POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE

2021

EXECUTIVE SUMMARY

The fifth-generation (5G) of wireless technology represents a complete transformation of telecommunication networks, introducing a vast array of new connections, capabilities, and services. These advancements will provide the connection for billions of devices and will pave the way for applications that will enable new innovation, new markets, and economic growth around the world. However, these developments also introduce significant risks that threaten national security, economic security, and impact other national and global interests. Given these threats, 5G networks will be an attractive target for criminals and foreign adversaries to exploit for valuable information and intelligence.

To address these concerns, the United States National Telecommunications and Information Administration (NTIA) developed the *National Strategy to Secure 5G*, a strategic document that expands on how the United States Government will secure 5G infrastructure domestically and abroad. The *National Strategy to Secure 5G* aligns to the *National Cyber Strategy* and establishes four lines of effort: (1) facilitating the rollout of 5G domestically; (2) assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure; (3) addressing risks to United States economic and national security during development and deployment of 5G infrastructure worldwide; and (4) promoting responsible global development and deployment of secure and reliable 5G infrastructure.

In alignment with Line of Effort 2 in the *National Strategy to Secure 5G*, the Enduring Security Framework (ESF) was identified to assist with assessing risks and vulnerabilities to 5G infrastructure. This included building on existing capabilities in assessing and managing supply chain risk. As a result, the ESF 5G Threat Model Working Panel was established.[1]

The preliminary focus of the 5G Threat Model Working Panel was to explore and prioritize potential threat vectors that may be associated with the use of 5G non-standalone (NSA) networks. The working panel reviewed existing bodies of work to identify and generate an aggregated list of known and potential threats to the 5G environment, determined and developed sample scenarios of where 5G may be adopted, and assessed risks to 5G core technologies. This analysis paper represents the beginning of the Working Panel's thinking on the types of risks introduced by 5G adoption in the Unites States, and not the culmination of it. This product is not an exhaustive risk summary or technical review of attack methodologies and is derived from the considerable amount of analysis that already exists on this topic, to include public and private research and analysis.

[1] The ESF is a cross-sector working group that operates under the auspices of Critical Infrastructure Partnership Advisory Council (CIPAC) to address threats and risks to the security and stability of U.S. national security systems. It is comprised of experts from the U.S. government as well as representatives from the Information Technology, Communications, and the Defense Industrial Base sectors. The ESF is charged with bringing together representatives from private and public sectors to work on intelligence-driven, shared cybersecurity challenges.

CONTENTS

INTRODUCTION

While the transition to 5G presents a wealth of opportunities and capabilities, it also introduces new vulnerabilities and threats. The following threat vectors identified by the ESF and 5G Threat Model Working Panel represent an initial list of threats across the various 5G domains. Within these three threat vectors are sub-threats that describe additional points of vulnerability for threat actors to exploit. While not all inclusive, these types of threats have the potential to increase risk to the United States as the country transitions to 5G.

Overview of Threat Vectors

Policy and Standards

The development of 5G policies and standards serve as the foundation for securing 5G's future communications infrastructure. Through global standards-setting bodies, like the 3rd Generation Partnership Project, Internet Engineering Task Force, and the International Telecommunication Union, telecommunications standards development organizations are developing technical standards and security controls that will influence the design and architecture of new technologies, such as autonomous vehicles, edge computing, and telemedicine. Given the impact that these decisions have on implementing and adopting 5G technologies, it is critical that international standards and policies are open, transparent, and consensus driven.

As new 5G policies and standards are released, there remains the potential for threats that impact the end-user. For example, nation states may attempt to exert undue influence on standards that benefit their proprietary technologies and limit customers' choices to use other equipment or software. There are also risks associated with the development of standards, where standard bodies may develop optional controls, which are not implemented by operators. By not implementing these subjective security measures, operators could introduce gaps in the network and open the door for malicious threat actors.

Supply Chain

Supply chain risk refers to efforts by threat actors to exploit information and communications technologies (ICTs) and their related supply chains for purposes of espionage, sabotage, foreign interference, and criminal activity. The 5G supply chain is similarly susceptible to the introduction of risks like malicious software and hardware, counterfeit components, poor designs, manufacturing processes, and maintenance procedures. The exposure to these risks is heightened by the broad appeal of 5G technologies and the resulting rush to deployment. This may result in negative consequences, such as data and intellectual property theft, loss of confidence in the integrity of the 5G network, or exploitation to cause system and network failure.

With the potential for the connection of billions of 5G devices, there is an increased risk for untrusted or counterfeit components to be introduced within the 5G supply chain. This could include compromised devices or infrastructure that ultimately affects end-user devices, such as computers, phones, and other devices. Untrusted companies or government-backed suppliers also contribute to the supply chain risk, especially those that have significant international market share within telecommunication networks. For example, those countries that purchase 5G equipment from companies with compromised supply chains could be vulnerable to the interception, manipulation, disruption, or destruction of data. This would pose a challenge when sending data to international partners, where one country's secure network could be vulnerable to threats because of an untrusted telecommunication network in another country.

5G Systems Architecture

5G system architectures are being designed and developed to meet increasing data, capacity, and communications requirements. Although 5G component manufacturers and service providers are enhancing security through technology improvements, both legacy and new vulnerabilities may be exploited by malicious actors. Additionally, 5G networks will use more ICT components than previous generations of wireless networks, which could provide malicious actors with other vectors to intercept, manipulate, disrupt, and destroy critical data. The increased capacity of 5G facilitates the proliferation of the Internet of Things, which adds numerous and potentially less secure devices into the 5G network. This increased diversity of components can lead to complexity within the 5G architecture and may introduce unforeseen, overall system weaknesses or vulnerabilities.

As new 5G components and technologies are developed and deployed, new weaknesses will be discovered. The future 5G systems architecture (e.g., software defined networking, cloud native infrastructure, network slicing, edge computing) may introduce an increased attack surface for malicious actors to exploit. For example, the overlay of 4G legacy and 5G architectures could provide the opportunity for a malicious actor to carry out a downgrade attack, where a user on a 5G network could be forced to use 4G, thereby allowing the malicious actor to exploit known 4G vulnerabilities. These threats and vulnerabilities could be used by malicious threat actors to negatively impact organizations and users. Without continuous focus on 5G threat vectors and early identification of weaknesses in the system architecture, new vulnerabilities will increase the impact of cyber incidents.

5G THREAT VECTORS

Building upon the three threat vectors of Policy and Standards, Supply Chain, and 5G Systems Architecture, the following descriptions detail sub-threats of each primary threat vector.

Policy and Standards Sub-Threat Vectors

Open Standards

As adversarial nations contribute to the development of technical standards, the potential exists for standards to include untrusted technologies and equipment that are unique to their systems. These proprietary technologies and equipment may limit competition and force customers to adopt untrusted, new technologies. The lack of interoperability with these untrusted proprietary technologies limits the ability of trusted companies to compete in the 5G market. The custom 5G technologies that do not meet interoperability standards may be difficult to update, repair, and replace or they could be entirely invisible to the customer. This potentially increases the life-cycle cost of the product and delays 5G deployment if the equipment requires replacement.

Optional Controls

Standards bodies develop protocols for mobile telecommunications, some of which contain security controls that are either required or optional. Network operators that do not implement optional security controls may have more vulnerable networks and be at higher risk for cyber-attacks.

Supply Chain Sub-Threat Vectors

Counterfeit Components

Counterfeit components are more susceptible to cyber-attack and are more likely to break because of their poor quality. Compromised counterfeit components could enable a malicious actor to impact the confidentiality, integrity, or availability of data that travels through the devices and to move laterally to other more sensitive parts of the network.

Inherited Components

Inherited components may come from extended supply chains consisting of third-party suppliers, vendors, and service providers. Supply chains may be compromised via attacks on suppliers, including suppliers of suppliers, who may have weaker security controls and audits on their development, production, or delivery channels. Flaws or malware inserted early in the development phases are more difficult to detect and could lead to the developer marking the component as legitimate through digital signatures or other approvals. These vulnerabilities could then later be exploited by malicious actors.

5G Systems Architecture Sub-Threat Vectors

Software/Configuration

Unauthorized access to software or network components provides a malicious actor with the opportunity to modify configurations to reduce security controls, install malware on the system, or identify weaknesses in the product. These vulnerabilities could be exploited for increased persistent and privileged access within a system or network.

Network Security

5G technologies enable the potential for billions of connected network devices, supporting a wealth of new capabilities and innovation. These devices and infrastructure capabilities, such as cellular towers, beamforming transmission, small cells, and mobile devices, introduce the opportunity for malicious actors to expose vulnerabilities across an increased set of threat vectors. If network devices were compromised through a network layer exploit, malicious actors could obtain unauthorized access to the 5G network, potentially disrupting operations and enabling the interception, manipulation, and destruction of critical data.

Network Slicing

Network slicing allows users to be authenticated for only one network area, enabling data and security isolation. However, network slicing can be difficult to manage, and the slices add complexity to the network. While there are standards defining specifications for how operators build their 5G networks, there are no clear specifications for how network operators should develop and implement security for network slicing. Improper network slice management may allow malicious actors to access data from different slices or deny access to prioritized users.

Legacy Communications Infrastructure

While 5G network infrastructure is designed to be more secure, many of the security specifications and protocols from 4G legacy communications infrastructure are supported in 5G networks. This legacy communications infrastructure contains inherent vulnerabilities that, if not addressed, can be exploited by malicious actors.

Multi-Access Edge Computing

Multi-Access Edge Computing (MEC) transforms the way data is processed and stored by moving some core network functions closer to the end user at the network edge, rather than relying on a central location that may be hundreds of miles away. The introduction of untrusted 5G components into the MEC could expose core network elements to risks introduced by software and hardware vulnerabilities, counterfeit components, and component flaws caused by poor manufacturing processes or maintenance procedures.

Spectrum Sharing

To reach its potential, 5G systems require a complement of spectrum frequencies (low, mid, and high) because each frequency type offers unique benefits and challenges. With an increasing number of devices competing for access to the same spectrum, spectrum sharing is becoming more common. Spectrum sharing may provide opportunities for malicious actors to jam or interfere with non-critical communication paths, adversely affecting more critical communications networks.

Software Defined Networking

Software Defined Networking (SDN) is an architecture for automatically configuring routes across a network, primarily using an SDN controller. While SDN improves network flexibility and eases management, malicious actors may embed code in SDN controller applications to constrict bandwidth and negatively affect operations.

POLICY AND STANDARDS THREAT SCENARIOS

NATION-STATE INFLUENCE ON 5G STANDARDS

Open Standards

OVERVIEW

Undue influence from nation-states in sector specific or emerging technology standards, (e.g., autonomous vehicles, edge computing, telemedicine) can negatively affect the competitive balance within the 5G market, potentially limiting the availability of trusted suppliers and leading to a situation where untrusted suppliers are the only options. Nation-states may pursue early adoption of emerging technologies to increase their global influence over 5G technologies and lead to an environment in which U.S. companies are forced to use untrusted components within their networks.

SCENARIO

The Healthcare and Public Health sector is forced to adopt standards developed by a nation-state that benefit their manufacturing and cyber capabilities while putting the U.S. at a disadvantage. U.S. hospitals begin to adopt telesurgery to provide better support to rural and disadvantaged communities, as well as to meet the growing demand for the emerging service. The same nation-state started its development of telesurgery hardware and software several years ago and is now a global leader in the field. U.S. hospitals are forced to either use their untrusted technologies or use similar technologies from trusted providers that are built according to the nation-state's de facto standards. The nation-state can influence these companies to develop or utilize technologies that puts the U.S. at a disadvantage and inhibits market growth.

UNIVERSITY IMPLEMENTATION OF OPTIONAL 5G SECURITY CONTROLS

Optional Controls

OVERVIEW

Organizations and communications providers that choose not to implement optional security controls will likely have more vulnerabilities and be at higher risk for cyber-attacks. In these instances, nation-state actors, who have contributed to security control development or are aware of vulnerabilities in systems that do not have them implemented, may target those entities. As a result, malicious actors could identify and utilize methods to take advantage of private networks that do not put these optional controls in place.

SCENARIO

Across the U.S., 5G begins to replace Wi-Fi in homes, offices, and in large private networks. A university implements a 5G network across its large campus but does not adequately configure or maintain all of the recommended, but optional, security controls. Many of the optional security controls, as outlined by primary standards bodies, are followed by telecommunications companies and other enterprise adopters. The university's decision not to implement all of the security controls results in significant cybersecurity gaps within their network. A malicious actor targets and tests for lack of these controls and exploits them within the university's 5G network.

SUPPLY CHAIN THREAT SCENARIOS

IMPLEMENTATION OF COUNTERFEIT COMPONENTS

OVERVIEW

Counterfeit components are inserted at the component manufacturing or distribution stage in the supply chain in order to impact components delivered to a subset (potentially a targeted subset) of downstream customers. Counterfeit parts look like regular parts and are a form of fraud. Counterfeiters prey on customers seeking high-quality parts from reputable manufacturers and instead are unknowingly sold substandard or defective parts. A counterfeiter's "intent to deceive" is the difference between a counterfeit part and a faulty part, which has defects or malicious functionalities that are unknown to the manufacturer or the distributor.

SCENARIO

A malicious actor identifies a government contractor that provides ICT components and attempts to sell modified or counterfeit products to them at discounted prices. While the contractor is legitimate and has the most to lose from counterfeit products, they are unaware that there is a potential problem and do not conduct an initial analysis of possible counterfeiting risks that exist within its industry. To save money, the contractor purchases the counterfeit components from the malicious actor and inserts them into their product. The counterfeit part has gone undetected in usability and functional testing and is placed into production. The resulting effect on the overall system and the end customer can take a variety of forms, such as impacting system performance, the availability of critical services, or resulting in the loss of data.

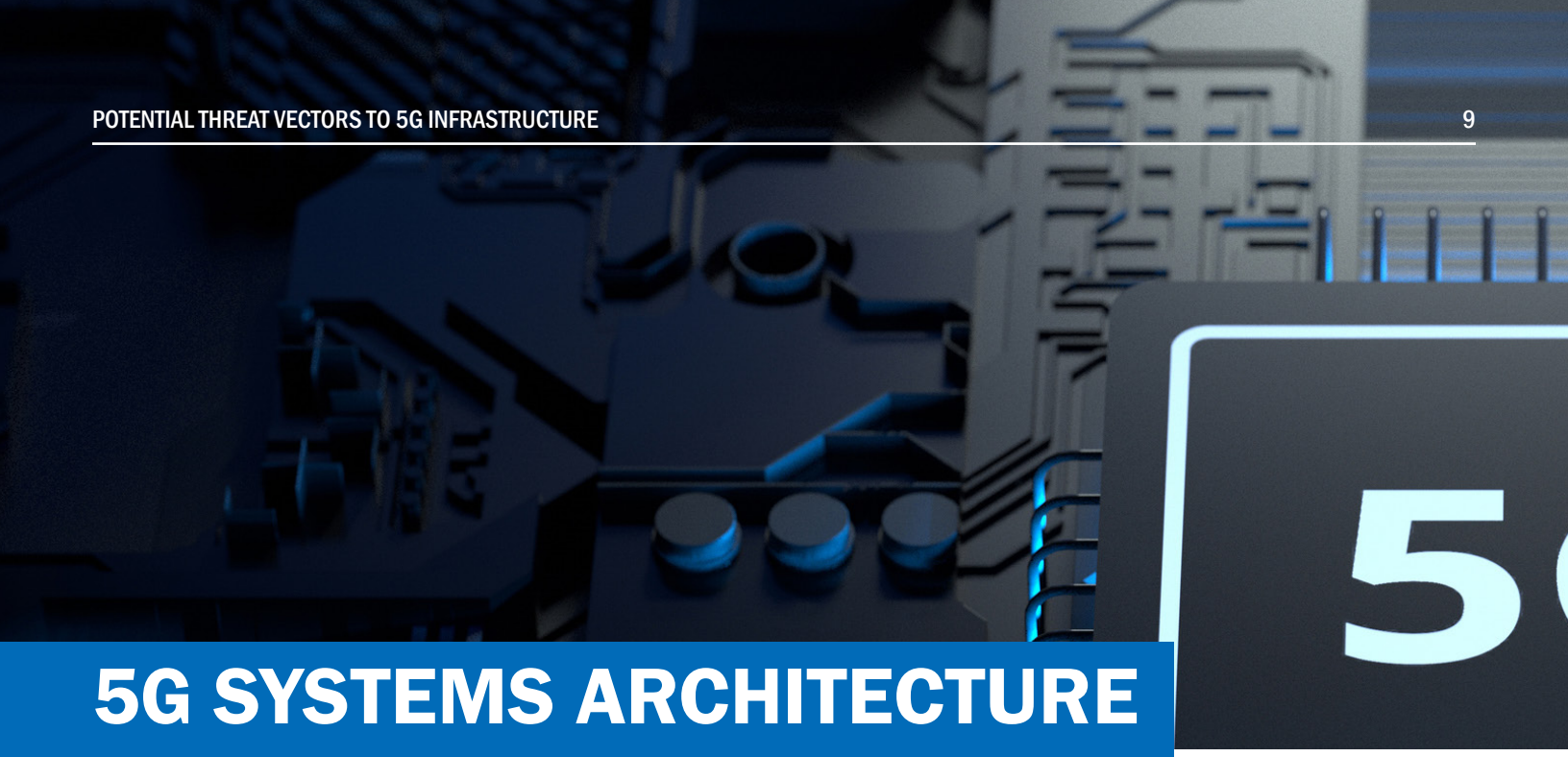
UNINTENTIONAL ADOPTION OF UNTRUSTED COMPONENTS

OVERVIEW

A software supply chain attack occurs when malicious code is purposefully added to a component that is sent to target users. The code may be introduced to the component in several different ways, such as via compromise of the source code repository, theft of signing keys, or penetration of distribution sites and channels. As a part of an authorized and normal distribution channel, customers unknowingly acquire and deploy these compromised components on to their systems and networks. Advanced malicious code typically does not disrupt normal operations and may not activate for several days or weeks, thereby remaining hidden from typical application and software testing practices.

SCENARIO

A telecommunications company buys core network systems management software from a trusted provider; however, unbeknownst to the trusted provider, one of the components it uses in the product has been compromised and now contains malicious code. This is a threat that results from inheriting risk decisions made by a supplier within the supply chain that impacts the end user of the final product or service. The deeper into the supply chain it occurs, the more difficult it is to identify in advance. This inserted vulnerability may be used by the malicious actor as a part of a larger attack chain that uses the malicious code to gain access within the core network of the telecom and pivot towards other attack vectors.



5G SYSTEMS ARCHITECTURE THREAT SCENARIOS

INHERITED VULNERABILITIES FROM 4G NETWORKS

OVERVIEW

5G builds upon previous generations of wireless network and will initially be integrated with 4G Long Term Evolution (LTE) networks that contain legacy vulnerabilities. While 5G technologies are being designed to be more secure than previous mobile network generations, they may be vulnerable to certain legacy exploits, such as Signaling System 7 (SS7) and diameter protocol vulnerabilities, because they will initially be overlaid on the existing 4G LTE networks.

SCENARIO

A threat actor gains access to a 5G small cell near a United States Government (USG) office and configures the small cell to allow for 4G spoofing. The threat actor then forces a downgrade in the 5G network to a vulnerable 4G configuration, which allows them to use vulnerabilities within SS7 to gain access to ICT components in use by employees in the nearby USG office. The threat actor can then use that information to gain further access into more secured networks, potentially gaining access to sensitive data.

FIRMWARE VULNERABILITY WITHIN THE MULTI-ACCESS EDGE COMPUTE

Multi-Access Edge Computing

OVERVIEW

Unlike traditional network configurations, Multi-Access Edge Compute (MEC) delivers core traffic functions like data processing and storage within the last mile of telecommunication networks. The presence of system components, such as hypervisors, operating systems, and applications in the MEC, may provide malicious actors with additional attack vectors to intercept, manipulate, and destroy critical data. Untrusted components or malware inserted within the MEC may impact user privacy by providing malicious actors the capability to clone devices and impersonate end-users to make calls, send texts, and use data. Malicious actors can use untrusted components or malware to gain access to the MEC and end-user components, leveraging them to gain access to the wider radio access network (RAN).

SCENARIO

A firmware vulnerability in the MEC allows a threat actor to gain a persistent foothold on the MEC system, which allows them to deny access to data and impact the ultra-low latency required by many 5G use cases. The malicious actor can use this access to impact the confidentiality, integrity, and availability of the network by stealing sensitive sensor and user equipment data, modifying data streams, and denying access to certain data or sensor streams. The malicious actor now has the bandwidth to gain full access to the RAN and is able to clone end-users' devices.

GLOSSARY

TERMS	DEFINITIONS
3G	Third generation communications system, bringing Internet and higher bandwidth to mobile devices.
4G	Fourth generation communications system, offering speed and congestion improvements over 3G
4G Spoofing	An attack where an agent can subvert the security and privacy controls of 4G to enable phone call and messaging blocking, interception and spoofing, location tracking, and targeted phishing attacks. Some security and privacy controls in 5G have been similarly spoofed.
Attack Surface	The places in a computer or communications network where a trust boundary might be crossed by an unauthorized person or software/hardware.[1]
CNCF	Cloud Native Computing Foundation
Controls	Prevent threats from exercising a vulnerability.[2]
Core Network	"The core network forms the bridge between the RAN and the Internet, the wired telephone system, and Internet protocol-based (IP-based) services. The core network controls RAN functions on the entire network: All data (e.g., voice, video, text) on a network traverse the core, and it determines how those data are routed."[3]
Cyber Actor	An agent employing a computer and/or network-based action against a target.
Downgrade Attack	An attack where the threat actor forces a network to downgrade from 5G to a 4G configuration which has security vulnerabilities
Edge Compute	The distribution of compute power closer to the edge to provide better quality of experience and to fulfill new use-cases.
ICT	Information and communications technology
IMSI	International mobile subscriber identity
Malicious actor	An agent accessing a network or computer with malicious intent.
MEC	Multi-Access Edge Compute, delivers 5G services from a distributed cloud enabling new mobile use cases. It is a distributed cloud with multiple sites that bring the execution environment geographically closer to the UE. The main benefits of MEC are low latency, high bandwidth, device density, data offload, and trusted computing and storage. These benefits enable 5G use cases like enterprise private networks for industrial IoT, smart cities, autonomous vehicles, remote surgery, virtual reality, cloud gaming, and high-quality video streaming without buffering.
NSA	5G non-standalone

[1]Shostack, Adam. Threat Modeling: Designing for Security. Wiley, 2014.
[2]Pfleeger, Charles P., et al. Security in Computing. Pearson India Education Services, 2018.
[3]Rasser, Martinj, and Ainikki Riikonen. Center for a New American Security, 2020, Open Future: The Way Forward on 5G, www.cnas.org/publications/reports/open-future.

TERMS	DEFINITIONS
RAN	Radio Access Network "The RAN is "the part of a telecommunications system that connects individual wireless devices to other parts of a network through radio connections." While the interfaces to do so are open and standardized, the equipment needed—base stations, radio amplifiers, management systems—are closed (not interoperable with other vendors) and do not completely abide by these standards. RAN equipment is vendor-proprietary, and the global market is dominated by just a handful of manufacturers: Huawei, Nokia, Ericsson, and to a lesser extent Samsung and ZTE. In 4G, the fourth generation of wireless telecommunications, this part of the network is called "the edge." "There are only two major non- Chinese suppliers of RAN equipment: Nokia of Finland and Ericsson of Sweden. Samsung of South Korea is a distant third. Given the importance of RAN to future critical digital infrastructure, the industry is too consolidated to ensure sufficient supply chain diversity and security."[4]
SA	5G standalone
SDN	Software Defined Network
S-NSSAI	Single Network Slice Selection Assistance Information
SS7	Signaling System No. 7, a telephony protocol used to manage telephone connections.
Threat Agent	An agent actively attempting to exploit a vulnerability.
Threat Model	"Threat modeling is about using models to find security problems. Using a model means abstracting away a lot of details to provide a look at a bigger picture, rather than the code itself. You model because it enables you to find issues in things you haven't built yet, and because it enables you to catch a problem before it starts. Lastly, you threat model as a way to anticipate the threats that could affect you."[5]
Threat Vector	The path or means by which a threat may exploit a vulnerability
Trust Boundary	The boundaries in a computer or network over which agents of different organizations or trust levels interact. "Threats are not restricted to trust boundaries but almost always involve actions across trust boundaries."[6]
UDM	User Data Management
UE	User Equipment
UMTS	Universal mobile telecommunications system
URLLC	Ultra-Reliable Low-Latency Communications
USG	United States Government
USIM	Universal Subscriber Identity Module
Vulnerability	A weakness in a computer system or network that could be exploited to cause harm or disruption.[7]
V2X	Vehicle-to-Everything
VNF	Virtualized Network Function

[4]Rasser and Riikonen. Open Future: The Way Forward on 5G.
[5]Shostack. Threat Modeling: Designing for Security, 3.
[6]Shostack. Threat Modeling: Designing for Security, 541.
[7]Pfleeger, Security in Computing.


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA