Free markets. Real solutions.

R STREET POLICY STUDY NO. 206
September 2020

5G AND ZERO TRUST NETWORKS

By Jim Baker and Kathryn Waldron

CONTENTS

INTRODUCTION

As the public health and economic crises resulting from COVID-19 have revealed, global society depends heavily on a complex and multifaceted digital ecosystem. Such dependence may be existential; that is, society would be crippled and lives lost if it collapsed for a significant period of time. At the very least, governments would find it exceedingly difficult to protect the health, safety and welfare of their citizens, while public and private sector entities would struggle to meet basic needs, such as food delivery and the provision of electricity, water, heat and cooling. In particular, the most vulnerable people in society—the elderly, young children and those who are infirm or disabled—might not survive a prolonged and widespread internet failure. All of this is especially true in the current crisis where society is under tremendous strain. In light of this, ensuring the safety and security of the digital ecosystem and the confidentiality, integrity and availability of the communications and other data transmitted, processed and stored on that ecosystem is an essential government function. However, governments cannot go it alone, as they depend heavily on the private sector companies and individuals who own and operate most of the internet.

As a result of the ongoing rollout of fifth-generation (5G) wireless technology, the digital ecosystem will undergo significant changes. At this early stage, it is difficult to ascertain exactly what these changes will look like and what broader impacts they will have on society. But, given the vast improvements 5G will bring, the ability to receive more data, faster will likely make us even more dependent on technology, while increasing the need for data security. As a result, network providers, operators and device manufacturers will have to respond in various ways.

The inherent design of global 5G networks will include numerous security enhancements over prior generations of wireless technology. For example, they will employ high-quality encryption to protect the content of—and certain metadata associated with—wireless communications as they are transmitted. This will close a long-standing security gap that enabled malicious actors to acquire unique identifying information about devices transmitting on wireless networks.[1] Nevertheless, several unresolved 5G security gaps likely will exist with respect to both hardware and software elements of the network.[2] As a result, from a risk-management perspective, it makes sense to presume that some important parts of the network will be untrustworthy.

Addressing this trust gap effectively requires rethinking internet security in some fundamental ways, including the adoption of a Zero Trust approach to some elements of the internet itself, and consistently using strong—that is, well-

1. "5G Policy Primer: Future Wireless Networks Will Have Unprecedented Security," AT&T, January 2020. https://policyforum.att.com/wp-content/uploads/2020/03/5G-Security-Whitepaper-March-2020.pdf; and John Marinho, "What's New in 5G Security: A Brief Explainer," Cellular Telecommunications Industry Association (CTIA), June 12, 2019. https://www.ctia.org/news/whats-new-in-5g-security-a-brief-explainer.

2. Tom Wheeler and David Simpson, "Why 5G requires new approaches to cybersecurity: Racing to protect the most important network of the 21st Century," Brookings Institution, Sept. 3, 2019.https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity.

designed and properly implemented—quantum-proof, end-to-end encryption of all data on 5G networks. This includes encrypting the content of communications and as much of the external routing and metadata as possible.

Accordingly, the present study discusses the application of the Zero Trust Network (ZTN) concept to 5G wireless technology. In particular, it focuses on employing a Zero Trust model combined with strong encryption to help mitigate some of the risks associated with the confidentiality, integrity and availability of data—three important concepts in the field of information security—in a 5G environment.[3]

To do so, we use the National Institute of Standards and Technology's 2017 Risk Assessment strategy to assume (rather than debate) these threat vectors. We then propose the "Zero Trust plus strong encryption" model as a methodology for reducing cyber risk more effectively going forward.

5G TECHNOLOGY

The term "5G" refers to a collection of new wireless network technologies which, used together, promise to revolutionize how the world communicates. The three main promises of 5G are greater bandwidth, faster data speeds and lower latency ("lag time"). These three factors are important because they will allow an unprecedentedly vast number of devices (including every component of the Internet of Things) to exchange data extremely quickly. They also offer the potential for better communication with, and control of, machines where any delay in real-time communication could have disastrous effects, such as in the case of autonomous vehicles or robots used to conduct surgery.[4]

Each new generation of telecommunications technology has allowed for increases in the speed with which data can travel. Increased download speeds have allowed for better communications and coverage, and have led to a span of other innovations and services.[5] Just as 4G was significantly faster than 3G, 5G will be significantly faster than its predecessor. In part, this is because 5G networks can be built around three different bands of wavelength spectrum—low-band, mid-band and high-band, or millimeter waves. These spectrum bands have different characteristics that affect their ability to deliver data. Low-band spectrum (frequencies under 2.5 GHz), for example, has longer wavelengths that allow for wider coverage. However, there is a limited amount of low-band spectrum available, since a large portion of it has already been allocated to uses such as public television. Meanwhile, mid-band spectrum (frequencies between 2.5 and 6 GHz) offers faster speeds, but the shorter wavelengths also equate to shorter coverage. Additionally, these radio waves have more difficulty penetrating buildings and other structures, so cell towers must be constructed closer together. High-band spectrum (frequencies greater than 6GHz) exacerbates these challenges because of its extremely short range and thus, until now, its use has been limited. In order to utilize high-band spectrum more broadly, 5G providers will likely increase the number of cell towers and antennas, particularly in densely populated urban areas.[6]

Although higher-frequency waves require a greater number of antennas to cover a similar geographic area when compared to lower-frequency waves, the antennas utilized by mid- and high-band spectrum are also much smaller than those required for low-band spectrum. While older cell towers used Single Input Single Output (SISO) systems that only had one branch for transmitting data and one for receiving, 4G LTE networks have started to include Multiple Input Multiple Output (MIMO) systems that have more than one branch for each. Massive MIMO systems will have up to hundreds of branches for transmitting and receiving data, possibly because of the small size of the antenna needed for high frequency 5G.[7]

Massive MIMO is only one of the technological foundations of 5G. These developments include beamforming, which is a "traffic-signaling system for cellular base stations that identifies the most efficient data-delivery route to a particular user [... reducing] interference for nearby users in the process,"[8] and quadrature amplitude modulation (QAM), which is a method of embedding more data in radio frequencies, allowing for higher data rates. Some of these methods are already being used in 4G LTE networks, and the initial rollout is focused on non-standalone (NSA) 5G, or the kind built on existing 4G infrastructure.[9] However, not all features

3. In the cybersecurity context, "confidentiality" refers to the preservation of restrictions around who can access certain data, particularly of a personal or proprietary nature; "integrity" refers to protecting transmitted data from improper modification or destruction; and "availability" ensures timely and reliable access to data. See Michael Nieles et al., "An Introduction to Information Security," National Institute of Standards and Technology, June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

4. "What is 5G?", Verizon, last accessed Aug. 25, 2020. https://www.verizon.com/about/our-company/5g/what-5g.

5. "What is the difference between 3G, 4G and 5G?", Verizon, Nov. 11, 2019. https://www.verizon.com/about/our-company/5g/difference-between-3g-4g-5g.

6. Brian Underdahl, *5G for Dummies, Sprint Business Special Edition* (John Wiley & Sons, Inc., 2018), pp. 9-10. https://business.sprint.com/wp-content/uploads/sites/2/2018/05/5G-For-Dummies-Sprint-Business-Special-Edition.pdf.

7. Ibid., pp. 12-14.

8. Amy Nordrum et al., "5G Bytes: Beamforming Explained," Institute of Electrical and Electronics Engineers, July 15, 2017. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-beamforming-explained.

9. The standards for 4G infrastructure were released in 2017 by the 3rd Generation Partnership Project (3GPP), an international standards-setting organization. 3GPP also developed the standards for 5G New Radio (NR), which is the radio interface and radio access technology required for 5G cellular networks. See, e.g., "What is 5G NR?", Verizon, Dec. 6, 2019. https://www.verizon.com/about/our-company/5g/what-is-5g-nr.

of 5G can use existing infrastructure and thus Standalone (SA) 5G will eventually follow.[10]

Security Challenges to 5G

A key technical aspect of 5G infrastructure is the distribution of different types of data between the core and edge of the network. The "core" of existing telecommunications networks is the centralized data hub where data is sorted and processed on its journey from one device to another. The devices, cell towers and antennas outside the core comprise the network's "edge," with a clear security perimeter dividing the two. Most network security has traditionally focused on protecting the core, since the edge is just following the core's commands. And although some experts still adopt this core/edge distinction with respect to 5G architecture, prudent information security risk management must consider the vulnerabilities of the entire system and act accordingly to mitigate residual risk. This is particularly true because, in 5G architecture, the distinction between the core and edge is less clear. To accommodate faster data processing power, 5G is designed to distribute core processing across the entire network, and this redistribution necessarily changes the focus and location of the security perimeter, and the feasibility of protecting it against intrusions.

Accordingly, the U.S. Department of State's Bureau of Global Public Affairs has explained:

> Boosting processing power across all parts of the network makes 5G faster. But this means there will no longer be an "edge of the network," and the entire network will require as much protection as the core does with today's 4G technology.[11]

The 5G network will need protection from a wide range of potential bad actors, including individual hackers, politically motivated "hacktivists" and state-sponsored threats. And accordingly, numerous public- and private-sector entities have expressed potential supply chain concerns regarding the security of 5G equipment provided by telecommunications equipment manufacturers that are domiciled outside the United States.[12]

Ultimately, it may be difficult or impossible for anyone to prove publicly and convincingly that all 5G hardware and software network elements pose little or no security risk. There have been conflicting public statements by governments and manufacturers on the topic, resulting in some degree of debate. Regardless of the disagreement, the reality is that any manufacturer of programmable network components that has the capability to update the software on such devices could introduce vulnerabilities into the system—intentionally or by mistake—that a malicious actor could exploit. Accordingly, it makes more sense simply to assume that some elements of the network are untrustworthy and proceed to manage those risks accordingly.

TOWARD A MORE USEFUL RISK ASSESSMENT

According to the National Institute of Standards and Technology's 2017 publication, risk management requires organizations to: (1) frame; (2) assess; (3) respond to; and (4) monitor risk.[13] More specifically, it explains:

> With respect to information security, risk management is the process of minimizing risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system.[14]

Consistent with this definition, the key feature of the NIST guidance for the purposes of the present study is that it argues against a version of risk assessment that seeks only to avoid risk altogether. Instead, in order to operate effectively, decision-makers need to think clearly, systematically and realistically about the risk they face, and then determine how best to deal with it. In this regard, it is critically important to: (1) accurately perceive reality and avoid falling prey to a range of cognitive biases; (2) identify and prioritize the key assets that require protection; (3) understand as clearly as possible the probabilities of bad outcomes; (4) put in place effective strategies to reduce the risks identified; and (5) endeavor to establish metrics and measures to assess how well those strategies are working.

ZERO TRUST THINKING AND ENCRYPTION

The traditional perimeter defense model of cybersecurity is based on the idea that operators can protect a network by essentially building a wall around it to keep malicious actors out. This can be accomplished through, for example, the use of firewalls at the edge of a local area network where it connects to the internet or other networks, and by employing virus scanning software and physical security safeguards

10. Hannes Ekström, "Non-standalone and Standalone: two standards-based paths to 5G," Ericsson, July 11, 2019. https://www.ericsson.com/en/blog/2019/7/standalone-and-non-standalone-5g-nr-two-5g-tracks.

11. Leigh Hartman, "Get smart: Core vs. edge in 5G networks," U.S. Dept. of State, Sept. 17, 2019. https://share.america.gov/get-smart-core-vs-edge-in-5g-networks-infographic.

12. Whether or not those manufacturers do, in fact, pose a threat and what strategies are available to deal with them is the subject of a forthcoming study that will be released later this month.

13. Michael Nieles et al., "An Introduction to Information Security," National Institute of Standards and Technology (NIST), U.S. Dept. of Commerce, June 2017, p. 34. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

14. Ibid.

(e.g., fences, guards and guns). In this model, the security around the perimeter is assumed to protect everything within from infiltration, and thus routers, computers, printers, scanners, applications, data flows and users are trusted fully and considered safe from malicious actors and malware. This is essentially a "100 percent Trust" model inside the perimeter.

Increasingly, however, the perimeter model does not work, primarily because perimeter defenses are too often unsuccessful at keeping out bad guys. And, while perimeter defenses are still necessary and provide some level of protection—especially against certain types of intrusions and malicious actions, and against some less-sophisticated adversaries—they are no longer enough to ensure that a network is properly defended. And this is where the Zero Trust model comes in.

Zero Trust: From Theory to Practice

According to John Kindervag, who is widely credited with introducing the Zero Trust model in 2010, part of the problem with traditional cybersecurity models is that they are built on the concept of 'trust but verify.'[15] Network operators designate certain devices, applications and users as "trusted" and then allow them broad—and excessive or unnecessary—access to other parts of the network. Moreover, this problem is exacerbated by the fact that system administrators often do not do enough to actually verify that so-called trusted devices, data or entities are who or what they purport to be.[16] For this reason, Kindervag's preferred model is to 'verify and never trust.'[17]

With this strategy in mind, Kindervag's Zero Trust model has three key features:

1. All resources are accessed in a secure manner regardless of location.
2. Access to anything on the network is on a strictly enforced "need to know" basis.
3. All network traffic is inspected and logged.[18]

In practice, these three features taken together mean that networks must be segmented much more thoughtfully and rationally, with well-designed and managed gateways controlling and monitoring access between the various segments.[19] Among other things, this means that network operators can—and should—strictly limit access to the most important parts of the network (such as locations where personally identifiable information or PII, credit card data, healthcare data and sensitive intellectual property are processed and stored), and provide broader access to less-sensitive machines and data (such as where publicly available data is located). According to Kindervag, this is a more secure, efficient and scalable design—especially in high-mobility contexts where users are located in multiple geographic locations.[20]

If properly designed and implemented, Zero Trust can help network administrators protect key systems and data from both external and internal threat actors. For example, under such an architecture, all attempts to access data are challenged and validated at all times—irrespective of whether the attempted access to the system and data comes from inside or outside the organization.[21] This is because adversaries who have penetrated the network can use: (1) a variety of active measures to move around the network to access, control or alter hardware, software or data; or (2) passive means to collect sensitive information about the network and the data that travels or is processed and stored on it.

As we understand Kindervag's way of thinking, the benefit of such a "worst-case scenario" model is that once an operator presumes infiltration (rather than presuming that perimeter defense efforts will succeed), they also have to assume that all the devices, users, applications or dataflows on the network are insecure. This forces them to establish a series of mechanisms to challenge, validate, segment and restrict elements and users of the network, and to encrypt data as much as possible. And, indeed, strong encryption is an increasingly vital corollary of the Zero Trust model.

However, it is one thing to describe a Zero Trust model and to articulate its benefits, and quite another to design, build and operate one successfully, as the latter requires redesigning and rebuilding a network from the bottom-up while, at the same time, making sure that it continues to operate successfully during the transition period. Moreover, it is often very hard to inventory all the devices that comprise a large network, the numerous software programs that run on it, and the datasets stored and processed. Successfully identifying all of the users—authorized or not—on a network can also be a challenge. Moreover, figuring out how to eliminate all concepts of trust at every level on a large network and get-

15. See, e.g., John Kindervag et al., "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, Sept. 17, 2010. https://www.ndm.net/firewall/pdf/palo_alto/Forrester-No-More-Chewy-Centers.pdf; John Kindervag et al., "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, Nov. 5, 2010. http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf, and Introducing.

16. John Kindervag, "Video: Zero Trust Network Architecture," Palo Alto Networks, July 30, 2012. https://www.paloaltonetworks.com/resources/videos/zero-trust.

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid.

21. "No More Chewy Centers," pp. 3-4. https://www.ndm.net/firewall/pdf/palo_alto/Forrester-No-More-Chewy-Centers.pdf.

ting everyone involved in running the network to fully and continuously buy-in to such a model will never be easy. It is also not practical to redesign entire networks overnight, so it is probably more realistic to think about evolving a local area network toward a Zero Trust model over time—or, in essence, to start with one part of the network, employ Zero Trust in that segment and then work outward from there.

Currently, Zero Trust concepts are most frequently employed in limited and defined networks that are owned and operated by, for example, a corporation, university or other distinct entity. Yet, despite their designation as 'limited,' such networks are often very large, have multiple remote data centers and users, and increasingly rely on access to a variety of cloud services for processing and storing data. The Defense Innovation Board (DIB), for example, has described numerous potential benefits of the Zero Trust model for DoD internal networks, including the ability to better track and block external attackers, minimize internal human error, improve management of data access rules to facilitate secure sharing throughout the network, and faster adoption and implementation of critical network technologies, such as machine learning and cloud computing.[22]

With respect to the broader application of Zero Trust to external 5G networks, in April 2019, the DIB issued a report on the challenges and opportunities that DoD faces.[23] Given that the U.S. military must operate around the world, and that the vast majority of systems it relies on may depend on 5G infrastructure made in foreign countries, the report acknowledged that this "would pose a serious threat to the security of DoD operations and networks" and that "the growth in the number of connected devices increases the potential 'attack surface' for adversaries to target."[24] This problem is exacerbated by the fact that the "larger volume of data being transferred will make it more difficult to detect malicious traffic on a network."[25] Accordingly, to assume malicious traffic as a given is a unique benefit of the Zero Trust model, even on this larger scale.

Indeed, because of the inherent need for the DoD to communicate effectively, efficiently and securely at all times—and often on third-party networks that are not secure—in order to conduct complex, dangerous and time-sensitive operations, the DIB report recommended that the DoD must adopt a Zero Trust model and that: "Information access should no longer be granted simply through attachment to a specific network, and instead should be granted through various security checks within the network."[26]

Of course, system administrators in theory have complete control over the design and operation of their networks. As a result, they can implement a Zero Trust model if they choose. But no single government, organization or other entity has complete control over how the global internet is designed and implemented, or what equipment and software is used throughout the network. To be sure, there are international standards-setting organizations that exert significant influence over how global networks function. But the level of control they have is highly dissimilar to that possessed by a systems administrator in charge of a local area network. Accordingly, governments, organizations and individuals have to figure out how to engage securely with a network they do not control and should not trust (i.e., the internet). And, currently, one of the best ways to engage successfully with external Zero Trust networks is to make widespread use of strong encryption.

Enhanced Use of Encryption

The internet carries a wide variety of data, including information pertaining to financial transactions and other corporate operations, airline and other travel information, civilian and military governmental communications, and personal communications (such as emails and instant messages) to and from journalists, dissidents, human rights advocates and other individuals. All internet users have a strong interest in ensuring the confidentiality, integrity and availability of the data they transmit or receive, and all of that data faces a range of information security risks. Those risks have increased in certain ways because of the dramatic shift toward cloud-based services for processing and storing data, even though the use of cloud services potentially provides huge cybersecurity benefits overall. As a result, there is risk that sensitive organizational data could be compromised: as it is transmitted to or from the cloud; while it is processed or stored in the cloud; or as it is transmitted between various data centers owned by the cloud service provider. And, once again, all of these risks could grow with the transition to 5G.

One potential way to deal with all of this information security risk is to ensure that every packet is encrypted at all times, and that data is unencrypted only when absolutely necessary.[27] Indeed, strong encryption can protect both the contents of a communication and at least some of the metadata

22. Kurt DelBene et al., "The Road to Zero Trust (Security)," U.S. Dept. of Defense, Defense Innovation Board, July 9, 2019. https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

23. Milo Medin and Gilman Louie, "The 5G Ecosystem: Risks and Opportunities for DoD," U.S. Dept. of Defense, Defense Innovation Board, April 3, 2019, p. 21. https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

24. Ibid.

25. Ibid.

26. Ibid., p. 29.

27. Evan Gilman and Doug Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., 2017), p. 16.

associated with it.[28] As policymakers plan for the future, it is important to note that quantum computing technology in the next 10-20 years could enable an adversary to decrypt some encryption systems that are currently in use and considered safe.[29] For this reason, it is especially vital that all encrypted communications transmitted via risky equipment and software are quantum resistant.[30] Accordingly, as part of applying a Zero Trust model to the DoD's internal networks, it should also plan to move to quantum-resistant key exchange mechanisms.[31]

To be sure, even though quantum resistant encryption systems will help mitigate significantly the risk to the confidentiality and integrity of data on Zero Trust networks, the information security benefits of such systems appear to be less with respect to protecting the availability of data. Strong encryption (especially of metadata) will make it harder for a hostile actor to effectively degrade or disrupt targeted communications, but other means are necessary to better ensure the availability of data (such as utilizing multiple network service providers that rely on different infrastructure).

In April 2020, one element of the DoD followed the DIB's recommendations when the United States Air Force selected Wickr, Inc. to provide it with secure, end-to-end encrypted messaging services to operate on ZTNs globally, while also providing a mechanism to ensure compliance with all DoD security and record retention requirements.[32] According to Wickr, it designs its products:

> on the assumption that nothing can be trusted along the communication path between a message sender and a message receiver—not the network, not the systems used to store and route the messages, and not the people managing the systems.[33]

For this reason, its platforms employ "[m]ilitary grade end-to-end encryption" and run "the only triple encrypted zero trust [Software as a Service] platform on the planet."[34] The company has also written specifically about the ZTN concept and the importance of maintaining the security of communications sent over global networks:

> Zero Trust systems are built to provide trusted service in an untrusted world. Instead of engaging in the increasingly difficult task of fixing or avoiding untrusted services altogether, we can find safe ways to use them despite their shortcomings.[35]

According to Wickr, because of its product, Air Force personnel will be able, "to securely communicate anywhere in the world, without the risk of being breached or hacked."[36] It also notes that its product is:

> highly scalable [...] with full administrative and compliance controls enabled to meet [...] DOD security requirements while providing an easy to use solution for zero trust, encrypted messaging, audio and video calling with screen share, large file transfers, and secure storage.[37]

All of this suggests that the Air Force may use Wickr's encryption system for both unclassified and classified communications. The Air Force's use of such technology to protect the security of critical operational communications makes perfect sense for military planners who have rightly adopted a Zero Trust mindset.

VIEWING THE INTERNET ITSELF AS ZERO TRUST

In addition to its defense uses, it is also advisable to use such technology to protect vital private- sector communications and data. In fact, everyone—companies in the food supply chain, hospitals, journalists, civil society groups and even individuals—need to adopt military-grade encryption precisely because foreign military and intelligence

28. With respect to encrypting certain metadata, see, e.g., Selena Deckelmann, "Firefox continues push to bring DNS over HTTPS by default for US users," The Mozilla Blog, Feb. 25, 2020. https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users.

29. Medin and Louie, p. 29. https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

30. "Statement of Director of National Intelligence Daniel R. Coats, Senate Select Committee on Intelligence," Worldwide Threat Assessment, Jan. 29, 2019, p. 16. https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; "Implications of Quantum Computing for Encryption Policy," Carnegie Endowment for International Peace and Princeton University Working Group on Encryption, April 25, 2019. https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985.

31. Medin and Louie, p. 29. https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

32. Wickr, "Wickr Selected as Only Secure Communication Platform for Strategic Expansion Initiative with U.S. Air Force," Press Release, Apr. 9, 2020. https://wickr.com/secure-communication-platform-for-air-force.

33. "Toward a Zero-Trust Future," Wickr, 2019, p. 3. https://wickr.com/resources/toward-a-zero-trust-future.

34. "Why Wickr," Wickr, 2020. https://wickr.com/why-wickr. It should be noted that United States Attorney General William Barr has criticized the commercial use of "military-grade encryption" by the public. See, e.g., Roll Call, "Barr's call for law enforcement access to commercial encryption," YouTube, Jan. 31, 2020. https://www.youtube.com/watch?v=Y5wZF4V3qc4.

35. "Toward a Zero Trust Future," p. 4. https://wickr.com/resources/toward-a-zero-trust-future.

36. "Wickr Selected as Only Secure Communication Platform for Strategic Expansion Initiative with U.S. Air Force." https://wickr.com/secure-communication-platform-for-air-force.

37. Ibid.

organizations pose real and immediate threats to society as a whole.[38]

In light of this, arguably the most important part of an effective 5G information security risk management strategy for the future is a complete shift in thinking. To be sure, network operators and service providers know they must protect data while it is in transit on the internet, as there are many malicious cyber actors in the world. Indeed, people have known for years that the internet is a dangerous place, which is why, for example, encryption is widely used today to carry a variety of sensitive and important network traffic, such as data pertaining to financial transactions and communications such as Gmail. However, generally speaking, most people do not think of the infrastructure of the internet itself—including all the wireless transmission systems and domestic and international cable networks that comprise it—as a potential threat vector.

On this account, threat actors that are connected to the internet differ significantly from threat actors that find ways to become part of the internet itself. Of course, for many years people have known that governments have conducted electronic surveillance at various points in the global network. Likewise, most people understand that there are enhanced cybersecurity risks in taking smartphones and other electronic devices to places run by authoritarian regimes. However, the potential presence of untrustworthy or compromised equipment in global 5G networks themselves makes those networks risky in unfamiliar ways. And since people will never know exactly where untrustworthy or compromised equipment is present or exactly how their communications will be routed to or from the intended destination, everyone should assume that their communications and data—especially data that is transmitted outside the United States—could be exposed to bad actors at some point. Unfortunately, this means that the new best practice is to treat the internet itself as Zero Trust and rely heavily on strong encryption for all data transmitted, processed or stored anywhere on it.

Indeed, as John Kindervag summarized, "Zero Trust is not a project but a new way of thinking about information security."[39] And, part of that new way of thinking is that public and private sector leaders and policymakers must view the widespread use of robust, "military-grade encryption" as central to protecting data in a Zero Trust world.[40]

CONCLUSION

The Zero Trust model—including the widespread use of robust encryption—provides a highly useful way for public- and private-sector leaders and policymakers to more effectively address some of the cybersecurity risks associated with the presence of vulnerable equipment in global 5G networks. Society is highly dependent on the digital ecosystem and thus we must endeavor to ensure the confidentiality, integrity and availability of the data stored, processed and transmitted. A Zero Trust approach is the more effective strategy. Fortunately, it appears that— at a minimum—elements of the United States Department of Defense understand both the threat and some of the ways to mitigate it. Hopefully, other elements of the government and the private sector will follow their lead.

ABOUT THE AUTHORS

Jim Baker is the former Director of National Security and Cybersecurity at the R Street Institute and a lecturer at Harvard Law School. He is also the former General Counsel of the Federal Bureau of Investigation. The views expressed are his own and do not necessarily reflect those of any of his current or former employers.

Kathryn Waldron is a fellow with the National Security and Cyber Security team at the R Street Institute.

38. FBI, "NSA and FBI Expose Russian Previously Undisclosed Malware Drovorub in Cybersecurity Advisory," Press Release, Aug. 13, 2020. https://www.fbi.gov/news/pressrel/press-releases/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecurity-advisory.

39. "No More Chewy Centers," p. 10. https://www.ndm.net/firewall/pdf/palo_alto/Forrester-No-More-Chewy-Centers.pdf.

40. Jim Baker, "Rethinking Encryption," Lawfare, Oct. 22, 2019. https://www.lawfareblog.com/rethinking-encryption.