Drexel Hamilton
A Service-Disabled Veteran Owned & Operated Business

Drexel GPS – "Outside the Wire"

The Global Supply Chain Disruption – Wakeup Call for 5G in the U.S?

Photo Credit: Getty Images/iStockphoto

There are many lessons to be learned from the Covid-19 pandemic-most of them are still being written. As of this writing Covid-19 is still indeed a pandemic and far from being eradicated. The world is striving to return to and define what the definition of a "new normal" is as we continue to battle against the virus amid seesawing lockdowns, and vaccine-resistant strains. One of the biggest lessons highlighted during this time is the fragility of the global supply chain as a result of decades of practices that placed a significant and lopsided premium on efficiency rather than resiliency of its networks. The result has been shortages and delays in everything from furniture to critical semiconductors.

5G represents revolutionary change in technology and will be instrumental in everything from finance to military defense capabilities. Amid the backdrop of increasing global tensions and a shift to what appears to be a much more aggressive military stance by China in Asia and the African continent as well, this should be a logistical wake-up call for the United States to develop smart policy free from partisan politics to accelerate and develop domestic infrastructure capabilities in all critical areas of 5G utilizing an all-hands on deck approach. This includes private sector partnerships to ensure that the US is not only a leader in 5G but is capable of projecting and exporting the expertise and capabilities of that leadership globally. Doing so will reap economic as well as political benefits.

Any logical focus on China should thrusts 5G into the spotlight. This emerging technology has enormous promise and potential for future use across a broad and increasingly widening variety of applications, many of which have yet to be invented. The government of China is currently directing an enormous allocation of resources towards not only developing, but perhaps even more importantly, seeking to dictate the specifications on which the future of 5G infrastructure is built globally. The high priority and relevance of this investment is reflected in a 2017 China Academy of Information and Communications (CAICT) report which

predicts that by 2030, 5G will account for roughly 800 billion (USD) in economic activity for China. CAICT also forecasts that by 2025, China alone will account for over 420 million 5G connections, representing nearly 40% of the global total. The impact of these actions can and will influence the national security of the United States and should be viewed in the context of the Chinese Communist Party's overall strategy. 5G should be a vital area of focus for the security and economic well-being of the United States when developing a comprehensive, dynamic, and viable national security strategy.

The term 5G itself is the nomenclature given to the latest iteration of wireless communications technology. As advances in speeds and technology in wireless have progressed, the iterations such as 1G, 2G, 3G, and 4G have been used to identify significant advancements in wireless capabilities. The "G" denotes when a transition point is reached as a result of advancements in various applications such as encoding, air-interfaces, and hardware. The new technology is no longer efficiently backward-compatible with the older one. An important aspect of how 5G functions and why it poses a totally new challenge for cybersecurity is that its core networking functions are software-based as opposed to being developed around a hardware-centric system. There are many advantages to a software-based network, including lower operating costs, reduced local hardware footprints, and enhanced capabilities required for today's global internet. However, when evaluating the integration of 5G from a cybersecurity professional's perspective, a key concern must be the increased ease and access to deploy unmanaged and unsecured software-defined devices on networks that presents heightened risks by introducing additional attack surfaces.

Decentralized software-based networks present unique challenges and can be more difficult to protect. IoT (internet of things) technology is expanding globally, and that expansion will be positively correlated to advances in 5G availability. IoT's platforms will increase the number of attack surfaces and threats to networks that must be defended exponentially. In a fully integrated IoT environment, large initiatives like Smart Cities and autonomous vehicle fleets, along with small non-traditional items not currently included in most cyber-threat matrixes will need to be accounted for in a cybersecurity strategy such as home appliances and even light bulbs.

A critical element of 5G is that it is very spectrum-dependent, and that spectrum requirement is a key component the Chinese BRI/DSL (Belt & Road Initiative/Digital Silk Road) strategy is seeking to exploit. The optimal bandwidth for 5G to operate based on cost and data capabilities is in the sub-6 GHz spectrum. The higher spectrum frequencies, particularly at the 24 and 28Ghz, are referred to as millimeter-wave (mmWave) 5G and at this range allows for more channels (data) per allocated amount of bandwidth. However, the drawbacks at these frequencies include reductions in both transmission distance and building penetration. According to multiple studies, mmWave 5G at the currently accepted U.S. telecom standard of 425 MHz of spectrum at 28 GHz was not only 4 times more expensive to deploy but that the current Chinese 5G standard of 250 MHz of spectrum at 3.4 GHz would provide 5G coverage to 54.1% of the US at 100Mps with 22% of that area achieving 1Gbps. In comparison, the mmWave achieved a coverage area of only 11.9% at 100Mbps with only 3.9% of that achieving 1Gbps.

The sub-6 spectrum is the model that the Chinese are promoting and building globally in conjunction with the

Digital Silk Road initiative. The target countries for BRI expansion are looking towards 5G as a means to digitally "leapfrog" and thereby jumpstart their economies through modernization of these communication networks, ditching the established model of waiting for the pricing of older slower legacy systems to drop down to a level they can afford. Chinese telecom equipment from the likes of Huawei, China Telecom, and ZTE provides a lower/low-cost solution. The United States has not traditionally enjoyed the "first-mover" advantage when it comes to adopting new wireless technologies from their inception. Instead, what the U.S. has historically proven effective at is catching up and surpassing the rest of the field when it did enter the arena. This was in no small part because private industry, including the telecoms, had full access to the assigned frequency spectrums on which to develop products and services.

Currently, this is not the case with the sub-6 spectrum which, based on a cost/coverage/data-capacity ratio, is considered the optimal range for 5G, yet is not readily available to private industry for commercial use. The Department of Defense (DoD) owns and controls this sub-6 spectrum of 5G and there is significant pushback within the DoD against giving it up and/or changing current spectrum allocations. This is one of the major factors involved with the current U.S. telecom industry's decisions to use mmWave as its5G standard as opposed to sub-6. It should be again noted that the majority of 5G plans globally are designed on the sub-6 spectrum.

This is highly significant for a variety of reasons. As of this writing, there are no U.S. companies that manufacture 5G telecom equipment for wireless access stations and other systems at scale that are critical for the implementation and operation of a 5G network. Seventy-five percent of the world's 5G equipment manufacturing is done by 5 companies, 3 of which are Chinese owned: Huawei, ZTE, and China Telecom. EU companies Ericsson and Nokia make up the other 2. Of the 5, the Chinese companies account for approximately 60% of that manufacturing.

The primary concern is not that the U.S. will be unable to develop a 5G network based on mmWave standards, currently Swedish-based Ericsson is supplying that very equipment to U.S. telecoms such as Verizon and AT&T. However real risk lies in the US becoming technologically "isolated" due to non-compatibility issues from the rest of the world if it maintains the current course and does not provide solutions for private markets, (particularly the major U.S. based telecoms), to access the sub-6 5G spectrum while simultaneously not providing incentives and alternatives to dissuade BRI-targeted countries from utilizing Chinese equipment and standards for 5G.

Historically, aside from 1G, the United States has never been the first to embrace the newest "G" iterations of wireless technology. Where the US has led is in the subsequent innovation and associated businesses created around developing applications that utilized these technologies, particularly with 4G. The U.S. was able to accomplish this in many cases by leveraging its ability to provide a robust and accessible market for telecom manufacturers that provided an incentive for them to provide low/lower cost 3G/4G equipment both commercially and at the consumer level. This technology- its affordability and the resulting ease of access to it- resulted in many of the innovations and business developments based on 3G and 4G to originate in the United States.

The advantages that the U.S. has historically benefitted from when it comes to innovation and design which are later exported globally could potentially be severely curtailed due to the lack of developing domestic expertise on the sub-6 spectrum. If China is successful in shaping the global 5G standard while also becoming the dominant manufacturer and provider of 5G telecom equipment, this reinforces the concerns raised by some in the cybersecurity community who point to Article 47 of the Chinese Cyber Security Law enacted in 2017. According to the provision, "**Network Operators are required to monitor the information released by their users for information that is "prohibited from being published or transmitted by laws or administrative regulations**."

Article 47 is very important to take note of especially if viewed as a component of the Chinese BRI doctrine/strategy. In 2016 China passed its first comprehensive digital privacy/security regulation known as the **CSL** (Cybersecurity Law). It has many articles within it which seem to be taken directly from the pages of the EU's GDPR playbook, but it also has many opaque and unclear definitions.

The wording of Article 47 sets up a plausible scenario in which a private, yet Chinese-owned company enters into an agreement with a government to provide 5G infrastructure, equipment, and support This company (e.g., Huawei/ZTE) could be categorized as the "Network Operator", making it liable under a loosely interpreted definition of the CSL to comply in accordance with Article 47 and provide some type of "backdoor "network access.

This analysis of that CSL provision is not a statement to make an accusation at this time that the Chinese government or Chinese telecom companies engaged with providing BRI assistance are installing these types of network backdoors. However, from a national and global security/cybersecurity perspective, this is a scenario that should be properly vetted and not ignored when developing and determining associated policy.

NOTE: The BRI/DSL definition of "support" includes the fiber-optic backbone that 5G networks will operate on and not just the wireless components of its infrastructure. Fiber-optic backhaul functions have distinctly different core functions than the 5G wireless technologies that are the focus of this edition of "Outside the Wire". So, while they are not the focus of this analysis at this time it can be assumed that when "support" or "infrastructure" is mentioned when referencing BRI/DSL- that a component of the fiber-optic transport layer is implied.

The current technological landscape that we are operating in will change dramatically with the advances that are made possible with 5G. Building the infrastructure of future 5G networks should be viewed in the same regard and level of significance as the laying of the first transatlantic cable between Europe and The United States in 1866.

In the aftermath of that milestone, England held a dominant market share of the transatlantic cables along with the associated command and control of them. On August 5th, 1914, a day after declaring war on Germany, Britain cut five of Germany's telegraph cables. Those cables remained disabled for the remainder of the conflict. Had that not occurred would the outcome of the conflict be different? Historians will debate about

that incessantly. However, what should not be debated is that the ability to monitor, disrupt or completely cut off an adversary's communication networks at will is always an advantage in warfare.

That same capability (backdoor network access) even if not in an armed conflict would still be a distinct advantage for a sovereign nation today especially in today's digital world and the development of data-driven areas of the economy such as Fintech. China's Digital Silk Road strategy as it pertains to 5G is not designed to make major financial gains into the market share of the telecoms currently operating out of the United States. It is better defined as a global strategy aimed at acquiring market share in areas of the world that the United States and U.S. companies currently have little to none. Thereby establishing itself (China) as the dominant market force while simultaneously as a result of BRI contracts and agreements, erecting barriers to entry for U.S. companies to enter these markets, including 5G.

This could theoretically provide China and Chinese companies with a profitable and reliable global revenue stream. Combining this result with success in dictating and shaping the global 5G infrastructure standards, China would place itself in a position to shift away from its current economic practices which are based largely on a program of stealing the innovation and IP of other nations and achieving one of its desired goals by displacing the United States as the hub for wireless communications tech innovation. China would then, in theory, take the lead in the design of applications based on 5G as a result of the development of its domestic talent pool and SMEs (subject matter experts) in the field as a result of the exportation of Chinese 5G infrastructure and equipment to BRI-targeted countries and in short order globally to non-BRI areas of the world that will rely on the systems that would make up the core of their 5G network.

Many lessons will be learned from this pandemic. Will building up critical 5G domestic capabilities be one the U.S. learns in time?