

An Overview of 5G and Potential Vulnerabilities

A Primer

TLP: **CLEAR**

B-2023-05-22a

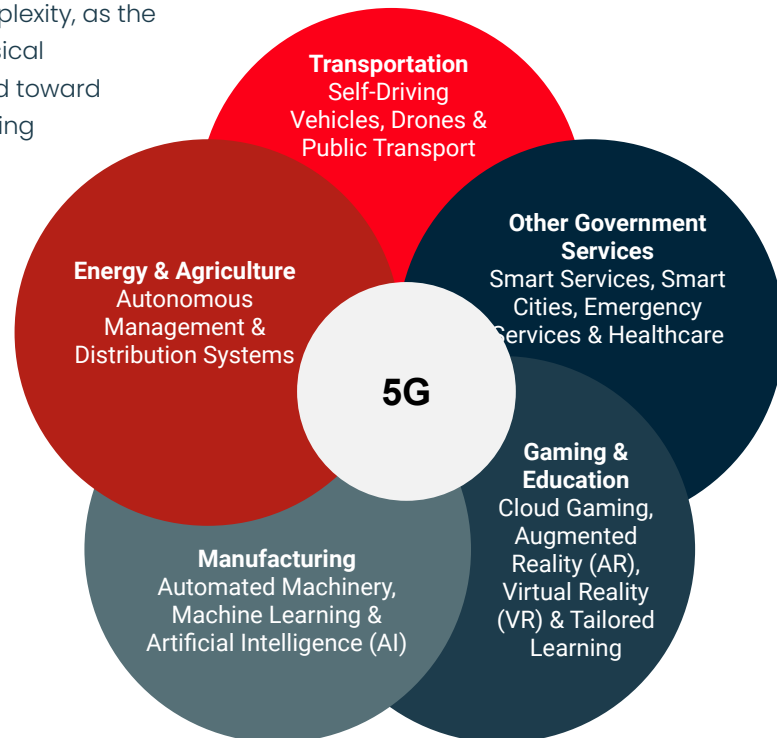


Key Takeaways

- 5G offers significant upgrades in speed, bandwidth, energy efficiency, and reliability when compared to preceding wireless technology. These improvements are predicted to benefit mobile users, organizations, and industries.
- The improved specifications of 5G enable the introduction of new networking features, such as network slicing, edge computing, and real-time processing. These are designed to enhance network efficiency, utility, reliability, and security.
- Since its 2018 launch, 5G implementation has been largely restricted to North America, East Asia, and Western Europe. Factors hindering global proliferation include cost, supply chain challenges, the absence of a potential user base in some areas, and a lack of digital infrastructure readiness.

An Introduction to 5G

5G refers to the standard of fifth-generation wireless network technology currently in varying stages of rollout across the globe. The technology will eventually serve as a successor to 4G Long-Term Evolution (LTE) technology, which has dominated mobile wireless communications since its first commercial deployment in 2009. Compared to 4G LTE, 5G is designed to offer users significantly improved speed, with maximum data download speeds of 10 Gbps—which is around 100 times faster than 4G LTE on capable devices within range of the necessary infrastructure.[1] The benefits of 5G are far more extensive than faster internet speeds; the technology is regularly described as revolutionary rather than an upgrade. The increased bandwidth and reliability, along with improved energy efficiency and lower latency, permit the adoption of applications requiring real-time or near-instant data transfer. An array of different industries are anticipating the benefits this can offer, which are underpinned by autonomous technology and smart systems. Despite proliferating faster than any preceding mobile networks, the implementation and commercial availability of 5G has been subject to criticism across North America, Western Europe, and Asia. For example, 5G was reported to have been available to 40 percent of the population in the United Kingdom two years after launch; the average across the European Union at the same time was just 10 percent. By contrast, 4G LTE was available to 80 percent of people after its launch[2]. This is very likely indicative of the network's complexity, as the higher frequencies used by 5G necessitate significantly more physical infrastructure than that of 4G LTE. The rollout is also primarily aimed toward urbanized, technologically-advanced societies with accommodating infrastructure that host organizations capable of benefiting from 5G adoption. Societies lacking digital-readiness and a sufficient range of end-users will be unable to take advantage of the full array of benefits offered by 5G networks, and thus are highly unlikely to offer an attractive investment opportunity to vendors. These areas likely remain content with other mobile networks and are not driving global 5G demand. The COVID-19 pandemic, concerns over public health risks, geopolitical disputes, and the ongoing global semiconductor shortage affecting supply chains have very likely exacerbated delays to rollouts.[3] However, despite a seemingly slow and geographically uneven rollout, the overall uptake of 5G is growing exponentially as of May 2023. Reporting approximates that there were one billion 5G subscriptions across the globe at the end of 2022, which is forecasted to rise as high as five billion by 2026.[4,5]



FOOTNOTES

- [1] [hXXps://www.qualcomm.com/5g/what-is-5g](https://www.qualcomm.com/5g/what-is-5g)
- [2] [hXXps://www.lightreading.com/5g/how-5g-rollout-became-such-long-hard-slog/d/d-id/771979](https://www.lightreading.com/5g/how-5g-rollout-became-such-long-hard-slog/d/d-id/771979)
- [3] [hXXps://www.vanillaplus.com/2022/09/18/72698-3-reasons-why-europes-5g-roll-out-is-lagging/](https://www.vanillaplus.com/2022/09/18/72698-3-reasons-why-europes-5g-roll-out-is-lagging/)
- [4] [hXXps://www.thalesgroup.com/en/worldwide/digital-identity-and-security/magazine/5g-progress-report-launches-subscribers-devices](https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/magazine/5g-progress-report-launches-subscribers-devices)
- [5] [hXXps://www.computerweekly.com/news/252524590/Global-5G-subscriptions-growth-stays-strong-in-Q2-2022](https://www.computerweekly.com/news/252524590/Global-5G-subscriptions-growth-stays-strong-in-Q2-2022)



An Overview of 5G and Potential Vulnerabilities

A Primer

TLP: CLEAR

B-2023-05-22a

Key 5G Cyber Vulnerabilities



Growing Digital Attack Surface



Widespread Implementation, Reliance, and Criticality



Network Slicing Misconfiguration



Legacy Infrastructure and Inherited Vulnerabilities



Edge Computing Misconfiguration



Supply Chain Vulnerabilities



Political Influence, Policy, and Standardization

5G Security Overview

5G infrastructure and networks are embedded with enhanced security measures when compared to 4G LTE, improving on existing features such as stronger encryption and multi-factor authentication and implementing new features integrated within the security architecture. These include secure boot, configurable Non-Public Networks (NPN), Network Slice Specific Authentication and Authorization (NSSAA), and Trusted Execution Environment.[6] Reporting suggests that cyberattacks against 5G networks are taking place, with ransomware and social engineering noted as the most common methods.[7] However, there is a roughly even chance that many of these are the result of known vulnerabilities from legacy architecture, as ambitions of widespread 5G Stand Alone (5GSA) have not yet materialized.[8] Disclosures of 5G-specific attacks are expected to increase with the widespread rollout of 5GSA network architecture, reducing the likelihood that reports focus on 4G LTE aspects of 5GSA infrastructure. As 5G is early in its life cycle, sufficiently high-payoff opportunities to target these networks specifically likely remain unavailable to most threat actors. Furthermore, threat actors' ability to successfully target existing 4G LTE networks very likely provides little incentive to change tactics, techniques, and procedures (TTPs) or develop new methodologies necessary to exploit vulnerabilities in 5G networks. As 5G becomes more widespread, it is almost certain to increasingly attract the attention of nefarious actors such as cybercriminals and hackers seeking to exploit networks for financially or politically-motivated gain. However, as 5G becomes increasingly embedded into critical organizations' networks, services, and infrastructure, other highly-capable nation state and state-affiliated entities will very likely pose an increased threat.

This report will expand on some of the primary cybersecurity vulnerabilities of 5G by examining what the key terms mean, the threat vectors by which they may be exploited, and what a successful attack may accomplish. Due to insufficient example case studies, this analysis of the cyber threats to 5G is currently primarily based upon the vulnerabilities likely to exist within the technology, alongside established knowledge of how, when, where, why, and by whom telecommunication systems are currently targeted. This list of potential threat vectors is non-exhaustive, as the rapid proliferation of 5G networks will very likely lead to the uncovering of new vulnerabilities, particularly as the TTPs of malicious groups evolve and mature. Physical security—including the threat from sabotage—lies outside the scope of this report; however, this should be noted by 5G telecom hardware users as a significant threat vector, as 5G is forecasted to deploy up to 10 times as much network infrastructure as 4G LTE, with much of it in remote and hostile environments.

Key Takeaway: Despite a lack of high-profile attacks targeting 5G infrastructure, rapid proliferation over the next few years is almost certain to drastically change the cyber threat landscape.

What is Zero-Trust Architecture (ZTA)?

ZTA is a set of cybersecurity paradigms often associated with 5G networking. They emphasise the movement of defenses from static and perimeter-based to the end-user and related assets. This is under the presumption that there should be no implicit trust for users based solely upon the physical location of their devices.

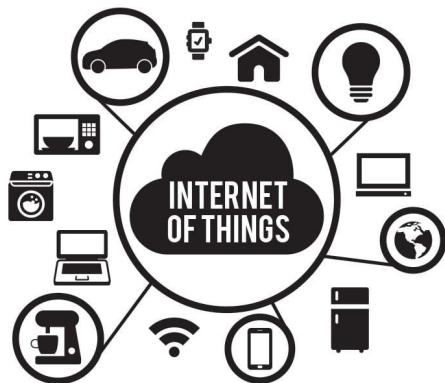
FOOTNOTES

- [6] [https://www.5gamericas\[.\]org/wp-content/uploads/2021/12/Security-in-5G.pdf](https://www.5gamericas[.]org/wp-content/uploads/2021/12/Security-in-5G.pdf)
[7] [https://www.cybersecuritydive\[.\]com/news/5g-security-breaches/636693/](https://www.cybersecuritydive[.]com/news/5g-security-breaches/636693/)
[8] [https://www.cybersecuritydive\[.\]com/news/5g-network-security-CISA/626808/](https://www.cybersecuritydive[.]com/news/5g-network-security-CISA/626808/)



Growing Digital Attack Surface

Assuming current projections for widespread 5G proliferation are accurate, the network will be comprised of several billion end-point devices that are exposed to the internet by the end of the decade—and many more times that in applications, websites, codes, and other digital entry points. This network of a multitude of interconnected smart devices is referred to as the Internet of Things (IoT), and, while not a new concept, the proliferation of 5G is expected to enable the IoT's rapid growth.



Source: TheNewStack

What is the Internet of Things (IoT)?

- The IoT refers to a collection of physical devices capable of network connectivity or that are otherwise able to collect and exchange data from an application. To achieve this, a connected device would only need to be individually addressable, as well as possess a processing capability.
- These so called “smart devices” can include anything from a mobile phone, traditional computer, or smart home appliance to sensors enabling industrial-scale machinery to process live data. This will increase output reliability, accuracy, and application while furnishing organizations with data that can provide invaluable insight and improve overall efficiency.

Despite offering many benefits to users, the IoT brings its own security challenges. One such challenge is the increased attack surface and the subsequent threat vectors that may be exploited by malicious actors. Inherently more complex to protect, a large attack surface mandates a holistic and comprehensive approach to threat analysis and mitigation. Despite 5G offering additional organic protection measures over its predecessor networks, the exponential increase of devices capable of smart connection is very likely, over the short mid-term, to drive the growth of the 5G network and the IoT, resulting in a constantly evolving threat landscape.

Exacerbating this issue is the likelihood that the majority of smart devices will, at least initially, lack the security measures needed to safeguard the network. Vulnerabilities such as weak default login credentials, slow manufacture software updates, insecure data transfer capabilities, and cloud misconfiguration threaten to increasingly present IoT networks as an appealing target to threat actors.[9] Furthermore, organizations in the early stages of 5G adoption may often not approach these issues diligently. Whether due to avoidance of operational disruption, a lack of awareness, or simply a scarcity of the resources required to systematically manage smart devices, organizational cybersecurity risks becoming outdated.

The IoT has been introducing new vulnerabilities to the cyber threat landscape since the term was first coined in the early 2000s. Attacks have since been observed against security cameras, domestic heating equipment, and vehicles.[10,11,12] The proliferation of 5G is very likely to advance its growth exponentially, as organizations and individuals seek to improve the efficiency and productivity of their enterprises. With the proliferation of the IoT and ever-growing digital attack surfaces, legislation mandates stronger minimum security protocol in capable devices.[13] However, new legislation is likely to lag behind the fast uptake of smart devices and will face challenges in cross-industry standardization, as well as in ensuring compliance in a reasonable timeframe. Threat actors will be able to exploit vulnerabilities in these devices by using them as a means to move laterally across the wider network. Malicious payloads may then be delivered, such as ransomware or infostealers. If successfully leveraged against an organization heavily reliant upon local networks, these types of attacks may cause significant financial or reputational damage. There is also a risk of Distributed Denial-of-Service (DDoS) attacks, which can have even greater impact in terms of organizational disruption and down-time. The cross-industry nature of these networks will guarantee their appeal to a large variety of threat actors with varying capabilities and risk appetites, such as hacktivists seeking to disrupt engineering projects, cybercriminals seeking to extract private data from electronic devices, or state-level capabilities seeking to disrupt the agricultural or industrial output of an adversarial state. Upon the widespread adoption of 5G networks, the cyber threat landscape will be even faster-changing and diverse in its threat actors, targets, and TTPs, creating a long-term challenge for security personnel.

Key Takeaway: The IoT can greatly improve the efficiency of organizations—but at the expense of a greatly increased attack surface offering additional vectors for threat actors to exploit.

FOOTNOTES

[9] [https://quantumpc\[.\]com/misconfiguration-cloud-security/](https://quantumpc[.]com/misconfiguration-cloud-security/)

[10] [https://www.verkad\[.\]com/uk/security-update/report/](https://www.verkad[.]com/uk/security-update/report/)

[11] [https://www.cm-alliance\[.\]com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities](https://www.cm-alliance[.]com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities)

[12] [https://www.bleepingcomputer\[.\]com/news/security/new-stuxnet-variant-allegedly-struck-iran/](https://www.bleepingcomputer[.]com/news/security/new-stuxnet-variant-allegedly-struck-iran/)

[13] [https://digital-strategy.ec.europa\[.\]eu/en/library/cyber-resilience-act](https://digital-strategy.ec.europa[.]eu/en/library/cyber-resilience-act)



An Overview of 5G and Potential Vulnerabilities

A Primer

TLP: CLEAR

B-2023-05-22a

Widespread Implementation, Reliance & Criticality

The advantages of 5G adoption are almost certain to be appealing to organizations wishing to improve their efficiency. The prospect of interconnecting smart devices, low latency, and improved security is very likely to drive proliferation over the next decade across industries such as education, transport, emergency services, manufacturing, and publicly-funded sectors.[14] While these benefits may transform organizational productivity, this is not without risk; the adoption of 5G will likely introduce additional end-point devices from which a threat actor can move laterally toward the compromise of business-critical IT assets. Vulnerable devices can include printers, vending machines, and other devices that would not traditionally possess the security protocol needed to safeguard their networks. In the early years of widespread 5G adoption, it is very unlikely that original equipment manufacturers (OEMs) will equip such devices with sufficient security measures, and many devices will not be capable of receiving remote software updates. Some organizations are well-versed in the threats posed by cybercriminals and have robust IT resilience and continuity plans in place. However, during a period of mass 5G proliferation, it is very likely that organizations will find these plans outdated, their IT departments unequipped and unprepared, and their understanding of the cyber threat landscape redundant. This introduces a further risk of widespread, hasty investments being made in inefficient security measures that are not enterprise-grade and only further increase vulnerabilities.

Urban areas with a multitude of services connected by a high-speed network such as 5G are often referred to as smart cities. While not yet a truly realized concept, smart cities will connect not only the data necessary for the running of public services but also that of private citizens.[15] A network of this size will almost certainly be an attractive target to financially-motivated threat actors. This extent of interconnectivity at the state level will also offer high-risk, high-reward opportunities to politically-motivated threat actors of increased capabilities—such as nation state-affiliated groups capable of launching catastrophic attacks like device hijacking, DDoS, or Permanent Denial-of-Service (PDoS) with the aim of ceasing government function.

Ideologically-motivated threats actors such as cyber terrorists and sophisticated hackers may have similar aims, though likely have less capability. Security of 5G networks will almost certainly become not just a matter of personal communications security but also a matter of national infrastructure security, leading to them being an attractive targets to cyber terrorism and state-backed cyberattacks.

Key Takeaway: 5G's broad utility encourages its growth. This will increase the reliance placed upon its function and the criticality of its compromise, heightening its allure to threat actors.

What is Network Slicing?

- Network Slicing is a key architectural feature of 5G, underpinned by Software Defining Network (SDN) and Network Function Virtualization (NFV). The technology enables the splitting of a physical network into multiple end-to-end, virtualized, and isolated networks known as slices.
- Network operators will be able to define the requirements of each slice. These may include Extreme Mobile Broadband (eMBB) for large bandwidth applications, Massive Machine-Type Communications (mMTC) for a high number of low-traffic devices, or Ultra-reliable Low-Latency Communications (urLLC) for edge-computing capabilities.

Network Slicing Misconfiguration

5G Network Slicing improves both the capacity of a network and its security through segregation. Each network slice is isolated from the rest via unique security protocols and will only allow access from authorized devices. If correctly configured, the compromise of one slice should not grant unauthorized access to the others, stopping further compromise. The correct configuration is a critical and ongoing caveat to this, however, as network slicing drastically increases the complexity of a network. Attacks leveraging misconfiguration could have wide-ranging implications if threat actors are able to bypass system monitors or security features. Denial of Service (DoS) attacks may be used to target vulnerable network slices, allowing threat actors to disrupt the service after gaining access. Furthermore, Man-in-the-Middle (MitM) attacks targeting networks with insufficient encryption could enable threat actors to tamper with sensitive information or steal it for ransom. Attacks such as these have the potential to grant access to associated, misconfigured network slices. In this case, it is possible that a complex attack leveraging multiple of these TTPs could occur.

Many organizations using private networks already find their security a significant challenge, and the introduction of 5G and SDN features will only exacerbate this. A report from 2018 suggests that one third of successful attacks of a 4G LTE network were reported to be at least partly due to incorrect configuration.[16] Legislation guiding the standards to be adopted in the building of private 5G networks will be referred to for decreasing the risk of vulnerabilities and incorrect configuration. However, no such guidance exists for the proper implementation of network slicing—or the security protocols that should be adopted by both vendors and end-users.[17]

Key Takeaway: Despite being a security feature, network slicing expands both the digital and physical attack surface of a network, increasing the need for ongoing security scrutiny.

FOOTNOTES

[14] <https://www.solutions30.co.uk/connectivity-hub/which-sectors-will-benefit-the-most-from-the-realisation-of-5g/>

[15] <https://www.idb.org/what-are-the-cybersecurity-risks-for-smart-cities/>

[16] https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[17] https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5g-infrastructure_508_v2_0%20%281%29.pdf



An Overview of 5G and Potential Vulnerabilities

A Primer

TLP: CLEAR

B-2023-05-22a

Legacy Infrastructure and Inherited Vulnerabilities

5G offers significantly improved security features over 4G LTE, such as enhanced encryption, authentication management, and secure signaling. However, as of early 2023, the vast majority of active 5G networks are Non-Standalone (NSA)—meaning they are reliant at least in part upon 4G-era infrastructure. There are several ways in which this increases the vulnerability of the network, such as the inheriting of dated security protocols from legacy infrastructure. 4G LTE networks have been targeted in several high-profile DoS, malware, and interception attacks and have had their fundamental vulnerabilities exposed.[18,19,20,21]. These vulnerabilities are very likely to undermine the security of 5G networking if a common infrastructure is shared.

One such vulnerability is the reliance upon a 4G LTE EPC. While 5G Standalone (SA) implements a “secure by design” architecture, 4G LTE was not built with the same extent of security in mind and is more vulnerable to attacks such as DoS, malware, and MitM. There is also a risk posed by the huge number of legacy 4G LTE, 3G, or 2G devices connected to these networks. These older devices often lack the capacity to receive the latest security updates and have inadequate built-in features to protect against contemporary threats, presenting an attractive intrusion vector for threat actors seeking to gain access to a 5GNSA network. 5GNSA networks are also vulnerable to threat actors downgrading the capabilities of a 5G network to, for example, 4G LTE. Threat actors can not only conduct DoS or disruption attacks, they can also exploit known vulnerabilities in 4G LTE networks by circumventing 5G security measures.

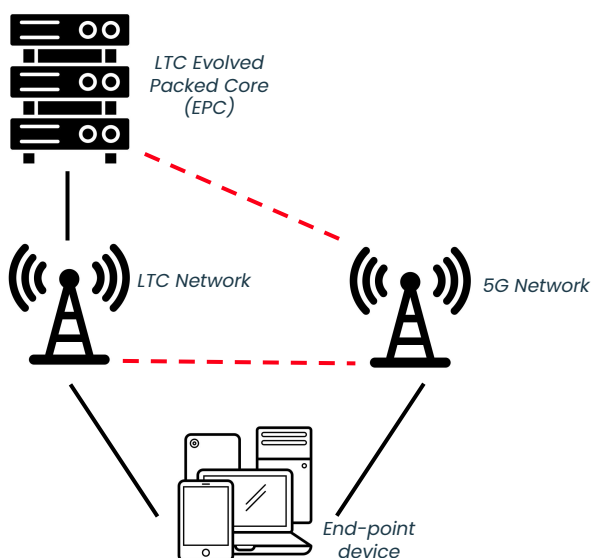
A network comprised of multiple architectures increases the points at which various generations of technology integrate, creating additional complexities and security gaps. The extent to which these vulnerabilities are present in a given 5GNSA network will almost certainly vary depending on the configuration and protocols implemented. While 5GSA will very likely mitigate many of these vulnerabilities, it will likely take a number of years before this technology is widely implemented.

Key Takeaway: Currently, the most common configuration of 5G networks have likely inherited vulnerabilities from the legacy infrastructure on which they rely. Future 5GSA is very likely to offer additional security.

What is 5G Standalone (5GSA)?

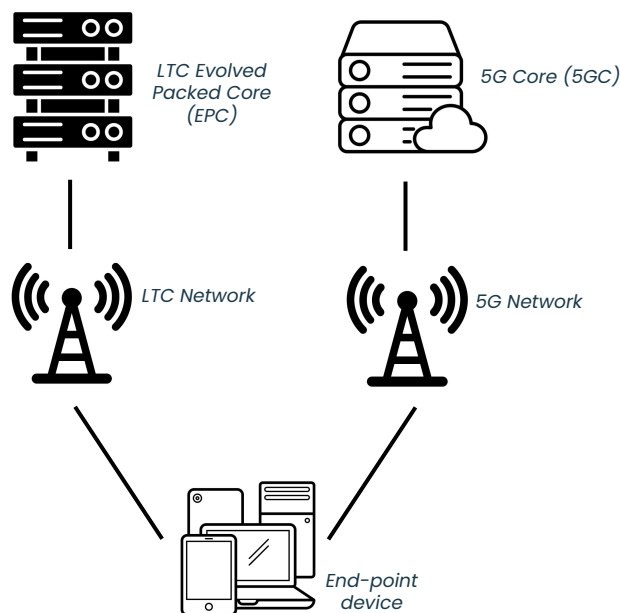
- 5G Standalone refers to a network comprised solely of 5G-era technology, including a 5G New-Radio (NR) core network. This is an advancement over 5GNSA, in which NR relies upon an LTE Evolved Packet Core (EPC) serving both 4GLTE and 5G networks.
- 5GNSA offers vendors the advantages of faster adoption and cheaper investment, while end-users receive increased data speeds and network reliability.

5G Non-Stand Alone (5GNSA)



Source: ZeroFox Intelligence

5G Stand Alone (5GSA)



FOOTNOTES

- [18] <https://www.bleepingcomputer.com/news/security/vodafone-portugal-4g-and-5g-services-down-after-cyberattack/>
[19] <https://www.bleepingcomputer.com/news/security/croatian-phone-carrier-data-breach-impacts-200-000-clients/>
[20] https://syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf
[21] <https://www.infosecurity-magazine.com/news/all-4g-networks-susceptible-to-dos/>



What is Edge Computing and Multi-Access Edge Computing?

- Edge computing is a subset of cloud computing, whereby a distributed IT architecture enables data to be processed, analyzed, and stored closer to the data source or end-user. This increases the efficiency of moving large amounts of data at low latency, while increasing reliability.
- While edge computing is a conceptual network model, multi-access edge computing (MEC) is a standard architecture specifically focused on bringing computing resources closer to the mobile edge.[22] This term is often associated with 5G networks.

Edge Computing Misconfiguration

Edge computing, and specifically MEC, are integral aspects of 5G operating at its full potential. Features such as Artificial Reality (AR), Virtual Reality (VR), the automation of vehicles and machines, cloud gaming, and the broader IoT will rely on the low latency and increased reliability of MEC. It also brings security benefits, such as reduced data exposure, a distributed security architecture, and improved network resiliency. The concept is not risk-free, however, as managing security at the edge is more complex.[23] The proliferation of endpoint devices not only increases digital attack surface but also risks introducing devices with insufficient security protection. In the case of edge computing, this includes other edge infrastructure, such as servers, gateways, and other network components—all of which will need additional management to defend against unauthorized remote access and physical tampering. The movement away from the use of large data centers such as those offered by Google and Microsoft will inevitably result in the proliferation of smaller, widely-distributed facilities that will be managed more locally. There is a roughly even chance that, although this can increase resiliency overall, additional vulnerabilities will be presented should facility owners not have the capabilities to ensure ongoing configuration and maintenance. These vulnerabilities would be particularly significant in locally-processed sensitive data, such as in healthcare, defense, or various commercially-sensitive outfits.

The reliance of MEC on vast numbers of interconnected edge nodes also presents potential vulnerabilities. If not properly secured by the appropriate network segmentation measures, such as Virtual Local Area Networks (VLANs) and Software-Define Networking (SDNs), vulnerabilities can be leveraged by threat actors seeking to steal sensitive data or carry out DoS attacks. If organizations are to protect their 5G capabilities, correct configuration and maintenance of on-site or local data facilities will be an imperative and fundamental aspect of business resilience.

Key Takeaway: Edge computing grows a network's attack surface by the introduction of additional servers, gateways, and edge nodes. This will increase not only resiliency but also the complexity and importance of network configuration.

Supply Chain Vulnerabilities

5G supply chains will almost certainly become increasingly complex, relying on a multitude of third parties, which will increase the risk to operators and end users. 5G vendors will very likely face greater challenges in ensuring the accountability, integrity, and safety of the components used in their networks due to the larger attack surface and likelihood they will be subject to malicious intent.

The potential introduction of malicious hardware or software poses a significant risk. If undetected, these could be leveraged to deploy malicious payloads and conduct espionage, data theft, or DoS attacks. Compromising a single weak point could impact thousands of downstream customers. Supply chain attacks on network providers could be catastrophic—particularly given the criticality of the networks—and have severe reputational and financial consequences for vendors.[24] Counterfeit components may be installed (intentionally or unintentionally) to cut costs, obtain a competitive advantage, or disrupt services. This becomes increasingly likely with network vendors turning to smaller, less reputable suppliers to meet consumer demands, as well as using manufacturers in locations where legislative standards and checks are less stringent.

5G network supply chains vulnerable to data interception or redirection will very likely become attractive targets for threat actors, given that 5G is expected to play a key role in the SDN functionality of critical infrastructure and services in developed nations. Due to the importance of maintaining the integrity of information and access, network providers may face increased pressure from governments to avoid using vendors based in territories that may be more conducive to state intervention. Such attacks would likely be conducted by highly-capable threat actors leveraging stealthy methodologies. Mitigating these threats during design and rollout phases, as well as leveraging a ZTA approach, will help facilitate a “ground-up” and holistic approach to security that goes some way towards mitigating the potential threat.

Key Takeaway: 5G's supply chain will be exposed to an increasing number of parties as the network proliferates. This increases the likelihood of it being subject to threat actors with malicious agendas.

Key Standardization Bodies

- Third Generation Partnership Project (3GPP) is an umbrella term for a group of widespread organizations responsible for the global standardization of 5G and its predecessors, such as 4G LTE and 3G.
- The performance requirements of 5G are outlined by the ITU Radiocommunications Sector (ITU-R) within the International Mobile Communications (2020) (IMT-2020), which outlines mandated baselines for network speed, latency, and density.
- The Internet Engineering Task Force (IETF) partners with 3GPP in the development of new technologies such as network virtualization and key specifications surrounding IP protocols.

FOOTNOTES

[22] <https://www.etsi.org/technologies/multi-access-edge-computing>

[23] https://www.eyl.com/en_g/telecommunications/how-the-upside-risks-of-5g-balance-the-downside-security-risks

[24] <https://www.fortiguard.com/outbreak-alert/solarwinds>



Current Key Players in 5G Rollout

- Samsung has been regarded as one of the industry leaders in 5G since 2011. Together with Verizon, Samsung brought 5G to commercial America in 2018.
- Huawei enjoyed 4G success thanks to a diverse portfolio and offering end-to-end cellular networks; it has been a leader in 5G technology despite political tensions.
- AT&T claimed to be the first to deliver 5G to the United States and remains heavily involved in its proliferation.
- Other key players include Ericsson, Nokia, Intel, and Cisco.

Political Influence, Policy & Standardization

Since its inception, 5G has found itself repeatedly at the forefront of geopolitical competition. There are several reasons for this, such as states seeking a technological advantage over adversaries and the profitable opportunities in exporting vast amounts of 5G components to meet the growing international demand. There has been significant and ongoing concern expressed over the possibility of state-affiliated manufacturers using this demand as a means for intelligence collection and data theft. These risks are intrinsically linked to the cyber threats in 5G networks—particularly as 5G is very likely to become a dominant tool used in critical national industries and the infrastructure of the developed world. This results in a large part of a nation's cybersecurity integrity being reliant, in part, on favorable state relations—something which is difficult to predict and results in expense and disruption should alternative suppliers be needed. Aspects of this have already manifested across the developing world as a small number of tech giants seek to establish 5G dominance overseas, decreasing vendor diversity and increasing reliance—and ultimately increasing vulnerability.[25] Furthermore, vendors will very likely continue to be scrutinized by state and private entities to the extent that international sanctions are imposed, risking broader technological trade barriers and decreasing vendor diversity in associated supply chains. Standardization of 5G is also an ongoing issue, as stakeholders seek to deploy a network capable of global interoperability and compatibility. Stakeholders overseeing this are diverse in geographic location, expertise, goals, and affiliations. While this has many positives (primarily, the addressing of diverse customer requirements), it also poses risks such as lack of strategic oversight and varying priorities amongst stakeholders. A lack of comprehensive standardization, regulations, and strategy is very likely to result in issues within spectrum allocation, roaming, network integration, and service compatibility—all of which may present vulnerabilities exploitable by various threat actors. This will be an ongoing challenge in order to ensure the common interests of 5G consumers are safeguarded against the evolving threat landscape.

The Future of 5G Cyber Security

Over the next two to three years, it is almost certain 5G proliferation will increase exponentially in countries with established networks and consumers. It is likely that, in this time, threat actors of all capabilities will conduct reconnaissance in search of vulnerabilities that can be exploited for financial, political, or competitive gain. High-impact attacks are unlikely, however, largely due to a lack of high-payoff opportunities. Any successful attacks would very likely be against 5G NSA networks leveraging known vulnerabilities in 4G LTE infrastructure. Over the next three to six years, it is very likely that 5G networks will be widespread across Western Europe, East Asia, North America, and, increasingly, the developing world. Driven by features such as Fixed Wireless Access (FWA), SA, IoT, and the high-performing mmWave spectrum, 5G will likely have begun to transform an array of industries, replacing technologies such as 4G LTE and wired broadband.[26] It is likely that fundamental flaws in 5G will be exposed and exploited by threat actors in high-profile attacks, likely against private sector industries such as manufacturing, retail, and energy, which, among others, stand to benefit the most from swift adoption. By 2035, it is almost certain that the majority of new 5G connections will stem from the enterprise market rather than mobile consumers.[27] Organizations in many industries will be operating at increased efficiency but also with an increased reliance on SDN network technologies. Successful attacks are likely to occur regularly, in part due to the array of opportunities presented by such widespread adoption. As the cyber threat landscape evolves, security practices and end-user understanding will be required to develop with it. From basic cyber hygiene to advanced mitigation methods, goalposts will continue to shift, and the bar for effective security will inevitably rise. This will be required at the personal, commercial, and state level to enable modern network technologies to safely provide their transformational benefits without exposing users to malicious threat actors.



Source:

https://www.researchgate.net/figure/The-5G-future-diagram-3_fig1_341649564

Key Takeaway: A lack of vendor diversity will continue to provide opportunities for state-affiliated vendors to monopolize the market in countries seeking to implement 5G, leading to opportunities for political leveraging and influence exertion.

FOOTNOTES

[25] [https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public\(1\).pdf](https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf)

[26] <https://www.5gamerica.com/understanding-millimeter-wave-spectrum-for-5g-networks/>

[27] <https://www.mwcbarcelona.com/press-releases/second-wave-of-5g-30-countries-to-launch-services-in-2023>

Key Recommendations

- Practice basic cyber hygiene measures, such as ensuring endpoint devices are always updated with the latest manufacturer security patches and firmware; implement strong passwords; enable authentication methods such as MFA wherever possible; and be aware of granted permissions.
- Organizations seeking to implement 5G into their networks should first ensure they have a basic understanding of contemporary vulnerabilities. IT departments should be properly aware and resourced with relevant skill sets.
- Organizations should ensure business resilience, IT continuity, and crisis response plans are appropriately updated to reflect the threats posed by 5G adoption.
- Organizations should continually work toward a security culture. This can include employee awareness training, regular risk assessments, and security vulnerability assessments.
- Engage regularly with 5G vendors and external cybersecurity experts to ascertain the extent of the threats posed, as well as which security measures best complement organizational requirements.
- Make proper use of 5G security features, such as enhanced encryption, secure edge computing, and network slicing.



APPENDIX A: ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 12:00 PM (EDT) on May 18, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

APPENDIX B: Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use TLP: CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP: CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready to See for Yourself?

> Request a Demo:

Sign up on zerofox.com/request-a-demo

> Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400

