Governance Studies
at BROOKINGS

REPORT
DECEMBER 2022

5G IS SMART, NOW LET'S MAKE IT SECURE

BY TOM WHEELER AND DAVID SIMPSON

Governance Studies
at BROOKINGS

5G IS SMART, NOW LET'S MAKE IT SECURE

REPORT | DECEMBER 2022

TOM WHEELER is a visiting fellow in Governance Studies at the Brookings Institution and formerly served as the chairman of the Federal Communications Commission (FCC).

DAVID SIMPSON is a professor in the Pamplin College of Business at Virginia Tech and formerly served as chief of the Public Safety and Homeland Security Bureau (PSHSB).

ABOUT GOVERNANCE STUDIES

The Governance Studies program at Brookings is dedicated to analyzing policy issues, political institutions and processes, and contemporary governance challenges. Our scholarship identifies areas in need of reform and proposes specific solutions with the goals of: improving the performance of the national government; informing debate; and providing policymakers with expert analysis and ideas to ensure better institutional governance.

ACKNOWLEDGEMENTS

The authors wish to thank those who provided their counsel and review in the preparation of this paper – Wade Baker, Eric Burger, Brett Haan, Sean Joyce, Len Kennedy, Michael Loch, Rafi Martina, Mark Montgomery, Stephanie Pell, Jeffrey Reed, John Scott, Bill Stueber, and Michaela Vanderveen. The observations and conclusions of this report, however, are solely those of the authors. The authors also wish to thank Antonio Saadipour and Adelle Patten of the Brookings Institution for their help in the final preparation of this report.

Amazon, AT&T, Meta, Microsoft, TMobile, Verizon, and Qualcomm are general unrestricted donors to the Brookings Institution. The findings, interpretations, and conclusions posted in this piece are solely those of the authors and not influenced by any donation.

ABOUT THE BROOKINGS INSTITUTION

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s) and do not reflect the views of the Institution, its management, or its other scholars.

CONTENT

CONTENT

EXECUTIVE SUMMARY

> From smart cities, to smart cars, to smart factories, the future will be built on ubiquitous microchips connected by wireless networks.

Fifth generation (5G) technology promises to bring the high-speed, low latency wireless infrastructure necessary for the "smart" era. Moving from promise to reality, however, will require those networks to be secure.

The introduction of 5G networks is both a response to the massive wave of digitization that is sweeping the economy as well as a stimulant to its further expansion. By some estimates, half of all worldwide data traffic over the next five years will be generated not by people, but by computerized devices requiring no human intervention.[1]

Fifth generation wireless networks will deliver amazing and important new capabilities and services. Yet, 5G also brings with it new cybersecurity challenges. Securing networks that utilize potentially insecure components while operating in an inherently insecure world is a new challenge. It is a problem that is expanded by how the exponential growth in data traffic threatens the efficacy of traditional traffic-based cybersecurity monitoring.

The purpose of this paper is not to criticize the amazing engineering that produced 5G, but to call attention to how these decisions, by introducing a new network architecture, have fallen short in affirmatively addressing avoidable cybersecurity risk while also introducing new cybersecurity concerns, and to suggest how those concerns might be mitigated by a combination of agile regulatory oversight, corporate focus, and government funding.

INTRODUCTION

> Fifth generation wireless is not simply an incremental improvement of existing 4G functions; it ushers in an era where the wireless Internet of Things (IoT) will provide capabilities that enable entirely new devices and use cases to automate aspects of our lives.

Both the technology and its effects can be revolutionary. Unfortunately, implementations in the U.S. market, to date, can best be described as evolutionary, with most consumers seeing marginal service improvements accompanied by growing pains. When 4G networks were first introduced in the U.S. in 2010, they became the basis for innovation in mobile applications. Fifth generation networks have the potential to go well beyond today's smartphone apps, enabling enhanced mobile broadband (eMBB) communications, ultra-reliable low latency communications (URLLC), and machine-to-machine (M2M) communications, including tens of billions of devices that will be embedded in vehicles, sensors, machines, and medical and other instruments to create an Internet of Things (IoT).

The slow rollout for advanced 5G functions in the U.S. market can be attributed to several factors—one of which is insufficient attention toward securing the new landscape. The promise of the "smart" era is compromised when the networks and user equipment are not secure end-to-end. One hundred percent of cyberattacks traverse a public network at some point. The nation's networks are the attack vectors of the 21st century as surely as roads and waterways were the attack vectors of history. The rollout of 5G should close off attack vectors, not create new ones.

In 2019, the authors wrote about how the Trump administration's hyper-focus on Huawei's 5G network hardware was obscuring the broader security challenges resulting from 5G's substitution of software for hardware.[2] Since then, the cyber threat has been greatly expanded. As consumers and companies become ever more aware of the implications of 5G's vulnerabilities, it can only have an adverse effect on adoption and investment.

"The promise of the 'smart' era is compromised when the networks and user equipment are not secure end-to-end. One hundred percent of cyberattacks traverse a public network at some point."

Today, the 5G standard has reached the point where it is stable enough to scale for widespread rollout.[†] That the rollout is occurring increases the importance of putting in place recognized and enforceable cybersecurity safeguards for 5G.

The 5G standard brings with it two compounding cybersecurity challenges. In the first challenge, the standard "virtualizes" many of the network functions formerly performed by hardware to now be performed by software. Because software is hackable, network infrastructure that is built on software code is inherently vulnerable.

The second challenge to cybersecurity is delivered by how network operators have responded to the move from hardware to software: supplementing and, in some cases, replacing traditional infrastructure vendors and their closed proprietary systems with an expanded set of vendors supplying equipment using "open" protocols. Such diversity of suppliers could become a *per se* invitation to a new diversity of unaddressed attack vectors if it merely has a business objective and is not part of a more thoughtful cyber-resiliency objective.

The expanded cybersecurity challenge of commercially deployed 5G has yet to be adequately met either by industry or government. The wireless industry's push for 5G technology and its implementation through open equipment specifications is first and foremost (and appropriately) a business decision. The sequencing of that decision, however, cannot skip over its cybersecurity implications.

It is essential that national policy establishes expectations for the security and behavior of the new network. Such a 5G cybersecurity policy should include:

- **Identification** and assignment of the risks and responsibilities created by 5G, both at the industry and government level;
- **Recognition** that the shift from the 4G consumer smartphone market to new machine-to-machine (M2M) brings with it different data utilization, including automated features with no human intervention, and a volumetric increase in connections and traffic;
- **Reconciling** the business objectives of 5G supplier diversity with the supply chain risks it creates;
- **Responding** to the complexity of the virtualized 5G architecture and how it creates a whole new set of potential vulnerabilities in the supply chain for software, hardware, and services, including contract development, open-source code, and multi-access edge cloud computing;
- **Avoidance** of the industrial model for regulatory oversight in favor of a more agile multistakeholder approach;

[†] The agile development of the 5G standard will reach a "functional freeze" (Release 18, Stage 2) in March 2023. This will stabilize enough aspects for incorporation into chipsets, software, and hardware for deployment so as to scale beyond initial trials.

- **Competing** not just in our own domestic market, but creating solutions that equip U.S. companies to compete and influence global wireless telecommunications markets;

- **Recognition** that 5G cybersecurity is a national security issue worthy of national financial support.

Make no mistake about it, 5G wireless networks can usher in a new era of wonderous capabilities that will help consumers, companies, and communities. It can help grow the economy with exportable new products and increased productivity. We saw this happen in the 4G decade when the U.S took the lead in the app economy because its wireless network, connected device standards, and digital platform interfaces created a home field advantage for entrepreneurs. If the U.S. is to likewise lead in the IOT-enabled smart economy, that home field must be secure. Failing to address cyber risk appropriately will slow U.S. deployment of advanced 5G capabilities, suppress use case demand signals, impair the ability to protect intellectual property, chill 5G investment, and expose critical infrastructure to increased risk of catastrophic failure.

Failure to lead, through U.S. 5G cyber risk mitigations, threatens not only 5G, but also all the dependent lines of business. There will be an advantage to the nation that reconciles cyber, privacy, and tech innovation with oversight that establishes expectations for 5G security that are agile enough to encourage investment while keeping pace with technology, markets, and the activities of aggressors.

The "smart" future rests on secure pathways that will deliver its transformational promise. The discussion that follows explores the cybersecurity ramifications of 5G technology and proposes a plan for the implementation of national cybersecurity oversight, including the funding of the network-level implementation of such security initiatives.

"Failure to lead, through U.S. 5G cyber risk mitigations, threatens not only 5G, but also all the dependent lines of business."

PART 1

THE 5G CYBER PARADOX

SUMMARY

Fifth generation wireless networks are a paradox: as they improve the efficiency and capabilities of the communications infrastructure to enable a new generation of services, they introduce new security vulnerabilities that threaten both the networks and those who rely on network connectivity.

At the heart of both the benefits and risks of 5G are two developments:

1. **The 5G standard's "virtualization" in software of network operations previously performed in purpose-built hardware.**

2. **The push for modular interoperability of network infrastructure in place of once proprietary special purpose network equipment.**

From the radio portion of the network to the transport network, to the activities of the network core, the functions of 5G networks are being performed in virtualized software and opened to new equipment and service providers. This introduces whole new networks and network capabilities while also allowing both legacy and new network operators to manage their networks better, more flexibly, and at lower cost. **The new architecture also adds three new security vulnerabilities.**

The first challenge is the cold reality that **software can be hacked** whether it's in hardware selected and operated by a telecommunications company or whether it's placed in common-purpose hardware operated by a third-party entity. Throughout the world, criminal and nation-state hackers are persistently engaged in seeking network access, corrupting data, denying service, and extorting users. When networks ran on proprietary equipment utilizing proprietary software, the ability to protect against such attacks was more clearly focused. Today, hackable software designed to work on common purpose IT equipment from a broad universe of suppliers has replaced what was previously a small number of vendors working with a small number of telecommunications operators. While technologically this is a step forward, it should also be recognized for the significant shift it creates in cyber risk exposure and responsibility for mitigating that risk.

The second challenge is that the creation of common interoperable capabilities **expands the infrastructure service and supplier base without transparency** into the new providers' security practices, origins, and motives. The

provenance of both software and firmware takes on added importance as the number of component suppliers increases. This potential vulnerability is increased by the allowable variation in how the technology stack for 5G is implemented and the undefined risk responsibility for end-to-end integration.

> **"There is no comprehensive identification and assignment of the risk responsibilities inherent in end-to-end 5G services as diverse as the Internet of Things (IoT), smart cities, robotics, and industrial automation."**

The ability of network providers to self-assemble components from multiple vendors increases the opportunity for the introduction of vulnerabilities while simultaneously making security assurances more difficult. The open interface capability of the new software-based architecture also creates the opportunity for new private network entrants to offer wireless service in competition with the existing wireless providers, thus introducing the possibility of additional attack vectors and vulnerabilities.

The third challenge results from **the absence of meaningful oversight** to address the first two realities. There is no comprehensive identification and assignment of the risk responsibilities inherent in end-to-end 5G services as diverse as the Internet of Things (IoT), smart cities, robotics, and industrial automation. Securing a distributed network built utilizing hackable software from a diverse universe of suppliers for widely deployed data-dependent automation requires more than voluntary actions without enforceable expectations.

Yet, the charters developed for industrial-era network regulatory bodies have not kept pace with such information economy needs. The shift to software-defined wireless broadband networks exposes this shortfall. In place of the industry's desired *laissez-faire* approach, there is a need for a regulatory construction with not just the necessary authority but also the critical knowledge, skillsets, and collected data necessary for the responsible oversight of a dynamic set of technology providers and vendors. This must be accompanied by the development of an evolved set of regulatory activities that reduces rulemaking and introduces mechanisms for continuous engagement. Regulators and service providers must appreciate opportunities and risks together without the significant lag inherent with Industrial Era regulatory norms.

Exploiting software

Networks built on software are vulnerable to malicious actors for two major reasons: designed access and discovered access. Both techniques benefit from the interconnection

that makes the internet possible.

Designed access is straightforward. The developer of the software purposefully includes hidden vulnerabilities such as backdoor access, zero-day opportunities, and other malicious activities. There are also situations where developers have out-sourced code writing to subcontractors that inserted vulnerabilities. Like the sleeper cells of human espionage, these capabilities quietly rest unnoticed until activated.

Discovered access exploits the human frailties of code developers. Errors in the design of the product, sloppy code construction, and the incorporation of third-party code all create exploitable vulnerabilities. Criminal enterprises and nation-states are constantly trolling open-source libraries and software developers in search of such entry points. In the past, open-source software had a dedicated volunteer community to discover vulnerabilities and provide remediation. The proliferation of open-source software and continuous update cycle has altered this calculus.

> "Electronic networks are the attack vectors of the 21st century."

Getting the incentives right for open-source sustained code review is essential. Whether exploit access is designed or discovered, it is facilitated by the connected network itself. Hackers located thousands of miles away can simply ride the internet to probe for, discover, and exploit vulnerabilities. Perversely, the network delivery of software updates to improve functionality or patch security vulnerabilities can become a pathway to implant or exploit the software running the network.

Exploiting network vulernabilities

Electronic networks are the attack vectors of the 21st century. Criminals and countries, acting individually or in concert, daily pursue these attack paths to achieve their own goals at the expense of those operating and using the networks.

Nation-states including Russia, North Korea, Iran, China, and others maintain aggressive cyber intrusion programs. The 2021 SolarWinds attack against the cloud service companies essential to so many businesses was executed by Nobelium, a company working directly for Russian intelligence services.[3] The Not-Petya attack in 2017, for which six Russian intelligence officers were charged by the Justice Department, cost businesses over $10 billion in lost revenues and remediation costs.[4] Maersk Line, for instance, had to stop vessels at sea in mid-transit because they lost access to data essential to loading, offloading, and routing of cargo.[5]

Criminal enterprises, nation-states, and their apparatchiks have reportedly been behind attacks on hospitals, police, firefighters, 9-1-1 services, schools, and other public institutions. As public services incorporate 5G-enabled functions, it is a logical expectation

that adversarial intelligence services and criminal elements will see expanded attack opportunities.

China's cyber activities — And beyond

The emergence of redesigned 5G networks happened at the same time when Western governments were becoming increasingly concerned about the cyber activities of the Chinese government. The U.S. government has responded by focusing on the long-range strategic issues raised by China, including the ongoing security threats to government networks and systems. There has been less federal focus on the security issue of non-government pathways. While federal network security is being tightened, the commercial networks that will deliver the "smart" era to citizens, companies, and communities remains without meaningful technical risk oversight.

According to FBI Director Christopher Wray, Chinese government hacking activities are "Bigger than that of every other major country in the world combined."[6] China was behind 67% of state-sponsored cyberattacks between mid-2020 and mid-2021, according to one analysis.[7] It is not just China, however, that is a cyber belligerent. The Russian GRU and its various subcontractors have long been involved in destructive attacks.

Yet it is China that has staked out a substantial position as a supplier of network equipment and created concerns about the security of Chinese network equipment suppliers such as Huawei, including whether that equipment could be compromised by design. Director Wray identified a Chinese cyberattack technique that is frighteningly similar to creating a by-design network vulnerability for cyber exploitation.[8] In this example, U.S. companies operating in China were required to use specific government-sanctioned tax software. Unbeknownst to the users, the software secretly installed maliciously hidden backdoors into the companies' private networks.

Because of such worries, the U.S. Congress passed legislation prohibiting the domestic use of communications equipment that could pose a national security threat.[9] This has resulted in a mandate to remove Huawei-built wireless equipment that had already been installed by some small rural wireless providers. Such a policy is important but should not be allowed to misdirect attention away from the broader issue of software vulnerability. While companies such as Huawei and ZTE are high-profile Chinese vendors, the move to software-enabled networks has opened the door to others who would seek to exploit the 5G network for profit or political/strategic purposes—or both. Cyber criminals, for instance, can be expected to take advantage of the expanded attack surface of 5G.

From business intiative to "Huawei Killer"

The rearchitecting of network infrastructure to become more open and interoperable was

originally developed as a business initiative to reduce costs and increase capabilities. It took on geopolitical significance in response to the concerns about Chinese equipment from companies such as Huawei. If open equipment could end network reliance on a single provider, it was reasoned, such multi supplier diversity could provide an alternative to closed end-to-end systems reliant on Chinese equipment.

Such a strategy had the intended added advantage of playing to the strength of Western software developers and stimulating Western economic growth with Western-based technology. The U.S. Congress appropriated $1.5 billion for a Public Wireless Supply Chain Innovation Fund to expand the activities of U.S. companies in the 5G technology stack, largely rationalized as supporting an alternative to Huawei.[10] The hoped-for results of this market intervention will be seriously impaired, however, if American networks and suppliers cannot demonstrate that the attendant cyber risk responsibilities have been addressed.

A new Pandora's Box?

Moving from single-sourced to multi-sourced infrastructure can be a security improvement—but it is not a security solution. The motivation for the move was not security, and the implementation is not a security outcome.

Supplier diversity and cybersecurity are not synonymous; the presence of the former does not assure the latter. This is especially true when the diverse suppliers are not only delivering hackable software-based products, but also may not prioritize cybersecurity.

Software has a supply chain just like any other product. Seldom is a piece of software built from scratch, but is "typically compiled from existing code libraries, both open source and proprietary."[11] The National Institute of Standards and Technology (NIST) defines a software supply chain attack as "when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customer. The compromised software then compromises the customer's data or systems."[12] Supply chain exploits can be achieved upon the software's installation or through subsequent updates for routine patching or functional upgrade.

"Supplier diversity and cybersecurity are not synonymous; the presence of the former does not assure the latter."

The provenance of each component of each piece of the software is therefore especially important in a world of multiple suppliers and even more sub-suppliers. The potential for trojans to be part of infrastructure does not disappear by banning Chinese hardware if the software replacing it or the in-service sustainment of the code is compromised. Expanding

infrastructure from hardware to software also welcomes new exploiters that had not previously had a hardware foothold as well as for incumbent suppliers, such as those from China, to attack through non-Chinese products and infrastructure where possible. All this underlines the need to protect critical infrastructure software regardless of the code's origin.

Such provenance review and protection are especially important for open-source software. The U.S. Departments of Commerce and Homeland Security "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry" warned such vulnerabilities come not only from overt intrusions, but also from the use of open-source software.[13]

Open-source software is available from publicly accessible code libraries which developers incorporate into the product they are assembling. By one analysis, "the average modern software application contains 128 open-source dependencies."[14] NIST warns, "Customers often accept third-party [open-source] software defaults without investigating further."[15] Because of this, and because the code will, by design, change frequently, it is essential on a continuing basis to know both who wrote and who is sustaining the code, as well as where that is being done.

One of the most important code-based functional improvements to 5G is the ability to coordinate activity across multiple service providers offering unique capabilities to corporate and government enterprises. This is enabled by an orchestration layer of software that provides continuous interchange between the status of networks and applications and resource demands. This new orchestration, by design, brings an additional set of innovative companies and their code into the control plane for 5G enabled services. Sharing necessary control data with a larger set of downstream service providers further complicates the security challenge.

"Opening Pandora's Box with virtualized open network infrastructure reveals new multinational and multifaceted threats."

Software code typically "requires frequent communication between a vendor's network and the vendor's software product located on customer networks"[16] to deliver both updates and improvements—a process called DevOps. This means that software protection, like the code itself, must be sustained throughout its lifecycle regardless of the source of the code. Such a process should utilize the Zero Trust "never trust, always verify" technique that constantly reassess not only the code's origin, but also all internal and external activities that could affect its security. Zero Trust puts a "protective wrapper" around the data so that it's useless when it's exfiltrated out of context. While essential in a modern, mature cybersecurity program, Zero Trust alone is not sufficient to prevent the full range of attacks on availability, integrity, and confiden-

tiality.

While China has been the principal concern in 5G cybersecurity, nations such as Russia, Iran, North Korea, and others harbor their own cyber penetration goals. Cyber criminals are also very aware that 5G networks will support greatly expanded parts of the economy, thus offering new opportunities for their exploits. Opening Pandora's Box with virtualized open network infrastructure reveals new multinational and multifaceted threats.

Exploiting the standards process

The technical standard for 5G networks was developed in a consultative process among the major holders of infrastructure and component patents. Each of these companies negotiates to include their intellectual property in the standard, thus triggering a royalty payment if the standard contribution is used for implementation. Essentially, this process is an oligopoly. Three quarters of the 5G patents are owned by seven companies. Huawei is the largest holder of 5G patents, controlling 18%. ZTE, another Chinese company, controls 4%, Nokia 7%, and Ericsson 4%. The only major U.S. patent holder is Qualcomm's 12%.[17]

In the last decade, Huawei has made it a corporate objective to improve their wireless standards influence and benefit. When compared to 4G, Huawei has improved both the quantity, quality, and value of their submissions to the standards process. In the 4G standard, Chinese companies held less than 2% of the patents; in the 5G process, Chinese companies dominated the outcome. Part of the strategy for accomplishing this is to "flood the zone" with well qualified engineers, dwarfing U.S. participation in the standards body deliberation (for which participation comes with practical participation costs).[18] This is happening at the same time when U.S. wireless engineers, eligible for security clearances typically associated with cutting edge U.S. cyber research—and thus essential as an early warning capability—continue to decline in number.

Implementation of the 5G standard revolves around "Standard Essential Patents" (SEP)—a portfolio of intellectual property for which royalty must be paid whether used or not. Whether each of these SEPs is indeed "essential" rather than the product of trade-offs among the standard-setting participants to scratch each other's back with royalties becomes a cybersecurity concern. Various studies have concluded that only between 20% and 30% of all declared patents are truly "essential."[19] While there is no requirement to use each SEP, each must nonetheless be paid for. This can lead to an "I've paid for it, so I might as well use it" attitude and can have the effect of expanding opportunities for any SEP owner with malicious intent to "burrow in" for exploit at a later date in the life cycle when the 5G community is looking elsewhere. At the same time, "user's choice" also complicates security risk assessments as not all implementations are alike.

Public-private opportunity

Cybersecurity is first and foremost a management challenge. Technology plays an important role, but management practices are the first line of defense.

Acting alone, neither government nor private companies (whether networks or their suppliers) can meet the cyber management challenges of 5G networks. Governmental processes are habitually slow and tend to produce rigid regulations that are antithetical to the rapidly evolving and agile reality of digital innovation. Networks and their suppliers, on the other hand, are saddled with the need to produce financial results in a world where the return on corporate cyber investment is relatively low and often not visible to impacted parties. Cybersecurity, when it is addressed, becomes a cost center facing strong incentives to reduce costs in instances where risk is hard to identify and ROI is illusive. Furthermore, cybersecurity is a "whole of the networks" challenge since the investment of one company can be compromised by the vulnerability created by another network's failure to be as diligent.

The future rests on secure pathways. The management solutions to the 5G cyber challenge requires meaningful oversight to address how it pushes risk towards consumers and communities. This means the development of a new agile, yet enforceable, public-private program to create forward-looking security practices and procedures rather than relying on good intentions and after-the-fact patches. Shared risk is always a challenge as it's not always obvious who should pay to address different risk elements, who executes the remediation and who determines sufficiency. This is not done well today and should motivate new cybersecurity risk engagement between industry and government.

"The management solutions to the 5G cyber challenge requires meaningful oversight to address how it pushes risk towards consumers and communities."

Because secure 5G networks are a national necessity and cybersecurity is a "whole of the networks" problem, the cost of providing such security should be a shared public-private expense.

PART 2

THE VIRTUAL REVOLUTION

SUMMARY

The 5G headlines are about faster speeds and lower latency—but those are simply the effects of expanded spectrum pathways coupled with a revolutionary network redesign. The real technology innovation—and threat vector—in 5G that makes this possible (and sustainable across an ever-changing technology landscape) begins with the "virtualization" in software of functions previously performed by hardware, followed by their commoditization.

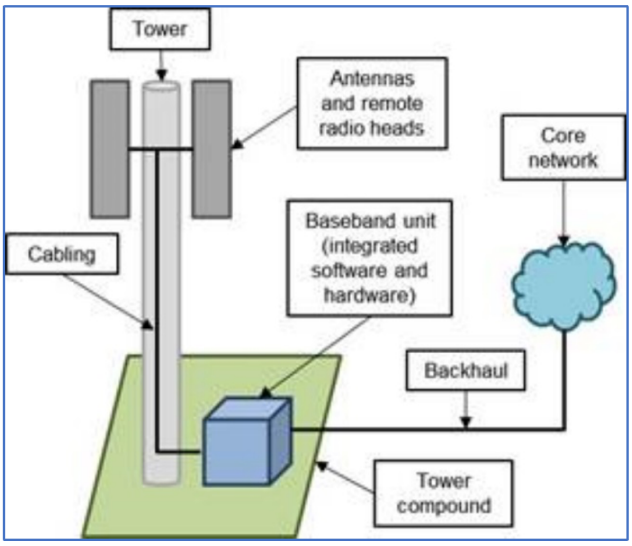
The digital revolution has redefined how telecommunications networks operate. Over the last several years, the move from hardware to software has been an ongoing piece-by-evolutionary-piece project for wireless networks. The 5G standard brought that home with an all-IP configuration that creates a network that is effectively the connecting of computers with voice, video, text, data, and analysis tools distributed across converged storage, compute, and communications infrastructure.

Virtualizing networks

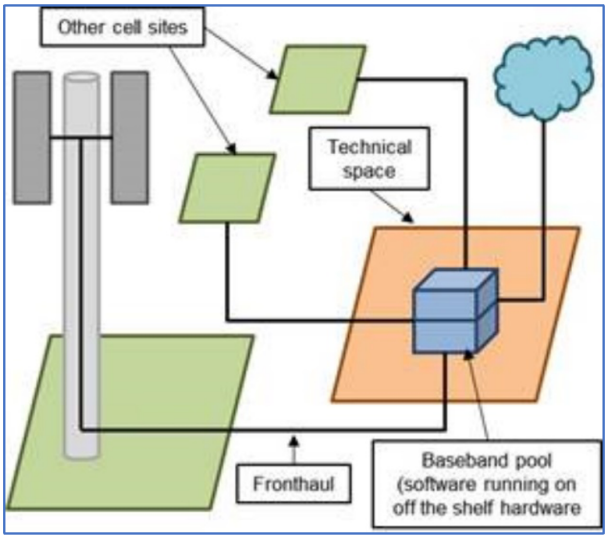
Once the functions of a wireless network begin to be implemented in software—as 5G does—the network architecture begins to evolve. As the following diagram of the radio access network (RAN) illustrates, virtualizing specific pieces of the network hardware, such as the baseband unit that reformats radio signals for the network, allows its functions to be centralized and shared to both lower cost and increase productivity. Similarly, virtualizing core network functions into the cloud where costs are shared with other users means capital and operating costs are less than a standalone core.

Comparing traditional and virtual networks[20]

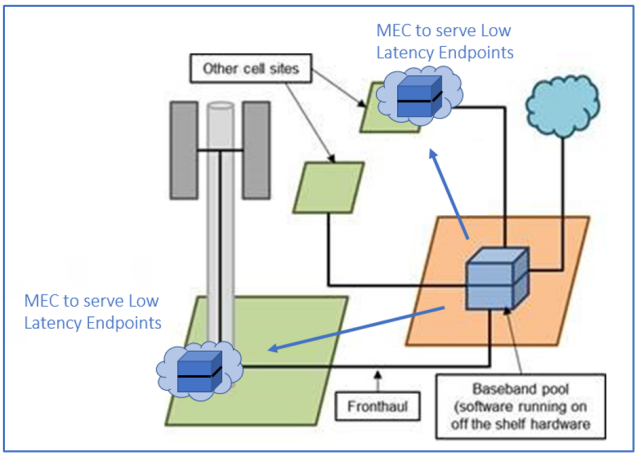
Virtualization also allows for flexibility in network design to deliver different service levels. In instances where the back-and-forth time to a connected device is a priority, the cloud may move closer to the network's edge to reduce latency. Such a design is called Multi-access Edge Computing (MEC).



Traditional RAN



Virtual RAN



Multi-access Edge Computing Configuration

O-RAN

The virtualization of the 5G standard opens the door to the introduction of multiple providers—and new providers—of network components.

The essential functional component of a wireless network—comprising by some estimates up to 60% of the network's total capital and operational expense[21] —is the radio access network (RAN) that translates signals between the wireless and wired portion of the network.[22] The equipment for these activities has traditionally been made by companies such as Nokia, Ericsson, and Huawei. Typically, a mobile network provider will choose a single supplier's RAN for a specific geographic area. Because the equipment lacks interoperable interfaces with the equipment of other suppliers, this decision effectively locks the network into the technical practices and product pricing of that vendor. It was this technical lock-in to a single supplier that caused much of the initial concern about

Huawei infrastructure.

> **"The introduction of open, interoperable, and less expensive network systems, along with moving the network core into the cloud, has opened the door for companies other than traditional networks to offer 5G service."**

Such closed proprietary solutions are the antithesis of how the companies that use the commercial networks build their infrastructure. When a company such as Google, for instance, seeks to expand its server farms, it can choose among multiple open-interface equipment suppliers, as opposed to wireless carriers' need to work with a single vendor. The result of such openness stimulates competition that drives down prices while driving up functional capabilities.

Opening the RAN to multiple vendors holds the promise of bringing similar benefits to wireless network providers. The term "O-RAN"—short for Open RAN—while specifically referencing the network's RAN, has become a generic description for the commodification of virtualized network functions, not just in the RAN but also the transport network and the movement of the network core functions into the cloud. The greatly increased set of technology and provider options should provide enduring downward price pressure and more frequent functional enhancements.

While the benefits of O-RAN are real, so are the risk elements resulting from the disaggregation of network components. A report from the U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Agency (CISA) concluded, "Open RAN is an exciting concept…However, with those benefits come the potential for additional security concerns."[23]

Together, the vulnerabilities inherent in the 5G standard and O-RAN require a new oversight framework to ensure that customers and communities enjoy the network's new benefits without exposure to catastrophic consequences.

Competitive benefits

The introduction of open, interoperable, and less expensive network systems, along with moving the network core into the cloud, has opened the door for companies other than traditional networks to offer 5G service. Copying the pay-as-you-go software as a service (SaaS) model, these companies offer private 5G networks as a service (NaaS) for factories, warehouses, and other campus-like settings.

Utilizing either licensed or unlicensed spectrum, these "5G in a box" providers can make

use of the same diverse supply of interoperable products as do the traditional networks but without the big network's cost overhead. These offerings are often bespoke implementations that are optimized for an enterprise's desired functions and lowest sustaining costs. Once again, however, this 5G product creates a paradox of welcome competition with unwelcome security concerns.

What about security?

The concern about Huawei equipment in a world of single-supplier networks was that it could allow for espionage, sabotage to the network and other critical infrastructure, or even a total shutdown of the network. Breaking the dependency on a single provider through a diversity of equipment choices theoretically can have the added benefit of offering increased security by breaking the equipment bottleneck. A "must use" legacy position could open the door to nefarious activities or, even absent ill intentions, de-prioritize the discovery of inherent vulnerabilities.

Excluding equipment companies from China and other adversarial nations is the definitive supply chain security solution, however, only if one assumes that there will be no effort to circumvent that exclusion. The unanswered question is whether China and others have already made the pivot to focus on the opportunities represented by the 5G standard's virtualization and the O-RAN push for multiple interoperable suppliers. To assume the pivot has already been made is the only responsible conclusion.

The future development and implementation of O-RAN will, of course, determine its security performance. While the O-RAN Alliance has created a Cybersecurity Working Group, it is important to note that O-RAN adds no new mandatory security requirements beyond those already in the 5G standard. The O-RAN specifications in their original release neither acknowledged nor proposed solutions for many of the inherent cyber threats.[24] The open and interoperable architecture of O-RAN, however, does open the door to new exploitations. The ability of ill-intentioned players to infiltrate the expanded number of suppliers, coupled with the difficulty tracking the security of each of those multiple vendors ends up being an expansion of cyber risk rather than a reduction.

"Excluding equipment companies from China and other adversarial nations is the definitive supply chain security solution, however, only if one assumes that there will be no effort to circumvent that exclusion."

The future rests on secure pathways. The European Union's analysis of 5G cybersecurity found that while O-RAN brings the benefit of supplier diversity, it "still lacks maturity and cybersecurity remains a significant challenge."[25] Because of issues such as an

expanded attack surface with more entry points for malicious actors, increased risk of misconfiguration, and the impact on other network functions, the EU report "recommends a cautious approach towards this new architecture."[26]

PART 3

WHEN INFRASTRUCTURE IS CODE

SUMMARY

Since the magnetic telegraph, communications networks have been the connection of hard assets. The digital revolution and 5G have exchanged those hard assets for software code that performs the same functions.

Such software-based networks are a network operator's dream, offering new capabilities at lower capital and operating costs. A key part of that is to embrace moving core network functions to the cloud.

As network operators become the orchestrators of software, as opposed to managers of hardware, they inherently must rely on software code produced by others that is run on computers managed by others. In such an environment, the reliability and provenance of that code, as well as the sustained security practices of the service provider become a paramount concern.

Never has so much been said—and misunderstood—about new wireless technology than what has transpired regarding 5G. It is virtually impossible to turn on the television without being exposed to an advertising barrage about the 5G service of wireless carriers. For a while during the previous administration, 5G also became a metaphor for politicians to discuss commercial relations with China. Both descriptions contain components of fact, but both miss the heart of the opportunity and the risk of 5G.

5G is not a product, it is a standard. Although it is sold in advertising as if it was a product, like all standards, it is its implementation that is determinative.

The standards process

The establishment of 5G technical standards was the result of a multiyear process administered by Third Generation Partnership Project (3GPP), created in 1998 to bring together national Standards Development Organizations (SDOs) from around the world.[27] As the name suggests, it began with the creation of the 3G standard and has kept functioning as technology and the marketplace evolved. The development of a 6G standard is already underway.

The standards process, which started as an effort by state-owned PTTs and their suppliers (with AT&T representing the Unit-

ed States) to coordinate technology development for interconnected networks, has evolved into an oligopoly dominated by infrastructure and device vendors such as Nokia, Qualcomm, Ericsson, Samsung, ZTE, and Huawei. The companies each pursue their own vision for the design of the next generation network. Utilizing technical summits to share developments and explore consensus, a standard is ultimately decided by a vote of those willing to pay the costs of engaged, peer-respected participation. Such votes are often determined by which idea had the most supporters attending a particular meeting. With 3GPP corporate participation being increasingly foreign, active participation in the 'horse trading' for votes entails overseas meetings and challenging coalition building activities.

"The role of standard setting takes on increased significance when infrastructure is code divorced from hardware ownership."

China's efforts to align international standards with their geopolitical objectives has added international intrigue to the standards process. Huawei, which grew rapidly as an equipment provider spurred by low prices and financing supported by the Chinese government, brought similar aggressiveness to the standards setting process. As a result, Huawei—which was ranked seventh in 4G patents—walked away the big‡ winner in the 5G standard, owning 18% of the patents for 5G.[28] At the very time when U.S. domestic policy was shifting away from oversight of the activities of international standards bodies, China moved in.§

The role of standard setting takes on increased significance when infrastructure is code divorced from hardware ownership. The linkage between standards setting and Chinese policy prompted the U.S. Congress to include in the 2021 National Defense Authorization Act instructions for the National Institute of Standards and Technology (NIST) to study, "the effects of the policies of the People's Republic of China and coordination among industrial entities within the PRC on international bodies engaged in developing and setting international standards for emerging technologies."[29] The report is expected in January 2023.

‡ Qualcomm and others note that number of patents doesn't completely tell the story as quality of patent will ultimately determine use for implementation. Still, the significant increase in accepted Chinese contributions and leadership role within 3GPP for cryptographic, control plane, and non-terrestrial network interfaces is impressive and concerning.

§ In 2016 the authors oversaw an initiative at the FCC to tie the entry of 5G technology into the United States to the inclusion of acceptable cyber protections in the then-developing standard. This included a Notice of Inquiry (NOI) that sought information from the nation's best minds on what those protections should be. Upon taking over in 2017, the Trump FCC eliminated the initiatives.

When infrastructure code is disaggregated from operators obligated by license for security outcomes, networks are *per se* vulnerable. The role of standard setting to determine whose software is required by the standard and the cybersecurity risk expectations, therefore, takes on increased significance.

Breaking the oligopoly

The move to break the control of the dominant infrastructure vendors began in 2016 under the leadership of Facebook.[30] A coalition of companies whose future was tied to continuously evolving networks with compute and storage at the edge combined to create the Telecom Infra Project (TIP).[31] Its vision of interoperable network components from multiple providers has evolved into a TIP relationship with the network-led Open RAN Alliance.

As befitting an internationally connected network, the O-RAN Alliance includes networks and suppliers from throughout the world. The founding members—each with veto power—are AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, and Orange. Thirty-six members of the Alliance are headquartered in China.[32] These include Chinese companies, some of which are on the U.S. Entities List because of security risks.[33] A founding member of the O-RAN Alliance is China Mobile which the FCC has denied the right to operate in the United States because of its ties to the Chinese government.[34] China Mobile co-chairs 10 of the 14 O-RAN Alliance working groups.[35]

O-RAN is not a technical standard like 5G, but rather a means of implementing new architectural capabilities made possible by the 5G standard through open interfaces and use of the cloud. The first goal of O-RAN is a business goal: the Interoperability of network equipment so as to decrease costs and increase performance. The geopolitical realities of such supplier diversity were more by happenstance than by design.

The rise of the O-RAN design drives the second part of the 5G paradox: how the beneficial diversity of suppliers results in potential cybersecurity vulnerabilities. The EU's Report on the Cybersecurity of Open RAN expresses the concern that the initiative's focus on supplier diversity has outpaced its focus on security.[36] Leading the charge for worldwide O-RAN in lieu of legacy wireless technologies is just as likely to result in Chinese or other high-risk nation of origin versions of O-RAN 5G. China has incumbent advantage in Africa, South America, and much of the Indian Ocean and Pacific regions and capable O-RAN solutions.

Newton's Law meets networks

Even in telecommunications networks, every action has an equal and opposite reaction. As interoperable equipment threatened to break the infrastructure oligopoly, savvy infrastructure companies expanded their efforts as patent owners rather than hardware providers. Regardless of who made the final piece of network gear, it had to be built to the standard and pay royalties to the owner of the intellectual property dictated by the standard.

It thus became a corporate necessity for the infrastructure companies to have their patented intellectual property rights (IPRs) included in the standard as "standard essential patents" (SEP). This became a process of old-fashioned horse trading where the parties would negotiate, "I'll agree to put a piece of your IPR in the SEP if you'll agree to this piece of mine."

Standard essential patent dealmaking was the first step in what became the "patent pincer" strategy to maximize revenue for the companies, even if they were no longer physically making hardware. The second step, once having made it into the SEP, is to array attorneys to bring lawsuits against those who either work around agreed upon SEP components or do not pay the required royalty.

"The use of open-source components in software can further accentuate the cyber risk."

The revenue-enhancing patent pincer has an added benefit for those with ill intentions. A standard can become a potential attack vector when its implementation compels (or allows) malicious software to exploit a poorly designed function. Thus, if there are security vulnerabilities hidden or accepted in a standard and malicious software takes advantage of it, the legal enforcement of the standard's patent rights enables the software's widespread propagation. When almost a quarter of the 5G patents come from Chinese companies (Huawei 18%, ZTE 4%), there are plenty of opportunities for potentially harmful pathways into the nation's essential 5G networks.

Do you know where your software has been?

The security risk to 5G networks grows with the expansion of software components from different suppliers. It is a risk that is further expanded by the multiplicity of components from sub-suppliers that are included in a single piece of software. Ultimately, the connected updating of software for new functionality, patching of discovered vulnerabilities, and securing against new threats creates the vehicle for the delivery of such vulnerabilities.

The use of open-source components in software can further accentuate the cyber risk. There was a 650% increase in software supply chain attacks in 2021 "aimed at exploiting weaknesses in upstream open-source ecosystems."[37] The Departments of Commerce and Homeland Security report on the software supply chain was explicit: "The ubiquitous use of open-source software can threaten the security of the software supply chain given its vulnerability to exploitation."[38]

Yet, in a competitive market that rewards "speed to functional innovation," cybersecurity, if it is addressed, has a modular focus—one that typically does not imagine all the ways in which a module might ultimately be used. An agile software development

best practice today intentionally employs a "borrow rather than build" reuse of available open-source code to rapidly introduce new functions. Such a decision is "a minefield of known (and unknown) security risks."[39] The 2021 State of the Software Supply Chain report concluded,[40] "Members of the world's open source community are facing a novel and rapidly expanding threat…aggressive attacks implanting malware directly into open source projects to infiltrate the commercial supply chain."[41] This is occurring in an environment, one research project found, where only 14% of surveyed software developers listed security as a priority and 67% admitted that they routinely left known vulnerabilities and exploits in their code.[42]

> "The role of Chinese code hidden in non-Chinese open systems software conveniently skirts the focus on Chinese hardware."

The concerns about Chinese infrastructure suppliers does not abate as networks move from hardware to software. The original concern about Huawei hardware—a concern O-RAN was hailed for addressing—was that its software could contain backdoors that could be made available to the Chinese government. The potential for similar trojans to be included in or introduced after-the-fact in software utilized by open infrastructure suppliers cannot be dismissed. The role of Chinese code hidden in non-Chinese open systems software conveniently skirts the focus on Chinese hardware. The push to include as many pieces of proprietary intellectual property as "standard essential" broadens the aperture for such software exploitation.

The risk from malicious code continues across the lifecycle of a codebase that is regularly changing. This underscores the role for oversight and illuminates the potential for competitive distinction for code developed and sustained in the U.S. Establishing provenance for U.S.-developed 5G O-RAN code and preserving its integrity as it's used in global technology markets will not only address cybersecurity risks at home but also provide competitive alternatives in nations with high-risk providers today.

When infrastructure code is in the cloud

Virtualization has not only opened the door to new suppliers of previously proprietary products, but also has moved the hosting of many of those software functions to centralized server farms colloquially known as the cloud. The major wireless networks have already announced hosting relationships with cloud services such as Amazon Web Services and Microsoft Azure.[43] A report by the Center for Strategic and International Studies identified a global strategy of Huawei's to become a dominant provider of cloud services throughout the world.[44]

While concerns regarding lock-in with a single RAN vendor have strongly motivated wireless service providers to push for O-RAN, there does not seem to be the same concern for the increased role that hyperscale cloud service providers will play in 5G. AT&T's decision to sell its core network to Microsoft Azure, not only outsourced the 5G core control plane, but also locked them into a single supplier in the way that O-RAN was supposed to eliminate. This is not to say the cloud relationship is not beneficial, but that it raises new vulnerabilities that must be anticipated and dealt with. These include issues ranging from the delineation of cyber responsibilities between public and private cloud services to the assignment of risk responsibilities.

> **"Providing cloud-based competitive '5G in a box' as an alternative for enterprise networks introduces yet another set of cyber intrusion possibilities."**

Adding to the cyber challenges of the cloud is that access to the cloud is often via the internet, thus adding an additional attack vector. In addition, as Multi-access Edge Computing (MEC) brings the compute function from a distant computing cloud even deeper into the coverage area, it introduces new security challenges.

Use of the cloud and MEC for computational purposes illustrates the greater complexity of 5G and Open RAN about which the EU report warned.[45] Performing the network's basic functions in the cloud suddenly makes the cloud provider a new player in network security, thus adding another level of cyber complexity.* Providing cloud-based competitive "5G in a box" as an alternative for enterprise networks introduces yet another set of cyber intrusion possibilities.

In the "smart" era, **everything builds upon the security of the networks** connecting the smart devices. Behind the EU's generically bland "added complexity" concern about 5G Open RAN lies a new architecture and the failure to identify the cybersecurity risks and mitigation responsibilities that result from the virtualization of multiple functions in the cloud.

Some argue that everyone knows that one cannot trust the security of the networks and

*The authors have experience with the outstanding security of one of the largest cloud providers and its ability to identify and trace attacks. As cloud services become commoditized, however, not all companies will be able to offer such levels of service. As cloud activities play an increasing role in networks, the multiplicity of providers will create the same kind of security concern as the multiplicity of other networks suppliers. Cloud service providers are very careful to delineate the boundaries of their responsibilities to secure customer loads in their cloud. Nonetheless, the very same clouds have examples where customers that failed to understand their security roles suffered a devastating cyberattack.

takes appropriate measures. Such a transfer of responsibility to those using the network is precisely the problem.

Increased machine-to-machine data communications at the edge of 5G networks will undoubtedly attract efforts by third-party groups to exploit vulnerabilities for the monetary and intelligence advantage of their sponsors. The role of cloud at the edge will increase risk from this vector. As telemedicine, self-driving cars, financial transactions, biometric trust mechanisms, patterns of life surveillance and other highly personal activities increasingly find new 5G-enabled functions, the potential harm to individuals will also go up if cybersecurity is not prioritized at the 5G edge and clear risk responsibilities are not established.

PART 4

FLASHING LIGHTS

SUMMARY

The telecommunications industry stood out in 2021 as a target for cyberattacks. The 2021 CrowdStrike Threat Hunting Report concluded that targeted intrusions into telecommunications networks accounted for 40% of all state-nexus incursions.[46]

5G enters this environment as a new innovation-enhancing, cost-reducing technology for already vulnerable networks. Multiple federal agencies have identified the problem and proposed standards for secure networks.

We know the threats as well as how to mitigate them. Securing networks does not mean awaiting new technology, but rather instituting management across the networks to mitigate the new problems.

Billions for "rip and replace", but not a penny for cybersecurity

During the Obama administration, the federal government advised wireless network operators of the threats inherent in using Chinese equipment. The four major network providers—Verizon, AT&T, TMobile, and Sprint—all observed the warning and did not buy Huawei or ZTE equipment. Unfortunately, a number of small rural wireless carriers prioritized the low prices they were getting from the Chinese companies over their responsibility to national security and installed Huawei 4G equipment. Those rural networks, of course, connected with the big national networks, thus providing a potential intrusion pathway. While the large carriers deserve praise for not buying Chinese equipment when the issues where identified, they did not address the shared risk with their interconnected small carriers and opposed increased FCC focus on systemic cybersecurity risk reduction, reporting, and accountability. As Huawei became a political issue, the FCC announced that its program to subsidize high-cost rural infrastructure deployment[††] would no longer support those companies utilizing the Chinese equipment.[47] The companies ran to Congress pleading for the government to pay the replacement cost. The Congress appro-

[††] The anomaly of this action is that the Trump FCC chose to address cybersecurity only for a handful of small companies covering only a fraction of the population while failing to make cybersecurity protection the responsibility of all wireless companies.

priated $1.8 billion[48] to replace equipment that should not have been purchased in the first place. The companies now complain the replacement cost is closer to $5 billion.[49] Congress is investigating ways to get them the additional funds.

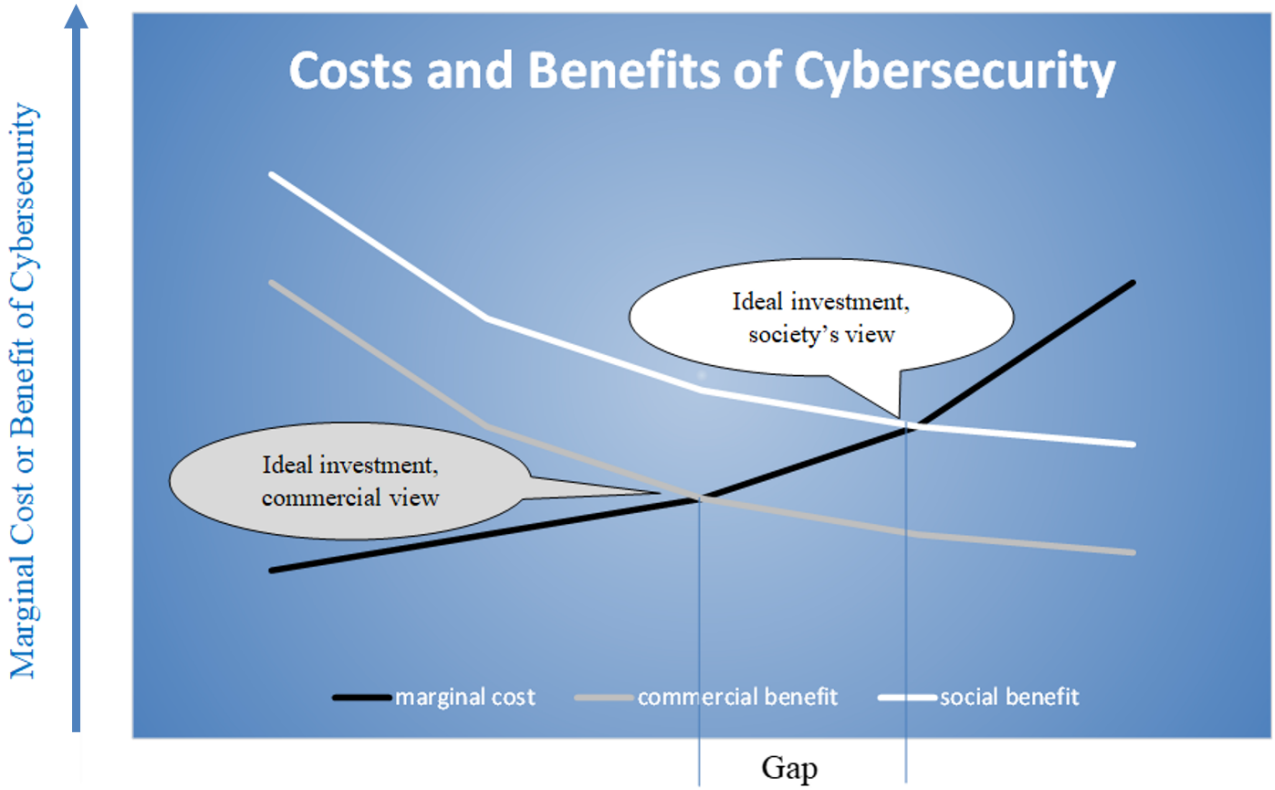
This "rip and replace" program was seen as a prime opportunity to introduce supplier diversity through open network architecture. Yet thus far, most of the Huawei network equipment has not been ripped out and replaced. Amazingly, Congress did not require the recipients of the windfall bailout to establish best practice cybersecurity programs or include cybersecurity protections in their new deployments.[50] Planning to replace Huawei with O-RAN's supplier diversity theoretically solved the "Huawei problem," but, as we have seen, it also opened the door to new cyber threats arriving from diverse network suppliers. Even when U.S. policy insists on using non-Chinese suppliers, the largest component of 5G standard essential patents is from Chinese companies. The rip and replace program could have been the controlled experiment for developing wireless provider security processes for maximizing and sustaining the cybersecurity of O-RAN equipment, but it is not.

The ROI incentive gap

It is not unusual that a wireless company—particularly a small company with few employees—would seek to spend as little as possible on cybersecurity. As commercial entities, the providers of 5G services operate in an environment that pressures against investment that does not directly lead to profit. Cybersecurity is a cost center rather than a profit center. The nation's commercial network providers are forced to strike a balance between the costs and benefits of investing in cybersecurity.

Yet, the interconnected nature of the internet creates a "whole of the network" reality where the actions or inactions of one network provider can affect other networks. A 2017 FCC White Paper titled "Cyber Risk Reduction" concluded, "Reducing risk to our communications networks is complicated by unique economic forces…Unfortunately, relying on market forces alone fails to adequately weigh the risks imposed on third parties who rely on the networks and the services they provision."[51]

"As commercial entities, the providers of 5G services operate in an environment that pressures against investment that does not directly lead to profit."



The gap between the ideal level of investment in cybersecurity and that which the networks determine to be commercially acceptable is illustrated in this graphic from the FCC White Paper.

The disconnect between cybersecurity expenditures and needs becomes manifest in the amount that telecommunications companies have been spending on research and development—including cyber R&D—that is both small and often shrinking.[52] Recognizing this, a consortium of non-network cybersecurity companies have come together to develop their own Open Cybersecurity Scheme Framework (OCSF).[53] The proliferation of Cybersecurity Frameworks from governments, standards bodies, and industry speak to the imperative for improved cyber posture but also reflect the confusion companies have on prioritization for risk reduction investments.

Take it or leave it cybersecurity

The 5G standard includes more cybersecurity tools than did 4G. There is a warning light flashing, however, that it is up to the individual companies whether to implement the protections.

The 5G standard attempts to deal with an expanded range of cyberattack vectors. Controls such as distributed denial of service (DDOS) detection and mitigation, expanded use of encryption, improved roaming security, Zero Trust enhancements for core signaling, as well as API and cloud security are included elements in the standards body of work. These security enhancements are all important. Whether they are sufficient in a virtualized environment operating on open

infrastructure protocols and whether they are even implemented are even bigger unanswered issues.

A flashing light in the United States is that the Trump FCC passed on the opportunity to require implementation of all the 5G standard's cyber protections in U.S. networks. In 2020, the FCC delegated the 5G cybersecurity question to its industry-dominated Communication, Security, Reliability, and Interoperability Council (CSRIC). The Council's recommendation was that each network company be allowed to determine which of the 5G cyber standards they would implement. It is a recommendation that the FCC accepted and has not been revisited.[54]

Defense Department recognition of the threat

The U.S. Department of Defense (DoD), recognizing the security vulnerabilities of 5G, has at the urging of Congress taken the initiative to secure military-related use of the technology. In September 2022, DoD and MITRE Labs, a federally funded R&D center, announced the FiGHT (Five G Hierarchy of Threats) Framework.[55]

The goal of the Framework is to reliably identify the integrity of a 5G network, its applications, and devices through a purpose-built model of anticipated adversarial behaviors. In the version 1.0 roll out, the FiGHT Framework includes 15 categories of attack tactics and over 80 specific 5G relevant attack techniques.

It is clear that the DoD sees that 5G warning lights are flashing. What's not clear is the commitment of the providers towards independently, affirmatively, and uniformly addressing the threat with equal vigilance. Many of the attack techniques cut across 5G service provider segments, with significant variation in code cybersecurity sustainment responsibilities, and the primary agency charged with oversight of the 5G providers, the FCC, has thus far not established clear expectations for 5G service providers or their vendors.

EU Open RAN and security report

The European Union is the only Western government to publicly address the potential security risks of O-RAN. Its "Report on the Cybersecurity of Open RAN" concluded that while there are security benefits to the diversification of suppliers, "cybersecurity is a significant challenge for the Open RAN concept."[56] The report warned that "by introducing a new approach, new interfaces and new types of RAN components potentially coming from multiple suppliers, Open RAN would exacerbate a number of the security risks of 5G networks and expand the attack surface."[57]

The report identified multiple "key risks that are amplified or brought by Open RAN." These include:

- More entry points for malicious actors, due to a potentially increased number of suppliers and components;
- An expanded threat surface and a more

complex environment leading to higher risks of vulnerability or failure;

- An increased risk of misconfiguration of networks;

- Technical specifications, such as those adopted by the O-RAN Alliance, not sufficiently mature and secure by design, and deficiencies in the O-RAN Alliance governance;

- New or increased dependency on cloud service/infrastructure suppliers;

- New potential risks and impact on other network functions due to resource sharing;

- The risk profile of a (potentially higher number of) individual suppliers continuing to be an important source of vulnerabilities.[58]

Because **everything builds upon the security of the network**, the EU report concluded, among other recommendations, with a call for, "Using regulatory powers to be able to scrutinize large scale Open RAN deployment plans from MNOs [mobile network operators]. [I]f needed, government should, 'restrict, prohibit, and/or impose specific requirements or conditions for the supply, large-scale deployment and operation of the Open RAN equipment.'"[59]

PART 5

IT'S NOT THAT WE DON'T KNOW WHAT TO DO

SUMMARY

It's not that we don't know what to do. We have just not developed a plan to do it.

Because networks interconnect, such a plan must be a "whole of networks" approach based on well-known security standards overseen at the network level by a single regulator. Because network security is a national challenge for which corporate returns are limited, it should be supported by the federal government.

"Cybersecurity in telecoms is garbage," Ian Levy, the then-Technical Director of the UK's National Cyber Security Center (NCSC) told the assembled audience at the 2022 Mobile World Congress.[60] Government has a once in a generation opportunity to change this, he said, but it will not be accomplished by the old style of regulatory micromanagement that was applied to the telephone network.

The Duty of Care

The basis for establishing cybersecurity protections for 5G networks was established hundreds of years ago as England emerged from the feudal era. As "common law" developed to replace the random rules nobles had imposed on serfs, one of those principles was the Duty of Care. Such a Duty of Care is simple: **the provider of a good or service has the obligation to anticipate and mitigate its potential harms.**

In a classic interpretation of the Duty of Care for the industrial era, the courts held the Buick Motor Company liable for the failure of a wheel on an automobile it assembled, even though Buick did not make the wheel.[61] The court's opinion found that neither the consumer nor the local dealership had meaningful insight to or control over the manufacturing process or material supply chain—but Buick did. The decision firmly placed the risk assessment and mitigation responsibility with the corporation in the best position to know details regarding assembled sub-systems and to control the processes that would address risk factors. The operators of 5G networks have a similar responsibility of vigilance over the services and products they deliver, even if it is a collection of multiple components from multiple sources.

A Cyber Duty of Care needs to be expected and enforced. The cyber risk inherent in 5G networks—even though it may result from

the software from a sub-supplier to the network—is an essential network responsibility. The highest and best level to address cybersecurity is at the network, not chasing after the network's multiplicity of suppliers. Such network expectations should be rewarded with appropriate incentives, whether regulatory, monetary, or in other forms.

"The reality that malevolent players act with agility and speed means the solution cannot rely on old style sclerotic and rigid regulatory micromanagement."

Seeking "Whole of the Networks" solutions

The old "single neck to choke" monopoly regulation model was simple: in return for that monopoly and guaranteed profit margins, the network operator submitted to regulatory micromanagement. Because 21st century digital networks have neither a monopoly nor guaranteed returns, and because keeping pace with innovation requires agility, the old regulatory model is no longer effective.

There remains, however, a need for government to establish policies that protect network users from adverse consequences. The most efficient point for such expectations is at the network level. The network companies' action or inaction oversees all aspects of cybersecurity. The question is: Who oversees the networks?

The 5G cybersecurity problem is exacerbated by the internet's interconnectedness. The term "internet" is a contraction of its original name "internetworking." The internet's breakthrough was the creation of a network of networks. It is this internetworking of multiple diverse and distributed networks that makes cybersecurity a "whole of the networks" challenge.

Every network is reliant on every other network. A failure or error in one part of the interconnected networks can become a threat that propagates across all networks. In addition, the networks are interdependent in that the data each collect can be essential to the Zero Trust efforts of other networks, enterprise users, and intermediary providers. It's not just that Zero Trust data transits over multiple provider networks; multifactor authorizations often rely on trust elements inherited from operations supported by other operators.

The fact that the 5G cybersecurity threat permeates all aspects of all 5G networks necessitates an all-networks solution.

The reality that malevolent players act with agility and speed means the solution cannot rely on old style sclerotic and rigid regulatory micromanagement.

Fifth generation network security requires specialized, focused authority to implement enforceable standards that reflect 5G's convergence of communications, computing, storage, and analytics utilizing a process similar to that which successfully produced the wireless standards themselves.

Beyond indentifying the problem

The U.S. Department of Homeland Security, Department of Commerce, and Federal Communications Commission have all identified the cybersecurity threat inherent in digital networks. Congress has passed legislation prohibiting the use of equipment that could pose a national security threat and asked the network companies to implement voluntary risk assessment capabilities.[62] In another statute, Congress required the FCC not to approve any communications equipment posing an unacceptable risk to national security.[63]

The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) has made solid progress securing federal systems and collaborating with infrastructure providers. CISA is responsible for overseeing 18 critical infrastructure sectors, of which communications is one;[64] yet, it lacks meaningful enforcement authority to mandate its cybersecurity expectations on those commercial networks.

The National Institute of Standards and Technology (NIST) of the Department of Commerce has done groundbreaking work to develop multiple cyber-promoting frameworks on Network Security,[65] Secure Software Development,[66] and Cyber Supply Chain Risk Management.[67] These well-conceived frameworks rely on voluntary industry implementation since the Department of Commerce lacks the requisite regulatory authority over telecommunications networks.

Congress has been very liberal in assigning funds to foster 5G experimentation within the executive branch. The Department of Defense (DoD) identified several 5G security and technology maturity gaps and has advanced prototypical solutions, such as the MITRE FiGHT™ effort described previously. The identified security gaps go beyond the 5G standard and must be mitigated as part of network implementations. These efforts, however, have not yet addressed 5G end-to-end cybersecurity challenges within their own networks and are not charged with securing commercial 5G network implementations.

The Biden administration has broadened 5G experimentation to include greater participation from non-DoD agencies. The Departments of Energy, Transportation, Commerce, Health and Human Services, the National Science Foundation, and others all have active experimentation activities underway and will certainly want to use DoD contracting experience to address 5G security gaps in their objective implementation.

Missing from this is oversight outside of the executive branch where markets live. Many of the 5G security gaps exist "in the seams" between provider layers. It's within this 5G network "commons" that the leadership of the Federal Communications Commission (FCC) is required. The FCC is the only federal

agency with the requisite regulatory authority over America's commercial networks. In 2014, over the objections of the agency's Republican commissioners, the FCC initiated a plan for public-private cooperative oversight of network security based on the NIST framework.[68] In 2016, the networks pushed back when the FCC sought assurances they were utilizing NIST best practices. When the Trump FCC took over in 2017, the effort was dismantled.[69] Since then, the FCC has convened a series of working groups to identify important 5G cybersecurity risks but has yet to establish cybersecurity protection expectations for the expanded set of providers in the 5G ecosystem.

Studies, statutes, and standards without enforcement are insufficient. The cyber threat in 5G networks requires moving from *ex post* reactions that might be described as shooting behind the target to *ex ante* implementation of a proactive plan. Today, there is no focused, proactive, agile, and enforced exercise of regulatory authority over the security practices of commercial digital networks, including the expanded vulnerabilities of the 5G standard and O-RAN.

New regulatory model

One of the reasons companies regulated by the FCC did not want the agency to exercise its cyber authority is because the agency's processes are too rigid and bureaucratic. As officials of the FCC, the authors struggled to deal with the cybersecurity of networks, only to be confronted by:

- Industrial-era procedural laws that made rulemaking activity cumbersome and non-rulemaking activity less than optimal;
- The incentive of bad actors to overcome any solution is typically greater than the incentive to maintain the necessary protection;
- Industry stakeholder fear of exposing their internally identified risk factors at precisely the time when sharing information about attacks would be of the greatest value for a collective defense.

"Cyber insecurity follows when risk reduction investments are not holistic and fail to continuously assess, appreciate and address emerging technological and threat landscapes."

We exist in a world where the rapid pace of technological change is exceeded only by the speed of those who would seek to exploit that technology for harm. A turgid, bureaucratized response to ever-evolving cyber exploits is like chasing mercury with molasses. The tools for dealing with network security, sup-

ply chain risks, and open-source software are increasingly well known. Cyber insecurity follows when risk reduction investments are not holistic and fail to continuously assess, appreciate and address emerging technological and threat landscapes. Rigid application of fixed security standards does not keep up with the threat. Successful cyber programs must be agile and include agile oversight.

Such uniform implementation of common expectations is a process in two parts. It begins with a policy declaration that cybersecurity must be a required forethought in the design, implementation, and operation of 5G networks, not a voluntary afterthought. The second part is the establishment of a private/public supervised process to develop agile and enforceable cyber expectations.

Such a private/public process must inform and be informed by regular engagement between the providers, their vendor communities, and government agencies representing consumer, citizen, and community risk concerns. The bias in such activities should be one of information exchange and collaborative defense against a common adversary. Enforcement should not be used to punish companies where the adversary got through strong defenses the government was aware of but instead be reserved for situations where companies have ignored warning signs and failed to establish and sustain best practice, best process risk management decision making.

New mandatory expectations

Because cybersecurity is a whole of the networks problem, it requires a common set of mandatory expectations applicable to all interconnected services. Except when required as a condition to providing services to the government, there has been resistance from network providers and policymakers to establishing mandatory cybersecurity protections for 5G.

"Operators of 5G networks currently have no incentive other than market pressure to invest in cybersecurity, nor the capability to police interconnectivity that lies beyond their domain."

The Trump FCC left it to the companies whether to implement the cyber protections built into the 5G standard and did not use the NIST framework to drive specific risk reduction efforts with either the 5G standards bodies or with U.S. providers. Congress asked, not ordered, the networks to voluntarily implement cyber risk assessment and mitigation programs. NIST created the framework for such efforts but lacks enforcement tools.

Meanwhile, Zero Trust mechanisms are left to a wide landscape of 5G and cloud providers, public networks, vendors, data applications, and cybersecurity companies without any objective architecture that balances public/private, enterprise/individual, public safety/national security, or other nuanced equities.

> **"In the 'network of networks' that is the internet, there must be a common set of required expectations accompanied by consequences for noncompliance."**

Experience shows that voluntary programs are not enough. Operators of 5G networks currently have no incentive other than market pressure to invest in cybersecurity, nor the capability to police interconnectivity that lies beyond their domain. As the previously referenced 2017 FCC report observed, relying on such market forces is a recipe for failure.‡‡ A report from the UK government reached the same conclusion: "often telecoms providers have little incentive to adopt the best security practices."[70]

Absent universal and enforceable expectations, security frameworks such as those developed by NIST or those included in the 5G standard are invalidated. In the "network of networks" that is the internet, there must be a common set of required expectations accompanied by consequences for noncompliance.

The nation's interstate highways have mandated safety standards; the nation's digital highways should as well.

A new regulatory focus

Where the federal government has experienced its own cyber threats, it has developed its own set of standards. The Department of Defense, for instance, has specifications for every part of its connected systems. At the same time the Trump FCC backed away from developing required expectation for ISPs, the DoD leadership worked to establish rigid, checklist-oriented cybersecurity controls as contract obligations to be audited by a third party.

A lesson from the DoD experience is that self-attestation to cybersecurity risk reduction has not been sufficient. To replace self-certification, the DoD developed the Cybersecurity Maturity Model Certification.[71] Key to this approach under the Trump ad-

‡‡ The recently passed Broadband Equity, Access, and Deployment (BEAD) legislation which makes $42 billion available to bring broadband infrastructure to unserved areas could, in some circumstances, end up supporting wireless infrastructure. The legislation, however, leaves it to the states to define acceptable cybersecurity efforts using the NIST Framework.

ministration was the establishment of 259 specified requirements, of which 244 require third-party inspection and attestation. The fact that many commercial entities have been able to comply with such rules demonstrates that government-established and enforced standards are viable solutions. Hoping those standards will trickle down to broader commercial services, however, is not a viable cybersecurity strategy.

The authors are not suggesting there should be a checklist compliance approach to assuring cybersecurity. However, there does need to be an enumerative description of what constitutes good cyber hygiene and enforcement of its implementation. Such a cybersecurity oversight function must be centralized in a single federal agency.

Multiple federal agencies independently pursuing multiple non-regulatory 5G security agendas is a formula for excuses instead of execution. Regulations overseeing the deployment and operation of 5G networks should be the focused responsibility of a single federal agency with coordination responsibilities across the interagency being well defined.

Such oversight must cleave from the rigid micromanagement of the regulatory model designed for the industrial era to embrace a new model that follows agile 21st century practices.

A new regulatory design

The multiple NIST frameworks provide the roadmap for what needs to be done to protect 5G network security. The challenge becomes how to implement the frameworks apart from the traditional sclerotic and rigid regulatory process.

The command-and-control regulatory model previously applied to telecommunications networks is ill-suited—in fact, is counter-productive—to the fast-paced cyber challenge of the internet era. In its place, government should implement a public/private multistakeholder process for the establishment of cyber standards to be executed by the companies and enforced by the government.

“Such oversight must cleave from the rigid micromanagement of the regulatory model designed for the industrial era to embrace a new model that follows agile 21st century practices.”

The methodology for establishing such cyber standards should mimic the development of the industry’s technical standards process. The evolution from 1G, to 2G, to 3G, to 4G, to 5G, and now the ongoing development of 6G, demonstrates a successful process that constantly adapts to new threat and techno-

logical realities.[§§]

Under such a standard-setting process, the regulator would identify an issue and convene an industry/public body to develop a standardized approach to mitigate the problem. There are four key steps to such a process:

- ***Results Oriented*** – The process must begin with the expectation of meaningful results. The responsible agency should identify the specific issue(s) to be addressed and establish a timeline for results. The final recommendation should be ratified and/or amended by the agency. Failure to reach an acceptable conclusion would empower the agency to act unilaterally.

- ***Risk Identification*** – The agency should begin the process with its own detailed report on the problematic issues, along with suggested potential remedies. The resulting process, then, becomes the production of a meaningful outcome that solves or mitigates the identified issue(s). The Financial Sector has learned the hard way that periodic stress testing illuminates fault lines before catastrophic failure. Network cybersecurity also benefits from regular "stress testing" to illuminate missing and poorly implemented controls. Meaningful oversight should incent sharing of best practices and areas of emergent unaddressed risk.

- ***Multistakeholder*** – The participants in the process should be qualified experts representing a cross-section of all the interested parties, including industry, government, and civil society. Stakeholder risk roles must be continuously evaluated with a bias towards clear market-based alignment of risk mitigation ownership responsibilities. Government roles should be focused on cybersecurity externalities, not addressed by market forces.

- ***Meaningful Enforcement*** – The agency must have the authority on its own motion to enforce the standard and implementation outcomes. The bias in such enforcement should be to information exchange and collaboration against a common enemy. Enforcement should not be used to punish companies where the adversary got through strong defenses the agency was aware of but instead be reserved for situations where a company has ignored warning signs and failed to establish the multistakeholder developed best practices.

[§§] Whereas the "early Gs" were relatively static development efforts, the addition of 4G Long Term Evolution (LTE) greatly increased the frequency with which new functions and fixes for discovered problems were added to the standard. It was the precursor to the agility that exists in the standards process today.

New shared support: Protect America's Networks Fund

Those who know the networks best operate under business realities that are suboptimal for effective risk reduction. As we have seen, 5G networks operate in economic environments that pressure against investments that do not contribute to profit. This means that cyber protection has a weakest link problem where protective action taken in one instance can be undermined by the failure elsewhere to take similar action. This reality further weakens the incentive to invest in such protections. Cyber accountability, therefore, requires not only appropriate regulatory oversight, but also financial support for the universal implementation of agreed-to standards.

Because cybersecurity is a "whole of the networks" challenge, it must also be a "whole of the nation" responsibility. That there is a national interest in cyber protections is illustrated by the Broadband Equity, Access, and Deployment (BEAD) Program Congress passed as part of the Inflation Reduction Act.[72] The BEAD Program appropriated $42 billion to expand broadband into unserved areas. Significantly, it also required recipients of the funds to have a cybersecurity risk management program in place based on the NIST Cybersecurity Framework.[73] The BEAD Program funds attainment of those requirements for the four years of the grant.[74]

While the BEAD Program principally supports fiber-delivered broadband, its cyber funding sets a new policy benchmark. That the BEAD grants require (and pay for) the adoption of the NIST Cybersecurity Framework is a roadmap for the future.[75]

For decades, the FCC has administered the Universal Service Fund (USF) to subsidize network operators to make telephone and internet service available in high-cost areas.** A similar approach should be implemented to subsidize 5G network service Cybersecurity Risk Management programs for meeting regulatory standards that will assure each provider has an active and effective cybersecurity risk management program.

> "As we have seen, 5G networks operate in economic environments that pressure against investments that do not contribute to profit."

At present, the FCC's subsidy program appears headed for overhaul. Designed in the telephone era, the program is funded by a fee added to each telephone bill. Because the number of phone lines has been decreasing, the per line monthly fee has been increasing.

** It was this program that the Trump FCC used to cut off funding for rural wireless carriers using Chinese equipment.

Arguments have been put forth to require the service providers who use the broadband network—companies such as Amazon, Apple, and Netflix—to contribute as well.

That the explosion of cyber risks occurs at a time when the basic formulation for support of digital connectivity is under review presents an opportunity. There is a broad and pervasive national interest in shared financial support of the universal implementation of cybersecurity protections. The national priority for secure 5G networks, coupled with the business reality that cyber investment is a cost center rather than a profit center, justifies the modernization of the USF program to include a Protect America's Networks Fund.

> **"Cyber accountability, therefore, requires not only appropriate regulatory oversight, but also financial support for the universal implementation of agreed-to standards."**

Such a new program, of course, must be done thoughtfully so that cyber risk is not merely transferred to the government or capped by the availability of the Fund. But just as the original USF supported the added costs of delivering telephone service to high-cost rural areas by subsidizing those marginally higher costs, so should a cyber USF help defray the marginal costs of new cyber regulatory requirements.

It's all about the networks

Private industry has done an amazing job developing new wireless networks that embrace new technological capabilities. Now private industry is engaged in investing tens of billions of dollars to build 5G networks.

The high-speed, low-latency capabilities of 5G networks are essential to building the "smart" era. The potential of microchips scattered like digital dust across corporations, consumers, and communities requires wireless network connections. The attendant volumetric increase in network traffic and connections will overwhelm current security approaches. The emergence of cloud-like compute, storage, and communication capabilities wholly utilized and controlled at the edge of networks to support low latency robotic functions creates yet another new set of enterprise security challenges.

It has always been true that it was not the network *per se* that was transformational, but what that network enabled. Fifth generation networks will be a key enabler for the role that artificial intelligence (AI) will play in our smart economy. Wireless networks will be the workhorse for AI data collection supporting robotic activity in smart cities, smart business verticals, and smart consumer services. Investment in AI will be highly correlated with our trust in the networks that deliver data to

its algorithms. Trusted AI begins with and will depend on secure networks.

It is the networks that are essential. The digital future is built on 5G networks—and **those pathways must be secure.**

We know what is necessary to secure the networks.

We know network security must be prioritized.

Every network should be expected to meet enforceable security minimums and for public support of those efforts.

5G is smart, now let's make it secure.

EPILOGUE

ELIMINATING CYBER PATHOGENS

In the late 19th century, the industrial revolution pulled workers into condensed urban areas without the infrastructure necessary to support a sizable population. The lack of sewage and safe drinking water resulted in epidemics of cholera and other diseases that threatened everyone in the community regardless of position.

The epidemic of network-borne cyberattacks is the 21st century equivalent of 19th century water-borne disease. As the infestation problem that affects all is similar, so is its solution: the standardized and supervised hygiene of the system.

Industrial age sanitation began in the network with a water treatment plant. Standardized management processes were put in place to test every day to assure the water network was not spreading harmful pathogens. In a similar manner, the internet age requires a "data treatment plant" of standardized processes at the network level to assure the absence of digital pathogens.

"Water treatment plants are a physical instantiation of the idea that politics are the structures we create when we are in a sustained relationship with other people," Debbie Chachra wrote in her study of 19th century infrastructure "Care at Scale."[76] "[M]unicipal water and sewage systems function as the smallest-scale proof of concept for the value of building out collective systems…not for nothing is 'indoor plumbing' still a metonym for 'civilization.'"

The security hygiene of the most important network of the 21st century is the internet era's equivalent of indoor plumbing: a marvelous convenience that requires a standardized and managed process to assure its safety so that it may realize its potential.

"The epidemic of network-borne cyberattacks is the 21st century equivalent of 19th century water-borne disease."

ENDNOTES

1 Tim Pohlmann, "Who leads the 5G patent race as 2021 draws to an end?" November 3, 2021, *IAM*, https://www.iam-media.com/article/who-leads-the-5g-patent-race-2021-draws-the-end

2 Tom Wheeler and David Simpson, "Why 5G Requires New Approaches to Cybersecurity," Brookings Institution, September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

3 Joe Hernandez, "The Russian hacker group behind the SolarWinds attack is at it again, Microsoft says," October 25, 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft

4 Kim S. Nash, "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs," *The Wall Street Journal,* June 27, 2018, https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

5 Jill Leovy, "Cyberattacks cost Maersk as much as $300 million and disrupted operations for 2 weeks," *Los Angeles Times,* August 17, 2017, https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

6 Christopher Wray, "Countering Threats Posed by the Chinese Government Inside the U.S.," January 31, 2022, https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122

7 Kyle Alspach, "Russian hackers get the headlines. But China is the bigger threat to many U.S. enterprises," Protocol, August 3, 2022, https://www.protocol.com/enterprise/china-hacking-ipn-russia-cybersecurity

8 Christopher Wray, "Director's Remarks to Business Leasers in London," July 6, 2022, https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622

9 Secure and Trusted Communications Act of 2019, H.R. 4998, 116th Congress (2019-2020), https://www.congress.gov/bill/116thth-congress/house-bill/4998

10 CHIPS and Science Act, https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122 117th Congress, https://www.commerce.senate.gov/2022/8/view-the-chips-legislation https://www.democrats.senate.gov/imo/media/doc/USICA%20Summary%205.18.21.pdf

11 "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry," U. S. Department of Commerce and U.S. Department Homeland Security, February 24, 2022, https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry

12 National Institute of Standards and Technology, "Defending Against Software Supply Chain Attacks," April 2021, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

13 *Ibid*

14 *State of the Supply Chain Report,* Sonatype, p. 22, https://www.sonatype.com/resources/white-paper-2021-state-of-the-software-supply-chain-report-2021

15 *Ibid*, p. 5.

16 *Ibid*, p. 5.

17 *Op Cit., "Who leads the 5G patent race"*

18 YP Jou and Jackson Lin, "A deep dive into the quality of Huawei's 4G and 5G SEP portfolios," *IAM Media*, November 29, 2019, https://www.iam-media.com/article/deep-dive-the-quality-of-huaweis-4g-and-5g-sep-portfolios

19 Alan Weissberger, "New data from IPlytics and Tech+IP Advisoty LLC show regions and companies leading 5G Patent race," *IEEE ComSoc,* June 4, 2022, New data from IPlytics and Tech+IP Advisory LLC show regions and companies leading 5G Patent Race - Technology Blog (comsoc.org)

20 Illustration courtesy MoffattNatanson

21 "Reducing Total Cost of Ownership (TWO) with Open RAN," *Parallel Wireless*, August 19, 2021, https://www.parallelwireless.com/blog/reducing-total-cost-of-ownership-tco-with-open-ran/

22 Dan Jones and Corinne Bernstein, "Definition: radio access network (RAN), *TechTarget,* https://www.techtarget.com/searchnetworking/definition/radio-access-network-RAN

23 "Open Radio Access Network Security Considerations," National Security Agency and Cybersecurity and Infrastructure Security Agency, September 15, 2002, Open Radio Access Network Security Considerations (cisa.gov)

24 "ETSI releases first O-RAN specification," European Telecommunications Standards Institute (ETSI), and O-RAN Alliance, September 15, 2022, https://www.o-ran.org/press-releases/etsi-releases-first-o-ran-specification

25 European Commission, "Cybersecurity of Open Radio Access Networks," May 11, 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

26 *Ibid*

27 "About 3GPP," https://www.3gpp.org/about-3gpp/about-3gpp

28 *Op Cit*., "New data"

29 National Institute of Standards and Technology (NIST), U.S. Department of Commerce, *Study on People's Republic of China (PRC) Policies and Influence in the Development of International Standards for Emerging Technologies,* 86 Fed. Reg, 60801, November 4, 2021, https://www.federalregister.gov/documents/2021/11/04/2021-24090/study-on-peoples-republic-of-china-prc-policies-and-influence-in-the-development-of-international

30 Jay Parikh, "Introducing the Telecom Infra Project," Facebook, February 21, 2016, https://about.fb.com/news/2016/02/introducing-the-telecom-infra-project/

31 https://en.wikipedia.org/wiki/Telecom_Infra_Project

32 "The false promise of Open RAN," Digital Power China, August, 2022, https://dgap.org/en/research/publications/false-promise-open-ran , p. 15.

33 O-RAN Alliance members Inspur, Kindroid, Phytium, and H3C are on the Entity List. https://www.uscc.gov/sites/default/files/2021-04/Timeline_of_Executive_Actions_on_China-2017_to_2021.pdf https://www.commerce.gov/news/press-releases/2021/04/commerce-adds-seven-chinese-supercomputing-entities-entity-list-their; https://www.federalregister.gov/documents/2021/11/26/2021-25808/addition-of-entities-and-revision-of-entries-on-the-entity-list-and-addition-of-entity-to-the

34 "FCC Denies China Mobile Telecom Services Application," May 9, 2019, https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application

35 *Op Cit, "Fales Promise*, p. 16.

36 *Op Cit, State of Software Supply Chain*, p. 4.

37 *Ibid*, p. 4.

38 *Op Cit, State of Supply Chain,* p. 3.

39 *Op Cit, State of Supply Chain,* p. 6.

40 *Op Cit, State of the Supply Chain Report*

41 *Ibid,* p.10.

42 Steve Zurier, "Only 14% of developers consider security a top priority," *SC Magazine*, April 5, 2022, https://www.scmagazine.com/news/application-security/only-14-of-developers-consider-security-a-top-priority%ef%bf%bc

43 Mike Robuck, "Microsoft draws a bead on telcos with Azure for operators," *Fierce Telecom,* September 28, 2020, https://www.fiercetelecom.com/telecom/microsoft-draws-a-bead-telcos-azure-for-operators and Ammal Latic, et al, "TELCO Meets AWS Cloud: Deploying DISH's 5G Network in AWS Cloud," *AWS Industries*, February 23, 2022, https://aws.amazon.com/blogs/industries/telco-meets-aws-cloud-deploying-dishs-5g-network-in-aws-cloud/

44 Jonathan E. Hillman and Maesea McCalpin, "Huawei's Global Cloud Strategy," Center for Strategic and International Studies, May 17, 2021, https://reconasia.csis.org/huawei-global-cloud-strategy/

45 "Nowhere to Hide: 2021 Threat Hunting Report," *CrowdStrike*, https://go.crowdstrike.com/threat-hunting-2021-report.html

46 *Op Cit*, EU Open Radio Access report

47 https://docs.fcc.gov/public/attachments/DOC-373481A1.pdf

48 Secure and Trusted Networks Act, 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/4998

49 "Rosenworcel Notifies Congress of Demand for Rip and Replace Program," February 4, 2022 https://www.fcc.gov/document/rosenworcel-notifies-congress-demand-rip-and-replace-program

50 Tom Wheeler and David Simpson, "Billions for Broadband but not a Penny for Cybersecurity," *Seattle Times,* June 3, 2021, https://www.seattletimes.com/opinion/billions-for-broadband-but-not-a-penny-for-cybersecurity/

51 "Cyber Risk Reduction," Federal Communications Commission, January 2017, https://www.fcc.gov/document/fcc-white-paper-cybersecurity-risk-reduction

52 Iain Morris, "Telcos spend pathetically little on R&D, and it's often shrinking," *Light Reading,* August 8, 2022

53 "Cybersecurity and Technology Industry Leaders Launch Open-Source Project to Help Organizations Detect and Stop Cyber Attacks Faster and More Effectively," *Business Wire*, August 10, 2022

54 Howard Buskirk, "Most 5G Security Features Should Be Options, CSRIC Recommends," *Communications Daily*, December 10, 2020, https://communicationsdaily.com/news/2020/12/10/most-5g-security-features-should-be-options-csric-recommends-2012090055

55 "MITRE and the Office of the Undersecretary of Defense Announce FiGHT™ Framework to Protect 5G Ecosystem," September 26, 2022, https://www.mitre.org/news-insights/news-release/mitre-and-office-under-secretary-defense-announce-fighttm-framework

56 *Op Cit*, European Commission

57 *Op Cit*, European Commission, p. 16.

58 *Ibid*

59 *Ibid*

60 Conversation on stage with Tom Wheeler

61 MacPherson v. Buick Motor Company, 217 N.Y. 382, 111 N.E. 1050 (1916), https://www.lexisnexis.com/community/casebrief/p/casebrief-macpherson-v-buick-motor-co

62 Secure and Trusted Communications Act of 2019, H.R. 4998, 116th Congress (2019-2020), https://www.congress.gov/bill/116thth-congress/house-bill/4998

63 Secure Equipment Act, H.R. 3919, 117th Congress (2021), https://www.comgress.gov/bill/117th-congress/house-bill/3919

64 Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors, https://www.cisa.gov/critical-infrastructure-sectors

65 "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework

66 "Secure Software Development Framework," National Institute of Standards and Technology, February 2022, https://csrc.nist.gov/publications/detail/sp/800-218/final

67 *Op Cit*, Defending Against software Supply Chain Attacks

68 Brian Fung, "FCC unveils 'new regulatory paradigm' for defeating hackers," *The Washington Post,* June 12, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/06/12/fcc-chair-telecom-companies-must-do-more-to-defend-against-hackers/

69 The Trump FCC did ask the agency's Communications, Security, Reliability, and Interoperability Council (CSRIC), an advisory body composed of industry representatives, to evaluate the cybersecurity components that had been added to the 5G standard. The council's recommendation was the empty suggestion that each company should be free to decide whether these cyber protections should be implemented. This became Commission policy.

70 "UK Telecoms Supply Chain Review Report," Department of Culture, Media and Sports, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

71 https://www.acq.osd.mil/cmmc/about-us.html

72 https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/19/fact-sheet-the-inflation-reduction-act-supports-workers-and-families/

73 National Telecommunications and Information Administration, "Notice of Funding Opportunity: Broadband Equity, Access, and Deployment, p. 70.

74 Notice of Funding Opportunity, Broadband Equity, Access, and Deployment Program, National Telecommunications and Information Administration, U.S. Department of Commerce, Sec IV.c.2.c.vi, https://broadbandusa.ntia.doc.gov/sites/default/files/2022-05/BEAD%20NOFO.pdf

75 *Op Cit*., NTIA NOFO, Sec. V.H.1

76 Debbie Chachra, "Care at Scale: Bodies, agency, and infrastructure," *Comment Magazine*, August 5m 2021, https://www.cardus.ca/comment/article/cate-at-scale/

BROOKINGS

1775 Massachusetts Ave
NW, Washington, DC 20036
(202) 797-6000