Cover Page Photo: Courtesy Adobe

Key Acronyms

5G - 5th Generation

3GPP - 3rd Generation Partnership Project

5G NC - 5G Next Generation Core

5G PPP - 5G Infrastructure Public Private Partnership

AR/VR - Augmented Reality / Virtual Reality

BRI - Belt and Road Initiative

C2 - Command and Control

CCP - Chinese Communist Party

CISA - Cybersecurity and Infrastructure Security Agency

DDoS - Distributed Denial of Service

DHS - Department of Homeland Security

DPRK - Democratic People's Republic of Korea

DSS - Dynamic Spectrum Sharing

DoD - Department of Defense

FCC - Federal Communication Commission

FTC - Federal Trade Commission

GHz - Gigahertz

IMSI - International Mobile Subscriber Identity

IOT - Internet of Things

IRC - Information Related Capabilities

ISP - Internet Service Provider

ITU - International Telecommunication Union

MNO - Mobile Network Operator

NIST - National Institute of Standards and Technology

NR - New Radio

NTIA - National Telecommunications and Information Administration

PRC - People Republic of China

RAN - Radio Access Network

SBA - Service Based Architecture

SDN - Software Defined Networks

SIM - Subscriber Identity Module

SUPI - Subscription Permanent Identifier

TA - Target Audience

TTPs-Techniques, Tactics, and Procedures

WPK - Workers Party of Korea

ZPMC - Shanghai Zhenhua Heavy Industry

vRAN - Virtualized RAN

Key Findings

This team conducted research on security issues related to the introduction of 5G mobile communications into the United States and abroad. The topic of 5G has been subject to a certain degree of hype, mischaracterization, and misunderstanding. Because of this and the obstacles this presents to understanding the 5G world and its security implications, the objective of this paper is to take a survey approach to the 5G issue and its security implications in order to put the 5G issue into context. The paper begins with an overview of the 5G ecosystem as it is developing and will mature. For the purposes of this paper's discussion, 5G is best described as a fifth-generation wave of investment in mobile technology. The paper then looks at threats to 5G technology and 5G networks. These threats are primarily technical in nature. The next section looks at threats coming from the adoption of 5G technology. Here the team opens the aperture and looks at broader threat implications related to 5G such as social and political implications of the emergent 5G environment. This includes issues related to human rights. These are threats that have generally not been as widely discussed as the more traditional technical threats. Having established a baseline description of the 5G ecosystem and the threats, the team looks briefly at the international aspects of these issues and their regulatory and policy aspects.

In addition to the research captured in this white paper, the team drafted a 5G threat mitigation checklist. Resources such as checklists make the language simple and important for non-technical high-level leaders and decision makers to consider the integration of critical cybersecurity measures along with the cost attached to it as they plan to expand their infrastructure to integrate the cybersecurity of their 5G ecosystem. Checklists are very useful when it comes to the following points: Enterprise Resource Planning (ERP) Planning, Quality Control and Quality Assurance, a robust guide in Executive Board (EB) meetings of organizations and other high-level national and international meetings. The checklist serves as our tool to guide the policy-level leaders, heads of the public and private sectors to have internal discussions to check their current infrastructure and plan for future investments toward ensuring a secure 5G platform. The CEOs and leaders of the government and private sectors could use this tool along with their ERP team, to help the organizations enhance data security of their unified cloud-based digital platform.

.

5G Cybersecurity White Paper

Section 1: The Definition of 5G

Foundationally, 5G is defined as the fifth generation of mobile and cellular networks. However, extensive interviews with subject matter experts throughout the course of research for this paper revealed a diverse list of definitions, with many experts using different ones and others neglecting to define the term at all. Most of the apparent disagreements within the community of 5G experts are the result of different parties talking past one another, relying on incomplete understandings and assumptions. Therefore, beginning this paper by cataloging the range of definitions in use by the tech community focused on 5G is an inherently important contribution to the research. After all, the agreement of common objectives and defined terms is a prerequisite to effectively securing our emerging 5G infrastructure and safely deploying the benefits of this technological leap forward.

Throughout this piece, the applicable definition of 5G will be helped, whenever possible, by specifying which 5G feature is being referred to, in which context, and by whom. It is the answers to these three questions that begin to demystify 5G and its impacts on our lives.

A Brief History of the (5G) World

Several of the most experienced and technical experts interviewed for this piece claimed that defining 5G formally is easy – it is a set of technical ground rules that define the workings of a cellular network. This can include, for example, radio frequencies 5G uses and how various components like computer chips and antennas handle radio signals and exchange data. These specifications are articulated by a global industry association called the 3rd Generation Partnership Project (3GPP), which makes recommendations to a United Nations (UN) - sanctioned neutral governmental body called the International Telecommunication Union (ITU). The ITU formally adopts and promotes standards, which are then implemented by the industry entities within 3GPP via collaborative systems-engineering, and eventually spread to become the norm for 5G features across the broader tech sector. Technology specifications that define a phenomenon such as 5G evolve over time and are grouped by "release," with 5G being introduced to the world via a launch called 3GPP Release 15. This launch occurred via three separate parts, known as *drops*, from 2017 through 2019.

Each drop freezes a standard or specification. Drops are then integrated into commercial products, such as infrastructure like Radio Access Network (RAN), base stations, backhaul or core network elements, or in end-user devices like phones. Products based on a given release may come out months or even years after the initial release announcement. At any given time, there are parallel efforts of specification development and commercial production that vary across drops or releases, building on one another. Complicating this further is that each release contains new features.

Security features of 5G, for instance, continue to evolve. Commercial adoption of those features, like many other features of 5G, are not always required for a product to be "3GPP compliant." Many of the features that people often associate with 5G—including increased speed, decreased latency, increased ability to support multiple devices, and use of higher spectrum—were included in the second drop of Release 15, while several other features associated with 5G, like network slicing, private 5G networks, and dynamic spectrum sharing (DSS) were not available until 3GPP Release 16. Additionally, newer releases are expected, though currently delayed – demonstrating that the 5G standard and its associated features continue to develop.

The 5G Definition Problem - Separated by a Common Language

The formal definition of 5G, then, can be dependent on the 5G requirement or feature that users are interested in, and whether they are referring to the formalization of the standard or the commercial products that include those features.

Unfortunately, this is generally not the definition as understood by the public. The various marketing practices used by operators tend to obfuscate what each generation of technology entails. Rather, it is typical for operators to promote the adoption of early versions of a technology and build expectations, sometimes overly optimistically, to gain market share.

Concurrently, other factors affect the public's awareness and understanding of 5G. Governments auction spectrum, for example, are often held with the promise of making spectrum available to meet the public's needs for growing broadband. Some of those spectrum auctions, particularly for those < 3Ghz (Gigahertz) frequencies, could have been used by 4G networks, and so aren't necessarily formal 5G activities. Many of the frequencies specific to 5G are not being deployed and may in fact contribute to future generations of wireless broadband. The same could be true of new network RAN architectures such as Small Cell, which have smaller antennas placed closer to the user, typically using higher frequencies compared to 3G and 4G networks. This includes small radios located on the top of streetlight poles that might have a range of a few hundred feet, as opposed to large towers used by mobile operators, which could transmit a cross a radius of a mile or two.

An Uncertain Future – If We Build It, Will They Come?

5G might be more practically understood as the fifth wave of major investment by global wireless network operators. This wave includes massive spending to upgrade network infrastructure and roll out networks at various frequencies. It includes many technology features rolled out over a series of "5G" parallel drops and releases. However, for any feature, users need to look not only at its specification date, but at its adoption by telecommunication vendors and businesses. Importantly, those adoptions are a function of significant capital expenditures by firms facing stiff competition not only from their traditional competitors, but also subject to disruption from market dynamics and new operators, including cable companies. Changes to existing business landscapes, where

cloud and content providers compete for an unknown share of the end-user revenues, bring further complications.

Like other promising technologies and trends, 5G adoption is driven by real or potential demand within the marketplace. 5G might have business cases in self-driving cars and robotic remote surgery, but not until the businesses within those industries start to signal commercial interest and adoption of these platforms will those cases become a reality. The operator economics and ultimate return on major investments rests with subsequent demand for future products and features by 5G end-users.

This fifth wave might involve frequencies and network elements used in earlier waves of wireless Gs, or it might rely on features specific to a given 5G network release. At present, 5G as a term typically represents evolving specifications of highly virtualized network architectures that have enabled operators to move away from single-vendor driven hardware defined architectures to more diverse, lower-cost, software-defined architectures. However, depending on a user's background, it could also describe a future feature, such as the production availability of network slicing. This wave promised remarkable features and use cases: faster speeds, more security, more reliability, less latency, and perhaps lower cost, which could then translate into self-driving cars, remote surgery, and automated factories. All of these promises included a range of nuances and caveats. For example, 5G not only has lower latency (time delays), but also the ability to carefully control and manage ultra-low latency.

For the purposes of this paper, the wider, more inclusive definition of 5G will be used. It is shaped by 3GPP specifications and a myriad of factors and stakeholders, such as: operators' decisions, the adoption by likely thousands of new kinds of 'operators,' the economic ecosystems and capital markets of the operators, and the day-to-day decisions of millions of ordinary users.[1]

Section 2: Threats Emerging with the Onset of 5G

The Industry Sets its own Standards in a Vacuum of Enforced Regulations

Interviews with industry professionals from across the technology sector gave the impression that many companies today, faced with the emergence of 5G, are improvising. In 2022, a survey by Ernst and Young (EY) found that only 21% of 1,325 global businesses were investing in 5G.[2] With the lack of investments in 5G preparation, there are insufficient security measures supporting it and few rules to follow when companies do start the investing process. As of July 2023, all three major carriers in the country– Verizon, AT&T and

[1] "Technologies." *3GPP*, 8 Aug. 2022, www.3gpp.org/technologies/5g-system-overview. Accessed 26 July 2023.

[2] Ricadela, Aaron . "Four Years after Its Debut, 5G for Industry Is Just Starting to Connect." *Oracle.com*, May 2023, www.oracle.com/communications/5g-core/5g-traction/. Accessed 27 July 2023.

T-Mobile – offer 5G services. Other companies, including Qualcomm, Intel, and The People's Republic of China's (PRC) Huawei, have been developing 5G standards. [3]

Some companies have also been researching 5G and paving the way in setting standards of deployment. Samsung Electronics, for example, along with SK Telecom, demonstrated its 5G next generation core (5G NC) in 2018 based on 3GPP Release-15 Standards.[4] Another example is Huawei, which has researched 5G Cloud Applications and worked with Qualcomm to complete 5G New Radio (NR) interoperability and development testing based on consistent 3GPP standards. South Korea-based company LG Corp has also used Ericsson as a vendor to deploy 5G NR hardware and software also based on 3GPP standards.

Although 3GPP has set standards for mobile telecommunications, there remains a lack of formal security standards and regulations to guard against the risks that come with 5G. Currently, the Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security (DHS), has made progress collaborating with infrastructure providers. However, CISA lacks enforcement authority to mandate cybersecurity standards for private or commercial networks.[5] The National Institute of Standards and Technology (NIST), under the Department of Commerce (DOC), has a framework on network security [6] that relies on voluntary industry implementation. Although these security standards are available for private organizations to follow, their implementation remains a low priority for most of the industry.

Vulnerabilities of 5G Network Infrastructure

Many of the innovations that make 5G attractive also present inherent new risks, which then broadens the threat surface when compared to previous telecom generations. Key examples include:

Disaggregated Control Plane: Previous generations of telecom infrastructure featured radios, base stations, and other network elements sourced from the same vendor. One of the advantages of 5G is the ability to mix and match equipment from multiple vendors.[7] This

[3] Clark, Don, and Cecilia Kang. "Why Companies and Countries Are Battling for Ascendancy in 5G." *The New York Times*, 7 Mar. 2018, www.nytimes.com/2018/03/06/technology/companies-countries-battling-5g.html. Accessed 27 July 2023.

[4] "5G Companies: 12 Players Are Leading the Research." *GreyB*, 31 Dec. 2020, www.greyb.com/blog/5g-companies/. Accessed 26 July 2023.

[5] Wheeler, Tom, and David Simpson. "The Digital Future Requires Making 5G Secure." *Brookings*, Dec. 12AD, www.brookings.edu/articles/the-digital-future-requires-making-5g-secure/. Accessed 27 July 2023.

[6] NIST. "Cybersecurity Framework." *National Institute of Standards and Technology*, 2019, www.nist.gov/cyberframework. Accessed 26 July 2023.

[7] BROWN, GABRIEL . *Independent Market Research and Competitive Analysis of Next-Generation Business and Technology Solutions for Service Providers and Vendors Multi-Vendor 5G Core Networks: The Case for a Disaggregated Control Plane a Heavy Reading White Paper Produced for Oracle*.

concept is known as "open RAN" or O-RAN. It gives operators more leverage with vendors, and more flexibility in supply chains and deployment. However, diversifying vendors provides additional threat vectors.

The first threat is interoperability – does the equipment work well against a range of use cases? If an unforeseen and untested combination of environmental factors and network load triggers an event between network elements from different vendors, there could be a cascade into partial or complete outages. This same set of combinations could create vulnerabilities that bad actors could exploit to control, monitor, or take down critical 5G infrastructure. This increased complexity also creates situations in which 5G availability is reduced not by bad actors, but by events that begin with unforeseen operational problems, cascading through the system to create even larger events with severe consequences.

Network Function Virtualization: Network operators deploying 5G also benefit from its virtualization, where hardware is replaced with software. Instead of having a physical cabinet located at the base of each cell tower filled with proprietary hardware, operators can have many network functions virtualized, occurring in software throughout their networks. This virtualization is known as Network Function Virtualization (NVF), Software Defined Networks (SDN), or more commonly, virtualized RAN (vRAN). vRAN makes the network flatter, more distributed, with significantly lowered capital and operating network costs, while also accelerating deployment speed.

However, vRAN, especially when used with O-RAN, also provides new threat vectors to bad actors seeking to compromise a network. CISA has noted: *"5G networks are designed to be more secure than 4G. However, the complexity of 5G networks - with new features, services, and an anticipated massive increase in the number and types of devices they will serve, coupled with the use of virtualization and disaggregation of the Radio Access Network (RAN) and the 5G Core—expands the threat surface and can make defining the system boundary challenging*".

Cloud-native: All new virtualized functions reside somewhere, and 5G was purpose-built to be hosted on the cloud. The 5G Core (5GC) standards define Service-Based Architecture (SBA). SBA was designed to allow telecom operators to host their network functions with cloud providers, gaining additional deployment flexibility and cost savings through economies of scale. The disadvantage of cloud hosting is that it outsources a core security function to cloud vendors, creating a shared vulnerability matrix. Cloud skillsets are different from traditional telecom operations, shaping unique threats and vulnerabilities. As 5G Americas says, *"The cloud can potentially introduce increased supply chain risk due to virtualization, increased use of open-source software, and a larger array of third-party vendors."*

Pacing: One benefit to having an open 5G ecosystem is vendors are motivated to innovate and compete - this is the source of additional flexibility and cost savings. However, this market pressure prioritizes speed and innovation. In several of the interviews conducted, numerous senior industry and government officials shared their concerns that firms were incentivized to "innovate and monetize first, and secure second."

Evolving TTPs: 5G poses significant benefits to wireless network operators and users, which society quickly adapts to depend on. This makes the disruption of even one of those services attractive to several threat actors. This portfolio of features and benefits also opens the door to a host of new security concerns driven by a combination of the factors mentioned above.

Threat actors now have more tools, entry points, and vulnerabilities to leverage. As a result, 5G will certainly face rapidly accelerating tactics, techniques, and procedures (TTPs) used by bad actors. The EU-coordinated risk assessment of cybersecurity of 5G networks found that, although cyber risks were found in previous generations, *"their number and significance is likely to increase with 5G, due to the increased level of complexity of the technology and of the future greater reliance of economies and societies on this infrastructure. As 5G networks will be largely based on software, major security flaws, such as those deriving from poor software development processes within equipment suppliers, could make it easier for actors to maliciously insert intentional backdoors into products and make them also harder to detect."* [8]

Advantages of 5G

There are many advantages of the implementation of 5G into public and private sector companies, including improved encryption, enhanced threat detection, and enhanced cyber audits. With the 5G network, the use of the International Mobile Subscriber Identity (IMSI), also known as Subscription Permanent Identifier (SUPI) delivers control and best-in-class security to prevent malicious and unlawful interception. An IMSI is essentially a number that uniquely identifies every user of a cellular network, and the SUPI is the type of identifier, which is usually a string of 15 decimal digits.[9] Another advantage is threat detection. With the implementation of 5G, cybersecurity professionals can more quickly identify threats and disseminate time-sensitive information to be analyzed for intelligence and response planning.[10] 5G also improves cyber audits. Professionals will be able to perform more in-depth audits, allowing them to identify and assess more vulnerabilities faster and across more devices.

[8] *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks Report*. 9 Aug. 2019.

[9] Security, Help Net. "Recommendations to Enhance Subscriber Privacy in 5G." *Help Net Security*, 4 Sept. 2020, www.helpnetsecurity.com/2020/09/04/recommendations-to-enhance-subscriber-privacy-in-5g/. Accessed 27 July 2023.

[10] "How 5G Technology Affects Cybersecurity: Looking to the Future | UpGuard." *Www.upguard.com*, www.upguard.com/blog/how-5g-technology-affects-cybersecurity#:~:text=The%20vast%20speed%20improvements%20of. Accessed 27 July 2023.

5G Security Collaboration

The global race of 5G deployment has increased competition among countries. Control of the 5G market allows any government to influence economic growth, social engagement, and digital security. Many countries have been adopting their own 5G networks to avoid dependence on foreign networks. These independent networks create unintended consequences, such as challenges with interoperability, as well as posing a significant question about the security of 5G networks worldwide.

The implementation of 5G networks globally requires transparency, accountability, and cooperation from stakeholders in both the private and public sectors. The European Commission and European industries started the 5G Infrastructure Public-Private Partnership (5G-PPP) initiative in 2018 to build a path toward the next generation of communication networks, increase the competitiveness of the European industry, and open innovation opportunities in Europe.[11] Likewise, a group of companies established the Open RAN Policy Coalition aimed at standardizing and developing open interfaces to promote competition, spark innovation, and bolster the supply chain for advanced technologies, including 5G.[12] As 6G is expected to be adopted in the next decade, the White House hosted a full-day workshop with academia, industry, and civil society leaders, emphasizing the importance of international standards and continued partnership with like-minded partners and allies.[13]

Nations have adopted different strategies to accelerate their quest for global 5G dominance. According to Brookings, the United States lagged behind the PRC in its effort to reach 5G nationwide coverage in early 2020.[14] The United States took an industry-led approach and initially gave autonomy to private sectors to deploy 5G technologies to generate competition and foster innovation.[15] In contrast, South Korea and China took a more hands-on approach by offering significant government investment in research and development, creating advanced strategies and policies, and regulating the deployment of the 5G networks.

A predominantly industry-led approach by the United States in adopting 5G infrastructure may have stymied its nationwide implementation as each telecom company had its own 5G

[11] "The 5G Infrastructure Public-Private Partnership." 5G-PPP, European Commission, https://5g-ppp.eu/. Accessed 24 July 2023.

[12] Open RAN Policy Coalition. "About Us." Open RAN Policy Coalition, https://www.openranpolicy.org/about-us/. Accessed 24 July 2023.

[13] White House National Security Council, and Open RAN Policy Coalition. "Principles for 6G: Open & Resilient by Design." Open RAN Policy Coalition, 21 April 2023. https://www.openranpolicy.org/wp-content/uploads/2023/04/principles-for-6g.pdf. Accessed 24 July 2023.

[14] Lee, Nicol T. Navigating the U.S.-China 5G Competition. The Brookings Institution, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_5g_competition_turner_lee_v2.pdf.

[15] Hollander, Rayna. "The Complete Global 5G Landscape: Market Leaders and Emerging Markets (Two Reports)." Business Insider Intelligence, February 2020, https://store.businessinsider.com/products/the-global-5g-landscape. Accessed 24 July 2023.

strategies and operational timelines, but the US government was pivoting to a more coordinated strategy as of July 2023. For example, the National Telecommunications and Information Administration (NTIA) and the Department of Defense (DoD) launched the 5G Challenge, a multistage prize competition targeted at industries, startups, academia, and telecommunication companies that was designed to accelerate the implementation of 5G open interfaces and streamline integration of multi-vendor interoperability.[16] Many of the potential threats to 5G stem from an absence or lack of cohesiveness and standardization across different platforms. According to the World Economic Forum, strong multi stakeholder cooperation, which includes regulators and policymakers, enterprise associations and international alliances, service and technology providers, and public-private partnership organizations, has a potential benefit of vast social and economic value with an estimated $13.2 trillion added by 2035 across industry sectors such as manufacturing, financial services, healthcare, transportation, retail, energy, and entertainment.[17]

5G critical infrastructure sectors are susceptible to malicious software, hardware, unauthorized, counterfeit, or untrusted manufacturing components. Some threat vectors to 5G infrastructure include, but are not limited to, policy and standards, supply chain, and 5G systems architecture.[18] For instance, a nation state may impose organizations to adopt standards that are beneficial to its cyber capabilities and boost its national economy. Additionally, supply chain cyber-attacks, such as the SolarWinds incident, emphasize the need for 5G supply chain security. A report from 5G Americas offers an example in which a 5G-enabled water quality monitoring system could be compromised by a supply chain failure and neglect to alert of a possible water contamination event.[19]

The European Union Agency for Cybersecurity outlines the 5G threat landscape and shares detailed descriptions of 5G threats to physical infrastructure, access networks, multi-edge computing, virtualization, and cybersecurity.[20] European Parliamentary Research Service

[16] National Telecommunications and Information Administration's Institute for Telecommunication Sciences, and Department of Defense Office of the Under Secretary of Defense for Research and Engineering. "5G Challenge." https://5gchallenge.ntia.gov/about. Accessed 24 July 2023.

[17] World Economic Forum, and PWC. "The Impact of 5G: Creating New Value across Industries and Society." The Impact of 5G: Creating New Value across Industries and Society, January 2020, https://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf. Accessed 24 July 2023.

[18] Cybersecurity & Infrastructure Security Agency, et al. "Potential Threat Vectors to 5G Infrastructure." 2021, https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf. Accessed 24 July 2023.

[19] 5G Americas. "Security for 5G." 5G Americas, December 2021, https://www.5gamericas.org/wp-content/uploads/2021/12/Security-in-5G.pdf. Accessed 24 July 2023.

[20] Lourenco, Marco Barros, and Louis Marinos. "ENISA Threat Landscape for 5G Networks." European Union Agency for Cybersecurity, 25 November 2019, https://www.researchgate.net/publication/337495468_ENISA_THREAT_LANDSCAPE_FOR_5G_NETWORKS. Accessed 24 July 2023.

delineates how 5G can affect politics, health, social welfare, and the economy.[21] Likewise, these wide-ranging societal impacts of 5G insinuate how a single entity cannot, and perhaps should not, implement the networks globally and solve all the problems and threats from 5G. The public-private partnerships at both domestic and international level are critical to the integration of the 5G ecosystem since it helps to escalate the efficiency and effectiveness of 5G deployment. Doing so also allows nations to not only achieve digital connectivity, improved communication, and increased productivity but also create societal equality, reduce a financial burden, alleviate security risks, and keep all parties accountable for privacy concerns.

5G as an Economic and Social Tool

5G presents a unique advantage compared to traditional internet service providers (ISPs) particularly in rural areas. According to a 2016 study, approximately two billion people lacked reliable access to the internet.[22] More specifically, according to the Federal Trade Commission (FTC) in 2020, about 22% of rural Americans did not have access to internet speeds of at least 25 Mbps, the minimum required to stream a Netflix movie in 4K.[23] Digging trenches to run coaxial cabling or fiber lines, necessary for traditional internet, is a cost-prohibitive endeavor for ISPs relative to the return on investment from subscriber dues in many rural areas, and as such many rural areas are limited to satellite-based internet. Starlink, a prominent satellite internet provider, has expanded high-speed satellite-based internet access to large parts of rural America. However, approximately half of the American Midwest lacked coverage as of July 2023.[24] 5G connectivity offers the ability to provide high-speed internet connectivity to millions of Americans without access by eliminating most of the cost of traditional infrastructure.

To assist with the digital divide in internet availability, the Federal Communications Commission (FCC) called for the rapid increase of 5G infrastructure while limiting costs.[25] This FCC ruling used small cell nodes to cover 300-500 feet each, requiring hundreds of devices to cover a small city.[26] Additionally, the ruling set fee caps that local governments could charge cellular providers to deploy these small cell nodes. When studied in the UK, researchers concluded that 90% of the population could be covered with reasonably fast

[21] European Parliamentary Research Service. "Mapping of 5G Technology in Europe." European Science-Media Hub, https://map.sciencemediahub.eu/5g#m=4/90/619.5,p=58. Accessed 24 July 2023.

[22] Chiaraviglio, Luca, et al. "5G in rural and low-income areas: Are we ready?" 2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT), pp. 1-8.

[23] FCC. Sixteenth broadband deployment report notice of inquiry.

[24] Starlink Coverage Map, https://www.starlink.com. Accessed 25 July 2023.

[25] FCC Fact Sheet. Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment.

[26] Miskimins, Jacki. "White Paper: Evaluating 5G Technology." Vantage Point, 10 July 2017, https://www.vantagepnt.com/2017/07/10/white-paper-evaluating-5g-technology/. Accessed 25 July 2023

5G, 50Mbps, but the remaining 10% remote areas would be too costly to provide high speed services.[27] This problem is likely magnified in the United States due to its significantly larger geographic size.

This digital divide in Internet availability became more apparent during the Coronavirus 2019 (COVID-19) pandemic. During the pandemic and ubiquity of professionals working from home, reliable internet access was essential for many Americans and amplified the existing divide.[28] With many Americans remote working and children attending digital schooling, rural areas were disproportionately affected by lack of high-speed internet access.[29] This need for internet availability extends beyond remote work and education. Much of rural America is farmland, producing approximately $307.4 billion worth of food annually, making this region the 3rd largest food producer in the world.[30] With the world population expected to grow to 10 billion by 2050, the food demand is also expected to increase by 50%.[31] To deal with the rise in expected food demand, the agriculture industry is looking to use 5G connectivity to enhance its capabilities. In 2022 John Deere showcased a fully autonomous tractor capable of functioning during adverse weather and permitting the farmer to perform other tasks simultaneously.[32] This tractor relies on 5G connectivity to upload the data gathered by its sensors into a neural network for processing and decision-making.[33] Additionally, farmers are beginning to rely on more "smart farming" to apply precise amounts of water, fertilizer, and herbicide to plants; drone operations to handle crop dusting; specialized cameras to monitor weeds and insects; and real-time livestock tracking.[34]

[27] Oughton, Edward J., and Zoraida Frias. "The cost, coverage and rollout implications of 5G infrastructure in Britain." Telecommunications Policy, vol. 42, no. 8, 2018, pp. 636-652.

[28] Atske, Sara. "The Internet and the Pandemic." Pew Research Center, 1 September 2021, https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/. Accessed 25 July 2023.

[29] "COVID-19 Magnifies Inequality in Internet Accessibility." Internet Society, 19 November 2020, https://www.internetsociety.org/news/press-releases/2020/covid-19-magnifies-inequality-in-internet-accessibility/. Accessed 25 July 2023.

[30] "4 Countries That Produce the Most Food Worldwide." Investopedia, https://www.investopedia.com/articles/investing/100615/4-countries-produce-most-food.asp. Accessed 25 July 2023.

[31] College Agriculture and life sciences. *GLOBAL AGRICULTURAL PRODUCTIVITY REPORT*. Accessed 25 July 2023.

[32] "John Deere Reveals Fully Autonomous Tractor at CES 2022." John Deere, 4 January 2022, https://www.deere.com/en/news/all-news/autonomous-tractor-reveal/. Accessed 25 July 2023.

[33] "John Deere Reveals Fully Autonomous Tractor at CES 2022." John Deere, 4 January 2022, https://www.deere.com/en/news/all-news/autonomous-tractor-reveal/. Accessed 25 July 2023.

[34] Carter, Jamie. "10 ways 5G will change farming and agriculture." 5Gradar, 7 January 2021, https://www.5gradar.com/features/ways-5g-will-change-farming-and-agriculture. Accessed 25 July 2023

Foreign control over 5G farming infrastructure presents significant risk, especially in rural agricultural areas in America and across the globe. PRC-tied Huawei maintains a dominant hold on 5G infrastructure worldwide, including providing most of the 5G infrastructure used to control smart agricultural equipment. Under its National Intelligence Law, the PRC could require Huawei to stop transporting the data for smart farming equipment used in other countries including the United States. The loss of connectivity could have far-reaching consequences worldwide as farmers adjust to reperforming tasks formerly outsourced to autonomous equipment. In 2021 the FCC voted to offer $1.9 billion in reimbursement to rural telecommunications carriers that replace their Huawei and ZTE equipment.

Another fundamental challenge of 5G is to ensure its rollout affects social development in a productive and sustainable way. In this context it is germane to consider the social impact of 5G by understanding the Sustainable Development Goals of the United Nations. The Sustainable Development Goals (SDGs) adopted by the United Nations in 2015 is a universal call to action to end poverty, protect the planet, and ensure that, by 2030, all people will enjoy peace and prosperity. The impact of 5G on the SDGs provides a valuable national and international context to the multidimensional power of 5G.

5G can deliver social values across 11 key areas that correspond to the United Nations' SDGs. The 5G-specific value derives mainly from contributing to good health and well-being (SDG 3), enhancing infrastructure, promoting sustainable industrialization, and fostering innovation (SDG 9). Other key areas in which social value is created through 5G include contributing to responsible consumption (SDG 12), enabling sustainable cities and communities (SDG 11) and promoting decent work and economic growth (SDG 8).

A Multi-Pronged Approach

To mitigate these cybersecurity implications, it is crucial for multinational governance organizations to prioritize organizing member states to adopt common standards of cyber defenses sufficient to protect systems in an evolving 5G environment. The reality of globalization tasks international organizations to also build the capacity of member states ill-equipped to maintain robust security measures, including encryption, authentication protocols, network segmentation, and regular security audits. The inclusion of multiple stakeholders, including governments, businesses and technology providers, and civil society leaders is essential to address these challenges effectively and ensure the resilience of international supply chains in the 5G era.

5G has several unique concerns, particularly regarding the reliance on foreign-operated infrastructure. There is no practical recommendation for wholly mitigating the possibility of a foreign nation-state disabling connectivity. Despite the FCC offering reimbursement for providers willing to replace foreign equipment, US-built infrastructure has lagged. Replacing infrastructure equipment is an expensive and time-consuming activity, requiring cellular providers to ensure that any replacement equipment is compatible with their existing equipment and will still be able to meet the requirements on "uptime," bandwidth, and speed specified in contracts.

Smart farm equipment, for example, requires 5G infrastructure to work. 4G connectivity does not have the bandwidth or speed required to transmit and process sufficient video, and wireless connectivity requires ISPs' willingness to perform costly investments in running networking cables to rural areas. As such, maintaining food supply volume in the farming sector requires the risk of 5G-dependent smart farm equipment. Industries heavily reliant on 5G-enabled IoT equipment would benefit from conducting simulated disaster scenarios in which equipment loses connectivity for 24-72 hours. During the tabletop exercises, businesses should consider how reliant they are on this equipment, what impacts the loss of this equipment would have on operations, and how quickly they could resume operations without the 5G-reliant equipment and at what capacity.

Section 3: Threats from 5G

Connectivity of Billions of Devices

In 2016, Kaspersky Labs reported that 78.9% of all detected cyber-attacks were botnet-assisted distributed denial of service (DDoS) attacks.[35] Denial of Service (DoS) attacks are attacks intended to degrade or block the availability of a targeted resource. A DoS attack may target an individual resource such as a website and deny access to legitimate users by flooding the website with more data than it can handle. DDoS attacks take the concept of a DoS and amplify it by using multiple malware infected computers (bots) to send data simultaneously. A DDoS attack can take the maximum data transfer rate of a single bot and add it to the maximum data transfer rate of every other bot. For example, a business network may have a maximum data transfer rate of 1 Gigabit per second (Gbps). A DDoS attack may use malware on 10 computers to launch 10 individual 1 Gbps attacks against the business simultaneously, oversaturating the business's maximum data transfer rate by 9 Gbps and preventing anyone from being able to visit the business website.

Typical DDoS prevention techniques focus on blocking the source of the DDoS traffic; however, the ever expanding nature of 5G connected devices means DDoS attacks could potentially scale to millions of sources.[36] The characteristics of 5G enable DDoS attacks at a scale potentially 20 times larger than the average nationwide maximum.[37] Across internet service providers, the average maximum speed offered to residential users is 1 Gigabit per second; however, 5G has a theoretical maximum of 20 Gigabits per second.[38]

In 2017, Google reported the largest DDoS attack ever at approximately 2.54 Terabytes per second (TB/s), or approximately 127 hours of 4K video every second, originating from

[35] Perez, Manuel G., et al. "Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigate Botnets." IEEE Internet Computing, vol. 21, no. 5, 2017, pp. 28-36.

[36] Perez, Manuel G., et al. "Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigate Botnets." IEEE Internet Computing, vol. 21, no. 5, 2017, pp. 28-36.

[37] Ghorbani, Hamidreza, et al. "DDoS Attacks on the IoT network with the Emergence of 5G." 2020 International Conference on Technology and Entrepreneurship - Virtual (ICTE-V), 2020, pp. 1-5.

[38] ITU-R. "Minimum Requirements related to technical performance for IMT-2020 radio interface(s)."

approximately 180,000 bots.[39] Averaging the 2.54TB/s across 180,000 bots results in approximately 14.2 Gigabytes per second (GB/s) from each bot, or roughly 71% of the maximum bandwidth 5G can theoretically support. Using this DDoS attack as an example and pairing it with the maximum theoretical speed of 5G means the attack could have been as large as 3.24TB/s, 162 hours of 4K video every second. The expansive push for 5G connectivity enables explosive growth in potential bots.

Smartphones are one of the most common 5G-enabled devices. Almost every midrange smartphone made today includes 5G connectivity, and almost every mobile carrier offers 5G data as part of their default mobile data plan. Mobile malware can add these devices to botnets, using them to launch DDoS attacks against organizations. Android and iOS malware has added smartphones to botnets; however, it's unclear if any of these devices have been used in a DDoS attack. Smartphone botnets represent a unique challenge for organizations defending against DDoS attacks due to their use of internet protocol version six (IPv6).[40] To provide connectivity to an ever-expanding number of 5G-connected devices, mobile telecommunication providers issue unique IPv6 addresses per device resulting in millions of individual IP addresses. Traditional DDoS mitigation techniques involve filtering potentially malicious IPs[41]; however, this mitigation is less effective against 5G-enabled bots because of the millions of unique IPv6 addresses.

5G enables a nearly infinitely scalable botnet technically capable of launching a DDoS attack larger than anything ever recorded. 5G connectivity allows malicious cyber adversaries to convert nearly any device into a weapon.

Foreign Leverage of 5G Threatens National Security

One of the primary concerns of 5G cybersecurity is the global hegemony of 5G infrastructure exhibited by foreign-affiliated telecommunication companies. In 2021, researchers at Cornell University estimated that PRC telecom giants Huawei and ZTE accounted for approximately 41% of the global 5G infrastructure, more than four times the amount of the largest American competitor, Cisco.[42] Additionally, Huawei makes up approximately 70% of Africa's 4G infrastructure and has the only formal agreement to provide 5G infrastructure in

[39] "Identifying and protecting against the largest DDoS attacks." Google Cloud, 17 October 2020, https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks. Accessed 25 July 2023.

[40] Yang, Xinyu, and Yi Shi. "Typical DoS/DDoS Threats under IPv6." 2007 International Multi-Conference on Computing in the Global Information Technology (ICCGI'07), 2007, p. 55.

[41] Žádník, Martin. "Towards Inference of DDoS Mitigation Rules." NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, pp. 1-5.

[42] Endresen, Janice. "Miles Ahead: China, Huawei, and 5G | BusinessFeed." Cornell SC Johnson College of Business, 15 February 2021, https://business.cornell.edu/hub/2021/02/15/miles-ahead-china-huawei-5g/. Accessed 25 July 2023.

South Africa.[43] As part of the Belt and Road Initiative (BRI), the CCP initiative to increase trade and cooperation in Asia, Europe, and North Africa, the PRC can pressure developing countries to enter into contracts with Huawei under the "Digital Silk Road." Using this initiative, Huawei has partnered with major telecommunication providers in Russia, South America, Iran, South Africa, Saudi Arabia, Oman, Indonesia, and more.[44]

Under the 2017 "National Intelligence Law of the People's Republic" article 7, the PRC can compel any organization or citizen to "support, assist and cooperate with state intelligence work."[45] The PRC can use this law to force Huawei or ZTE to perform actions supporting the national intelligence requirements of the State. Using this authority and the global placement of PRC telecommunications infrastructure, the global 5G spectrum becomes vulnerable to the controlling interest of one country.

Any country that controls 5G infrastructure can manipulate the confidentiality, integrity, and availability (CIA triad) of all who use it. More specifically, a controlling country can intercept, manipulate, or disrupt communications, exploit vulnerabilities in 5G infrastructure or devices connected to 5G networks, manipulate supply chains to degrade capabilities or conduct espionage in hostile countries. An example of the impacts of global telecommunication hegemony can be seen in the logistics sector. Approximately 80% of ship-to-shore cranes in the United States are owned by the PRC-affiliated company Shanghai Zhenhua Heavy Industry (ZPMC).[46] In 2019, ZPMC and Huawei partnered to integrate 5G connectivity in port operations.[47] Under the National Intelligence Law of the People's Republic, the PRC could use its 5G placement in cranes to shut down port operations.[48] Additionally, if the smart cranes are reporting data back to a larger logistics network, the prolific access to 5G infrastructure enables the PRC to manipulate the flow of information back into the larger network. Any foreign domination of U.S. infrastructure and operations threatens security.

[43] Sacks, David. "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond." Council on Foreign Relations, 29 March 2021, https://www.cfr.org/blog/china-huawei-5g. Accessed 25 July 2023.

[44] "How the U.S. Should Respond to China's Belt and Road." Council on Foreign Relations, https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/. Accessed 25 July 2023.

[45] "National Intelligence Law of the People's Republic of China." Brown CS, 27 June 2017, https://cs.brown.edu/courses/cs180/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf. Accessed 25 July 2023.

[46] G, Alex. "CHS China Select letter to DHS Re:ZPMC Crane Oversight." Homeland House, 30 August 2022, https://homeland.house.gov/media/2023/05/2023-05-10-CHS-China-Select-letter-to-DHS-re-ZPMC-Crane-Oversight.pdf. Accessed 25 July 2023.

[47] Huawei. 5G Smart Port White Paper. 2019. Huaewi, https://www.huawei.com/en/huaweitech/industry-insights/outlook/mobile-broadband/xlabs/insights-whitepapers/5g-smart-port-whitepaper.

[48] Dougherty, Chris. "Logistics for a New American Way of War."

Huawei as a Tool of PRC Influence

Typical discussions involving international security implications of 5G focus on Huawei. The PRC behemoth is the world's leading supplier of telecom equipment, including 5G, and is one of the 4 largest 5G vendors in the world (the other three being Samsung, Nokia and Ericsson). Many western companies have banned Huawei products and services, often labeling them as a 'bad vendor' whose products could allow the PRC unprecedented espionage opportunities.[49] This claim is akin to suggesting Huawei is a wolf in sheep's clothing, and the prescription for the perceived threat is to keep the vendor out of western countries. Many industry experts worry that Huawei will leverage its natural strengths (leading 2G, 3G, 4G and 5G products), significant economies of scale, and nation-state backed pricing subsidies to become a critical and irrevocable leading vendor and offer the PRC unprecedented access to parts of the world Beijing may be seeking to influence.

To understand the PRC's long-term strategy, one must first consider the industries that benefit from 5G. The sectors that benefitted the most from 4G include social media companies, and new forms of social media and other platforms are likely to launch new features that take advantage of 5G features. Smartphones are frequently used in banking; 4G and now 5G phones make payments, either using the built-in phone app (e.g., Apple Pay or Samsung Pay), or via an app downloaded like Google Pay, Venmo, or Zelle. Phones and apps keep us connected, informed, and entertained. Apps like YouTube and Khan Academy offer education, and Microsoft Office or Google docs host ongoing work projects for millions of users.

Huawei also has some options to respond to a theoretical ban of its products by western allies.[50] Huawei could pivot instead to faster developing markets such as in South America, the Middle East, Eastern Europe, Africa, and India. When Huawei wins a network deployment, it also makes significant inroads with sales of its handsets. Importantly, those handsets come preloaded with PRC-based applications like WeChat, TikTok, Baidu, TenCent and Kingsoft, setting the stage for most of the world to use PRC-based platforms to conduct their lives, with those technology companies steadily growing market share.

The potential advantages for the PRC of Beijing's global 5G strategy compound. 5G deployments are a massive consumer of semiconductor chips and cloud computing. The PRC's coordinated national strategy to uplift Huawei globally could directly lead to increased economies of scale across the semiconductor and cloud industries.

As a critical infrastructure provider, Huawei and the PRC gain additional geopolitical advantages. The PRC is positioning itself to hold virtual keys to every place with a cell site,

[49] Berman, Noah , et al. "Is China's Huawei a Threat to U.S. National Security?" *Council on Foreign Relations*, 8 Feb. 2023, www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security. Accessed 25 July 2023.

[50] Andy Blatchford. "Canada Joins Five Eyes in Ban on Huawei and ZTE." *POLITICO*, 19 May 2022, www.politico.com/news/2022/05/19/canada-five-eyes-ban-huawei-zte-00033920. Accessed 26 July 2023.

and access to electrical and other crucial critical network information. PRC leaders will be included in the disaster planning, business continuity, and resilience work in any country where they have a network. They'll have boots on the ground throughout the world servicing Huawei's infrastructure, with a significant risk of espionage to augment anything directly learned from their dominant position as the 5G network. PRC-based firms would also be well-positioned to become both preferred providers and preferred customers, gaining priority access to things like ports, rails, and construction around the world.

Threats to Civil Society and Governance

Another concern derived from governmental control of digital infrastructure is the potential for information operations. The U.S. Department of Defense defines information operations as "The application, integration, and synchronization of information-related capabilities (IRC) to influence, disrupt, corrupt, or usurp the decision-making of the target audience (TA) to create a desired effect to support the achievement of an objective."[51] Using this definition, we can classify cellular internet as IRC and a civilian population as the TA for an autocratic government. Joint Publication 3-13, "Information Operations," further defines the information environment as the physical, informational, and cognitive domains. We can associate these domains with 5G by defining the radio towers as the physical domain, the radio waves and technical controls of the data as the informational domain, and the intentions of foreign governments and minds of the population as the cognitive domain. By controlling the physical domain, an autocratic government could control the informational domain to manipulate the cognitive domain. More specifically, by controlling the cellular infrastructure, government entities can manipulate the information their population receives and, in turn, can shape perceptions and public opinion.

The Democratic People's Republic of Korea (DPRK) has a well-documented history of controlling information flow throughout its territory and should serve as a warning for what states can accomplish by controlling 5G infrastructure. Internet connectivity inside the DPRK is a tightly regulated intranet in which the Workers Party of Korea (WPK) controls the internet service providers and the cellular service.[52] Egyptian telecommunications company "Orascom Telecom Media and Technology Holding SAE," renamed to "Orascom Investment Holding SAE" in 2018, provides 3G cellular connectivity to the citizens of the DPRK. The DPRK State Security Services routinely monitor cellular usage and severely punish citizens who attempt to access foreign/international information.[53] The United Nations General

[51] Department of Defense. "JP 3-13, Information Operations." Defense Innovation Marketplace, 27 November 2012, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf. Accessed 25 July 2023.

[52] "A Look at North Korea's Tightly Controlled Internet Services." Business Insider, 23 December 2014, https://www.businessinsider.com/a-look-at-north-koreas-tightly-controlled-internet-services-2014-12. Accessed 25 July 2023.

[53] King, Robert R. "North Koreans Want External Information, But Kim Jong-Un Seeks to Limit Access." CSIS, 15 May 2019, https://www.csis.org/analysis/north-koreans-want-external-information-kim-jong-un-seeks-limit-access. Accessed 25 July 2023.

Assembly noted in 2013 that citizens of the DPRK are "denied the right to have access to information from independent sources…" and that "access to the internet is severely restricted and all media content is heavily censored and must adhere to directives issued by the WPK."[54]

Limited availability of internet connectivity enables governments to conduct information operations against citizens. By controlling the flow of information in a country, a government can shape the narrative to its benefit. Worse still, the extremely limited supply of 5G infrastructure could result in multiple countries being subjected to the information operations and communications censorship of a third-party, potentially foreign 5G supplier. Specifically, by subsidizing the cost of 5G infrastructure, the PRC positions itself to control the information flow of countries outside of its typical sphere of influence.[55] By providing cheap 5G connectivity especially in countries that historically do not have reliable, high-speed internet access, the PRC is able to shape the information environment and could manipulate the cognitive domain.

Section 4: Broader Regulations and Impactful Policy

The emergence of 5G technology not only brings immense potential for connectivity and innovation but also highlights a significant challenge due to the lack of standards, regulations, and policy. Without transparent guidelines, there is a risk of fragmented networks, compatibility issues, and security vulnerabilities. Robust standards are crucial for global interoperability, while regulations are necessary to address security risks and govern the responsible deployment of 5G. A comprehensive policy framework is necessary to ensure equitable access, fair competition, and ethical considerations. Collaborative efforts are needed to establish these frameworks and unlock the full potential of 5G while safeguarding the interests of individuals and society.

State of the Framework

In NIST's special draft publication titled "5G Cybersecurity Volume B: Approach, Architecture and Security Characteristics," published in April 2022, there is a focus on outlining the cybersecurity capabilities of the illustrative 5G network. The publication also includes a risk analysis of the network's security features. The method of the risk analysis provides an inventory of the technical security capabilities. Subsequently, it delves into the assessment of the threats and vulnerabilities that each capability is designed to mitigate. Lastly, it evaluates how these technical security capabilities align with the requirements specified in industry-specific references.

It is essential to address a significant concern regarding the deployment of cybersecurity measures for devices within the 5G ecosystem. Unlike previous generations, 5G heavily

[54] U.N. General Assembly. Report of the commission of inquiry on human rights in the Democratic People's Republic of Korea.

[55] Attrill, Dr. Nathan, and Audrey Fritz. China's Cyber Vision. 2021.

relies on cloud-based technology, which presents new opportunities for securing the 5G ecosystem. [56]

While this special publication is in its initial stages, it has the potential to identify gaps in 5G cybersecurity standards. By recognizing these gaps, it can provide valuable insights for standards development organizations, enabling them to address and educate themselves on potential areas of improvement.

Security Recommendations

In NIST's special draft publication 1800-33B, the initial phase of the project aims to tackle known security challenges from previous network generations. However, in the process, it may also reveal novel challenges that arise within the 5G ecosystem. This discovery process is crucial as it will pave the way for developing comprehensive policies, standardizations, and best practices to ensure the secure deployment of both the 5G ecosystem and the devices operating within it.

It must be noted that broader policy standards and recommendations are currently active on multiple fronts. The FCC has embarked on an extensive plan to expedite the implementation of 5G in the United States. This plan consists of three fundamental elements: the introduction of additional spectrum into the market, the revision of infrastructure policies, and the modernization of outdated regulations.[57]

Additionally, established under the European Electronic Communications Code (EECC), presents a technology profile specifically focused on 5G, complementing the technology-neutral guideline on security measures. It offers supplementary guidance to competent national authorities, aiding them in ensuring the effective implementation and reinforcement of security measures by mobile network operators. The primary objective is to mitigate potential risks to the 5G network.[58]

To further advance the development of policy standards and recommendations focused on enhancing security measures, the following aspects are crucial:

1. International Collaboration: Facilitating cooperation and coordination with international entities to address security concerns effectively.

[56] "NIST Requests Public Comment on Draft Guidance for 5G Cybersecurity." *NIST*, 26 Apr. 2022, www.nist.gov/news-events/news/2022/04/nist-requests-public-comment-draft-guidance-5g-cybersecurity. Accessed 27 July 2023.

[57] "The FCC's 5G FAST Plan." *Federal Communications Commission*, 15 Sept. 2016, www.fcc.gov/5G. Accessed 26 July 2023.

[58] "5G Supplement - to the Guideline on Security Measures under the EECC." *ENISA*, 7 July 2021, www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc. Accessed 27 July 2023.

2. Risk Assessment and Compliance: Conducting thorough risk assessments and ensuring adherence to compliance protocols to minimize potential vulnerabilities.
3. Supply Chain Security: Implementing guidelines and regulations to bolster the security of the supply chain involved in 5G infrastructure.
4. Security by Design: Incorporating security measures into the very foundation of 5G technologies and systems during their design and development phases.

5. Ensuring Proper Monitoring, Response, and Training: Vigilantly monitoring 5G networks, promptly responding to cyberattacks, and providing comprehensive training to personnel involved in managing the network's security.

6. Research and Development: Continuously investing in research and development efforts to stay ahead of emerging security challenges and develop innovative solutions.

These aspects collectively contribute to a robust security framework for 5G networks, mitigating potential risks and ensuring a safer and more resilient technological landscape.

A Multi-sector Approach to Counter Huawei's Dominance

When addressing foreign threats against U.S. national security, it is imperative to outcompete Huawei with commercially appealing alternate 5G vendors using a "ships and castles" strategy. Huawei is a powerful castle: its strengths are well-known and difficult to overcome by companies attempting to replicate its model.

A strategy to outcompete Huawei is to work with a portfolio of best-in-breed companies within each network function, all with proven mix and match interoperability. Customers can choose what they want and need and use market dynamics and this right sized approach to get better networks, cheaper than they might otherwise get from Huawei.

To compete in this domain, the United States and other countries will need to:

1. Foster O-RAN adoption, which is subsidized around formal interoperability one-and-done testing and certifications. There should be a use of market forces to align interoperability in areas where different operators have different standards/settings. Could live in NTIA, National Telecommunications and Information Administration funded by commerce, but should also support regional/global interoperability, perhaps in partnerships with other global bodies.

1. Develop a global corporate development effort around 5G, with a relatively small but robust portfolio of proven 5G best in breed vendors in all of the various network element areas (Radios/Antennas, system integration, Commercial Off The Shelf (COTS) servers, vDU/vCU, Cloud), using a mix of American and other companies offering shared most favored nation pricing to all, and assured interoperability and support

2. Hold informal regular O-RAN "plugfests" at universities and other commercial and innovations centers to encourage more standardizations and "wifi-like" build. RFP clearing house: The United States should offer a 5G RFP clearinghouse, supporting

any operator's efforts to plan their 5G deployment. This would give the US consolidated visibility to the diversity of varying requirements coming from the operator marketplace. In addition to providing support and information to operators, the US should also offer various grants/microgrants to incent operators towards a certain harmony of requirements, allowing 5G infrastructure providers to provide a narrower range of products, and achieve more competitive cost structures through economies of scale.

The United States will need a multi-sector response to compete with Huawei. The United States as of July 2023 had three different 5G workstreams, with little orchestration between them. These three work streams are:

a. Commercial Markets - There is little coordination within the US with companies that are directly or indirectly benefiting from global 5G adoption, even within each sector, much less across them. The Department of Commerce is the most likely agency to spearhead a coordinated response to the economic consequences of significant Huawei market traction and should develop a short and long term strategic plan to allow the global markets in various sectors to not become overwhelmed with Huawei's economies of scale.

b. Global Soft-Power/Politics - The Department of State, United States Agency for International Development (USAID), and other stakeholders are best positioned to coordinate responses to changing economic tides brought about by 5G. They need a short- and long-term strategic plan that can anticipate and adapt to the changing geopolitical landscape that is resulting from Huawei's 5G market traction.

c. Military innovation - The Department of Defense has historically played a role in developing and supporting the commercialization of the technology that we depend on in our daily lives from the computer mouse to voice recognition technology, and to the Global Positioning System (GPS).

There is a significant benefit to connecting them within an integral strategy that prepares the US and other countries to compete economically and politically with the PRC, even in markets where Beijing has won 5G network installations.

Conclusion

The recommendations in this whitepaper are not meant to be expansive. They could be small and targeted, yet coordinated, initiatives. Based on numerous interviews with stakeholders and subject matter experts, it is evident that there is great potential in each of these work streams but there has been little coordination among them in the United States. A concerted effort to bring these three streams together in a more cohesive way is essential to achieve long-term global market resiliency.

24 ***DISCLAIMER STATEMENT:*** *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.*

MEMBERS	COMPANY
Kyle W	US Government
Daniel T	US Government
Margaret R	US Government
Isaac J	US Government
Patrick Scannell	Consultant
Chandra Daniel	New York Medical College
Rhea Hulikantimath	Citigroup
Emily Wene	Citigroup
Jack L	Private Sector
Robert Kang	Booz Allen Hamilton

Daniel Roche	Northern Trust
Eric Rotzoll	***DHS***

ANALYTIC DELIVERABLE DISSEMINATION PLAN

New York Medical College

New York Academy of Medicine

UNFPA

UNODC

WHO

UNAIDS (Health Innovation Exchange)

NJSP

DEA

Department of Commerce

Department of State

National Council of ISACs

United States Telecom Association

Office of the Director of National Intelligence

DNI Cyber Threat Intelligence and Integration Center

FBI, including the Domestic Security Alliance Council

Intelligence Community Analytic Outreach Coordinators

Department of Homeland Security Headquarters and Components, including Component Intelligence Offices and CISA

DHS Association Partners

Previous participants in the AEP and IC Analyst-Private Sector Program

28 ***DISCLAIMER STATEMENT:*** *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.*