EDGE VS. CORE - AN INCREASINGLY LESS PRONOUNCED DISTINCTION IN 5G NETWORKS

2020

Cybersecurity and Infrastructure Security Agency

DRAFT//PRE-DECISIONAL

TLP:WHITE

KEY FINDINGS

The Cybersecurity and Infrastructure Security Agency (CISA) assesses that integration of untrusted[i] fifth generation (5G) core functions into the Radio Access Network (RAN) and the transition away from traditional network boundaries increases risk to telecommunication networks from equipment previously thought to be less critical (e.g., base stations, small cells). Accordingly, CISA recommends avoiding the use of hardware or software from untrusted entities that impact the operations of both the core and edge portions of the networks, and does not believe that the distinction between the two is meaningful from a risk management perspective. To reduce the national security risks associated with the implementation of 5G technology, network operators should use only trusted providers and encourage the continued development of trusted 5G technologies, products, and services across the entire 5G ecosystem.

SCOPE NOTE: CISA produced this Critical Infrastructure Security and Resilience Note to inform Agency leadership and partners about how edge computing increases the risks of installing untrusted components into 5G networks by moving core functions into the RAN edge. This product is intended to provide an overview of edge computing and represents CISA's analysis of the risks associated with the installation of untrusted components into 5G infrastructures. This analysis represents the beginning of CISA's thinking on this issue, and not the culmination of it. It is not an exhaustive risk summary or technical review of attack methodologies. This product is derived from the considerable amount of analysis that already exists on this topic, to include public and private research and analysis. Analysis of complex, sophisticated, and distributed cyber intrusions against 5G networks is beyond the scope of this product. At the time of this product's creation, 5G and edge computing standards, networks, and components are still under development.

[i] Untrusted companies are those that do not meet most, if not all, of the criteria in the Center for Strategic and International Studies' May 13, 2020 document, "Criteria for Security and Trust in Telecommunications Networks and Services." For more information refer to: www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

CONTENTS

What is Edge Computing 01

Mobile Edge Computing (MEC) - Edge computing Standard

Edge vs. Core - An Increasingly Less Pronounced Distinction

Risk From Untrusted Entities 03

Increased Risk Landscape

Software Assurance Concerns

Software Defined Networking (SDN) – A Key Enabler of Edge Computing

National Opportunities to Mitigate Edge Computing Risk 05

Encouraging continued development of trusted 5G technologies, software, and services

Restricting the use of 5G equipment from untrusted companies and those with poor hardware and/or software assurance

Continued engagement with the private sector on risk identification and mitigation efforts

WHAT IS EDGE COMPUTING?

Edge computing transforms the way data is processed and stored by moving some core network functions to be more proximate to the end user at the network edge rather than relying on a central location that may be hundreds of miles away.[1] Moving the data processing and storage closer to the point at which it is created minimizes the amount of long-distance communication required between a client and a server.[2]

Edge computing supports 5G emerging technologies by providing reduced latency and decreased core network traffic. For example, 5G will help autonomous vehicles that rely on immediate data processing and analysis to ensure near-instantaneous responses. An autonomous vehicle using edge computing sends data to a nearby access point where it is analyzed and returned, avoiding all the additional network hops it takes to send information to a centralized data center.[ii] Conversely, in a traditional network architecture, the autonomous vehicle would communicate with a centralized data center, which could increase the number of network hops and impact time-sensitive applications like high definition mapping, real time traffic flow, and industry specific logistical data.

Edge computing provides new possibilities for critical applications, particularly for those relying on ultra-low latency, such as telesurgery, thermal imaging for emergency response, traffic safety and control, and autonomous manufacturing. Figure 1 shows emerging technologies that are enabled by edge computing.

Edge computing provides network operators improved visibility over traditional networks and enables faster identification of potential security issues. Data that was traditionally sent to a data center at the core of network can now be scanned closer to where it originated, potentially allowing for faster remediation. This allows network defenders to allocate security resources, such as threat monitoring and analytic tools, to where they're needed most. While the move to edge computing presents opportunities to enhance the security and improve the reliability of 5G networks, the insertion of untrusted components within the RAN may negate any security advantages that edge computing offers.

[ii] A hop occurs when a packet passes from one network segment to the next as they travel between source and destination.

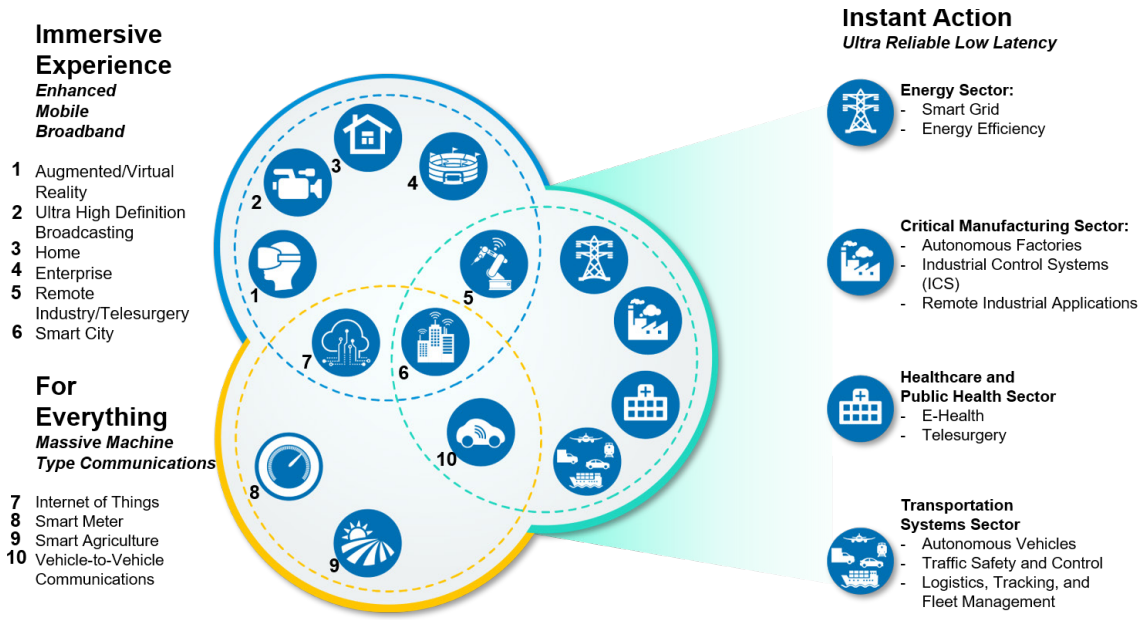


FIGURE 1 — EMERGING TECHNOLOGIES ENABLED BY EDGE COMPUTING

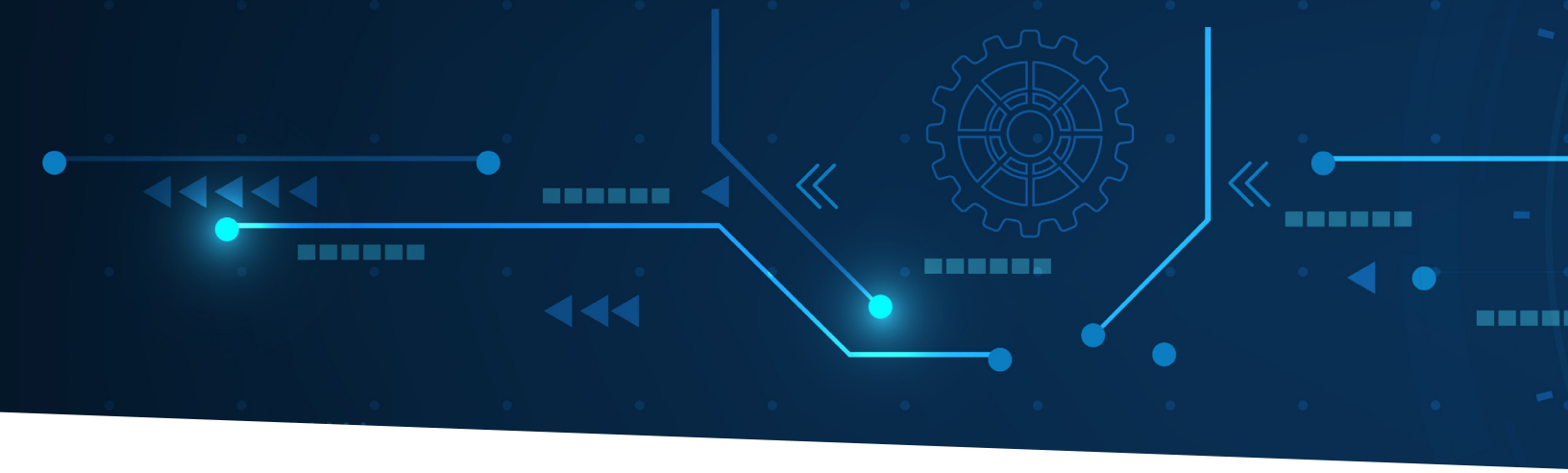
Multi-Access Edge Computing (MEC) - Edge Computing Standard

MEC is a standard architecture that exists within edge computing.[3] The communications industry widely accepts the MEC standard, and technologies must meet this standard for consideration in edge computing. Specifically, MEC is a type of edge computing that extends the capabilities of cloud computing by bringing it to the edge of the network. While traditional cloud computing occurs on remote servers located far from the user and device, MEC allows processes to take place in base stations, central offices, and other aggregation points on the network. This functionality increases network and data storage reliability and will limit the number service outages and cyber-attacks.[4] MEC also allows for the RAN to be available to third party application developers and content providers to allow for improved real-time optimization of applications and network resources.

Edge vs. Core - An Increasingly Less Pronounced Distinction

In a Third Generation/Fourth Generation (3G/4G) wireless network, devices such as smart phones and computers generate data that transmit to a RAN base station. The base station then connects wireless subscriber devices to the internet via the core network, which acts as the backbone of the U.S. communications infrastructure that routes and transports data, and connects the different parts of the RAN. A 3G/4G RAN includes thousands of base stations and antennas that relay information, but do not store or process it.[5]

Edge computing blurs the distinction that previously existed in wireless networks by hosting core resources within the RAN near base stations and closer to end users. While edge computing will support core functionality at the RAN, it is not part of the core and any issues that affect the edge may not reach the core network. The integration of some core functions into the RAN and the blurring of traditional network boundaries may increase the risk that compromises of previously non-sensitive equipment (e.g., base stations, small cells) will lead to greater impacts to the confidentiality, integrity, and availability of the overall network.[6]



RISK FROM UNTRUSTED ENTITIES

CISA assesses that the introduction of untrusted 5G components into the RAN 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. The integration of core functions into the RAN and the transition from traditional network boundaries increases risk to telecommunication networks from equipment previously thought to be less critical (e.g., base stations, small cells). This equipment, if exploited, will impact the confidentiality, integrity, and availability of the network.

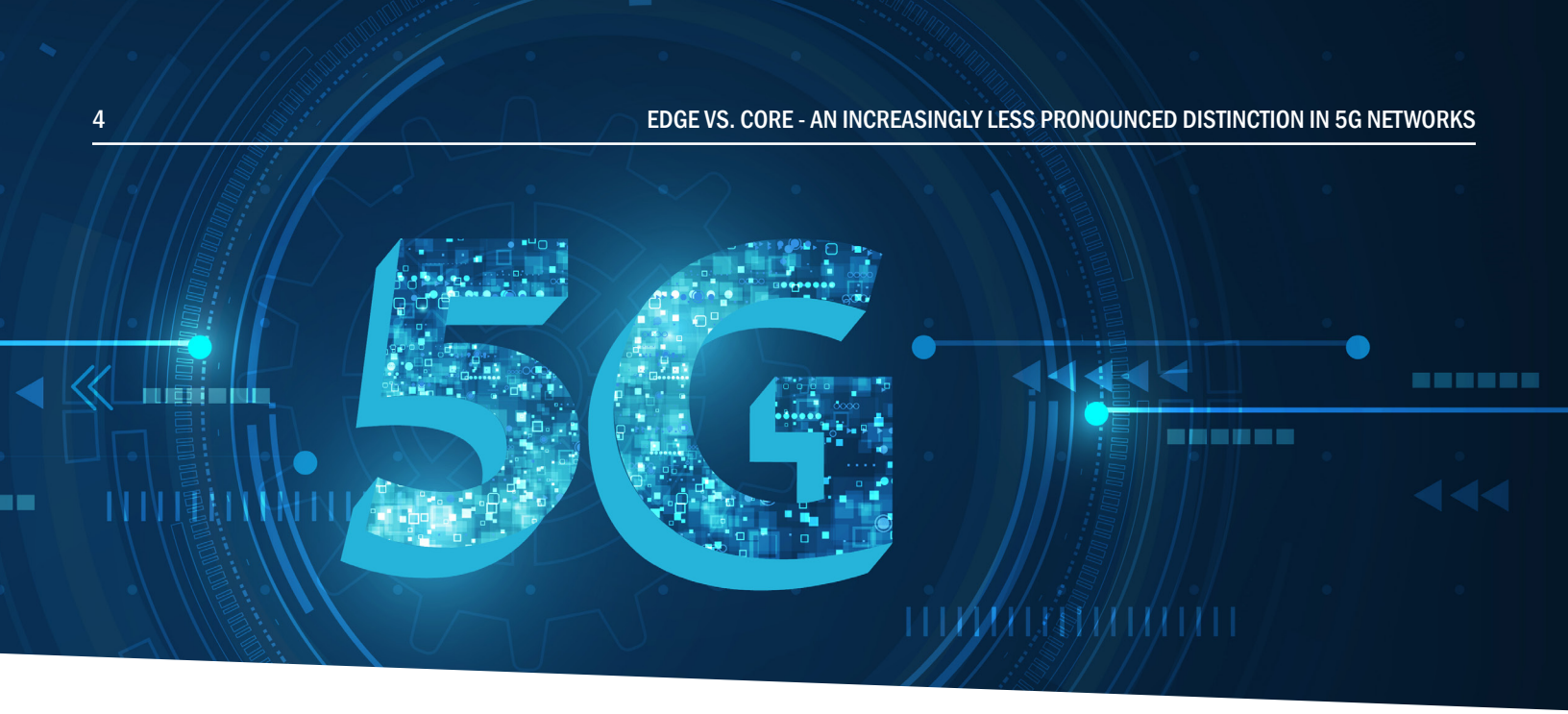
Risk Landscape

In edge computing, core traffic functions like data processing and storage exist within the last mile of telecommunication networks, unlike traditional network configurations.[iii] The ubiquity of core components in the RAN may provide malicious actors with additional attack vectors to intercept, manipulate, and destroy critical data. Untrusted components inserted within the RAN 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.[7]

Malicious actors can use untrusted components to gain access to Internet of Things (IoT) devices, which can be difficult to secure due to poor device management and platform diversity. Malicious actors may target IoT devices with attacks that exploit poor configurations, and then use those devices as a hop point in order to gain a foothold in RAN networks.[8]

Extending communication networks with edge computing changes the surface area for attacks, and may compound risks for networks utilizing untrusted endpoint components. Malicious actors may use unsecure endpoints and IoT devices as attack vectors in distributed denial-of-service attacks, or as entry points to access core networking components. To mitigate these risks, network carriers have implemented network compartmentalization and isolation, which can limit the impacts from compromised components.

[iii] The last mile refers to the final leg of the telecommunications networks that deliver services for end-user applications.



Software Assurance Concerns

Untrusted entities can enable serious and systematic defects in their software engineering, maintenance, and cybersecurity practices.[9,10] Poorly developed code makes vulnerability management significantly more difficult, and can lead to unsupportable software. If a critical outage occurs, systems, programs, and data with code from untrusted entities are more difficult to recover and may lead to extended outage times.

The functionality of 5G and edge computing is reliant on proper cyber and network security. Untrusted entities with poor software assurance[iv] develop technologies that are vulnerable to cyber attacks and may be difficult to update, repair, and replace, potentially requiring costly ongoing management and mitigation support.[11]

Software Defined Networking (SDN) – A Key Enabler of Edge Computing

SDN is a software-based approach to network management that enables dynamic provisioning and policy-based management of network resources, allowing the network to make decisions for the operator to improve efficiency and utilization.[12] SDN enables edge computing by managing traffic between traditional cloud infrastructure and the edge, acting as a decision-maker for tasks and determining which should be processed at the network edge or in the cloud.[13] SDN has a single point of control known as the SDN controller, which if developed by an untrusted provider with poor software assurance and cyber security competence, could allow cyber actors to move laterally within a network and bypass security points. SDN is anticipated to be a foundational component of 5G, enabling improved virtualization, increased bandwidth and capacity, and reduced latency.

SPOTLIGHT:
Risk from Poor Coding Practices

In June 2019, Finite State, a cybersecurity vulnerability research firm, analyzed more than 1.5 million unique files embedded within 9,936 firmware images supporting 558 different products within Huawei's enterprise networking product lines. The report notes that Huawei used decade-old versions of libraries containing multiple vulnerabilities, and even found that Huawei engineers disguised known unsafe functions as the safe version. The results of the analysis showed that Huawei quantitatively poses a high risk to their customers, not only due to their failure to use commonly accepted secure coding practices, but also because of their attempts to purposefully disguise poor practices in order to deceive code reviewers.

[iv] Software assurance is the user's confidence that a software functions as intended, and is free of vulnerabilities throughout the product lifecycle.

NATIONAL OPPORTUNITIES TO MITIGATE EDGE COMPUTING RISK

CISA recommends avoiding the use of hardware or software from untrusted entities that impact the operations of both the core and edge portions of the networks, and does not believe that the distinction between the two is meaningful from a risk management perspective. To reduce the national security risks associated with the implementation of 5G technology, network operators should use only trusted providers and encourage the continued development of trusted 5G technologies, products, and services across the entire 5G ecosystem. Opportunities for the U.S. Government and industry to work together to maximize the benefits of next generation communication networks, and to promote security and resilience associated with emerging 5G technologies exist at the strategic level.

Opportunities for the U.S. Government and industry to work together to maximize the benefits of next generation communication networks, and to promote security and resilience associated with emerging 5G technologies exist at the strategic level. Follow-on efforts and discussions are necessary to expand on specific potential actions.

Encouraging continued development of trusted 5G technologies, software, and services

Reliance on untrusted 5G technologies often occurs because of relatively low costs associated with those technologies. Additionally, if untrusted companies' equipment and software is already installed as part

of the 4G (Long-Term Evolution) LTE network, lack of interoperability may make it impossible to install other companies' 5G equipment without replacing the existing 4G LTE equipment, which may be extremely costly. Some solutions such as national investment in research and development, promoting efforts to ensure interoperability, and promoting the standardization of open protocols within RAN componentry could lead to reduced risk and increases security across 5G network deployments.

Restricting the use of 5G equipment from untrusted companies and those with poor hardware and/or software assurance

The United States can take action to limit the adoption of 5G equipment that may contain vulnerabilities due to poor hardware and software assurance. Cybersecurity can be improved for U.S. communications across the federal enterprise by limiting the installation of 5G components from companies with poor security cultures and risky software assurance.[14] The United States can also promote proper engineering, maintenance, and cybersecurity best practices, which can improve software assurance and make U.S. communications infrastructure more resilient to cyber attacks. As practicable, CISA recommends not using 5G equipment from untrusted companies and those with poor hardware and software assurance.

Continued engagement with the private sector on risk identification and mitigation efforts

The U.S. Government can continue to work with the private sector—to include information and communication technology providers—to help mitigate vulnerabilities. The private sector can provide insights on where government support or intervention—such as through the development of best practices, the convening of industry and government partners, and the prohibition of untrusted equipment—will help secure edge technologies and 5G networks. As highlighted in a recent report by the Communications Security, Reliability, and Interoperability Council, 5G in standalone configurations actually presents opportunities for security enhancements over previous generations. These include increased home operator control, enhanced subscriber privacy, and user plane integrity protection in RAN.[15]

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This report is TLP: WHITE: Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp.

The Cybersecurity and Infrastructure Security Agency (CISA), National Risk Management Center (NRMC) is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.cisa.gov/national-risk-management.

PDM20030

---

[1] Keith Shaw. "What is edge computing and why it matters." *Network World*. November 13, 2019. https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html. Accessed on June 22, 2020.

[2] Federal Communications Commission (FCC) Technological Advisory Council: 5G IoT Working Group. "5G Edge Computing White Paper." https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2018/5G-Edge-Computing-Whitepaper-v6-Final.pdf. Accessed on June 22, 2020.

[3] ETSI. "Multi-access Edge Computing (MEC)" ETSI, https://www.etsi.org/technologies/multi-access-edge-computing. Accessed on Oct 5, 2020

[4] Connor Craven. "What's the Difference Between Edge Computing and MEC?" *SDX Central*. April 29, 2019. https://www.sdxcentral.com/edge/definitions/whats-the-difference-between-edge-computing-and-mec/. Accessed on June 22, 2020.

[5] Iain Morris. "Telecom industry rift widens over key 5G security issue." *Light Reading*. https://www.lightreading.com/carrier-security/telecom-industry-rift-widens-over-key-5g-security-issue/d/d-id/756247. Accessed June 22, 2020.

[6] European Commission. "The EU Toolbox for 5G security." https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security. Accessed on June 22, 2020.

[7] Andrew Coutes. "Meet the $250 Verizon device that lets hackers take over your phone." *Digital Trends*. August 1, 2013. https://www.digitaltrends.com/mobile/femtocell-verizon-hack/. Accessed on June 22, 2020.

[8] Microsoft Security Response Center (MSRC) Team. "Corporate IoT - a path to intrusion." *Microsoft: Security Research and Defense*. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/. Accessed on June 22, 2020.

[9] Gov.UK. "Huawei cyber security evaluation centre oversight board: annual report 2019." *Cabinet Office from the Huawei Cyber Security Evaluation Centre Oversight Board*. March 28, 2019. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019. Accessed on June 22, 2020.

[10] Finite State. "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd." https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf. Accessed on June 22, 2020.

[11] Gov.UK. "Huawei cyber security evaluation centre oversight board: annual report 2019." *Cabinet Office from the Huawei Cyber Security Evaluation Centre Oversight Board*. March 28, 2019. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019. Accessed on June 22, 2020.

[12] Michael Cooney. "What is SDN and where software-defined networking is going." *Network World*. April 16, 2019.https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html. Accessed on June 22, 2020.

[13] Andrew Froehlich. "Where does SDN fit in edge computing architecture?" *TechTarget: SearchNetworking*. November 2018. https://searchnetworking.techtarget.com/answer/Where-does-SDN-fit-in-edge-computing-architecture. Accessed on June 22, 2020.

[14] Rep. Mac Thornberry [R-TX-13]. "H.R. 5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019." U.S. Congress: House Armed Services Committee. https://www.congress.gov/bill/115th-congress/house-bill/5515/text. Accessed on June 22, 2020.

[15] Communications Security, Reliability, and Interoperability Council VII. https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii. Accessed on June 30, 2020.

Cybersecurity and Infrastructure Security Agency