous countries have begun choosing suppliers for their 5G networks, the United States government (USG) has emphatically told governments around the world that Huawei cannot be trusted to be a supplier to their 5G networks and has put heavy pressure on a number of governments to bar Huawei from 5G development. Donahue articulated his concerns somewhat more dispassionately than most, with an emphasis on what is critical from a national security perspective. He also stressed the importance to the United States and the global community of promoting greater

Andy Purdy is Chief Security Officer, Huawei Technologies, USA; Vladimir M. Yordanov is former Global Cybersecurity and Privacy officer, Huawei technologies; Yair Kler is Head of Solution Security – Europe, Middle East, Africa Region, Huawei Technologies.

competition among telecom equipment providers, which we agree is good for everyone.

This article attempts to explain why we believe that those who argue for the need to block Huawei and assume that Huawei's European competitors' products are worthy of trust, are wrong. Making a determination that a supplier is trustworthy based on the country in which it is headquartered is a misguided and dangerous approach. The article also describes a framework for a holistic cybersecurity strategy that ensures resilient and secure networks—including those with Huawei technology—are available to the United States and its allies, even on the worst possible day.

Washington's Problem and Donahue's Solution

5G will have a major impact on the world economy. It will bring massive cloud-based computing power to the end-user and create new jobs by digitizing and 5G-enabling current and new industries. A 2019 study conducted by the market survey firm IHS Markit, commissioned by the U.S.-based chip and telecom equipment maker, Qualcomm, concluded that by 2035, 5G will enable $13.2 trillion in global economic output, or the equivalent of adding 5 percent to global GDP.

Only a handful of vendors can supply end-to-end 5G equipment, and none of them is headquartered in America. The choices for 5G Radio Access Networks are limited mainly to Nokia, Ericsson, ZTE, and Samsung, but Huawei is generally acknowledged to be the leader in technological development and product range. Ericsson and Nokia are the closest runners-up.

The USG is opposed to using Huawei equipment in its networks and has put forth various reasons for its opposition, usually premised on the claim that China could imperil U.S. national security by using Huawei equipment to shut down networks, steal data, or conduct unauthorized surveillance. Donahue focuses on what he sees as the most significant national security risk to the United States of having Huawei equipment in a key network; that on the "worst possible day"—during a military conflict or a situation when the United States must be able to use military force or deter an adversary from a hostile action—U.S. telecommunications networks, and those foreign networks that enable communications by United States and allies' assets, may not be available if they include equipment supplied by a company headquartered in China. Donahue argues that even for fiber links that withstand hostilities, data traveling over such links could be "subject to disruption if the communications must pass through equipment provided by vendors from hostile countries." Moreover, the United States might not be able to rely on communications satellites as an alternative avenue for key communications.

According to Donahue, this risk cannot be mitigated because "with 5G, the distinction between the edge and the core largely disappears." He contends that this would prevent operators from maintaining proper isolation and, as a result, vulnerabilities at the edge could directly impact and expose the core network to unmanageable risks. Therefore, in his view, it is not enough simply to ban Huawei from the core of 5G; Huawei must be banned from supplying any equipment to any part of networks that may be depended on by the United States and its allies.

Having left the telecommunications industry in the United States to the unpredictability of market forces, the U.S. no longer has a domestic equipment vendor able to provide a full range of products. Moreover, the two European vendors, Nokia and Ericsson, that Donahue presumes are "trusted," are not on strong financial footing. They lack for example, adequate ability to invest in R&D. Donahue argues that, given the strategic importance of secure communications, the U.S. government should step in and either help to fund the development of a strong U.S. supplier or consortium-supplier, invest in telecom firms in friendly countries, or consider buying Nokia, Ericsson, or both. He concedes that this would likely cost tens of billions of dollars.

The Problem with a "Trusted Vendor" Strategy

In Donahue's view, Nokia and Ericsson can be trusted because they are headquartered in countries that are close U.S. allies: Huawei, conversely, cannot be trusted because its headquarters are in China—a strategic U.S. adversary. We do not argue that the two Nordic companies are not worthy of trust in a traditional sense, but strongly urge that the determination that a company is worthy of trust—and thus that its products should automatically be deemed trustworthy—should not depend solely on where the company is headquartered. A few recent cases demonstrate this reality.

In 2013, the retailer Target was attacked through a supplier of air conditioning services.[2] Because it was a trusted supplier, the A/C vendor had remote access credentials to parts of Target's servers for the purpose of monitoring temperature and energy use throughout Target stores. But by tricking one of the supplier's staff through a phishing email, hackers managed to piggy-back on the vendor's access privileges to steal customers' credit card data. The data breach ended up costing Target $292 million[3] in compensation, legal, and other expenses. This excludes lost sales and the impact on share prices.

In 2017, hackers used TeamViewer, a software program used by IT support technicians to repair computers remotely, to breach the servers of Piriform, a company that was in the process of being acquired by cybersecurity software provider Avast. While inside the network, the attackers introduced malware into CCleaner, a widely trusted registry-cleaning tool that has been downloaded more than 2 billion times worldwide. Throughout the acquisition of Piriform, users continued to install CCleaner on their computers. As a result, the corrupted version of the program allowed attackers to penetrate the servers of at least 11 companies, mostly in the IT sector.[4]

Also, in 2017, researchers identified a new type of vulnerability in Intel x86 architecture[5] called Meltdown, which could be exploited by adversaries to bypass computer security protocols and steal secrets processed on it. Additional research[6] identified new vulnerabilities, including Spectre, Spectre-NG, Foreshadow, TLBleed, and ZombieLoad, in Intel's CPU chips. The U.S. military and many other U.S. government agencies are major users of x86-based computers, largely because Intel is widely considered a trusted vendor.

Earlier this year, the *Washington Post* published the news that Crypto AG, a Swiss manufacturer of encryption devices, was owned by the CIA and the German spy agency BND. According to the report, for decades Crypto supplied compromised equipment to more than 120 governments. Backdoors installed by BND into Crypto's machines enabled the United States and Germany to intercept and decrypt highly classified communications from allied nations and foes alike. Buyers trusted Crypto's gear largely owing to Switzerland's carefully cultivated reputation for neutrality.

The common denominator in all of these incidents is that, in each case, attackers compromised the target systems through a trusted vendor. Trust that is not based on evidence is a network security design flaw.

Huawei is headquartered in Shenzhen (southeast China, next to Hong Kong), but both Nokia and Ericsson develop many of their products in China and manufacture hardware there. Ericsson operates five innovation centers in China, including one focused on 5G. Nanjing is the company's largest manufacturing and logistics base worldwide and the location where Ericsson makes its 5G gear. Ericsson has 11,000 staff in China, roughly 5,000 of whom work in R&D.[7]

NOKIA is a multinational communications and information technology company founded in 1865 with substantial operations in China. (Photo by Testing / Shutterstock.com)

Similarly, Nokia co-owns its Chinese subsidiary, Nokia Shanghai Bell, together with a Chinese state-owned enterprise, China Huaxin, which holds just over 49 percent of the venture[8] and has the right to nominate its CEO. From 2002 to 2017, the unit's chairman also acted as the Secretary of the Chinese Communist Party committee within the company (every company of a certain size that does business in China is required to have a Party committee).[9]

Were the United States to buy Nokia or Ericsson (or both), it would be acquiring firms with substantial operations in China, and large numbers of Chinese personnel. Instead of making assumptions about trustworthiness based on where a company is headquartered, it is preferable to focus on the assurance and transparency requirements and features of all the key players, including the telecom and mobile operators, on the one hand, and the equipment (and other third-party) suppliers, on the other.

5G in the U.S. Military

It is commonsense that U.S. national security communications must be available—worldwide—when needed. Donahue contends that if key communications networks are disrupted, the United States may not be able to count on the survival of communications satellites as an adequate alternative: He notes that even communications on still-operational fiber lines could be intercepted by adversaries, particularly if the equipment used was supplied by "vendors from hostile countries."

But the Department of Defense (DOD) is enthusiastic about the use of 5G by the military, as evidenced by a paper it published last year.[10] The paper mentioned several security concerns but, according to the DOD, these are manageable. In the meantime, the evolving industry standards for 5G security are providing demonstrable enhancements.

We must point out the obvious limitations of 5G for use by the U.S. military. First, the U.S. military operates globally but it will be a long time before civilian 5G networks are deployed everywhere the U.S. military or its allies operate. A quick look into the GSMA[11] mobile economy 2019[12] report reveals that by 2025, only 15 percent of the world's mobile network traffic will operate on 5G, while 25 percent of it will, of necessity, use 15- to 20-year-old 2G or 3G technologies. (2G and 3G do not satisfy even the most basic bandwidth requirements for 5G-enabled U.S. military applications.) Based on previous adoption rates of mobile technologies, it would be reasonable to estimate that it will take 5G between 20 and 30 years to reach 80 percent global coverage.

In addition, 5G networks are localized and operate within the coverage area (dictated by local circumstances of the particular state, operator, or geography). Therefore, when traffic is carried outside of state borders or between operators—for example, from a Middle Eastern country to the United States—it must traverse the global backbone and pass through various states and undersea cables, paths which are vulnerable to tampering and disruption, regardless of the vendor or equipment deployed. Thus, while some U.S. adversaries may be developing capabilities to remotely shut down wireless networks, another option is to "cut the wire" as *The National Interest* described in a 2018 article on Russian undersea capabilities. If you have access to a submarine, this direct route would likely be easier than trying to remotely shut down a distant network by routing attacks through multiple operators and their various security controls.

Second, on the "worst day," 5G could be unavailable in one or more of the key fields of operations. Mobile networks are vulnerable to signal jamming and GPS spoofing attacks. In late January 2020, the U.S. Navy conducted a large-scale GPS jamming exercise that covered 125,000 square miles in six U.S. states.[13] News reports also indicate that GPS jamming is widely used by Russia against U.S. fighter jets near Iran.[14] Given the range and reach of such jamming technologies and their potential impact on 5G networks national security critical communications need to have access to alternative network technologies in addition to 5G.

During a conflict, a communications network can come under attack from multiple vectors. To disable 5G networks, attackers will first select the easiest, most direct route offering the highest probability of success. Trying to hack into a 5G network that is designed to field such breaches is a comparatively harder way for an enemy to achieve the intended result.

Security Challenges Posed by 5G

In coming years, governments, businesses, and households will increasingly depend on information and communications technologies (ICT) for essential services. Digitized industries and businesses will create new products and services that use 5G's capability to seamlessly deliver cloud-based computing power to the user: 5G provides high speed, low latency, and the ability to support up to one million connections per square kilometer. The new network technology will be relied on to provide essential government services and manage critical infrastructure such as the

5G Repeater Tower, Mobile Phone Base Station. (Bill Oxford)

power grid, banking, aviation, telecommunications, and public transport, to cite a few examples. And apparently, as we just saw, DOD also plans to use it extensively for military-related purposes.

While the benefits will be numerous, the result of this enhanced connectivity and 5G-enabled services will be an expanded attack surface and a heightened risk of cyber breach or disruption in multiple domains. Attackers will have more potential entry points as they attempt to extract and modify data, disrupt services, and perpetrate other malicious exploits.

Such risks exist with 3G and 4G, but 5G increases their potential impact because more critical services will depend on telecommunications technology. Harm caused by unauthorized tampering with a 5G-connected device could propagate to the rest of the network, using 5G's higher speeds and lower latency to do more damage. In a worst-case scenario, a successful attack could deal a crippling blow to a government, knock out critical infrastructure, paralyze technologies needed for healthcare, and disrupt key supply chains.

In October 2019, the European Commission published a report on the implications of 5G deployment. The report identified five types of risk, linked to the following causes:[15]

- Insufficient security measures
- 5G supply chain
- Third parties such as foreign governments or organized crime
- Interdependencies between 5G networks and critical systems (such as basic infrastructure or healthcare)
- Multiplication of unsecured devices linking to the 5G networks.

These risks, while formidable, have been anticipated by the industry in the collaborative standards process—not just equipment suppliers, but also network operators, device manufacturers, and software developers.

Periphery and Core in 5G: a Distinct Separation

Donahue states that in 5G, "…the distinction between the edge and the core largely disappears," and as a result, Huawei would have access to an entire network even if it only supplies the radio equipment. In fact, although under 5G the core and the edge move closer together in a physical sense, the virtual distinction is maintained and the standards enhance security of both, particularly the "edge."

The distinction between the core and edge in the logical architecture of 5G is defined by 3GPP[16] and the European Telecommunications Standards Institute (ETSI),[17] and recognized by the U.S. Federal Communications Commission (FCC). In addition to the existing core, access, and transport sections of the network, this architecture introduces a new section of the network referred to as edge computing, also known as multi-access edge computing (MEC) in ETSI terminology. According to 3GPP 5G standardization documents, MEC is a disaggregated part of the core network, located closer to the access network in order to reduce network latency. It remains part of the core network and maintains clear logical separation from the access network; and it includes dedicated interfaces as well as possible physical separation. The 5G standards process makes clear that the core and edge separation will be maintained in 5G.

The continued virtual separation of the core from the RAN and the attendant security benefits have been confirmed authoritatively. In June 2019, Professor Alf Zugenmaier (Vice Chair of the 3GPP SA3[18]) and Professor Rahim Tafazolli[19] (University of Surrey), testified on the subject at a U.K. House of Commons hearing:[20] "The core network, as defined by the functions, may be moving out closer to the cell sites….but it is very clear what functions are core network and which are access network," Zugenmaier said. Tafazolli added that, "there is a clear distinction between core and radio access networks wired through a unified interface, which is standardized in the 3GPP standardization." Tafazolli further noted that, "operators have the option of buying the core from one vendor and radio access from other vendors."

A Holistic Risk-Mitigation Strategy for 5G Networks

Effectively managing the risk involved in 5G networks is feasible without barring suppliers and even while using equipment that is not deemed secure. The comprehensive strategy we describe below involves techniques recently endorsed and implemented by the most credible U.S. cybersecurity authorities. This holistic cybersecurity approach includes two design principles and three pillars. The two principles are trust minimization and the assumption of breach:

Trust Minimization; as discussed above, trust should be considered a fatal design flaw. Therefore, any security solution designed for critical infrastructure should minimize, as much as possible, the degree of trust in the underlying components, services, and personnel. Trust should be proven based on facts and should not be assumed.

Assume Breach;[21] a concept that was coined in the early 2000's [22] by Kirk Bailey, who suggested that organizations should build their networks based on the assumption that a well-funded adversary (e.g., a state-sponsored hacker) would be able to infiltrate any system. Bailey's proposed design principle resonated with the U.S. government. In 2016, General Michael Hayden (ret.), the former Director of the CIA and NSA, said, "Fundamentally, if somebody wants to get in, they're getting in… Accept that."[23]

These principles complement each other and should be the foundation for a robust risk-mitigation framework. Trust-minimization and assume-breach have successfully proven themselves under extreme, hostile conditions for the past decade. We mentioned earlier the Intel x86 vulnerabilities called Meltdown, Spectre, Spectre-NG, Foreshadow, TLBleed, and ZombieLoad. Although the vulnerabilities impacted the deepest layer of the system, that is, the hardware layer, the damage was minimal. Leading cloud service providers in the United States had generally adopted a breach-assumption approach that prevented and mitigated serious consequences.

We will now discuss three pillars of a holistic cybersecurity strategy. The first two pertain to trust minimization, while the third relates to anticipating and countering breaches.

Pillar I: Standardization

Standardization is an important pillar in the cybersecurity domain. It provides a common set of guidelines, requirements, and recommendations in a transparent, verifiable, and reproducible manner. Standardization provides experts and laymen, businesses, regulators, and customers with a clear and common understanding of good versus bad. Once set, these common guidelines, requirements, and recommendations are continuously validated and verified by operators and regulators in the domain or industry covered.

The 3rd Generation Partnership Project (3GPP) is the standardization body responsible for the development of 5G standards. Headquartered in France, it coordinates global standard-setting activities for seven national or regional telecom standards groups. Within 3GPP, the SA3 working group is dedicated to the development of security specifications. The SA3 working group includes vendors and operators from around the world. They work together to define cybersecurity enhancements and mitigations that address the risks and challenges identified through a comprehensive risk assessment.[24] In addition, other standardization bodies, such as the European Telecommunications Standards Institute (ETSI), develop and define the security specifications for some of the underlying technologies, such as network function virtualization (NFV),[25] which drive 5G.

Both 3GPP and ETSI have worked extensively on 5G security standards. 3GPP, for instance, developed security enhancements including an overall 5G security architecture, a new 5G key management scheme, enhanced radio access network (RAN) security with user plan integrity protection, network slicing security, network domain security, and management security and cryptographic algorithms.

Representatives of the U.S. government have expressed concerns about the security and reliability of 5G networks. However, scholars at prominent U.S. think tanks noted[26] that the United States has not actively participated at meetings where security standards are being set. Presently, European and Asian vendors account for over 95 percent of all 3GPP SA3 security-related proposals. During the last four years (2016-2019), Chinese vendors submitted over 1,600 5G security proposals alone. Conversely, during the same period, the United States only put forward a handful.

This is seemingly about to change. In May 2020, the Department of Defense (DOD) published its 5G Strategy document[27] acknowledging that "DOD has not engaged with the governance bodies that set mobile wireless industry standards." DOD observed that, "to promote high-quality, protected, and reliable 5G devices and applications, the U.S. must play a lead role in shaping information and communications technology standards."

5G standards will continuously evolve in subsequent 3GPP standards releases.[28] In mid-June, the Department of Commerce issued a new rule[29] allowing U.S. companies to work with Huawei on 5G standardization. Active involvement of the U.S. government and U.S. companies in security standardization will help to ensure that national-level security requirements are captured and reflected in the evolving standards.

Pillar II: Verification and Testing: Security Assurance Specifications [SCAS]

Given the sophistication and resources of a small number of nation states and their capability to virtually implant hidden functionality in hardware and software, it is important that everyone's products be subject to scrutiny to manage the real risk in cyberspace.

Verification and testing align with the principle of trust minimization and are therefore an essential part of a holistic, risk-mitigation strategy. Verification ensures that products and services provided by any vendor satisfy a set of well-defined requirements, thereby reducing the risk that a product behavior is inconsistent with the agreed specification, including in failure scenarios.

Security testing goes a step further by ensuring that the system security properties are not violated even under hostile and/or unpredictable conditions. Various security certification schemes have developed over the past 30 years for the evaluation of vendors' and operators' security posture. These include product-specific standards efforts such as ISO 15408 (Common Criteria) and GSMA/3GPP NESAS/SCAS, as well as company-level risk management schema such as ISO/IEC 270xx, ISO/IEC 28000, and ISO 22301, to name a few.

3GPP and GSMA introduced two new enhancements aimed at increasing operators' security assurance in 5G products with transparency; SCAS—SeCurity Assurance Specifications, and NESAS—Network Equipment Security Assurance Scheme.[30] Together these represent a major contribution toward clear requirements and an independent testing regime for telecommunications equipment.

The work done to date by ISO, 3GPP, or GSMA should be applauded and supported, but it is essential that the collaborative effort continues forward with even broader, more robust input. Currently, operators and vendors do not have clear, comprehensive, standards-based guidance about what equipment they will be allowed to deploy in various countries around the world. 5G verification and testing is a work in progress, which needs additional collaborators.

As is the case for standards-setting, the United States has contributed little to discussions on verification and testing. Such security assurance frameworks would increase business certainty and efficiency, improve the security posture of operators and vendors, and promote transparency. On June 3, 2020 DOD announced, as part of its 5G Strategy, seven new locations for 5G testing.[31] [32] 5G Core security experimentation will take place at Joint Base San Antonio. This development, we feel, puts the United States in a position to help drive the development, strengthening, and adoption of global security standards and testing regimes.

Pillar III: Multi-Level Cyber Resiliency

In 5G networks, developing cyber-resilient systems requires the participation of all key stakeholders. The five main stakeholders in the 5G network are mobile network operators (MNOs), suppliers of services, equipment vendors, vertical industries, and governments. A multi-level cyber-resiliency strategy articulates goals for each of these stakeholders. It also identifies inter-dependencies between stakeholders at the federal and state levels (for example, when a single network hub is shared by multiple operators, which when compromised may pose a national-level risk).

The National Institute of Standards and Technology (NIST) defines cyber resiliency as, "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[33] Cyber resiliency derives from the breach-assumption design principle. It acknowledges that despite standardization and testing, system defenses will be breached. According to NIST; "modern systems are large and complex entities and as such, adversaries will always be able to find and exploit weaknesses and flaws in the systems."

Cyber-resiliency is a realistic, rational approach that has been endorsed and advocated by some of the main agencies in the U.S. government. The U.S. Defense Science Board Task Force has stated that, "susceptibility to the advanced cyber threat by the Department of Defense is also a concern for public and private networks. Cyber resiliency is a critical factor."[34]

Resiliency does not ensure full system integrity. But implemented correctly, it ensures that systems will be able to perform their most critical tasks. "From the perspective of cyber resiliency, system elements or constituent systems that are less critical to mission or business effectiveness can be sacrificed to contain a cyber-attack and maximize mission assurance," NIST advises.

The concept of cyber resiliency is a flexible one that can be adapted to various scenarios. Every organization has different goals and priorities, so each organization has to determine what its mission-critical tasks are. This definition of priorities informs network designers of the resiliency objectives. A top objective might be, "Preclude the successful execution of an attack or the realization of adverse conditions." But at another organization, the top priority could be, "Restore as much mission or business functionality as possible after adversity."

To achieve their cyber-resiliency goals, network designers can choose from a wide array of proven techniques. Below are some of the techniques relevant to 5G security:

- Contextual Awareness; construct and maintain current and correct representations of the system's security posture, revealing patterns or trends in adversary behavior.
- Analytic Monitoring; maximizes the ability to detect potentially adverse conditions and identify potential or actual damage.
- Coordinated Protection; requires an adversary to overcome multiple safeguards (i.e., implement a strategy of defense-in-depth), increasing the cost to the adversary and raising the likelihood of detection.
- Deception; hide critical assets from adversary or expose covertly tainted assets.
- Substantiated Integrity; detect attempts by an adversary to deliver compromised data, software, or hardware, as well as successful modification or fabrication.

Resources availability is one of the components of cyber-resiliency. This essentially refers to the ability to obtain critical system components even in times of crisis. The early days of the COVID-19 pandemic, when countries—even close allies—were hoarding medical supplies, served as a reminder of the importance of ensuring critical resources availability even under the most abnormal circumstances. To do this national governments need to systematically identify key components that need to be stored and for how long. For a superpower like the United States, it may in addition be appropriate to have at least some capability for strategic local manufacturing. This is the approach that is apparently being followed with Taiwan Semiconductor,[35] a critical supplier of electronic components, which has agreed—in principle—to build a plant in Arizona.

With a well-designed cyber-resiliency strategy, countries can be predominantly vendor-agnostic in cybersecurity terms. The United States could potentially allow any vendors, regardless of their state of origin, to be in any section of the network, including the network core. While this may sound risky to some, especially given the current political environment, this conclusion is built on analysis by world experts, as well as on a rich foundation of sound academic work.

In the next section, we look at supplier diversity. This is one of the most frequently cited elements of a cyber resiliency strategy. As we will see below, it is not primordial in importance, and it is certainly not a cure-all.

The Pitfalls of Relying on Vendor Diversity

Politicians and the media sometimes cite supplier diversity as a silver bullet to address cybersecurity risks. It was mentioned prominently in the EU 5G toolbox released earlier this year.[36] In fact, supplier diversity plays a relatively minor role in cybersecurity. And if misunderstood or poorly implemented, supplier diversity can actually become a threat to network integrity.

Diversity is only one of fourteen resiliency techniques listed both by NIST and MITRE.[37] According to NIST, diversity encompasses six different sub-categories, including architectural diversity, design diversity, synthetic diversity, information diversity, path diversity, and of course supply chain diversity.

Diversity can enhance cyber resiliency, but it can also undermine it. In its cyber-resiliency design principles document,[38] MITRE noted that,

> Diversity can be problematic in several ways: first, it can increase the attack surface. Rather than trying to compromise a single component and propagate across all such components, an adversary can attack any component in the set of alternatives, looking for a path of least resistance to establish a foothold.
>
> Second, it can increase demands on developers, system administrators, maintenance staff, and users, by forcing them to deal with multiple interfaces to equivalent components. This translates into increased lifestyle costs. (These costs have historically been acceptable in some safety-critical systems.) This can also increase the risk that inconsistencies will be introduced, particularly if the configuration alternative for the equivalent components are organized differently.
>
> Third, diversity can be more apparent than real (e.g., multiple different implementations of the same mission functionality all running on the same underlying OS, applications which reuse software components). Thus, analysis of the architectural approach to using diversity is critical.

While we understand why supplier diversity is prominent in public discourse on 5G security, its importance must be kept in perspective.

Network Resiliency Under Extreme Conditions

Modern military conflicts put communication networks under extreme duress. The U.S. military can resort to alternative and highly robust systems when necessary. We very briefly present some examples below.

The Defense Advanced Research Projects Agency (DARPA) has been working on mobile ad hoc networks (MANET)[39] since the early 1970s. These networks can be deployed in hostile environments ensuring the bandwidth requirements of U.S. forces would not be impacted by enemy threats. And low-orbit, high-speed satellite technology, such as those currently being developed by U.S. vendors,[40] can be further enhanced and secured to satisfy current and future availability, confidentiality, and integrity requirements.

Resilient-system design is another tool that could be used on actual or likely battlefields. Military and intelligence agencies are proficient at building applications and services that can share information using multiple concurrent communication paths based on the networks' availability. This ensures that if network disruptions occur in one operator or in multiple operators, communication channels will still operate, even under hostile circumstances.

To enhance the resiliency and survivability of U.S. military networks and foreign networks that support the U.S. military in other countries requires investment in technology and personnel. Rather than spending tens of billions of dollars to acquire or subsidize Nokia or Ericsson, we propose that U.S. network resiliency would be better served by spending on refining and deploying technologies that can survive hostile environments, developing people who can build and operate such networks, and conducting R&D to develop better tools and protocols to achieve greater assurance.

Conclusion

Excluding certain vendors while trusting others without assessing and addressing real cybersecurity risk, makes no sense from an economic or cybersecurity perspective. The United States is so intent on blocking Huawei from U.S. and allies' networks that it is considering alternatives that could cost tens of billions of dollars; buying or investing in Nokia or Ericsson, or both, or investing in an alternative U.S. company or consortium, or some alternative technology. Opposition to Huawei bridges the acrimonious political divide in the United States like few other contemporary issues.

Trustworthiness does not play a role in cybersecurity. What matters far more is the transparency of telecom suppliers' operations, including whether and how they provide ongoing support to the operator after equipment is installed. Selecting a supplier should be based on the quality and reliability of its products, their demonstrable conformance to standards and best practices, as well as compliance with regulatory and contractual requirements.

Some have said candidly about Huawei that "it is not about the company, it is about the country." Given the availability of trustworthy, transparent and—as seen earlier in this article—proven risk-mitigation mechanisms, the U.S. government's decision to ban Chinese equipment vendors appears clouded by geopolitical concerns; namely China's rise economically, militarily, and technologically.

Banning vendors reduces competition and ironically increases the cybersecurity risk; the UK's Intelligence and Security Committee (ISC) stated in July 2019 that, "limiting the field to just two vendors,.., would increase over-dependence and reduce competition, resulting in less resilience and lower security standards."[41] [42] We believe that global vendors play an essential role in the competitive landscape, bringing unique expertise, experience, and knowledge. Greater competition brings multiple benefits; greater innovation, lower prices, and—when well-implemented—greater resilience.

Huawei's top executives have stated that they are interested in talking with the U.S. government about how the company can address cybersecurity concerns and demonstrate that neither Huawei products nor its employees are subject to the undue influence of the Chinese (or any other) government. Huawei would discuss manufacturing in the United States,[43] opening Huawei to independent testing pursuant to recognized standards and best practices for telecom equipment,[44] or licensing Huawei's 5G technology to a U.S. company or consortium.[45]

If domestically fostering a vibrant technology and telecom sector is the policy of the United States, then the way forward is a tried and true one: Form a private sector-led, public-private partnership to develop and implement a U.S. industrial technology innovation strategy. This will involve investing in R&D, providing sectoral incentives, funding university research, attracting the smartest minds in the world, and encouraging foreign investment.

It is not clear what the U.S. government will do next. But with trade tensions poised to weaken global growth, and roughly half the world's population still lacking internet access, one can hope that Washington will begin focusing on how to promote the spread of safe digital technology. PRISM

Endnotes

[1] Thomas Donahue, "The Worst Possible Day: U.S. Telecommunications and Huawei," *PRISM* 8.3, (2019):15, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3.pdf, p. 15.

[2] Liam Tung, "Target hackers hit air-conditioning firm first as a way in," *ZDNet,* February 6, 2014, https://www.zdnet.com/article/target-hackers-hit-air-conditioning-firm-first-as-a-way-in/.

[3] Target Annual Report, (2016): 44, https://corporate.target.com/_media/targetcorp/annualreports/2016/pdfs/target-2016-annual-report.pdf.

[4] Lily Hay Newman, "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner," *Wired,* April 17, 2018, https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/.

[5] x86 refers to Intel's CPU architecture developed by Intel. X86 is used in hundreds of millions of computers in the U.S. and worldwide.

[6] Lindsey O'Donnell, "ZombieLoad: How Intel's Latest Side Channel Bug Was Discovered and Disclosed," *Threatpost,* May 20, 2019, https://threatpost.com/zombieload-how-intels-latest-side-channel-bug-was-discovered-and-disclosed/144849/.

[7] Zhao Juntao, "President of Ericsson China: epidemic spread, global 5G demand has not been weakened," interview by Liu Yuying, March 30, 2020, https://www.tellerreport.com/business/2020-03-30---president-of-ericsson-china--epidemic-spread--global-5g-demand-has-not-been-weakened-.SyeikYbyvU.html.

[8] Nokia Corporation, *Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture,* May 18, 2017, https://www.nokia.com/about-us/news/releases/2017/05/18/nokia-and-china-huaxin-sign-definitive-agreements-for-creation-of-new-nokia-shanghai-bell-joint-venture/.

[9] Telecoms, "Nokia and Ericsson have links to China's Communist Party," *Telecomstechnews,* August 13, 2018, https://telecomstechnews.com/news/2018/aug/13/nokia-ericsson-china-communist-party/.

[10] Defense Science Board, "Defense Applications of Fifth Generation Network Technology," June 24, 2019, https://www.hsdl.org/?abstract&did=828623.

[11] The GSM Association (GSMA) represents the interests of mobile network operators worldwide. Its members include over 750 mobile operators. Other companies active in the telecommunications industry also participate in GSMA activities.

[12] GSMA, "The Mobile Economy 2020" (2020), https://www.gsma.com/r/mobileeconomy/.

[13] Tom Demerly, "U.S. Navy Now Jamming GPS Over Six States and 125,000 Square Miles," *The Aviationist*, ' January 23, 2020, https://theaviationist.com/2020/01/23/u-s-navy-now-jamming-gps-over-six-states-and-125000-square-miles/.

[14] David Axe, "Why and How Russia Is Jamming American Fighter Jets Near Iran," *The National Interest,* January 17, 2020, https://nationalinterest.org/blog/buzz/why-and-how-russia-jamming-american-fighter-jets-near-iran-115021.

[15] European Commission and the Finnish Presidency of the Council of the EU, "Member States publish a report on EU coordinated risk assessment of 5G networks security," October 9, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

[16] The 3rd Generation Partnership Project, better known as 3GPP, is a confederation of standards organizations which develop protocols for mobile telecommunications. 3GPP will be described in more details further down in the section on standardization.

[17] The European Telecommunications Standards Institute is one of the leading standard-setting organizations worldwide. Will be discussed later in this paper.

[18] The SA3 working group within 3GPP is dedicated to the development of security specifications.

[19] Tafazolli is Professor of Mobile and Satellite Communications at the University of Surrey, Director of the Institute of Communication Systems, and Director of the 5G Innovation Centre.

[20] The hearing focused on the U.K.'s telecommunications infrastructure. It was organized by the Science and Technology Committee of the House of Commons. Minutes available here: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.html.

[21] Jeffrey J. Guy, "Who coined "assumption of breach?," *Armatum Networks,* May 11, 2012, http://armatum.com/blog/2012/who-coined-assumption-of-breach/.

[22] Ernie Hayden, "Data breach protection requires new barriers," *TechTarget,* May 2013, https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers.

[23] John Miller, "FBI fighting two-front war on growing enemy - cyber-espionage," *CBS News,* May 23, 2012, https://www.cbsnews.com/news/fbi-fighting-two-front-war-on-growing-enemy-cyber-espionage/.

[24] 3GPP, "3GPP Specifications per TSG/WG," https://www.3gpp.org/DynaReport/TSG-WG--S3.htm.

[25] ETSI, "Network Functions Virtualisation (NFV)," https://www.etsi.org/technologies/nfv.

[26] Theresa Hitchens, "US Risks Losing 5G Standard Setting Battle To China, Experts Say," *Breaking Defense,* May 11, 2020, https://breakingdefense.com/2020/05/us-risks-losing-5g-standard-setting-battle-to-china-experts-say/.

[27] Department of Defense," Department of Defense (DoD) 5G Strategy (U)," May 2, 2020, https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf.

[28] During the development of the 3GPP 5G security standards, Dr. Anand R. Prasad, then chairman of the 3GPP SA3, noted that "the reassessment of other security threats such as attacks on radio interfaces, signaling plane, user plane, masquerading, privacy, replay, bidding down, man-in-the-middle and inter-operator security issues have also been taken in to account for 5G and will lead to further security enhancements." https://www.3gpp.org/news-events/1975-sec_5g.

[29] https://www.cnet.com/news/us-firms-now-allowed-to-work-with-huawei-on-5g-standards/.

[30] SCAS is a set of security specifications for 5G equipment and NESAS defines security requirements and an assessment framework to audit the vendor's product development and lifecycle management process. Vendors would verify their products in special ISO 17025-certified, GSMA-recognized testing labs. These new security-assurance schemes provide additional validation that products adhere to the security specifications, further minimizing the need to rely on the trusted vendor approach. Various leading European regulators have been evaluating NESAS as well as other cyber-security certification schemes as potential candidates for 5G certification.

[31] Corinne Reichert, "US Defense Department ramps up 5G testing," *CNET,* June 4, 2020, https://www.cnet.com/news/us-defense-ramps-up-5g-testing/.

[32] Department of Defense, "DOD Names Seven Installations as Sites for Second Round of 5G Technology Testing, Experimentation," June 3, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2206761/dod-names-seven-installations-as-sites-for-second-round-of-5g-technology-testin/.

[33] Ron Ross, "Building Cyber Resilient Systems," National Institute of Standards and Technology, https://csrc.nist.gov/CSRC/media/Presentations/building-cyber-resilient-systems/images-media/Building-Cyber-Resiliency-MITRE-20180508.pdf.

[34] Ron Ross, Victoria Pillitteri, Richard Graubart Deborah Bodeau and Rosalie McQuaid, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," National Institute of Standards and Technology, November 2019, https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final.

[35] Debby Wu and Ian King, "Taiwanese Chipmaker Plans to Build $12 Billion Factory in Arizona," *Time,* May 15, 2020, https://time.com/5837274/tsm-chip-plant-arizona/.

[36] European Commission, "Secure 5G networks: Questions and Answers on the EU toolbox," January 29, 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

[37] MITRE is a federally funded research and development corporation. MITRE describes its main areas of research as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

[38] Deborah Bodeau and Richard Graubart, "Cyber Resiliency Design Principles," *MITRE,* January 2017, https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[39] DARPA, "DARPA Seeks Clean-Slate Ideas For Mobile Ad Hoc Networks (MANETs)," April 4, 2013, https://www.darpa.mil/news-events/2013-04-30.

[40] Kristin Cooke, "SpaceX Satellite Internet: What You Need to Know about Starlink," *Satelliteinternet*, May 8, 2020, https://www.satelliteinternet.com/providers/starlink/.

[41] Kat Hall, "Excluding Huawei from UK's 5G will harm security, MPs warn," *The Register,* July 19, 2019, https://www.theregister.co.uk/2019/07/19/excluding_huawei_from_5g_will_harm_security_mps_warn/.

[42] Full report: https://www.parliament.uk/documents/other-committees/intelligence-security/Critical-National-Infrastructure-Report.pdf.

[43] Reuters, "Huawei to Build First European 5G Factory in France to Soothe Western Nerves ," *Voice of America,* February 27, 2020, https://www.voanews.com/silicon-valley-technology/huawei-build-first-european-5g-factory-france-soothe-western-nerves.

[44] Aurel Dragan, "Huawei opens a Center for Cyber Security Transparency in Bruxelles," *Business Review*, June 3, 2019, https://business-review.eu/tech/huawei-opens-a-center-for-cyber-security-transparency-in-bruxelles-197636.

[45] Arjun Kharpal, "Huawei's offer to license 5G tech to US firm to create an American rival is still 'on the table'," *CNBC,* February 26, 2020, https://www.cnbc.com/2020/02/26/huawei-reiterates-offer-to-license-5g-tech-to-us-firm-to-create-rival.html.