THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

DRAFT NSTAC REPORT TO THE PRESIDENT

on Software-Defined Networking

TBD

Table of Contents

Executive Summary

In September 2019, the Executive Office of the President (EOP) tasked the President's National Security Telecommunications Advisory Committee (NSTAC) with examining the implications of software-defined networking (SDN) on the Nation's national security and emergency preparedness (NS/EP) communications and information and communications technology (ICT) infrastructure.

In networking, SDN and network functions virtualization (NFV) represent an ongoing shift away from legacy technologies based upon hardware to software based networks that leverage standard, commercial off-the-shelf, or commodity-based hardware.

This shift is structurally transforming the ICT ecosystem and allowing networks to become more flexible and adaptive.[1] SDN's more flexible architecture has proven to be beneficial during the ongoing response to the coronavirus (COVID-19) pandemic.

The NSTAC examined best practices for SDN and related technologies; identified the associated challenges and opportunities; and assessed current utilization and corresponding risk mitigations. Building off the recommendations outlined in the 2017 *NSTAC Report to the President on Emerging Technologies Strategic Vision*, this examination sought to make specific recommendations to the EOP regarding SDN policy. The key findings and recommendations of the NSTAC are summarized below.

Key Findings

- The enterprise networks and the global network infrastructure are **migrating quickly to an SDN environment**, due to the performance, flexibility, adoptability, resiliency, security, and cost advantages provided by network virtualization. As network infrastructure migrates to SDN, all network users, including providers, enterprises, and consumers, will

SDN and COVID-19

Flexible architecture enabled by SDN has proven vital to maintaining network performance during COVID-19. In early April 2020, the Federal Communications Commission reported that United States' internet traffic rose by 25 to 30 percent on fixed networks, and 10 to 20 percent on wireless networks. AT&T reported that demand for its virtual private networking service increased 700 percent during the pandemic. However, AT&T was able to accommodate the traffic surge by leveraging its investments in SDN and NFV. This outcome is not limited to AT&T. The communications sector has also reported that their networks have been able to meet the increased demand. USTelecom and the National Cable and Telecommunications Association have reported COVID-19 network performance data, which indicates that service providers have kept pace with demand, which can be partially attributed to SDN.[2,3,4,5]

[1] President's National Security Telecommunications Advisory Committee (NSTAC), NSTAC Report to the President on Emerging Technologies Strategic Vision, July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

[2] Andre Fuetsch, "How a Software-Centric Network Keeps Business Customers Connected in a Highly Safe Manner," AT&T Technology Blog, April 2, 2020, https://about.att.com/innovationblog/2020/04/anira.html.

[3] Mike Dano, "AT&T: Software-Defined Networking (SDN), Network Functions Virtualization (NFV) Helped Meet COVID-19 Traffic Demands," *LightReading*, April 2, 2020, https://www.lightreading.com/cloud-native-nfv/atandt-sdn-nfv-helped-meet-covid-19-traffic-demands/d/d-id/758661.

[4] "Network Performance." USTelecom. USTelecom, 2020, http://www.ustelecom.org/research/network-performance-data/.

[5] "COVID-19: How Cable's Internet Networks Are Performing-Metrics, Trends, and Observations." The Internet and Television Association (NCTA). *NCTA*, https://www.ncta.com/COVIDdashboard.

become dependent upon SDN. SDN simplifies the ability to: (1) integrate networking with cloud-based services, which are already fully leveraging SDN; and (2) migrate towards new operational capabilities that are built upon SDN functionality. Carriers and service providers, as well as other public and private sector enterprises, are increasingly using SDN. For example, SDN has been advantageous in dealing with the profound changes in the ICT environment caused by the COVID-19 pandemic. Another accelerating trend for SDN is the buildout of fifth generation (5G) mobile infrastructure. By definition, 5G infrastructure is software-centric and virtualized. As such, SDN will play a critical role in networking the various service-based applications in 5G implementations. In the enterprise domain, SDN adoption has accelerated via the deployment of software-defined wide-area networking solutions to implement high performance wide-area networks via lower-cost, commercially available internet access.

- **The United States, along with its allies, is the global leader** in the development and deployment of SDN. The major U.S.-based carriers and service providers have already transitioned a significant portion of their global network infrastructures to SDN. This migration: (1) builds on and enhances U.S. leadership in virtualization and ICT innovation; and (2) illustrates that SDN technologies have reached a level of maturity such that they can be securely implemented at scale. While there are challenges with operationalization and security when transitioning to new technologies, the SDN deployments by U.S.-based carriers, service providers, and enterprises demonstrate that these challenges are manageable and SDN can be deployed as secure networking technology.

- SDN adoption is a well-established trend and is increasingly becoming the basis of future communication network architectures. SDN-based architectures disrupt current supply chain models, resulting in an **opportunity to create a more future-oriented supply chain** for network investments. The transition to SDN plays to the strengths of companies with existing leadership in silicon, cloud, and software, all of which exist within leading U.S. technology companies. To this end, leveraging trends in SDN can pave a path of innovation to **support the goal of defending and sustaining U.S. leadership in 5G wireless technologies and beyond**. Rarely do emerging technology trends afford such a compelling venue to support the Administration's strategic goals. Thus, U.S. participation in the evolution of a new SDN supply chain ecosystem is of global importance.

- The shift to SDN has profound implications for the **global ICT supply chain**, as individual and organizational networks move away from dedicated hardware-based devices and appliances to less expensive, flexible systems in which the primary value is provided by software. In the near-term, SDN will reduce product development cost and time to market, lowering barriers to market entry, spurring investment, and promoting innovation, as it expands and diversifies the global supply chain. To ensure the broadest opportunity over the long-term, it will be important to **standardize interoperability features** into all elements of SDN to enable multi-vendor architectures and inter-network compatibility.

- The Nation's critical infrastructure are built upon and utilize a wide variety of privately-operated networks. To fully realize the benefits SDN can bring to NS/EP functions, there will need to be broad **coordination across public and private entities.**

- **Enhanced security is a core capability** of SDN. As envisioned, SDN can facilitate the incorporation or addition of sophisticated security features in real-time, using artificial intelligence to rapidly detect and actively mitigate malicious activities. SDN architectures are designed to be more secure, resilient, adaptable, and resistant to the evolving threat environment than corresponding hardware-based deployments.

- Consistent with industry's approach, **the security of SDN's** software-centric architecture and potential use of open source componentry **must be addressed** at all levels of implementation and lifecycle management. A continued evolution of corporate security posture and software maintenance methodologies is a critical component of SDN technology adoption. While SDN transfers significant functionality from specialized hardware to software running on commodity hardware, it remains important that such hardware come from trusted suppliers. A key aspect of hardware security and supply chain continuity hinges on tight control over the manufacturing processes.

- SDN drives an architectural shift from a hardware-centric network design methodology to one that is software centric and distributed. Consequently, implementing **SDN requires different skill sets** compared to traditional networking approaches. **Organizations must invest to train staff and build expertise** in SDN deployment and operations.
- **Government agency use cases are not well represented** in the industry consortia and standards bodies that guide SDN development. Specifically, the Government has not addressed SDN use cases for classified networks.

Recommendations

- The Administration should encourage and support the continued deployment of SDN technology in the U.S. and allied nation ICT environments. Policymakers should consider how to promote the use of open architectures with particular focus on 5G and beyond.
- The Defense Community and the Intelligence Community (IC) should expand efforts to define their specific requirements and use cases for SDN and related technology specific to their unique needs, which can be shared with private sector SDN providers and relevant standards bodies. In collaboration with the private sector, the Defense Community and IC should also determine how the capabilities might be leveraged for adoption in the national security environment.
- The Government establish policies to help educate U.S. departments, agencies, and critical infrastructure operators on the full range of SDN and related technology capabilities to enhance their mission performance, improve security, and lower costs.
- Working with Congress, the Administration should: establish policies and incentives to encourage U.S.-based investment and innovation in research and development of SDN and related technology capabilities and standards; (2) encourage best practices for secure implementation; and (3) promote deployment of these capabilities within the U.S. Government and allied nation ICT environments. Policymakers should also consider updating acquisition strategies and mechanisms around SDN and related technology-based services.

The complete list of recommendations is included in the *Recommendations section*.

Report Overview

Scoping and Charge

In September 2019, the Executive Office of the President (EOP) tasked the President's National Security Telecommunications Advisory Committee (NSTAC) with examining the implications of software-defined networking (SDN) on the Nation's national security and emergency preparedness (NS/EP) communications. As indicated in the 2017 *NSTAC Report to the President on Emerging Technologies Strategic Vision*,[6] the shift towards SDN began with the arrival of cloud computing, a technology that disrupted the traditional enterprise network architecture by providing on-demand, compute resources for hosting virtualized applications in globally distributed infrastructure.

In response to the EOP's request, the NSTAC examined best practices for SDN and related technologies; identified the associated challenges and opportunities; and assessed current utilization and corresponding risk mitigations. By building off the recommendations outlined in the 2017 *NSTAC Report to the President on Emerging Technologies Strategic Vision*, this study sought to make specific recommendations to the EOP regarding SDN policy by examining: (1) best practices for deploying SDN across federal networks and critical infrastructure; (2) how SDN can address risks posed to NS/EP communications and the information and communications technology (ICT) supply chain; and (3) methods to balance security and cost.

Subcommittee Process

The NSTAC used several research methods, including receiving subject matter expert (SME) briefings and reviewing reports and articles on SDN. The NSTAC heard from public sector, private sector, and academic experts on the emergence of SDN, how SDN is being deployed in networks including 5G, the security impacts of SDN and the potential for SDN to impact the future of the communications network supply chain and the impacts on NS/EP functions.

To this end, the NSTAC:

- Conducted bi-weekly meetings with the subcommittee members;
- Received 28 briefings from SMEs across private industry, academia, the analyst community, and the public sector;[7]
- Reviewed federal ICT policies, regulations, guidance, and reports; and
- Reviewed current industry best practices and relevant technology research.

Summary of Report Structure

The report is divided into the following areas:

- Overview of SDN: Provides background information on SDN, including architecture fundamentals, primary advantages, and typical challenges.
- SDN Deployment Scenarios: Describes the primary ways in which SDN has historically been deployed across ICT networks and forward-looking architectures such as virtualized Open Radio Access Networks (O-RAN), as well as laying the groundwork of fifth generation (5G) technologies and service-based architectures (SBA).
- SDN Security: Focuses on key security risks and mitigations, including supply chain considerations, as well as potential benefits of a properly designed and deployed SDN environment.
- The Role of Standards and Open Source Software: Outlines the intersection between standards driven and open source software development, as well as their relation to the ICT ecosystem, network functions virtualization (NFV), and 5G.
- Perspectives from the SDN Market Segments: Analyzes the primary market segments that SDN impacts, including telecommunications service providers; infrastructure/technology suppliers; cloud services; and end users/enterprises.

[6] President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on Emerging Technologies Strategic Vision*, July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

[7] Please refer to Appendix C, Briefers, for the full list of briefers.

- Impact on NS/EP Communications: Summarizes SDN's impact on NS/EP communications.
- Recommendations: Outlines the NSTAC's proposed recommendations, organized in the following manner:
  - Actions that could indirectly benefit the U.S. Government, including:
    - Accelerating SDN deployment across the ICT ecosystem;
    - Expanding participation in relevant standards bodies and working groups;
    - Increasing funding and education for SDN technologies and studies; and
    - Supporting greater information sharing on best practices for SDN deployment, with an emphasis on network security and resilience, open source development, and risk mitigation.
  - Actions that could directly benefit to the U.S. Government, including:
    - Reframing existing policies and procedures to accelerate the adoption and deployment of software-based network services, such as SDN;
    - Increasing U.S. workforce capabilities and scale across SDN and other new technologies;
    - Defining a consistent and clear risk-based approach to security, which includes SDN, NFV, cloud services, and other new technologies;
    - Leveraging synergies involved in the deployment of new technologies (e.g., SDN) to incorporate automation and enhanced security measures;
    - Applying secure and consistent lifecycle management practices across all software deployments, including those with open source; and
    - Increasing the level of engagement with suppliers of SDN and other new technologies.
- Conclusion: Highlights the report's key findings, concepts, and proposed next steps for wide-scale SDN adoption across industry and Government.

Overview of SDN

Background

SDN and NFV represent an ongoing shift in networking away from legacy technologies based upon hardware to software based networks that leverage more standard, commercial off-the-shelf (COTS), or commodity-based hardware. This shift is structurally transforming the ICT ecosystem and allowing networks to become more flexible, programmable and adaptive.[8]

Meanwhile, the number of devices connected to networks has been growing exponentially. Hardware-centric networks, as expressed through Moore's Law,[9] kept pace with demand during the pre internet (pre-2000) and early-internet stages (pre-2010); however, these networks became outdated post-2010. Today, applications or services—and even entire industries—can quickly rise and rapidly create new sources of network traffic. By re-architecting the network to be software-centric, network operators, enterprises, and other entities can build a platform that has the right agility and economics to outpace demand and quickly introduce new technology and services to customers.

Evolution of the Network

Telecommunications operators have traditionally built networks by interconnecting components that provide various network functions, including switches, routers, access nodes, multiplexors, and gateways. Most of these network functions were implemented as integrated and closed systems, such as unique hardware tightly-bundled with unique and inseparable software, along with a vendor-specific management and automation systems. For operational ease, network operators would often use one or two vendors for a given class of network components. Since most deployed network hardware components are amortized for many years, this creates vendor lock-in for both hardware and software, with limited options for upgrading as technology advances.

Over the last decade, network operators have moved from a hardware-centric network design methodology to one that is software-centric. In this new model, hardware consists of standardized and commoditized white boxes (e.g., standardized compute hardware). The network functions are implemented as virtualized software applications running without specific dependencies on the hosting white box hardware. Virtualization enables the same hardware to concurrently support multiple virtual network functions (VNF). Combining this software-based approach with virtualization technology and white box hardware allows network operators to efficiently scale their networks to match demand and ensure maximum usage of network resources. Moreover, each piece of hardware can be upgraded independently as server technology advances.

Figure 1 below illustrates this design shift where the modular hardware components are white boxes and the software applications are running within standard virtual machines.

[8] President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on Emerging Technologies Strategic Vision*, July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

[9] Moore's law is a 1965 observation made by Intel co-founder Gordon Moore that the number of transistors placed in an integrated circuit or chip doubles approximately every two years. Because Moore's observation has been frequently cited and used for research and development by multiple organizations, and it has been proven repeatedly, it is known as Moore's law. ("Moore's Law." Techopedia. Techopedia, June 14, 2012, https://www.techopedia.com/definition/2369/moores-law.)

Whitebox: Shift to Open & Flexible

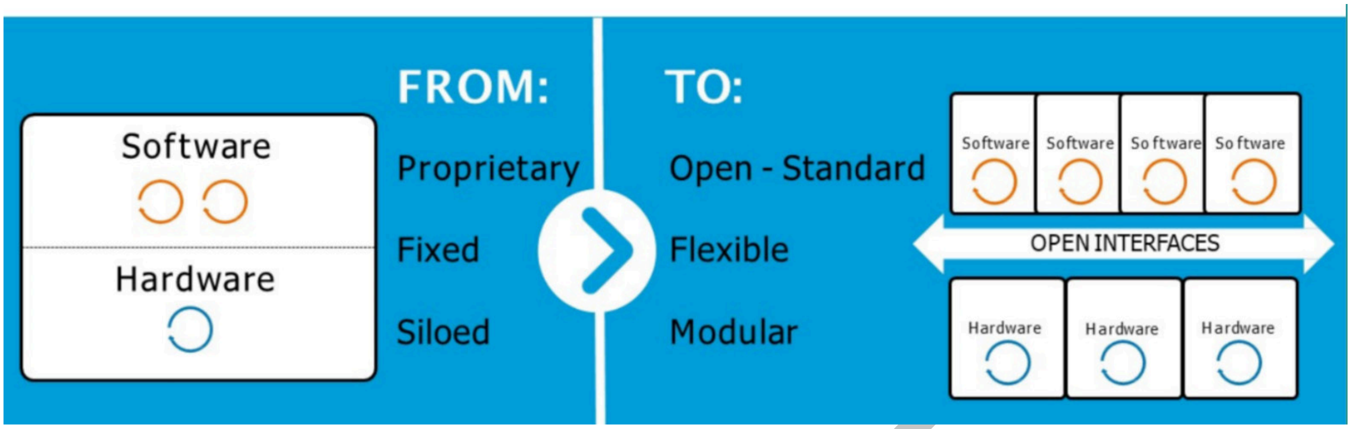
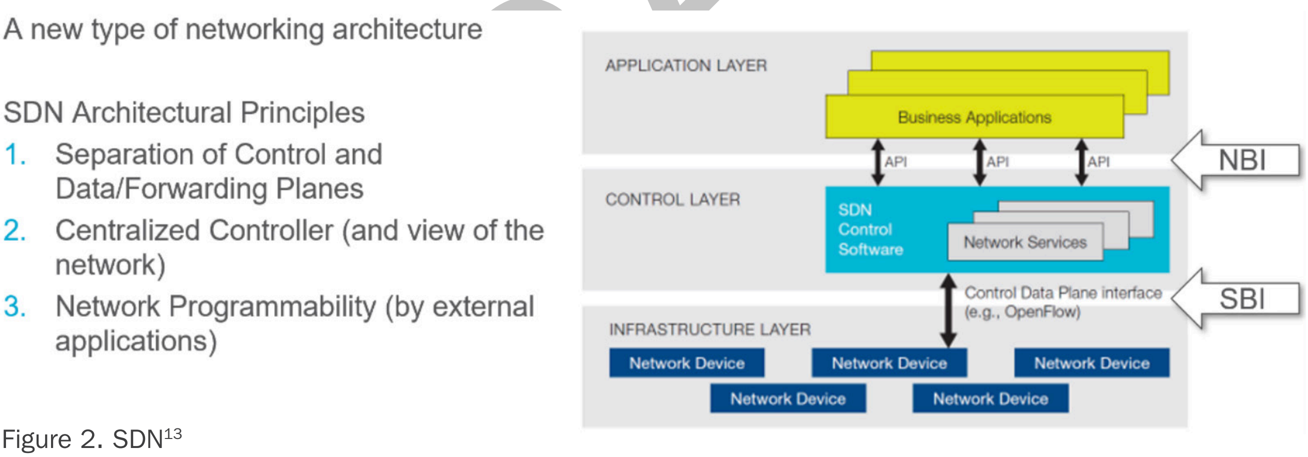


Figure 1. Whitebox: Shift to Open and Flexible[10]

Architectural Changes in Virtualized Networks

SDN and virtualization have transformed the ICT ecosystem by enabling networks to be more adaptive and cost-effective.[11] The core attribute of SDN is functional separation, which involves the decoupling of the network's control plane (i.e., the systems that configure the data plane) and data plane (i.e., the underlying systems that move traffic to the configured destination). These networks are built, operated, and managed by software.[12] The Figure 2 below illustrates this point.

SDN



A new type of networking architecture

SDN Architectural Principles

1. Separation of Control and Data/Forwarding Planes
2. Centralized Controller (and view of the network)
3. Network Programmability (by external applications)

Figure 2. SDN[13]

In addition to the separation of control and data, the centralization of the controller, more comprehensive views of the network, and enhanced network programmability through an application layer are the key architectural principles of SDN. The advances in cloud computing that began in the mid-2000s were fundamental to the exponential growth of SDN architecture and related services over the last 20 years.

[10] Alicia Abella, AT&T, "AT&T's Software-Defined Networking (SDN) Transformation" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, May 26, 2020).

[11] Adrian Belmonte Martin, Louis Marinos, Evangelos Rekleitis, George Spanoudakis, Nikolas Petroulakis. "Threat Landscape and Good Practice Guide for SDN/Fifth Generation (5G)," *The European Union Agency for Network and Information Security*, January 27, 2016, https://www.enisa.europa.eu/publications/sdn-threat-landscape.

[12] "NFV 101 Networking Foundations Guide." SDxCentral. https://www.sdxcentral.com/networking/nfv/definitions/nfv-101-networking-foundation-guide.

[13] Terry Bush, Ericsson, "NSTAC SDN Brief" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 28, 2020).

As SDN has enabled the separation of network functions from dedicated hardware, the nature of the network has transformed. In a software-defined environment, common network elements are centralized and exist in the cloud, which introduces flexibility and new efficiencies that surpass the limitations of hardware dedicated to specific functions. Before cloud computing, the traditional network consisted of hardware appliances dedicated to specific functions (e.g., web servers, routers, switches, email servers) placed on premise or in a data center. Moreover, appliances were deployed throughout the network in a decentralized manner. In this environment, enterprise information technology (IT) staff were responsible for procuring, configuring, and securing network equipment on an element-by-element basis and were often required to be physically present with the equipment during these procedures.[14]

Cloud computing disrupted the typical model for enterprise architecture. This approach aggregated hardware resources in large data centers to create an ecosystem where ICT infrastructure is centralized and virtualized. Currently, cloud providers offer a suite of services that allow users to remotely manage and configure all hardware and software assets, including the related networking components, using software application programming interfaces (API).

Modern networks can be created, altered, and dismantled virtually and remotely from a single location as software-centric designs rest on top of standard, COTS, or commodity-based hardware. The availability of these low-cost alternatives coupled with NFV make it possible for enterprise IT leaders to implement network changes in near real-time, reducing the need for a costly and time-intensive redeployment of physical infrastructure. SDN and NFV are core to most orchestration, data center network virtualization platforms, and software-defined wide-area network (SD-WAN) implementations.

The trajectory of SDN has evolved as basic ICT functional components continue to shift to a cloud-based environment, and from a physical cloud to a virtual one.[15] The benefits of this transformation must be considered in the context of growing enterprise and government demand for the multilayer optimization, openness, programmability, simplification, and automation provided by SDN.[16] The growth of SDN architectures is also occurring at a time where all vertical enterprises, in order to remain innovative and competitive, face enormous pressure to digitize core aspects of their business at ever-accelerating rates.[17]

The network operators' interest in SDN has been accompanied by key technology development and adoption trends, including the explosion of mobile, internet-connected devices (some estimate nearly 15 billion Internet of Things [IoT] devices by 2022) and the rapid adoption of cloud architectures in the data center delivering common compute, storage, and virtualization capabilities."[18, 19] Disaggregation has created an environment where vendors must now compete to provide both hardware and software applications that are independent of one another, and interoperable with other market offerings.

SDN Advantages

SDN's technology advantages are multi-faceted. SDN provides software centricity, fine-grained network policy, and enhanced visibility into the networking stack layers, which enhances network adaptation, automation and service deployment lifecycle. The following subsections will elaborate on SDN's primary technology advantages.

Infrastructure Benefits

SDN's disaggregation of network control from the network data plane frees operators from vendor specific solutions. The SDN architecture enables the networking control plane and data plan to leverage white box technologies and be realized via different

[14] NSTAC, *NSTAC Report to the President on Emerging Technologies Strategic Vision*, July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

[15] *Ibid*

[16] Anil Simlot, "Importance of SDN for a Service Provider" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

[17] David Ward, "SDN and Virtualization Technologies in Communication Networks to Thwart Cyber Threats and Improve Security" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 7, 2020).

[18] *Ibid*

[19] The Institute of Electrical and Electronics Engineers (IEEE). "Advancing SDNs: A Survey," IEEE, October 12, 2017, https://ieeexplore.ieee.org/document/8066287.

implementation approaches. The primary options include: (1) white box or COTS appliance hardware; (2) virtual routing and switching functions in virtual environments; and (3) software operating system (OS) networking stacks (e.g., open OS).

Given the multiple options for constructing an SDN data plane, network operators can select the optimal technology to meet both networking and hosting infrastructure requirements.

Networking Benefits

SDN provides several key technology advantages over traditional networking architectures, including:

- SDN's separation of control functions from forwarding functions with open API enables greater automation and programmability in the network in the areas of configuration, policy adaptation, monitoring, and troubleshooting.
- SDN technology can overlay onto multiple network infrastructure topologies, allowing it to be introduced in a measured way that incurs less risk and disruption to network operations.
- SDN allows an operator to use standard internet connections and unmanaged links to deliver service assurance on par with highly-managed network links implementing protocols such as Multiprotocol Label Switching (MPLS).
- SDN allows the policy-based isolation of network workloads (i.e., micro-segmentation). Micro-segmentation can be used for both service assurance and security countermeasures, as it improves service assurance through grouping and isolating traffic according to quality of service policy. With respect to security, micro-segmentation allows for isolation of malicious traffic and gives network operators greater control over server-to-server traffic.[20] If breaches occur, micro-segmentation can isolate applications or sessions, limiting lateral movement by malicious attackers.
- SDN technology allows multiple virtual routing and forwarding tables and virtual private networks (VPN) links to share a common transport infrastructure. This was not feasible with previous VPN technologies. Organizations with multiple business units and sites can isolate network traffic by establishing group-specific policies.
- SDN packet-forwarding controls enable significant flexibility compared to traditional networking controls. Network operators can programmatically modify, enrich, filter, or trigger policy actions on any header field. The range of forwarding policy actions contrasts with the limited scope of traditional routing, label switching router/MPLS, and other switching technologies.
- SDN's ability to operate over multiple transport links with application awareness and automated policy can improve network resiliency through:
  - Congestion mitigation by rebalancing traffic across available links in real-time;
  - Layer 2/Layer 3 fast failover; and
  - Expedited disaster recovery by re-purposing network capacity to most critical applications.

Network Administration Benefits

Inherent to SDN's architecture is the concept of centralized control, orchestration, and policy. These characteristics enable organizations to adopt and deploy network-wide policies in a manner that is simpler than traditional networking models. A benefit of consistent network and application performance is that it facilitates business continuity across varying network topologies.

The ability to efficiently deploy and enforce centralized security policy enables enterprises and agencies to homogenize their security postures throughout the network and move away from point solutions with disparate configurations. This capability is especially important as mobility and bring-your-own-device policies have enabled end-users to access and consume applications over multiple modalities.

[20] Gordon Moore, "Cramming More Components onto Integrated Circuits," Electronics, Volume 38, Number 8, April 19, 2965, http://www.monolithic3d.com/uploads/6/0/5/5/6055488/gordon_moore_1965_article.pdf.

SDN mandates strict adherence to programmatic APIs, which help enterprises and agencies orchestrate and automate functionality for configuration, software upgrades, and policy changes. This approach reduces the operational overhead for network administration and improves end-user experiences as zero touch provisioning reduces the need for onsite technical support. Zero-touch provisioning and automation are especially beneficial for multi-site enterprises as branch office deployment, management, and troubleshooting can be done remotely. Additionally, organizations can efficiently introduce new capabilities to a subset of users or sites to verify performance to improve the likelihood of a successful upgrade.

In the event of network issues, an SDN architecture affords full-stack insights to unlock a level of visibility that has been difficult to attain with fully integrated, proprietary solutions. If implemented correctly by skilled network operators, SDN minimizes the time to detect root cause and remediate network issues therefore raising the bar on the network service-level agreement.

Application Benefits

Primary application benefits include: (1) application-aware routing; and (2) application chaining.

Some SDN products have the capability to inspect traffic at Layer 7 in order to apply routing policies for specific applications. There are SDN technologies currently in production that can identify thousands of distinct applications and implement network policies in-line with the performance requirements of each application. These features help organizations optimize application performance at a more granular level by constantly monitoring latency, delay, jitter, and other characteristics in real-time, while also shifting to the most cost-effective transport method to meet performance thresholds.

Application chaining involves combining the capabilities of SDN with virtualization. It is the ability to dynamically insert or remove an application in the form of VNF into a service flow.[21] Virtualization enables the instantiation of the application, while SDN enables the connectivity of the application to the service flow. The timing of VNF insertion may be at the beginning of service creation or initiated by a trigger while the service is operating. This concept is especially powerful in the area of security. More specifically, a security event can trigger chaining for security applications (e.g., deep packet inspection [DPI], intrusion detection systems [IDS]/intrusion prevention systems [IPS], log/tap) into a service flow for deeper inspection and ultimate mitigation.

SDN Implementation Challenges

While SDN offers substantial benefits, there are also operational challenges that need to be addressed when transitioning network architectures to new technologies. Organizations must carefully architect networks, train staff, and build SDN deployment and operations expertise.

Organizations need to consider that vendor interoperability between transport, controller, and application domains has not been established. While not unique to SDN, interoperability will remain an issue until standards are developed around the new interfaces between platforms and technology stacks. Standards bodies and industry consortiums are in the early stages of driving standardization of SDN interfaces and APIs. Consequently, scaling SDN across networks and implementing different vendor technologies is not as easy today as it could be. SDNs can interoperate using both open APIs on either side, as well as leveraging existing networking technologies for communicating relevant metadata, technologies such as virtual local area networks (vLAN) tagging, MPLS, and Border Gateway Protocol. But deeper and more seamless integration is still a work in progress. The prevailing industry view is that SDN vendor interoperability will be challenging in the near to mid-term.[22, 23, 24]

[22] Andrew Gottlieb, Oracle, “Delivering Reliability and Quality of Experience with Failsafe Software-Defined Wide-Area Networks Technology” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 17, 2019).

[23] Roy Chua, AvidThink, “State of SDN 2019” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 19, 2019).

[24] Anil Simlot, “Importance of SDN for a Service Provider” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

The Government has a large number of legacy networks and devices, many of which implement protocols and features not widely deployed in the private sector. These networks may require SDN vendor customization and ultimately delay or inhibit SDN adoption in these network domains.

Organizations often deploy SDN in a virtualized environment which introduces operational complexities that are different when compared to traditional closed, hardware-based environments. Several notable complexities associated with virtualized environments include: impacts on performance and reliability; security due to multiple service layers and increased complexity; and infrastructure realized by a highly distributed supply chain.

Companies and agencies must be vigilant with respect to the SDN supply chain given the multi-vendor SDN environment. Organizations must scrutinize component supply chain risks and enact policies supporting frequent software updates to limit the impact of security attacks. To this end, processes will need to be adopted for acquisition and support of SDN solutions by deploying organizations.

There are far-reaching implications for organizations that leverage open source software as part of SDN adoption. In most scenarios open source community support of aging software versions expires faster than traditional vendor software support models. Organizations should carefully review open source support policies and adjust software upgrade frequency accordingly to avoid the risk of running software that is no longer receiving security patches or bug fixes. Additionally, organizations must establish processes for the comprehensive review of the dependencies between open source libraries and components before commissioning.

In consideration of the above and as part of any technology migration, an evolution of corporate security posture and software maintenance methodologies is strongly recommended in conjunction with the adoption of SDN technology.

SDN Deployment Scenarios

Several deployment scenarios and trends are transforming the implementation of networking products and communications hardware. These include cloud and edge computing, mobile access to office resources, wireless networking, and IoT.

Products are changing from fixed function, propriety, single purpose hardware devices to architectures with an increasing portion of built-in software running on commodity hardware. Some networking products are implemented completely in software and are intended to be deployed on virtual computing resources. Due to the changing nature of implementations and the greater complexity of modern networking scenarios, SDN adopters must gain a better understanding of the technology behind the solutions to achieve organizational goals.

This section outlines several representative scenarios involving SDN adoption by industry. It also discusses how the hardware and software implementing the solutions are changing, along with the implications that these changes have for adopters.

Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[25] Cloud service providers who maintain and enable access to computing resources for their customers have unique challenges associated with deploying resources that are solved by the application of SDN. For service providers, the cloud computing environment involves large-scale networks that must be reconfigured to address varying workloads. Through SDN, providers can more efficiently configure their networks for varying workloads that would be otherwise

[25] Timothy Grance and Peter Mell, “The National Institute of Standards and Technology [NIST] Definition of Cloud Computing,” *NIST Special Publication (SP) 800-145*, September 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

impossible at operational scale. For customers, SDN is used to provide flexible tools to configure connections between their virtual servers and to resources outside of the cloud service provider's data center. Each tenant in a shared cloud can create and destroy network access between virtual machines programmatically, enabling customers to have, for example, separate virtual networks for distinct traffic based on data sensitivity, testing versus production, and/or a need to access on-premise or internet-based resources.

Enterprise Wide-Area Networks

SDN can connect a company's headquarters, data centers, branch offices, and remote sites while optimizing the different network connections between them, such as MPLS and different internet service providers. Cloud providers with multiple data centers and a private network connecting them at high speeds can also use SDN to help their customers connect their own geographically-dispersed data centers through the cloud providers private network instead of the internet. SDN can be deployed incrementally or fully. For example, an organization may use SDN to handle traffic between data centers, but not route the traffic within them.

Edge Computing

Edge computing is a network architecture design where computing resources are deployed in the network near where the resources are consumed. The network edge is not a single point in the network topology. Rather, the edge consists of distributed micro data centers at increasingly closer points to the data sources such as regional hubs, mobile base stations, public cloud-onramp points, and the premises. With more devices generating data and new applications needing near real-time response rates from cloud services, there is a growing trend to move services close to the devices using the data. Large volumes of connected device data can be synthesized and aggregated without sending it to a central data center. Applications benefiting from the low latency provided by 5G technologies can be more responsive by using nearby compute services instead of communicating with a data center far away. As such, micro data centers are expected to proliferate. The flexibility that SDN affords can be used to more efficiently connect these data centers to wide-area networks and service chain the applications to accommodate varying data processing demands.

The deployment of edge computing, particularly in the context of 5G, is closely associated with IoT use cases. Scaling the number of IoT devices on the network depends on network access to the cloud to utilize machine learning and to process complex data handling. The networks to support these requirements have grown in complexity as volumes of devices, data and processing have accelerated. As edge compute is deployed in the context of production operational technology (OT) versus back office IT, the need to ensure the integrity and privacy of the data and devices become paramount. SDN and NFV technologies offer a practical approach to scaling the automation needed to support large volumes of connected devices securely.

NFV

Historically, network appliances were monolithic devices from a single vendor containing both hardware and software for a fixed function. Traffic was physically routed through the device, so it could perform its function. Currently, fixed function devices are being replaced by general computing platforms and software to virtualize network functions. NFV can be implemented with standalone general-purpose hardware hosting virtual machines or containers in a cloud environment. SDN controllers can route traffic through the virtual machine or container that implements the networking functionality to provide more flexibility at a lower cost. Additionally, SDN enables implementers to realize the full benefits of virtualized applications via flexible routing and connectivity to facilitate software-based application spin up/down, and elastic scaling, among other things.

SDN and 5G

SDN has been emerging in third generation (3G) and fourth generation (4G) core networks for several years. With the introduction of 5G, many of the same developments are now occurring in the radio access network (RAN). SDN is redefining the network architecture to support the requirements of the 5G ecosystem. Specifically, SDN will play a crucial role in the design of 5G wireless networks.[26] In particular, SDN will provide an intelligent architecture for network programmability, as well as the creation of multiple network hierarchies.[27]

As discussed in the 2019 *NSTAC Report to President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*,[28] SDN also has the potential to play a critical role in enabling the future wireless supply chain. In traditional wireless RAN deployments, vendors maintain key connections as proprietary, or closed interfaces. As such, a component from one vendor cannot interoperate with a component from another. Similarly, individual Evolved Node B (eNode B) network elements from one vendor have limited interoperability with eNode Bs from another vendor. This limited interoperability required operators to build networks with fully-integrated solutions from one vendor or another. Thus, while many operators use multiple RAN suppliers, operators typically needed to build with single vendor's equipment in any given geographic area.

There are developments underway to open and standardize the interfaces (e.g., O-RAN Alliance Telecom Infrastructure Project). This will allow different vendors to provide radio units, baseband units, and backhaul, and for network operators to shift to modular networks with different components and software sourced from different suppliers. This decoupling could enable more of the RAN to also shift to software and leverage virtualization.

One of the key other advantages of the deployment of SDN in the 5G ecosystem are the new security capabilities enabled by this architecture. 5G introduces the mobile edge that will embed various security capabilities including: (1) distributed denial-of-service (DDoS) detection and mitigation; (2) closed-loop security automation; and (3) edge virtual firewalls to protect the network and devices. 5G technology coupled with SDN enables rapidly adaptable and configurable security, as well as automates the detection and mitigation of threats targeted at users and networks from IoT devices.

The early deployment of SDN and NFV based solutions in the mobile packet core of the network have been used to reduce operational costs and improve speed to market by introducing easily managed and modified software-based components. As more and more components of the packet core become virtualized or containerized it becomes possible to create virtualized network slices that support more specialized use cases. For example, the 5G standard supports enhanced mobile broadband, which is a more robust, high speed version of the consumer experiences offered today. However, it also makes provisions for portions of the network to be configured to support ultra-reliable low latency communication connections suited to scenarios involving autonomously—or remotely—operated equipment or massive machine type communications to support scenarios involving large numbers of sensors deployment in a relative confined location. As operators look to build offerings to support more specialized industrial or public sector applications, software-based control of the network is a critical enabler to support the scalable and secure provisioning of these services.

SDN Security

Security Benefits

SDN provides network adaptability and orchestration to isolate, segment, and mitigate malicious traffic in real-time to limit the breadth of an attack. To fully take advantage of these capabilities, organizations should invest in training staff on SDN technology and dedicate resources to planning and advancing their networking and security goals leveraging methodologies such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and other relevant standards.

[26] Akram Hakiri and Pascal Berthou, "Leveraging SDN for the 5G Networks: Trends, Prospects, and Challenges," French National Center for Scientific Research-The Laboratory for Analysis and Architecture of Systems, https://arxiv.org/ftp/arxiv/papers/1506/1506.02876.pdf.

[27] SDxCentral Staff, "How 5G SDN Will Bolster Networks," SDxCentral, October 31, 2017, https://www.sdxcentral.com/5g/definitions/5g-sdn.

[28] NSTAC, *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, September 3, 2019, https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_0.pdf.

The list below enumerates several of SDN's primary security benefits. While some portion of the functionality may exist in traditional networks, SDN's real-time response capability enhances these capabilities.

- Centralized policy:
  - Homogenizes the security perimeter by way of universal policy across network domains; and
  - Facilitates real-time, network wide application of security policies.
- Fine grained policy and traffic control coupled with application awareness:
  - Enables network-wide monitoring of network and application behavior;
  - Enables the ability for precise application and session containment; and
  - Allows for policy based on application, service, and organization rather than physical configuration.
- Micro-segmentation:
  - Protects against lateral communications between servers (east-west) in contrast to traditional firewalls primarily offering north/south protection;
  - Decreases network attack surface through the implementation of secure zones and workload isolation; and
  - Enables the application of security policies to different segments and workflows (e.g., public facing versus sensitive government data versus IoT).
- Programmability and automation:
  - Facilitates automated responses to detected threats minimizing dwell time; and
  - Enables real-time traffic containment or re-routing to enforcement points or security services for deeper interrogation such as firewalls and intrusion and detection systems.
- Increased network visibility coupled with big data analytics:
  - Enables the detection of more sophisticated attack vectors;
  - Allows for machine learning and artificial intelligence (AI) to facilitate the detection of highly sophisticated and DDoS attacks and can adapt to new threats and network behavior models; and
  - Allows for security incidents to be more easily mapped to actionable intelligence via the real-time, programmable nature of SDN.
- Application chaining:
  - Enables real-time orchestration and scaling of security services such as:
    - IDS triggering DPI and IPS; and
    - Denial-of-service (DoS) attack triggering increased routing capacity scale-up to handle traffic volume.
- Zero-trust architecture (ZTA):
  - Ability to verify each access request to resources as though it originates from an uncontrolled network, improving security by:
  - Strongly authenticating every access request regardless of origin
  - Checking authorization against policy constraints
  - Inspecting for anomalies before granting access

Security Risks

SDN offers new capabilities to secure networks but also exposes new threat vectors that must be factored into the network security posture. The primary potential threat vectors associated with SDN are attacks on the:

- SDN controller/orchestrator;
- SDN data-plane;
- APIs;
- Communication channels between SDN devices and controller;
- Networking applications and services; and
- Underlying hardware.

Additionally, the SDN control and data planes most often run on shared network and compute infrastructure making physical separation and isolation from other workloads difficult. While micro-segmentation and virtualization offer containment capabilities, it must be noted that these capabilities are implemented in software as compared to traditional network equipment implementing varying levels of hardware-based separation. Consequently, this increases the risk of lateral movement across data streams, control streams, and applications in an SDN environment where the infrastructure is compromised.

Many of the traditional network threat vectors are valid against SDN implementations and cannot be ignored. For example, real-time attacks on the SDN data plane are envisioned to be similar to existing data plane attack vectors (e.g., DoS/DDoS). Moreover, threat vectors associated with virtualization infrastructure (e.g., OS, hypervisor) will exist in an SDN environment.

The security risks highlighted above are predominantly centered on SDN transport. There are broader supply chain security risks as part of SDN control that should also be considered. The disaggregation of the control plane from the data plane in the SDN architecture coupled with the openness of the interfaces expands the implementation options for SDN beyond traditional networking solutions. These include the following: (1) SDN componentry will be sourced from an ecosystem that is larger than traditional networking suppliers; (2) white box utilization opens the transport layer to independent vendor sourcing; and (3) SDN's software centricity likely increases the utilization of open source software in implementations.

Clearly, all the software based SDN security capabilities ultimately rely on hardware functioning as intended. While SDN white box hardware may be commodity in nature, its supply chain and a user's ability to rely on it gain additional significance in the context of critical infrastructure and NS/EP scenarios. Challenges noted by Mr. Stephen Hawkins, Computer Systems Researcher, Laboratory for Advanced Cybersecurity Research, included that SDN hardware and software came from unfamiliar vendors and the country of origin can be problematic.[29]

The above points contribute to increased supply chain risk for SDN implementations. However, there are multiple public and privately backed initiatives putting forward best practices for supply chain security that are relevant to SDN control including, but not limited to the:

- Federal Communications Commission (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) Advisory Committee reports;
- NIST *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*;
- Alliance of Telecommunications Industry Solutions (ATIS) 5G Supply Chain Working Group reports;
- The Department of Homeland Security (DHS) ICT Supply Chain Risk Management Task Force reports; and
- Third Generation Partnership Project (3GPP) Technical Specifications Group Service and System Aspects Working Group 3 – Security (SA3), which is responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols.

Subsequent sections of this report expand on these initiatives.

Security Mitigations

There are a variety of approaches to SDN security. Given the risks, it is critical that security controls are distributed and embedded throughout the network. Key security controls include identity and access management, data encryption, security scanning and vulnerability management and security monitoring the advanced threat analytics.[30] There are a variety of key components to an SDN security program including:[31]

- Industry compliance, ensuring the network remains compliant with 5G and other standards;
- Identity and access management on all access to network components with advanced capabilities such as multi-factor authentication and risk-based decision-making;

[29] Stephen Hawkins, Laboratory for Advanced Cybersecurity Research, "SDN" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 20).

[30] Rita Marty, "SDN Best Security Practices" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, May 26, 2020).

[31] *Ibid*.

- Continuous diagnostics and mitigation, which gathers information about the current state of the agencies' networks, including 5G networks;
- Network and system activity logs, which aggregate logs from network to provide real-time security posture data;
- Security information and event management, which collects security-centric information and uses it to identify potential attacks and refine access policies;
- Threat intelligence, which provides information about newly discovered attack vectors, vulnerabilities, malware and attacks;
- Secure communication using encryption to ensure confidentiality and integrity;
- DDoS protection against network and customers;
- Network controls such as access control, firewall, and proxy; and
- SDN-specific controls such as separation of data and control plane.

Security Standards

Standards work is a foundational component of security assurance, as it supplies guidance and frameworks that ensure security and privacy requirements are met consistently. For example, 3GPP standards have enabled mobile technology to be the fastest-scaling technology the world has ever seen. With investments and participation in developing global standards, U.S. communication services providers and their suppliers have enabled innovation at scale and made connectivity and devices available for consumers nationwide at affordable prices.

5G Security Best Practices

"To build secure systems it is important to take a holistic view and not only focus on individual parts in isolation. For example, interactions between user authentication, traffic encryption, mobility, overload situations, and network resilience aspects need to be considered together. It is also important to understand relevant risks and how to appropriately deal with them; threats need to be weighed against the cost of them materializing and the cost of applying countermeasures. This is what 3GPP does when developing the specifications that constitute the basis for the security of the 5G systems.

The holistic mindset is also manifested in the many organizations that are jointly developing the 5G system, each covering different aspects and/or focusing on specific parts. Relevant specifications and supporting studies and functions are produced by such organizations as the IETF, Groupe Speciale Mobile Association [GSMA], European Telecommunications Standards Institute NFV Working Group, and Open Network Automation Platform [ONAP], to mention a few."[32]

There are several key security considerations for examining the trustworthiness of a network that standards can bolster, including:

- **Product Capabilities**: Ensuring that security capabilities of the hardware and software align with minimum applicable requirements on an ongoing basis, including the integrity of the vendors' supply chain;
- **Context and deployment:** A context-aware analysis of network deployments, meaning that verification of secure configuration, the application of appropriate hardening according to how the product or solution is used, and awareness of the risks inherent in the specific environment the hardware and software is deployed; and
- **Operation**: Management of networks and operational security is significant but sometimes underemphasized. Human, organizational or process failures are still common causes for security and reliability incidents.

[32] Ericsson, "5G Security - Enabling a Trustworthy 5G System," January 8, 2020, https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security—enabling-a-trustworthy-5g-system.

In the long term, organizations should put additional focus on the need to protect networks over their entire lifecycle (i.e., security planning, evolving risk evaluation, and consistent adherence to best practice ways of working) and cover all phases of the supply cycle (e.g., development, operation, maintenance, and sustainability).

The 3GPP SA3 Working Group included several new security features in 5G specifications in response to previous vulnerabilities discovered in previous generations. Some of these features are optional and at the operator's discretion to implement. The GSMA is also working on security best practices for 5G and works closely with the 3GPP SA3 to fill any potential gaps in implementations. CSRIC reviewed and reported on 5G security in CSRIC VI and found that many of the optional security features should be mandatory to ensure networks are more secure. This also aligns with the findings in the GSMA. If operators align with the GSMA and the FCC CSRIC recommendations, the United States' 5G networks should be more secure than if they simply followed 3GPP specifications.

At the time of this report, the FCC CSRIC VII has chartered two working groups to look at 5G security. Working group 2 is working on vulnerabilities in the transition to 5G (commonly referred to as non-standalone 5G) and working group 3 is looking at vulnerabilities in 5G standalone networks. It is highly recommended that the findings of these working groups be considered as well.

The Role of Standards and Open Source Software

SDN Evolution

Widely considered to be a foundational element of SDN, the OpenFlow concept was developed by leading network researchers at multiple universities in 2008[33] and subsequently standardized in 2009 by the Open Networking Foundation, formed by several major companies in the telecommunications and information technology space. OpenFlow defines switch behavior (how to handle and forward network traffic) and standardizes the communication between SDN controllers and switches. At around the same time, cloud service providers were launching software-defined virtual networks for the commercial cloud.

Subsequently, the Linux Foundation initiated several projects (e.g., the Open Daylight Project)[34] and other entities to develop and support open source software instantiations of OpenFlow to form the basis of the SDN controllers. The Open Daylight Program focused on network programmability and automation. Today, the major global telecommunications providers have joined with other industry segments through the Linux Foundation to develop open source software to provide comprehensive provisioning, management, policy, and operational control of virtualized network and cloud services.

The Figure 3 below provides an abbreviated history of network evolution initiatives leading to the current state of SDN.

SDN Abbreviated History

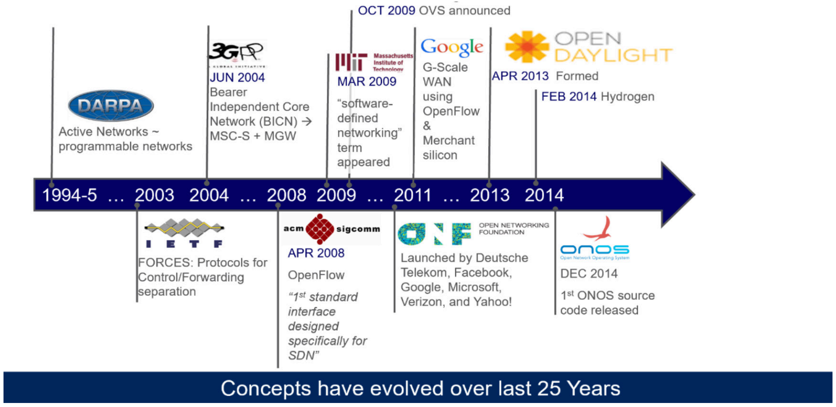

OCT 2009 OVS announced
DARPA
Active Networks ~ programmable networks
3GPP
JUN 2004
Bearer Independent Core Network (BICN) → MSC-S + MGW
Massachusetts Institute of Technology
MAR 2009
"software-defined networking" term appeared
Google
G-Scale WAN using OpenFlow & Merchant silicon
OPEN DAYLIGHT
APR 2013 Formed
FEB 2014 Hydrogen
1994-5 … 2003 2004 … 2008 2009 … 2011 … 2013 2014
IETF
FORCES: Protocols for Control/Forwarding separation
acm sigcomm
APR 2008
OpenFlow
"1st standard interface designed specifically for SDN"
ONF OPEN NETWORKING FOUNDATION
Launched by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo!
onos Open Network Operating System
DEC 2014
1st ONOS source code released
Concepts have evolved over last 25 Years

Figure 3. SDN Abbreviated History[35]

[35] Terry Bush, Ericsson, "NSTAC SDN Brief" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 28, 2020).

SDN's implementations and advancements have significantly benefited from open source initiatives. These benefits are not necessarily specific to SDN, but rather with the more the generalized benefits of leveraging open source projects with an active developer community. In particular, the following benefits are relevant to the advancements of SDN technology:

- An extended developer community on large open source projects results in accelerated development and deployment beyond what a single agency or company could achieve on their own;
- Cost savings are realized through cross-industry pooling of resources and contributions;
- Widespread deployment of open source creates faster solution hardening and establishment of best practices;
- Widespread deployment of open source can lead to the establishment of de facto standards; and

SD-WAN is a use case of SDN designed to provide connections between locations over wide areas with SDN controllers and switches. It can be deployed selectively over the connections between data center locations, pervasively within linked data centers themselves or some combination of the two. Most SD-WAN solutions use a combination of open source SDN code with vendor specific features. SD-WAN can lower the cost for organizations to connect data centers while also improving quality of services for networking dependent applications.

One of the challenges with SDN, specifically with the various SD-WAN platforms offered by a wide variety of vendors, is the need for new standards development to unlock cross-platform interoperability. The MEF (historically known as the Metro Ethernet Forum), was established as a in 2001 to standardize the services provided by carrier ethernet, and at the time of this report MEF had over 200 corporate members.[36] One area that MEF has focused on is standardization of services by SD-WAN vendors in their platforms, with publication in July 2019 of MEF-70, *SD-WAN Service Attributes and Services*,[37] and the recent MEF 3.0 *Global Services Framework*,[38] which includes SD-WAN, carrier ethernet, and other types of services, including security-on-demand. At the time of this report, several SD-WAN vendors[39] and service providers had achieved compliance certification to these standards. While certification of compliance with a standard does not guarantee that the technologies built to the standard will always be fully interoperable, MEF has a solid track record of working across industry to achieve positive outcomes.

With telecom providers leading the charge for more dynamic and open networks, there will continue to be widespread SDN adoption. Standards-based processes and interfaces help facilitate and maintain network connectivity between service providers. Adhering to common or standardized APIs, such as those defined in MEF's Lifecycle Service Orchestration,[40] helps enable real-time orchestration of on demand connectivity setup, control and monitoring across diverse multi-layer, multi-vendor, multi carrier networks.

NFV

The move to a software-based construct requires disaggregation of the telecommunications hardware and software and enables a high degree of operational automation. In 2017, more than 50 of the largest network and cloud operators representing 70 percent of the world's mobile subscribers, including from China, formed the Open Network Administration Platform (ONAP) project to deliver an open, standards driven architecture and implementation platform.[41] ONAP seeks to rapidly instantiate and automate new services and support complete lifecycle management of these

[36] "Members." Metro Ethernet Forum (MEF). MEF, 2020, http://www.mef.net/about-us/members-listing.

[37] "MEF 70: Software Defined-Wide Area Networks (SDN-WAN) Service Attributes and Services." MEF. MEF, April 2019, http://www.mef.net/resources/technical-specifications.

[38] MEF 3.0 Overview." MEF. MEF, 2020, http://www.mef.net/mef30/overview.

[39] "Services Certification Registry." MEF. MEF, 2020, http://www.mef.net/certification/services-certification-registry.

[40] MEF Lifecycle Services Orchestration (LSO) enables service providers to transition from a silo-structured business support systems/operation support system approach towards flexible end-to-end orchestration that unleashes the value of SDN and NFV. ("LSO." MEF, MEF, https://www.mef.net/lso/lifecycle-service-orchestration).

[41] The Linux Foundation Project, "Open Network Automation Platform," https://www.onap.org/about.

software-based VNF. As a result, operators can leverage their existing network investments while accelerating the development of a vibrant VNF ecosystem.[42]

ONAP enables several key capabilities including: (1) independent management of applications, networking, and physical infrastructure; (2) a service creation environment that is not limited by a fixed underlying network or compute infrastructure; (3) the automatic instantiation and scaling of components based on real-time usage; (4) the efficient reuse of modular application logic; (5) automatic configuration of network connectivity via SDN; and (6) user definable services.

In traditional wireless RAN deployments, vendors maintain key connections as proprietary and closed interfaces. This required network operators to build networks with fully integrated solutions from a single vendor. Thus, while many operators use multiple RAN suppliers, the operators typically needed to build with single vendor's equipment in any given geographic area.

These same developments are now occurring in the radio access portion of the network led by the O-RAN Alliance and other similar developments such as the Telecom Infrastructure Project. The O-RAN Alliance, is focused on the virtualization and standardization of interfaces in the 5G wireless infrastructure, working with ONAP in the core. Driven by major wireless carriers and IT companies worldwide, this effort will decouple the hardware portions of the RAN from the software portions and allow interchangeability of all the components within the infrastructure, breaking the vendor lock in business model common to the wireless industry, spurring innovation and competition, while speeding the introduction of new capabilities and services. This would allow different vendors to provide radio units, baseband units, and backhaul, and for network operators to shift to modular networks with different components and software sourced from different suppliers. This does not mean that all network functions must be virtualized, but it starts the process of introducing the same concepts being deployed in core networks to the RAN and therefore it is anticipated that a similar shift will occur. As of May 2020, O-RAN consists of 24 network operators and over 140 suppliers.[44]

Virtual RAN (vRAN) or cloud-RAN moves the controller functions of traditional base stations to servers at a central location, closer to the data center edge of the network. Using vRAN, operators can pool or adjust radio resources to better address the data traffic needs of application and IoT use cases. vRAN separates network functions from the underlying hardware, making the RAN environment more flexible and dynamic.

5G

The Nation's largest telecommunication service providers are heavily involved in the creation of global standards which are the underpinning of the framework that allows the global telecommunications infrastructure to operate across many disparate countries and thousands of service providers. The global standards bodies include the International Telecommunications Union (ITU), operating under the auspices of the United Nations, as well as diverse organizations such as the International Standards Organization, the Internet Engineering Task Force (IETF), the Internet Society, the International Committee for the Assignment of Names and Numbers, the Institute of Electrical and Electronic Engineers (IEEE), the World Wide Web Consortium, the Open Group, and in particular for cellular communications, the 3GPP. Currently focused on 5G, the 3GPP is a consortium of seven regional standards bodies who work in collaboration to define global standards for each generation of wireless to achieve global interoperability. The structure is designed to assure that no single region can dominate in the definition of future standards.

The U.S.-based standards organizations include the Alliance for Telecommunications Industry Solutions, which also serves as the North American regional partner in the 3GPP, the American National Standards

[42] *Ibid*.

[43] Iain Morris, "The Future's Bright, the Future's Open Radio Access Networks (O-RAN)," LightReading, June 28, 2018, https://www.lightreading.com/mobile/fronthaul-c-ran/the-futures-bright-the-futures-O-RAN/d/d-id/744294.

[44] "Membership Information." O-RAN Alliance, https://www.o-ran.org/membership.

Institute. Within the United States Government, the entities involved include NIST, as well as the National Telecommunications and Information Administration (NTIA) and the FCC, which manage and allocate radio frequency spectrum within government and the commercial sector respectively.

Perspectives from the SDN Market Segments

Telecommunication Service Providers

Telecom providers are moving rapidly to a core infrastructure supporting end point and enterprise services based on SDN, given the significant performance, security, and cost advantages of virtualization. Customers demand flexibility, self-service, and ease of use. SDN with edge computing, cloud, and network virtualization provide the technologies to meet those demands. There are several best practices for telecommunications providers to benefit from SDN and minimize risks, including: striving for simplicity and creating well-formed policies, roles, rules, and processes for network administration. Likewise, telecom providers should leverage the SDN scaled infrastructure to manage and audit changes, as well as provide transparency. From a customer perspective, the largest growth area to date in SDN has been the provision of SD-WAN services to enterprise customers large and small. Many experts regard SD-WAN as the most significant aspect of the trend to SDN, given its ability to provide flexible, secure, and reliable network services to all types of enterprise customers, including integrated access to cloud-based services. Many of the expert briefings provided to the NSTAC discussed the cutting-edge security features in the various SD-WAN products available in the marketplace, along with their other advanced capabilities.

SDN, NFV, and associated technologies like SD-WAN, have the potential to transform the service provider industry. These technologies can provide telecommunications providers with flexibility, ease of use, and newer capabilities.

A major component within this global trend is the move to open standards-based software for transport as well as service provisioning and management, running largely on generic hardware platforms that can assume the function that the software tells them to. SDN will enable a self-optimizing, resilient and secure global network infrastructure that can dynamically adapt to changing requirements and new applications, and rapidly provision new services, all with considerable savings over a traditional, hardware-based approach. This is particularly true in the deployment of 5G wireless infrastructure, where SDN and virtualization coupled with the use of open standards-based software will enable the rapid introduction of new applications and services, as well as spur innovation. This is a significant advantage as 5G will continue to evolve over the next several years as 3GPP releases functionality to the 5G baseline.

In considering the national security implications of SDN, many of the large, global Tier 1 carriers have already virtualized major portions and functions in their core networks. This trend is accelerating and migrating towards the RAN with the deployment of 5G wireless capabilities. For example, AT&T has announced that 75 percent of their core network capability will be virtualized by the end of 2020.[45] CenturyLink stated

SDN, NFV, and the Pandemic Response

A primary example of where SDN and NFV is in use today is in response to the coronavirus (COVID-19) worldwide pandemic. Service providers are challenged to meet the global network demands for more call processing, higher internet usage, and increased streaming as a result of this global pandemic. The flexibility and scalability of SDN and NFV allowed telecom providers to make rapid and dynamic changes to their wireline network in order to meet these demands.

[45] Mike Robuck, “AT&T on Target for Virtualizing 75% of its Network by 2020,” Fierce Telecom, January 3, 2020, https://www.fiercetelecom.com/telecom/at-t-target-for-virtualizing-75-its-network-by-2020.

that it is constantly evaluating and adding network infrastructure that can be virtualized to improve speed of capacity augmentations, and it now has 100 percent of its network under SDN control.[46] Its focus has been more on the benefit of quick service delivery and thus, it has focused on getting all network elements under software control to allow it to provision services faster and more efficiently.

On the wireless front, AT&T currently offers sub-6 5G service to 179 million people across 355 geographically-diverse markets. The company plans to support nationwide in 2020 and is offering 5G over millimeter wave spectrum in arts of 35 cities across the United States.[47] AT&T is also a founding member and the current chair of the O-RAN Alliance, which is developing O-RAN specifications for hardware and software components, and code, so that equipment and apps from different suppliers can work together. AT&T currently has several demonstrations and trials underway with companies such as Commscope, Intel, and Samsung. Dish Network, which has become the newest national wireless carrier with the closing of the T-Mobile/Sprint merger, has announced its plan to build an all virtual infrastructure, based on open standards and open-source software.[48] Similarly in Japan, Rakuten is in the process of deploying out a mobile network using cloud-based software and commoditized hardware instead of proprietary equipment.[49]

In addition, as part of their SDN virtualization strategies, major telecommunication providers are integrating public and private cloud-based services into their networks, both as part of their network services offered to end users and enterprises, as well as implementing appropriate portions of their SD-based capabilities in the cloud, moving away from the traditional host/dedicated server-based approach for network provisioning and management software. Containerization of the cloud-based services is being implemented to increase reliability and security.

These same developments are now occurring in the radio access portion of the network. This is a natural extension of the efforts around core networks. Further, as discussed in the *NSTAC Report to President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*, these developments may provide an option to address supply chain concerns by driving the industry toward a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry for new entrants in the marketplace.

Telecom Infrastructure Technology Providers and Developers

Since 2000, there has been a significant consolidation of the global market of telecommunications equipment suppliers, particularly in the radio infrastructure space. However, as wireless communications have become an integral part of the global network infrastructure, the difference between wired and wireless suppliers has been gradually disappearing. In fact, open global standards such as defined by 3GPP, a modular and standardized building practice has enabled an unprecedented degree of original equipment manufacturer (OEM) interchangeability. Today, 95 percent of all networks use multiple vendors, with frequent disruption and OEM swaps throughout lifecycles and service offerings. 5G will continue to evolve towards more open architectures, even within the various subsystems, enabling new entrants to address certain emerging product segments. Additional suppliers provide different elements of core network equipment, and evolving innovations in open and interoperable networking and virtualization will allow new participants to compete with established global suppliers.

The United States led the development of 4G technology and reaped the economic benefits, including $475 billion to Gross Domestic Product and 4 million jobs.[50] 5G will accelerate innovation and deliver even more transformative benefits to consumers and businesses alike with an estimated $500 billion to the U.S. economy and creating 3 million new jobs.[51] Technology will seek to capture the market segmentation value created by 5G networks in the future. Virtualization and SDN will be key drivers in this

[46] Anil Simlot, "Importance of SDN for a Service Provider" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

[47] "5G for You." AT&T. AT&T, 2020, https://about.att.com/pages/5G.

[48] Matt Kapko, "Dish Firm on 5G Costs," SDxCentral, February 20, 2020, https://www.sdxcentral.com/articles/news/dish-firm-on-5g-costs/2020/02/.

[49] Rakuten, "A World First for 5G: Rakuten Mobile and NEC Deploy Groundbreaking Radios for New 5G Network," Rakuten, April 9, 2020, https://rakuten.today/blog/rakuten-mobile-partner-profile-nec.html.

technology shift, due to several market-driven factors, and infrastructure and technology providers have shifted their research and development and delivery models accordingly.

Mobile broadband services to smartphones has dominated service and business models, with a high degree of the value and growth concentrated at the device and application ends. Using a universal service approach, as opposed to individualized slices of network services, for future use cases would significantly limit the economic return potential of 5G as an overall ecosystem.

Most industries need tailored network capabilities and business models to reach their end-users, customers, and partners. This has triggered the need for private SDN-based networks such as SD-WAN, along with private mobile network builds including network slicing alternatives that serve the same need. Infrastructure and technology providers have had to adapt accordingly, with more responsive build cycles and lifecycle management that encompasses diverse options, rather than a single line offering.

The introduction of a broad spectrum of new devices will require organizations to rethink their connectivity, risk profiles, and business models. With IoT and digital transformation moving into the industrial space, a plethora of new device types with less homogeneity than today's personal computers and smartphones will be connected with new and broader sets of applications. These will be not just internet-based applications and content, but rather real-time, mission-critical, industrial control systems and Supervisory Control and Data Acquisition platforms. Future actions to reduce risk across infrastructure, whether in the form of standards, incentives, or regulatory requirements should take the shifting device ecosystem into account. While further actions remain, several initiatives have begun the process to address this concern, namely the European Union Agency for Cybersecurity's Baseline Security Recommendations for *IoT*;[52] the United Kingdom's *Code of Practice for Consumer IoT Security*;[53] California Bill Number 327;[54] CTIA – The Wireless Industry Association's cybersecurity certification program for cellular0connected IoT devices;[55] and several NIST cybersecurity publications, including NIST Interagency/ Internal Reports 8259[56] and 8228.[57]

Zero-trust is a prevailing security concept that shifts security posture from an implicit trust model to an explicit trust model. Traditionally network traffic within a security perimeter was considered trusted and not subject to strict security policy. ZTAs treat "inside" and "outside' traffic similarly with the stipulation that all traffic is considered untrusted until verified.

ZTA

ZTA provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. ZTA is an enterprise's cybersecurity plan that utilizes zero-trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero-trust architecture plan.[58]

All users, devices (including device identity and hygiene) and services must be validated irrespective of how they attach to a network before network access or access to data is granted. This concept aligns well with 5G's core architecture and virtualized infrastructure, which stipulates that all network functions are required to authenticate per 3GPP.

[50] CTIA - The Wireless Industry Association, "U.S. Wireless Industry Contributes $475 Billion Annually to America's Economy and Supports 4.7 Million Jobs, According to New Report," CTIA, April 5, 2018, https://www.ctia.org/news/study-reveals-powerful-economic-impact-of-wireless-across-50-states.

[51] *Ibid*.

Unlike previous network transitions that were more like upgrades, 5G is a new and different technology and network architecture, designed with virtualization and cloud-based technology in mind. When fully deployed, 5G will be virtualized across a SBA, meaning that the core network functions will happen through a cloud-based and SDN. This will allow tailored security solutions such as network slicing for different network functions and private networks, which can significantly enhance network security, real-time network defense and improved elasticity. 5G will also allow for more finer grained data access control, topology obfuscation between network segments (and between operators), greater requirements on inter-element encryption, provisions for extended authentication, and enhanced privacy protections for subscribers, among other new capabilities, adding to more resilient, secure, and trustworthy networks.

With cloud-based technologies, software execution can be disconnected from specific physical hardware due to SDN and NFV. SDN offers flexibility in how to configure the routing paths between dynamically configured virtualized network functions. The introduction of AI and increasingly powerful computers, together with cloud technologies, will become a key driver of automation technologies. Consequently, the dominant tendency in these technology trends is already resulting in telecom networks becoming increasingly software driven. Distributed cloud computing makes it possible to create partitioning for better resilience and latency. From a security perspective, the distributed cloud may introduce new attack vectors against the 5G network if security is not built in. On the other hand, placing security functionality and mitigation mechanisms close to the attack source may isolate an attack to a local area. In an SBA, the different functionalities of a network entity are presented as services offered on-demand to other network entities.

The use of an SBA has, among other things, emphasized protection of the communication between core network entities at the Internet Protocol (IP) layer (typically by IP security). 5G core network functions support security protocols like Transport Layer Security (TLS) 1.2 and 1.3 to protect transport layer and OAuth 2.0 at the application layer to ensure that only authorized network functions are granted access to a service offered by another function. Improvements to interconnect security (between different operator networks) is also stipulated in 3GPP SA3 via three building blocks:

- Security edge protection proxy (SEPP) is being introduced in the 5G architecture. All signaling traffic across operator networks is expected to transit through SEPPs;
- Authentication between SEPPs will be required. This enables effective filtering of traffic coming from the interconnect; and
- A new application layer security solution on the N32 interface between the SEPPs is designed to provide protection of sensitive data attributes while still allowing mediation services throughout the interconnect.

Virtualized networks can provide improvements in dynamic services, the speed of rollout, network resiliency, and cost/performance benefits. However, a virtualized infrastructure also can consist of a highly distributed supply chain, with multiple functional layers

[52] European Union Agency for Cybersecurity (ENISA), “Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures,” ENISA, November 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[53] Department for Digital, Culture, Media, and Sport, “Code of Practice for Consumer IoT Security.” Gov.UK, October 2018, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

[54] California Senate Bill Number 327-Chapter 886, “An Act to add Title 1.81.26 (Commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, Relating to Information Privacy,” California Legislative Information, September 28, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[55] CTIA-The Wireless Industry Association, “Wireless Industry Announces New Cybersecurity Certification Program for Cellular-Connected IoT Devices,” CTIA, August 21, 2018, https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program.

[56] Michael Fagan, Katerina Megas, Karen Scarfone, Matthew Smith, “Foundational Cybersecurity Activities for IoT Device Manufacturers,” NIST, May 2020, https://csrc.nist.gov/publications/detail/nistir/8259/final.

[57] Kaitlin Boeckl, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina Megas, Ellen Nadeau, Ben Piccarreta, Danna Gabel O’Rourke, Karen Scarfone, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” NIST, June 2019, https://csrc.nist.gov/publications/detail/nistir/8228/final.

[58] Oliver Borchert, Sean Connelly, Stu Mitchell, Scott Rose, “Zero Trust Architecture,” NIST Special Publication 800-207, February 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.

to deliver a service, creating potential complexity in operations and lifecycle management. Virtualized networks can provide a similar level of security, as compared to coupled hardware/software, given that certain best practices and controls are followed, but the inherent complexity of an implementation can make this more arduous.

Utilizing SDN as part of a virtualized, 4G/5G network will be common for many implementations, due to the need for centralized orchestration and automation of services. The flow-based nature of SDN (separating the data channel into multiple flows and layers) compliments classic perimeter security model thinking and works well for virtualized security functions in service chaining. It also allows for dynamic and flexible security policy adjustments and resilience of network management if individual data planes are disrupted. However, the SDN controller is also a single point of compromise or failure and this must be considered in widely distributed architectures especially. North-bound interfaces must be monitored for malicious applications that are outside of the protected control layer and south-bound interfaces must have protected communication paths between the controller and switches.

Telecommunications infrastructure is advancing at a rapid pace and the use of virtualization and SDN will continue to expand and evolve. While standards will help enforce a baseline level of security, the collaborative efforts of infrastructure providers, technology developers, service providers and government entities will continue to lead the way in setting best practice examples for secure and high-integrity deployments.

Cloud Service Providers

From its earliest days, cloud computing has played an important role in the evolution of modern networking. All of the elements of the definition of cloud computing, as captured in the early and influential NIST definition, have had their influence.[59] For example, the on-demand service and broad network access aspects of cloud led to a common design pattern of APIs as well as human-oriented graphical consoles that are fully accessible on the Internet, with no intervening network barriers. Thus, to this day, many aspects of a modern cloud platform embody the core concept of a ZTA. None of the relevant security controls for many abstract services are related to network boundaries, perimeters, or firewalls. Even cloud services that are fully available on the internet may nevertheless have network-related controls for defense in depth. For example, many such services can be configured such that even a properly authenticated and authorized request must have a source network address that matches a specified address or range.

At the same time, early in the development of Infrastructure as-a-Service (IaaS) platforms, a key enabling element was the ability to host common OS such as Linux and Microsoft Windows. Splitting workloads belonging to different customers provided rapid elasticity using resource pooling of servers and virtual machine technology to provide customers with isolation and control. But server isolation alone was not enough; customers also demanded isolated networking as well, not only for its security properties, but also to allow easy Layer 3/4 connectivity to private enterprise and government networks. Industry standards for virtual networks at the time, such as IEEE 802.1Q vLANs and proprietary virtual routing and forwarding features of routers, were completely inadequate to the task of building up vast numbers of virtual networks and being able to create and configure them in seconds, if not milliseconds. In addition, traditional physical networks allowed for various insecure practices like Address Resolution Protocol spoofing, and cloud networks needed much stronger security and isolation properties. Traditional networks also lacked the metering and billing features required for measured service elements of the cloud.

As a result, cloud providers invented and deployed their own SDNs around their virtual machine (and related) compute services. That approach fully virtualized the network, provided strong security properties and isolation controls, and could be deployed, configured,

[59]The five elements are (1) on-demand service; (2) broad network access, (3) resource pooling, (4) rapid elasticity, and (5) measured service. (Timothy Grance and Peter Mell, "NIST Definition of Cloud Computing," NIST SP 800-145, September 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.)

and reconfigured in seconds via API calls. These SDNs can scale to tens if not hundreds of thousands of virtual networks overlaying the same physical network in a single datacenter. They also put the intelligence for network deployment and configuration in large scale distributed software systems, allowing the underlying physical network to be fast and less complex. Seeing the success of these technologies in the cloud, vendors of on-premises virtualization software soon added end-to-end virtual networking and virtual-physical gateways to their offerings, allowing customers to deploy similar kinds of SDN technology outside the cloud as well.

With the virtual network's intelligence implemented, managed, and automated in software, control plane demands exceeded the capabilities of traditional network equipment. The control planes of traditional equipment lacked the performance to service hundreds if not thousands of API calls per second, each changing the configuration of the device, which subsequently overwhelmed traditional network equipment and ultimately limited a network operator's ability to take full advantage of SDN. Cloud providers prioritized a flexible operational model that leveraged software programmable low-cost generic white box hardware over more costly, dedicated hardware solutions. As a cascading effect of their pioneering work in SDN, cloud providers began to develop their own networking equipment. They helped create a competitive market for fast and simple packet-processing application specific integrated circuits (ASIC), and a competitive market for simple switch/router chassis from original device manufacturers. Organizations only needed to develop and deploy OS and network management software, and often such software was available on an open-source basis. This has led to a highly dynamic, competitive market for commoditized networking gear, much like the market for data center servers.

As in cloud, software-defined networks had to be connected to more traditional networks. A variety of existing and emerging technologies were deployed to meet the need. Organizations first utilized traditional VPNs; however, this technology lacked the programmability and dynamic capabilities of a modern SDN. Therefore, customers and telecommunications companies provisioned MPLS networks to cloud provider "meet me" points for cross-connect to the cloud edge with product offerings like Amazon Web Service's Direct Connect, Microsoft Azure's ExpressRoute, and Oracle Cloud's FastConnect. Still, the customer-facing side of those offerings was manually deployed, and provisioning times could be measured in weeks or even months. More recently, the increasingly broad adoption of SDN technology outside the cloud by telecommunications companies and customers alike now enables an end-to-end dynamic, software-defined connectivity with features like near-instantaneous deployments, dynamic bandwidth allocation, and pay-as-you-go pricing, with resulting efficiencies and economies of scale. SDN capabilities and services outside the cloud provide benefit back to the cloud providers and their customers by allowing cloud workloads to be quickly stitched together with the broader IT and networking ecosystem with the simple pay-as-you-go contract and a few API calls.

End Users/Enterprises

The key end users for the scope of this report, and in the context of NS/EP communications, are the 16 critical infrastructure sectors as considered by DHS.[60] For these end users/enterprises, their primary needs for SDN will be for higher performance, more secure and robust edge devices (e.g., sensors), mobile communications and computing, and industrial control devices. Higher performance will be delivered by SDN's ability to create adaptive networks designed for their specific purpose bringing typically lower latencies. Organizations can deliver security improvements by creating custom protocols designed for their intended purpose and network slices that reduce the attack surface and provide specific security features desired for the intended purpose (e.g., encryption, authentication, auditing). Robustness will be improved for these sectors through SDN's features for proximity services networking and other mesh topologies, network slicing to reduce denial of service conflicts, and the ability to rapidly stand up alternative communication channels.

[60] "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency (CISA), last modified March 24, 2020, https://www.cisa.gov/critical-infrastructure-sectors.

Impact on NS/EP Communications

Given the many significant performance and cost advantages of SDN, deployment throughout the global ICT infrastructure is happening at a rapid pace, and it presents major benefits for NS/EP functions. The efficiencies and ability to deploy capacity on demand leveraging a cloud like architecture provide a level of flexibility bit available in legacy, hardware centric networks, and will enable network operators to better respond to NS/EP incidents. These have been demonstrated in real-time across the service providers in response to the COVID-19 pandemic as demand for bandwidth and cloud services at the edge and in the core increases to support the needs of first responders, the healthcare/medical community, distance learning, business continuity, and telework in both the public and private sectors. However, like any new capability, SDN presents challenges in maintaining security and minimizing risk. SDN introduces a more complex network architecture which requires a degree of expertise to manage and ensure security. However, existing proof points show that these are being actively addressed through careful planning and well-defined processes, coupled with increasing maturity and experience in deployment and operations management.

Recommendations

A summary of the NSTAC's recommendations is bulletized below, followed by the detailed recommendations that the NSTAC proposes regarding SDN's implications on the Government's NS/EP functions.

SDN Related Technology

"SDN related technology" includes 5G, cloud, NFV, mobile edge computing, ZTA, machine learning/AI, and automation in ways that enhance, support, or complement SDN. Over time, the list of technologies could increase or decrease as new innovations are developed

- The Administration should encourage and support the continued deployment of SDN technology in the U.S. and allied nation ICT environments. Policymakers should consider how to promote the use of open architectures with particular focus on 5G and beyond.
- The Defense Community and the Intelligence Community (IC) should expand efforts to define their specific requirements and use cases for SDN and related technology, which can be shared with private sector SDN providers and relevant standards bodies. In collaboration with the private sector, the Defense Community and IC should also determine how the capabilities might be leveraged for adoption in the national security environment.
- The Government should establish policies to help educate U.S. departments and agencies (D/A) and critical infrastructure operators on the full range of SDN and related technology capabilities to enhance their mission performance, improve security, and lower costs.
- Working with Congress, the Administration should: (1) establish policies and incentives to encourage U.S.-based investment, innovation, and research and development in SDN and related technology capabilities and standards; (2) encourage best practices for secure implementation; and (3) promote deployment within the U.S. Government and allied nation ICT environments. Policymakers should also consider updating acquisition strategies and mechanisms around SDN and related technology-based services.

The following activities could indirectly benefit the U.S. Government by advancing ICT, talent capacity building, and security. Specifically, the Federal Government should:

1. Encourage the global ICT industry and the U.S-based telecommunications service providers, to accelerate the rate of secure SDN and related technology deployment while assuring that the United States' NS/EP functions is enhanced.
2. Expand Federal Government participation in global standards bodies working in conjunction and support of the U.S. private sector for SDN and related technology (e.g., NIST, NTIA, Department of Defense, Department of State).

3. Promote open markets for U.S. developed ICT technology. Reinforcing its participation in global standards bodies, the U.S. should argue against country-specific standards that serve as barriers to market entry. As part of that process, the U.S. needs to be judicious when asserting that national security interests justify deviating from global standards, and it needs to be reasonably transparent about its rationale for any such deviations.

4. Increase funding for federal research and development in advanced and secure SDN and related technology. This should include: (1) funding for Federally Funded Research and Development Centers to perform testing of SDN and related technology; and (2) consideration of an exemplar network across multiple carriers providing a communications channel for critical infrastructure providers to communicate securely and resiliently with DHS' Cybersecurity and Infrastructure Security Agency (CISA).

5. Continue to expand efforts in science, technology, engineering, and mathematics education for qualified students in the United States and in allied nations to follow through on the education efforts called for in the 2018 *NSTAC Report to the President on a Cybersecurity Moonshot*.

6. Provide tax incentives to expand private sector investment in ICT standards, research, development, and deployment. The scope of deployment should include modernizing existing infrastructure and reaching underserved communities (e.g., building out rural networks so SDN and related technology benefits can be realized).

7. Expand efforts to partner with the private sector in providing security advice and guidance on emerging ICT technical capabilities and services, including, at the discretion of companies, collaborative open-source code review and red teaming activities to identify and eliminate potential vulnerabilities.

8. Promote SDN and related technology research to optimize open and transparent interfaces and interoperability of network layers and domains.

9. Expand efforts with the private sector to jointly review and share learnings on examples of SDN and ICT deployments to shape policies on best practices for operationalization and secure implementation with a particular focus on NS/EP communications and critical infrastructure.

10. Support the use of encryption to prevent network infrastructure providers from accessing communications which traverse their networks.

11. Revisit regulatory requirements, where appropriate, to ensure they evolve to encompass guidelines and requirements for securing SDN and related technology implementations in NS/EP communications and critical infrastructure.

The following activities could directly benefit the Federal Government D/As by accelerating the adoption of SDN-related technologies and cloud services. As such, the Federal Government should:

1. Consider incentives and policies to motivate companies that manufacture hardware and participate in software product lifecycles for SDN and related technologies to maintain trusted supply chains for U.S. Government and U.S. private sector adoption in critical infrastructure and NS/EP deployments. Policies should help ensure that the U.S. Government has sufficient access to timely hardware supply and software support that does not have critical dependencies on adversarial nations, regardless of future global turbulence.

2. Establish a Center of Excellence (CoE) to accelerate secure Government adoption of SDN and related technology with the following activities. Note: The CoE could be comprised virtually of existing organizations like NIST, CISA, DISA, coordinating together.

   Theme: Reframe existing policies and contract language to promote the adoption of new technologies common in the private sector.

   a. Establish policies that encourage the consideration of SDN and related technology by Federal Government D/As to satisfy their requirements for flexible, resilient, and secure services. For example, by reviewing existing Government policies and practices intended to achieve network security goals with traditional networking technologies, perimeter-based security, and on-premise computing resources and revising them to achieve the same goals using SDN and related technology solutions.

b. Provide template procurement and contractual language to help D/As engage vendors in adopting SDN and related technology while adhering to government security requirements (e.g., Trusted Internet Connection 3.0)

c. Provide guidance to help D/As identify candidate programs to migrate to SDN and related technology starting with lower impact programs and successively more mission critical programs over time.

d. Develop metrics-based plans to deploy SDN and related technology with milestones and budgetary incentives.

Theme: Support human capacity building.

a. Provide hiring assistance, education, training, skills development, and consultation.

b. Guide Government organizations through design, test, deployment, verification and monitoring and maintenance.

Theme: Consistency across Government.

a. For Government adoption of SDN and related technology, define risk-based security goals and policies.

   i. Define security goals and network security postures for different cyber threat situations (e.g., tied to Defense Readiness Conditions levels 1-5).

   ii. Have clear operational versus deployment/test policies.

   iii. Similar to how vendors have developed models for prioritizing private sector application traffic to optimize bandwidth for a business, work with vendors or internally to do the same for government applications or toolsets for organizations to do so themselves.

   iv. Recommend resiliency plans during times of lowered bandwidth and prioritization of critical traffic.

   v. Leverage risk management-based auditing to ensure Government security goals and policies are being met for SDN and related technology.

b. Recommend segmentation of different types of traffic (e.g., IoT coffee makers, Netflix traffic, and security cameras) and share risk mitigation strategies to prevent and remediate device and network compromise. For example, all unknown, unauthenticated or un-patchable devices should be moved into separate network segments.

c. Apply supply chain risk mitigation techniques to hardware procurement and reduce the number of hardware stock keeping units.

Theme: Leverage synergies possible with adoption of SDN and related technology to automate existing cybersecurity challenges and preempt future risks in both current and next generation networks.

a. Integrate support for automated asset detection, provisioning and management into networking technologies.

   i. Know what is deployed where and how it will be supported.

   ii. Keep track of devices that are not upgradable (for earlier retirement).

b. Use a consistent framework for software updates for assets, especially SDN devices and require mutual authentication based on Federal Information Processing Standards (FIPS) approved algorithms

c. Promote use of hardware roots of trust and trusted computing techniques (e.g., device identity, measurement, software bill of materials, attestation, update verification, and resilience).

d. Leverage investments in existing government certifications for SDN and related technology (e.g., build on the Federal Risk and Authorization Management Program [FedRAMP] for NFV applications hosted in data centers).

Theme: Source code management in Government and the supply chain.

a. Promote management of open source code used in SDN and related technology solutions, for example:

   i. Scan binaries for versions to build a software bill of materials.

   ii. Memorialize the build tools and source code incorporated into solutions. For example, if a public open source repository is tampered with, it should be possible to generate patches from a private copy for source and toolchains

c. Encourage vendors to scrutinize use of open source code. For example:

   i. Use static analysis tools (e.g., the Software Assurance Marketplace).[61]

   ii. Use secure development practices (e.g., ISO/IEC 27034-1)

Theme: Engage with vendors to support Government use cases.

a. Work with SDN and related technology vendors to implement Government-specific requirements into their hardware.

b. Consider certification programs for individual devices to meet Federal Government requirements and achieve interoperability of SDN and related technology components. These certifications may be incorporated into existing vendor programs such as FIPS, Joint Interoperability Test Command, and FedRAMP.

c. Participate in standards organizations to represent government use cases.

d. Ensure NIST takes SDN and related technologies and concepts into account in its future control frameworks, and appropriate compliance considerations are incorporated into the *Federal Information Security Management Act of 2002*, FedRAMP, and other programs/policies (e.g., the use of vendor tooling).

e. Promote the adoption of solutions with open and transparent interfaces and interoperability of network layers and domains during the procurement SDN and related technology.

f. Encourage SDN and related technology product vendors participation in the National Security Agency's Commercial Solutions for Classified Programs.

Conclusion

SDN and NFV represent a major advance in network technology which will have profound impacts for NS/EP. Global network infrastructure and enterprise networks are migrating quickly to a SDN environment, due to the performance, flexibility, adoptability, resiliency, security, and cost advantages provided by virtualization. The shift towards SDN and NFV is structurally transforming the ICT ecosystem and allowing networks to become more flexible and adaptive the benefits of which have demonstrated themselves in the response to the COVID-19 pandemic. SDN is integral to the development of 5G mobile infrastructures which, by definition, are software-centric and virtualized. SDN will play a critical role in networking the various service-based applications in 5G implementations. In the enterprise domain, the deployment of software-defined wide-area networking solutions has accelerated the adoption of SDN to implement high performance wide-area networks via lower-cost, commercially available internet access.

The United States, along with its allies, is the global leader in the development and deployment of SDN. As such, many network operators have already begun the migration to SDN. This migration: (1) builds on

[61] "Welcome to the Software Assurance Marketplace (SWAMP)." SWAMP. Continuous Assurance, https://continuousassurance.org.

and enhances U.S. leadership in virtualization and ICT innovation; and (2) illustrates that SDN technologies have reached a level of maturity that allows for secure implementation at scale. While there are challenges with operationalization and security, the SDN deployments by U.S.-based carriers, service providers, and enterprises demonstrate that these issues can be managed in the context of NS/EP communications.

SDN-based architectures also disrupt current supply chain models, resulting in an opportunity to create a more future-oriented supply chain for network investments. The transition to SDN plays to the strengths of companies with existing leadership in silicon, cloud, and software, all of which exist within leading U.S. technology companies. To this end, the Administration should leverage trends in SDN to pave a path of innovation to support the goal of defending and sustaining U.S. leadership in 5G wireless technologies and beyond. Rarely do emerging technology trends afford such a compelling venue to support the Administration's strategic goals. Thus, U.S. participation in the evolution of a new SDN supply chain ecosystem is of global importance.

In terms of recommendations, the Administration should encourage and support the continued deployment of SDN technology in the U.S. and allied nation ICT environments to determine how these capabilities might be leveraged by the Defense and IC's national security environment. As a result, policymakers should consider how to best promote the use of open architectures with particular focus on 5G and beyond. Also, the Defense Community and IC should expand efforts to define requirements and use cases specific to their unique needs, as well as share those with private sector SDN providers and relevant standards bodies. The Government should also establish policies to help educate U.S. D/As on the full range of SDN capabilities to enhance their mission performance, improve security, and lower their costs.

Finally, working with Congress, the Administration should: (1) establish policies and incentives to encourage U.S.-based investment and innovation in research and development of SDN capabilities and standards; (2) encourage best practices for implementation; and (3) promote deployment of these capabilities within the U.S. Government and allied nation ICT environments. Policymakers should also take into consideration the development of updated acquisition strategies and mechanisms for utilization of SDN-based services.

Appendix A: Adoption of Software-Defined Networks Examples

How Government Owned Networks Differ from Commercial Networks

Multiple levels of government own and/or use private networks that use virtualization. In some ways these are like commercial networks, but they often come with constraints not faced by commercial networks. This restriction drives the way that software-defined networking (SDN) or cloud technologies are implemented, and the ways that they can evolve. Government organizations are similar to commercial entities in that they often have an enterprise core with its own transport, storage and compute resources, cloud services, branch offices, and remote users. They differ from commercial entities in that many agencies are often required to comply with government policies, particularly those relating to cybersecurity. Between first responders, civilian agencies, and defense agencies, it is the civilian agencies whose business models best match the commercial SDN and network functions virtualization (NFV) model. Anecdotal reports from Dr. Yang Guo, Senior Scientist, Advanced Network Technologies Division, National Institute of Standards and Technology, suggests that introducing civilian agency use cases would likely require little effort.[62] The first responders' business models also match the SDN and NFV model, with the migration to 5G being an opportunity to introduce use cases. Defense agencies will likely take longer to match the SDN and NFV model, because they have the need for dealing with problems of secure gateways and transport mechanisms, and the need to accommodate expeditionary networks without fixed infrastructure involving multiple security levels and perhaps involving the security issues of networks of other countries.

Federal Government Civilian Agencies

Federal Government civilian agencies, for the most part, manage their own networks and therefore have discretion to decide how they structure their networks. They do not, however, have the same latitude as commercial entities in making network management decisions. The two major factors are purchasing policies and cybersecurity policies.

Regarding purchasing policies, the General Services Administration (GSA) through the Federal Acquisition Service (FAS) provides support to civilian agencies for purchasing network equipment. They provide the policies and guidelines for purchasing through their FAS Office of Information Technology Category. They also negotiate contracts with equipment and service providers and provide centralized procurement to facilitate purchases by individual agencies through their Enterprise Infrastructure Services arm. One of the goals of the GSA is to "improve the way federal agencies buy, build, and use technology."[63]

FAS has been involved in several initiatives, including Trusted Internet Connections (TIC).

TIC

"TIC, originally established in 2007, is a federal cybersecurity initiative intended to enhance network and perimeter security across the Federal Government. The Office of Management and Budget, Department of Homeland Security [DHS] Cybersecurity and Infrastructure Security Agency [CISA], and the GSA oversee the TIC initiative, setting requirements and an execution framework for agencies to implement a baseline perimeter security standard."[68]

[62] Dr. Yan Guo, NIST, "Some Thoughts on Software-Defined Networking (SDN) Security" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 3, 2019).

[63] U.S. Government Services Administration (GSA), "GSA Background and History - Mission and Strategic Goals." U.S. GSA. U.S. GSA, January 21, 2020, https://www.gsa.gov/about-us/background-history/mission-and-strategic-goals.

[64] "Trusted Internet Connections [TIC]." CISA. CISA, March 16, 2010, https://www.cisa.gov/trusted-internet-connections.

The latest version of TIC (3.0) alters the reference architecture for implementing perimeter security in an effort to enhance adoption of cloud services. Earlier versions depended on a reference architecture that centralized security services for internet access. All traffic to and from the internet was funneled through a set of security gateways that monitored traffic for attacks. Each agency had its own TIC access points. The access points collected information about threats and attacks.[65] It forwarded information to the National Cybersecurity Protection System (NCPS) analysis servers. NCPS servers analyze the data for threats and attacks. They provide cybersecurity guidance back to the access points to respond to these threats.

The centralized access to the internet made it difficult to implement cloud services, particularly for branch offices and remote users, since all cloud traffic had to be homed to the agency infrastructure that housed the TIC access point. TIC 3.0 introduces the concept of Policy Enforcement Points that can be placed at other locations. It also permits agencies to allow this information to be collected by cloud providers and delivered to a cloud log aggregation warehouse, and for the cloud providers to provide security services.

GSA maintains a program called the Federal Risk and Authorization Management Program (FedRAMP) that provides agencies with an authorization process for vendors for security related products and services.

A FedRAMP authorization can be used across agencies in the authorization process for services. DHS' CISA supports TIC 3.0 initiatives. In particular, CISA evaluates and authorizes use cases. The TIC 3.0 Use Case Handbook contains several use cases,[67] but the initiative permits agencies to consider solutions offered by vendors. CISA oversees and evaluates trials of new use cases and authorizes their inclusion in the use case document.

FedRAMP

"FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP enables Agencies to rapidly adapt from old, insecure legacy [information technology (IT)] to mission-enabling, secure, and cost-effective cloud-based IT.

FedRAMP created and manages a core set of processes to ensure effective, repeatable cloud security for the government. FedRAMP established a mature marketplace to increase utilization and familiarity with cloud services while facilitating collaboration across government through open exchanges of lessons learned, use cases, and tactical solutions."[66]

CISA provides several cyber services to agencies, including: (1) continuous diagnostics and mitigation (telemetry and analysis); (2) EINSTEIN (blocks cyberattacks and provide situation awareness); (3) TICs (enforce security policies); (4) NCPS (analyze threats and provide alerts); and (5) deployment and incident response services.

State and Local Governments

State and local governments have access to the services provided by GSA and DHS. Where local may differ from federal agencies and state governments is that they are often much smaller and may not have the critical mass to support large IT departments to implement or manage their networks.

[65] The sensors were operationally referred to as EINSTEIN.

[66] "About Us. 2020." The Federal Risk and Authorization Management Program (FedRAMP). FedRAMP, January 21, 2020. https://www.fedramp.gov/about.

[67] A suite of TIC 3.0 documents is maintained on the "Guidance Documents" subsection of the TIC page, https://www.cisa.gov/trusted-internet-connections.

Defense Agencies

Defense agencies support a variety of networks with differing security classifications. The classification process is used to support an information protection strategy. Allowing the movement of classified data from a network of higher classification (e.g., Top Secret) to a network of lower classification (e.g., Secret) is strictly forbidden. The rules for classifying information vary somewhat from program to program. The higher the classification level, the more sensitive the program tends to be about classification of facts through aggregation of information (e.g., knowing how to identify and to locate a classified process). This affects SDN deployment opportunities in two ways. In the first case, the network management authorities are different between networks in different security classifications, so achieving the goal of a control plane that permits exchange of information incurs more decision-makers (i.e., higher complexity). In the second case, information that discloses the topology of the network alongside any ability to identify individual functions within that topology can end up being classified, so control plane interaction between networks is more constrained.

If the network is wired as opposed to wireless, the typical strategy has been to insert high assurance Internet Protocol (IP) encryptors (HAIPE) between networks of differing classification. Although there exist some protocols for HAIPE to discover other HAIPE across the cipher-text network[68], the typical strategy is to configure the address on both the plain-text side and cipher-text side of the HAIPE manually. The HAIPE device supports some form of what is called consistent bypass. This means that some information is allowed to consistently pass between the plain-text network and the cipher-text network without going through the encryptor. Examples include quality of service (QoS) fields of a message that needs to receive the same QoS treatment on the cipher-text network that it enjoys in the plain-text network.

For wireless networks, the controlled interface between the plain-text network and the cipher-text network has additional information that needs to consistently bypass encryption. This includes functions like control over modems, radio frequency equipment, or antennas. Typically, each program chooses the wireless components that it will use, and then develops a custom set of filters to ensure that classified information will not bypass the encryption process through device control functions.

This behavior affects technologies like SDN in that neither the HAIPE approach nor the wireless encryption approach are certified to exchange control plane information with any cipher-text network used to transport that traffic. For classified networks, there is no automated process for one network to request cipher-text transport services from another network; these are defined only at network design time and implemented with manual configuration mechanisms. Therefore each network remains its own stovepipe

The problem of overcoming the cost and delay of manual intervention was one of the driving forces behind the development of SDN technologies. SDN networks have become self-configuring and self healing and that has allowed them to have lower cost and to be more flexible in meeting the needs of its users. Achieving this same goal on defense networks is a worthwhile objective.

It can be observed that each individual network could choose to implement SDN independently and achieve cost and flexibility benefits. From a multi-domain management perspective; however, one of the benefits of having a control plane between plain-text and cipher-text networks is that it fosters collaboration between network owners to work towards a consistent SDN deployment across programs. That may lead to lower cost and reduced deployment time.

Examples of SDN Technologies and Benefits

Organizations are adopting SDN in several ways. One key difference in the way that SDN is adopted is whether a telecommunications service provider adopts SDN for its own use (i.e., to more efficiently provide current services, or more rapidly introduce new services) or adopts SDN so that its customers can take advantage of its flexibility.

[68] Encryption devices like HAIPE have a plain-text side where data is un-encrypted, and a cipher-text side where data is encrypted.

Telecommunications service providers could be a commercial service provider (e.g., AT&T, CenturyLink, Verizon) or it could be a government civilian or defense network (e.g., Global Information Grid-Bandwidth Expansion, Secret Internet Protocol Router Network, Joint Worldwide Intelligence Communications System). Government service users include any size agency or department similar to how the user of services from commercial service providers could be any size enterprise.

The following are examples of how a telecommunications service provider might use SDN for their own network's benefit.

Optimizing Optical Fiber Bandwidth Usage

The optical layer is the lowest layer of telecommunications networks, where multiple wavelengths of light are multiplexed together to create the massive amount of bandwidth available today. The wavelengths are allocated into specific channels, and at times the way a network has evolved leads to inefficient gaps between channels. SDN is an excellent technique to analyze large portions of the network and then reallocate the wavelengths in a more efficient manner, thereby freeing up otherwise unusable optical spectrum.

The Layer-1 transport network enables different service types to coexist and share the same infrastructure transparently, without affecting each other's performance. As part of this, the optical transport network (OTN) can provide other services besides light paths, such as packet-switched virtual circuit or datagram services. These services can directly interface with user applications, or other layer combinations are possible such as IP over synchronous optical networking. OTNs are moving briskly to SDN through Open Line Systems and replacing proprietary hardware with open APIs and commodity hardware. Because OTN underpins every wide area network, it would be of national interest to ensure these concerns are addressed.

Path Optimization

At the Ethernet, IP, and Multi-Protocol Label Switching (MPLS) layers of networks is the ability to leverage the SDN concept of a Path Computation Engine (PCE) within a network controller. Traditional routing protocols work in a distributed, hop-by-hop manner. Although the protocols attempt to build a database of the entire network, each node runs an independent version of the path selection algorithm to determine where to send packets next. SDN embodies the concept of a more centralized controller, where information is sent to a PCE that can then make the most accurate and efficient decision on how traffic flows should be routed to meet their specific requirements. Using a PCE becomes a tool for a service provider to maximize certain aspects of the network (e.g., utilization, revenue), while minimizing other aspects (e.g., latency, cost, resources consumed).

Traffic Engineering

Another way to look at a PCE is to equate it to the concept of traffic engineering (TE). In this sense, TE can not only be used by the provider for greater efficiency of the entire network, but it can be used as a technique to implement customer policy. For instance, a customer may be an enterprise or government entity that requires its traffic to strictly avoid certain geographic areas (e.g., international traffic that should not transit through a specific country). SDN can ensure that the traffic's path adheres to the customer's policy.

Segment Routing

Segment routing (SR) is one specific technology that supports SDN. The basic premise behind SR is that the path a packet takes through the network is defined in the header of the packet and does not rely entirely in each node's independent decision to reach its destination. This is beneficial as it reduces the need to maintain state in the network itself. But another key advantage of SR is that it is SDN-ready: not only can distributed protocols be used to allow SR to function, but the protocol was designed to be able to take direction from a centralized SDN controller. This allows a PCE to push information to the edge nodes of a network, thereby allowing them to insert the segment identifications into each packet.

The follow are examples of how enterprises and the Government might use SDN for their benefit.

Software-Defined Wide-Area Networks (Optimize Multiple Connections)

Software-defined wide-area networks (SD-WAN) is an example of how an enterprise would leverage SDN to provide efficient, robust, and resilient service to its users. The basic premise of SD-WAN is to utilize several different techniques to provide connectivity (either to remote offices or individual users), and then use software to select the most efficient path based on several criteria. For instance, a remote office may have connectivity through a dedicated line (i.e., MPLS or Ethernet service from a service provider), or could have connectivity from a broadband service and have connectivity from a wireless service. SD-WAN would take all three connectivity techniques into consideration when decided how to route the traffic. For instance, the dedicated line may be used because it provides the most bandwidth with the lowest latency, but a broadband service may be chosen because it provides connectivity at the lowest cost. The wireless service may be designed as a back-up and would only be used if the dedicated line or broadband service is not available. Finally, some versions of SD WAN continuously monitor the quality of service characteristics of each connection (i.e., latency, loss and jitter of traffic) and may use any one of the connections based on a selection policy.

Dynamic Capacity (Network Slicing)

There are numerous circumstances when a business might require dynamic provisioning to support short-term needs for additional capacity, including events such as Black Friday, advertising promotions, or large-scale transfers of data. Network slicing represents a service that results from the interaction between an enterprise and a service provider. Network slicing is designed in a dynamic fashion so that a user requests a network slice with specific characteristics through an application programming interface request. The provider of the slice receives that request and then provisions the slice on its own network, and then possibly works to provision more connectivity beyond its own network. A network slice differs from a virtual private network (VPN) in that it is extended to the end-user, regardless of the access method. For instance, if a network slice were to include mobile users, the slice is extended to the end-user's mobile handset and includes any techniques required to provide dedicated channels or spectrum to that handset. In contrast, a VPN is typically implemented as a tunnel through an underlying network. Tunneling means that the original packet is encapsulated into another packet and the headers of the outer packet are used to forward the packet through the underlying network. Often the original packet is encrypted to provide confidentiality and some level of integrity guarantee. VPN would have no latency or throughput guarantees, whereas, network slicing could allocate more network resources from the service provider.

Network slicing provides the benefit of being able to procure a network that adheres to a variety of QoS levels, but that also meets other policies. For instance, a slice may be required to not multiplex traffic at the packet layer with any other networks. In that case, the slice may need to be provided using optical transport network or dense wavelength division multiplexing technology. The enterprise may also have very strict requires for networks of specific use. For instance, a command and control network might have strict tolerances on latency and may require the highest availability a network can offer. Other networks provided to the same organization may have more administrative needs (i.e., networks primarily devoted to email). These slices can be provided with lower tolerances.

Federal Government

Federal, state, and local government stakeholders often have additional security, compliance, or mission goals which benefit from the flexibility of SDN and NFV technologies for adopters in the commercial sector. Combining the adoption activities for SDN with other transformations to modernize data networks, adopt cloud applications or zero-trust networks at the same time can help achieve organizational goals holistically instead of repeating similar cybersecurity activities incrementally.

NSTAC briefers provided examples of prototyping SDN adoption and a desire for policy revisions to enable evaluation and planning activities as part of larger digital transformation activities.

Prototyping examples for operational technology (OT) environments indicated significant benefits in understanding networking environments and traffic by identifying all devices, network connections and traffic. SDN holds promise in terms of providing a way to identify incorrect network usage and vulnerabilities in other products. The ability to implement strong and detailed security policies with SDN will reduce attack surfaces by denying unwanted network traffic and providing defense in depth. The dynamic ability to easily increase network security posture based on external events will be beneficial for some environments. SDN showed the potential to increase the resiliency of critical infrastructure systems by pre-planning responses for network events. The research department of one Government Intelligence Community agency indicated they operated their own environment using SDN.[69]

Briefers for this report did not cover state and local governments explicitly, however many of the recommendations could be valuable for them to consider.

First Responders

First Responder Network Authority

The First Responder Network Authority (FirstNet) was created as part of the *Middle-Class Tax Relief and Job Creation Act* (2012).[70] From 2001 to 2012, multiple large disaster relief efforts showed that equipment from the various first responder agencies was often incompatible. Establishing a working network for a large-scale disaster was difficult. The existing land mobile radio equipment had been designed for voice, and had little in the way of data capability, which was becoming increasingly important to respond to events. First responders were using cellular phones to supplement but the public cellular network could be overwhelmed by events that involved a large number of people, and many parts of the country had poor or no cellular service. The law allocated 20 megahertz of spectrum and $7 billion to establish a broadband network dedicated to first responders.[71]

FirstNet built a long-term evolution-based network with very good nationwide coverage. It covers 76 percent of the land area of the continental United States, and more than 99 percent of the population.[72] There are goals to maintain technology, and FirstNet is studying fifth generation (5G) network deployments.

The network supports more than one million connections for first responders over more than 10,000 agencies.[73] In this way, FirstNet is not like an enterprise network; it is an access technology for 10,000 enterprise networks. Although there may be ongoing data interaction between some of these networks, the vast majority operate their transport, storage, and compute functions independently.

Notwithstanding the large number of diverse organizations that participate in FirstNet, one of its goals is secure information exchange.[74] One aspect of this goal is the need for collaboration across government for standardized governance and procedures to simplify and integrate access and exchange of information with select national level data sets. Another aspect calls for improvement in the performance and use of identity, credential, and access management. This goal places the policies and standards development at the national level, even if the day to day operations remain at the level of the individual agency.

When FirstNet moves to 5G, the possibility of exploiting network slicing to share transport, compute, and storage infrastructure emerges. It is unknown how individual organizations (mostly state and local governments) will react to this, but many of the smaller organizations could see cost reductions if they did not have to negotiate and manage their own IT support. It is also unclear how many service providers this transition might involve creating an SDN core capable of supporting network slicing.

[69] Stephen Hawkins, Laboratory for Advanced Cybersecurity Research, "SDN" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

[70] "First Responder Network (FirstNet) Authority Roadmap." FirstNet. FirstNet, 2019. https://www.firstnet.gov/system/tdf/FirstNet_Roadmap.pdf?file=1&type=node&id=1055.

[71] "FirstNet: The History of Our Nation's Public Safety Network." FirstNet. FirstNet, https://firstnet.gov/about/history.

[72] "FirstNet Nationwide Coverage." FirstNet. FirstNet, January 20, 2020, https://www.firstnet.com/coverage.html.

[73] AT&T, "FirstNet Soars with Over 1 Million Connections and Launch of 'FirstNet One,'" December 16, 2019, https://www.firstnet.com/community/news/firstnet-soars-with-over-1-million-connections.html?LinkID=Connections.

[74] "FirstNet Roadmap." FirstNet. FirstNet, 2019. https://www.firstnet.gov/system/tdf/FirstNet_Roadmap.pdf?file=1&type=node&id=1055.

Military

Defense Information Systems Agency

Multiple defense agencies are represented in the Federal Government. Each has a significant latitude in making networking decisions. The Defense Information Systems Agency (DISA) provides many services to defense agencies. Its mission is "to conduct [Department of Defense (DoD) Information Network] DoDIN operations for the joint warfighter to enable lethality across all warfighting domains in defense of our Nation."[75]

DISA is currently piloting and deploying SDN in their infrastructure. Mr. Paul Inverso, Technical Manager for Software-Defined Enterprise at DISA, said in September of 2018 that the agency has progressed from piloting SDN initiatives to the deployment of full-scale production services based on software-defined technologies. The initial pilot provided rapid provisioning services for Layer 2 and Layer 3 virtual private networks for a portion the DISA IP network, he says. The pilot reduced service provisioning time by up to 45 days, Mr. Inverso says, "[b]ased on its success, the pilot is extending to the full IP network of more than 500 nodes…DISA is also upgrading the computer and communication infrastructure in all of its data centers with SDN technology. Initial deployments include SDN controllers providing automated control over network elements, while the orchestration function will be implemented in a later phase."[76]

Mr. Robert Kimball, Technical Adviser, Cyber Directorate, DISA, said that the agency has adopted "a much more expansive approach to software-defined technologies beyond SDN." The software-defined Enterprise at DISA "aims to introduce automation into every DISA program where it will improve service to the warfighter and our mission partners." The primary motivation for doing so is to reduce the time it takes to deliver services, whether in the WAN or data center, Mr. Kimball says. "DISA will also realize efficiencies, which will allow us to tackle more complex issues by reducing manual processes," he adds. Mr. Inverso says the DISA software-defined enterprise architecture is built from a hierarchical structure of orchestrators and controllers. "Orchestrators interact with business systems, mission partner requirements, and the operational state of the network to direct automation," he says. "The controllers will be network-specific and will implement the direction of the orchestrators and interface with the network equipment."[77]

A Defense Innovation Board publication on *Fully Networked Command, Control, and Communications* identified the challenge that "DoD networks must manage a growing amount of data traffic flowing between a growing number of endpoints", which SDN can help address.[78] Also there were the following recommendations about the potential benefits of SDN to the DoD:

- SDN can help deconflict DoD network traffic and reducing latency in data transfer by improving network efficiency and implementing policy-driven network supervision;
- SDN also creates an opportunity to improve DoD network security by providing a federated point that can monitor and log traffic, as well as distribute common security policies throughout the network. This will also help DoD efforts to shift to a zero-trust, least-privilege access model by creating better awareness of network mapping and standardizing security policies;
- SDN can also reduce overall DoD network administration costs by centralizing and automating many network management functions; and
- SDN will enhance the warfighter by identifying critical packets on the network and speeding up the rate of data transfer for high priority missions and environments.[79]

[75] "About Defense Information Systems Agency (DISA)." DISA. DISA, https://www.disa.mil/About

[76] Phil Goldstein, "Why DISA Has Embraced SDN for the Pentagon," FedTech, September 28, 2018, https://fedtechmagazine.com/article/2018/09/why-disa-has-embraced-sdn-pentagon-perfcon#:~:text=DISA%20announced%20its%20shift%20to,based%20on%20software-defined%20technologies%20.

[77] Phil Goldstein, "Why DISA Has Embraced SDN for the Pentagon," FedTech, September 28, 2018, https://fedtechmagazine.com/article/2018/09/why-disa-has-embraced-sdn-pentagon-perfcon#:~:text=DISA%20announced%20its%20shift%20to,based%20on%20software-defined%20technologies%20.

[78] Mark Medin, Mark Sirangelo." Defense Innovation Board: Fully Networked Command, Control, and Communications Recommendations. Department of Defense. October 25, 2019. https://media.defense.gov/2019/Oct/31/2002204194/-1/-1/0/DIB_FULLYNETWORKEDC3_RECOMMENDATIONS.PDF.

[79] *Ibid*.

Experiences with SDN/NFV

The overall level of experience with SDN solutions within Government agencies is still small. A few briefers provided examples. Mr. Stephen Hawkins, Computer Systems Researcher, Laboratory for Advanced Cybersecurity Research, reported that they had conducted several SDN field trials to better understand the technology.[80] Mr. Mark Hadley, Chief Cyber Security Researcher, National Security Division, Pacific Northwest National Laboratory reported that they had implemented several versions of an SDN solution targeted at industrial/energy control systems (called OT-SDN).[81] He reported being close to receiving an Authority to Operate (ATO) for their Ft. Belvoir installation, having gone through the Risk Management Framework evaluation process.

DoD Approved Products List

One product on the DoD Approved Products List (APL) claims that it is SDN capable. Allied Telesis has an SDN-capable switch that is on the APL.[82] The x310 series switches are SDN ready and are able to support OpenFlow v1.3. Schweitzer Engineering Laboratory's SEL-2740S is in the APL and authority to operate processes. Mr. Mark Hadley, Chief Cyber Security Researcher, National Security Division, Pacific Northwest National Laboratory reported being close to having his organization's version of OT-SDN on the DISA APL.

Other approved products will undoubtedly follow, and additional products will help foster adoption. Since vendors are the ones to add products to the list, there is an opportunity for the government to be more proactive about soliciting vendors to participate.

Enterprise

As indicated in the 2017 *NSTAC Report to the President on Emerging Technologies Strategic Vision*, the shift towards SDN began with the arrival of cloud computing, a technology that disrupted the traditional enterprise network architecture by pooling computing resources used across multiple enterprises to create "virtual machines." Cloud computing disrupted the typical model for enterprise architecture and helped to create an ecosystem where information and communication technology infrastructure is centralized and virtualized – first by centralizing hardware and resources in large data centers, and over time by offering a suite of services that allowed users to remotely manage and configure hardware and software assets. By re-architecting the network to be software-centric, network operators, enterprises and a range of other entities can build a platform that will have the right agility and economics to outpace demand and quickly introduce new technology and services to customers.

The benefits of this transformation must be considered in the context of rising enterprise and government demand for the key benefits SDN architecture can afford, including multilayer optimization, openness, programmability, simplification, and automation.[83] The growth of SDN architectures is also coming at a time when all enterprises, in order to remain innovative and competitive, face enormous pressure to digitize core aspects of their business at ever-accelerating rates.[84]

Enterprises are beginning their own conversion (re-architecting) to enable SDN/NFV in three primary areas: (1) modifying current enterprise infrastructure to support a SDN/NFV overlay; (2) leveraging commercial relationships to enable dynamic capacity provisioning/de-provisioning; and (3) leveraging commercial relationships to enable dynamic connections with other providers, most notably data centers or cloud-enabled environments.

Modifying Current Enterprise Architectures and Infrastructure

Enterprise networks are generally comprised of a diverse combination of enterprise-owned (private) infrastructure, leased infrastructure (generally through a network service provider), and data center and cloud providers. The enterprise networks are further extended by employee mobile devices, and internet-based infrastructure that might support enterprise operations.

[83] Anil Simlot, "Importance of SDN for a Service Provider" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

[84] David Ward, "SDN and Virtualization Technologies in Communication Networks to Thwart Cyber Threats and Improve Security" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 7, 2020).

In order for enterprise operations to enable their own transition, they are beginning to reconfigure their networks so they can drive towards more consistent network and application performance facilitating business continuity across the enterprise's varying network topologies. In many cases, this requires changes in the underlying type of infrastructure or elements throughout their networks, and this effort does not lend itself to a one-size-fits-all solution. Nonetheless, this effort is underway and will set the stage for hyper-utilization of SDN capabilities through the enterprise/end-user portion of the information and communications technology ecosystem.

Finally, in collaboration with their service provider, the enterprise can enforce routing policies for end users. For instance, a customer may be an enterprise or government entity that requires its traffic to strictly avoid certain geographic areas (e.g., international traffic that should not transit through a specific country), SDN can be used to ensure that the path traffic takes adheres to the policy.

Dynamic Connections for the Enterprise with SDN

As enterprises increasingly implement SDN in supporting their business operations, there will be an increasingly large shift from physical management of their networks and data center infrastructure to a virtual management. As such, it is projected that 75 percent of enterprise-generated data will be created and processed outside the data center or cloud by 2023, up from less than 20 percent today.[85] Increasingly network service provided are offering enterprises the ability to connect dynamically to numerous cloud providers or other SDN-based capabilities in the cloud, and enterprises are thus moving away from the traditional host/dedicated server-based approach for network provisioning and management software. Containerization of the cloud-based services is further being implemented to increase reliability and security for the enterprise needs. With this capability, enterprises can host critical functions in multiple cloud environments, can dynamically balance their operations to ensure a wide diversity of alternate operational sites to assure continuity of operations under any scenario.

[85] Anil Simlot, "Importance of SDN for a Service Provider" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

Appendix B: Subcommittee Roster

SUBCOMMITTEE MEMBERS

Mr. John Donovan, formerly of AT&T Communications, LLC, Subcommittee Chair
Mr. Scott Charney, Microsoft Corp., Subcommittee Chair
Mr. Raymond Dolan, Cohere Technologies, Inc., Subcommittee Chair

Mr. Christopher Boyer, AT&T, Inc., and Working Group Co-Lead
Ms. Amanda Craig-Deckard, Microsoft Corp., and Working Group Co-Lead
Mr. Kevin Riley, Ribbon Communications, Inc., and Working Group Co-Lead
Mr. Robert Spiger, Microsoft Corp., and Working Group Co-Lead

Mr. Christopher Anderson	CenturyLink, Inc.
Mr. Jason Boswell	Ericsson, Inc.
Mr. Jamie Brown	Tenable, Inc.
Mr. James Carnes	Ciena Corp.
Ms. Kathryn Condello	CenturyLink, Inc.
Mr. David Cooper	VMware, Inc.
Mr. Michael Daly	Raytheon Co.
Ms. Cheryl Davis	Oracle Corp.
Mr. Stephen Dudley	L3Harris Technologies, Inc.
Mr. Drew Epperson	Palo Alto Networks, Inc.
Mr. Jonathan Gannon	AT&T, Inc.
Mr. Jay Humphrey	VMware, Inc.
Mr. David Krauss	Ciena Corp.
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. John Nagengast	AT&T, Inc.
Mr. Thomas Patterson	Unisys Corp.
Mr. Jon Peterson	Neustar, Inc.
Mr. Travis Russell	Oracle Corp.
Mr. Mark Ryland	Amazon Web Services, Inc.
Mr. Brett Scarborough	Raytheon Co.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Anil Simlot	CenturyLink, Inc.
Ms. Kerri Snow	CenturyLink, Inc.
Mr. Milan Vlajnic	Communication Technologies, Inc.
Mr. Eric Wenger	Cisco Systems, Inc.
Mr. Alexander Wirth	Microsoft Corp.

Appendix B: Subcommittee Roster

SUBCOMMITTEE MANAGEMENT

Ms. Sandra Benevides, President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer (DFO)
Ms. DeShelle Cleghorn, NSTAC Alternate DFO
Ms. Kayla Lord, NSTAC Alternate DFO

Ms. Sheila Becherer, Booz Allen Hamilton, Inc.
Mr. Philip Grant, Booz Allen Hamilton, Inc.

Mr. Matthew Mindnich, Insight Technology Solutions, Inc.
Ms. Laura Penn, Insight Technology Solutions, Inc.

Appendix C: Briefers

Dr. Alicia Abella	AT&T, Inc.
Dr. Eric Burger	Office of Science and Technology Policy
Mr. Terry Bush	Ericsson, Inc.
Mr. Roy Chua	AvidThink
Mr. Neil Danilowicz	Versa Networks, Inc.
Mr. Ranil Dassanayaka	VMware, Inc.
Mr. Roger Entner	Recon Analytics, Inc.
Mr. Andrew Gottlieb	Oracle Corp.
Dr. Yang Guo	National Institute of Standards and Technology
Mr. Mark Hadley	Pacific Northwest National Laboratory
Mr. Stephen "Chris" Hawkins	Laboratory for Advanced Cybersecurity Research
Mr. Larry Horner	Intel Corp.
Dr. Raj Jain	Washington University in St. Louis
Mr. William Lemons	Fortinet Federal, Inc.
Dr. Yousef Khalidi	Microsoft Corp.
Mr. Stephen Kovac	Zscaler, Inc.
Ms. Rita Marty	AT&T, Inc.
Dr. Katia Obraczka	University of California, Santa Cruz
Mr. Matthew Palmer	SDxCentral, LLC
Mr. Bejoy Pankajakshan	Mavenir Systems, Inc.
Mr. James Richberg	Fortinet Federal, Inc.
Mr. Peter Rysavy	Rysavy Research, LLC
Mr. Mark Ryland	Amazon Web Services, Inc.
Mr. Steven Shalita	Pluribus Networks
Mr. Anil Simlot	CenturyLink, Inc.
Dr. Salvatore Stolfo	Allure Security Technology, Inc.
Mr. David Ward	Cisco Systems, Inc.
Mr. William Zielinski	General Services Administration

Appendix D: Acronyms

3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
AI	Artificial Intelligence
API	Application Programming Interface
APL	Approved Products List
ASIC	Application-Specific Integrated Circuits
ATO	Authority to Operate
CoE	Center of Excellence
COVID-19	Coronavirus
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CSRIC	Communications Security, Reliability, and Interoperability Council
D/A	Department or Agency
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODIN	Department of Defense Information Network
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DSR	Demand Signal Repository
DPI	Deep Packet Inspection
eNode B	Evolved Node B
EOP	Executive Office of the President
FAS	Federal Acquisition Service
FCC	Federal Communications Commission
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FirstNet	First Responder Network Authority
GSA	General Services Administration
GSMA	Groupe Speciale Mobile Association
HAIPE	High Assurance Internet Protocol Encryptors
IaaS	Infrastructure-as-a-Service
IC	Intelligence Community
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
IoT	Internet of Things
LTE	Long-Term Evolution
MEF	Mobile Ethernet Forum
MPLS	Multiprotocol Label Switching
NCPS	National Cybersecurity Protection System
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSTAC	President's National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
ONAP	Open Network Administration Platform
O-RAN	Open Radio Access Network
OS	Operating System
OT	Operational Technology
PCE	Path Computation Engine
QoS	Quality of Service
RAN	Radio Access Network
SA3	3GPP Technical Specifications Group Service and System Aspects Working Group 3 – Security
SBA	Service-Based Architecture
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SD-WAN	Software-Defined Wide-Area Network
SEPP	Security Edge Protection Proxy
SIEM	Security Information and Event Management
SME	Subject Matter Expert
SR	Segment Routing
TIC	Trusted Internet Connections
TLS	Transport Layer Security
VNF	Virtual Network Function
VPN	Virtual Private Network
ZTA	Zero-Trust Architecture

Appendix E: Definitions

Address Resolution Protocol (ARP): A protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the Internet Protocol (IP) address of the target node with which it wants to communicate. With that address, the responding node sends back its physical address so that packets can be transmitted to it. (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-45 Version 2)

Adversary: Any individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (NIST SP 800-30)

Agency: Any department, military department, government corporation, government controlled corporation, other establishment in the Executive Branch of the Government (including the Executive Office of the President), or any independent regulatory agency. This does not include: (1) the Government Accountability Office; (2) the Federal Election Commission;(3) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (4) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. (NIST Glossary of Information Security Terms – [Federal Information Processing Standards] 200; 44 United States Code [U.S.C.], Sec. 3502)

Amazon Web Services (AWS) Direct Connect: A cloud service solution that makes it easy to establish a dedicated network connection from the user's premises to AWS. Using AWS Direct Connect, users can establish private connectivity between AWS and their data center, office, or colocation environment. (AWS, https://aws.amazon.com/directconnect/)

Artificial Intelligence (AI): The intelligence exhibited by machines or software. A term popularized by Alan Turing, it historically describes a machine that could trick people into thinking it was a human being via the Turing Test. Recently, scientists within this field largely have abandoned this goal to focus on the uniqueness of machine intelligence and learn to work with it in intelligent, useful ways. (Newton's Telecom Dictionary)

Application-Aware Routing: Tracks network and path characteristics of the data plane tunnels between vEdge routers to collect information to compute optimal paths for data traffic. (Cisco Software-Defined Wide-Area Network [SD-WAN] Configuration Guide, Release 17.2, https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-17-2.pdf#page=337)

Application Chaining: A method for invoking multiple demand signal repository (DSR) applications in sequence on the same DSR. (Oracle, https://docs.oracle.com/cd/E86291_01/docs.81/20170711_115004_m_dsr_fabr_help/concepts/c_dsr_help_fabr_application_chaining.html)

Application Programming Interface: A system access point or function that has a well defined syntax and is accessible from application programs or user code to provide well-defined functionality. (NIST Interagency/Internal Report [NISTIR] 5153)

Application-Specific Integrated Circuits: Custom-designed and/or custom-manufactured integrated circuits. (Committee on National Security Systems Instruction [CNSSI] 4009-2015; Committee on National Security Systems Directive No. 505])

Availability: Ensuring timely and reliable access to and use of information. (NIST Glossary of Information Security Terms –NISTIR 7298 Revision 2)

Bring-Your-Own-Device (BYOD): A concept that allows employees to use their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices. This could include laptop/desktop computers; however, since mature solutions for securing and supporting such devices already exist, this document focuses on the emerging use case of mobile devices. (The White House, https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device#_ftnref1)

California Senate Bill 327: Requires a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified. (California Legislative Information, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327)

Cloud Computing: A model for enabling on-demand network access to a shared pool of configurable information technology (IT) capabilities/resources, (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. (CNSSI 4009-2015; NIST SP 800-145)

Commercial Off-the-Shelf: A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public (NIST IT Laboratory Glossary)

Communications: The totality of users, devices, data, and applications on modern networks. (The President's National Security Telecommunications Advisory Committee [NSTAC] Secure Government Communications [SGC)] Subcommittee Definition)

Communications Security, Reliability and Interoperability Council (CSRIC): Provides recommendations to the Federal Communications Commission (FCC) regarding ways the Commission can support the security, reliability, and interoperability of communications systems. CSRIC's recommendations focus primarily on a range of public safety and homeland security-related communications matters. (FCC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0)

Compute Service: A cloud computing fabric controller, which is the main part of an Infrastructure-as-a Service (IaaS) system. (Openstack, https://docs.openstack.org/ocata/config-reference/compute.html)

Containerization: Type of virtualization strategy that emerged as an alternative to traditional hypervisor-based virtualization. Container-based virtualization involves creating specific virtual pieces of a hardware infrastructure, but unlike the traditional approach, which fully splits these virtual machines from the rest of the architecture, containerization just creates separate containers at the operating system level. (Techopedia, https://www.techopedia.com/definition/31234/containerization-computers)

Continuous Diagnostics and Mitigation (CDM) Program: Helps strengthen the cybersecurity of government networks and systems. CDM provides federal agencies with capabilities and tools that: (1) find cybersecurity risks on an ongoing basis; (2) prioritize these risks based upon potential impacts; and (3) enable cybersecurity personnel to focus on the most significant problems first.(U.S. General Services Administration, (https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm/continuous-diagnostics-mitigation-cdm-tools-special-item-number-sin-information-for-vendors#:~:text=Expedited%20Awards%20-%20The%20CDM%20program%20is%20eligible,flexibility%20and%20speed%20to%20market%20for%20emerging%20technologies.)

Control Plane: Part of a network which carries information necessary to establish and control the network. It is part of the theoretical framework used to understand the flow of information packets between network interfaces. References to the control plane are often included in diagrams to give a visual representation of network infrastructure. (Techopedia, https://www.techopedia.com/definition/32317/control-plane)

Coronavirus (COVID-19): The infectious disease caused by the most recently discovered coronavirus. This new virus and disease were unknown before the outbreak began in Wuhan, China, in December 2019. COVID-19 is now a pandemic affecting many countries globally. (World Health Organization, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses)

Critical Infrastructure (CI): Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. CI can be owned and operated by both the public and private sector. (*CI Protection Act of 2001*, 42 U.S.C.519c [e]; NIST Glossary of Information Security Terms – CNSSI 4009, Adapted)

CTIA – The Wireless Industry Association's Internet of Things (IoT) Certification for Cellular Connected Devices: Aim of this certification is to "protect consumers and wireless infrastructure, while creating a more secure foundation for smart cities, connected cars, mHealth and other IoT applications." (CTIA, https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program)

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber-attacks. (NIST Glossary of Information Security Terms – CNSSI 4009)

Data Plane: Allows for a modular terminal to actually host the gateway itself and requires that all participants follow a common notion for network management. (The Institute of Electrical and Electronics Engineers [IEEE] Explore – Government Reference Architecture Data Plane Gateway, https://ieeexplore.ieee.org/document/6415568)

Deep Packet Inspection (DPI): Technology that significantly enhances the security and management of current networks. Combined with software-defined networking (SDN), DPI becomes an even more powerful tool that can centralize network strategy control and quicken automation (IEEE Explore – Data Inspection in SDN Network, https://ieeexplore.ieee.org/document/8639202)

Defense Readiness Conditions (DEFCON) Levels 1 – 5: Any one of five levels of U.S. military defense readiness that are ranked from 5 to 1 according to the perceived threat to national security, with DEFCON 1 indicating the highest level of perceived threat (Merriam-Webster Dictionary)

Denial-of-Service (DoS): An attack that occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. DoS is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users (Cybersecurity Infrastructure Security Agency [CISA], https://www.us-cert.gov/ncas/tips/ST04-015)

Dense Wavelength Division Multiplexing (DWDM): Used for systems with more than eight active wavelengths per fiber. DWDM dices spectrum finely, fitting 40-plus channels into the same frequency range used for two Coarse Wavelength Division Multiplexing channels. (Ciena, https://www.ciena.com/insights/what-is/What-Is-WDM.html)

Department of Defense Information Network (DoDIN): Globally interconnected, end-to-end set of electronic information capabilities and associated processes for collecting, processing, storing, disseminating, and managing digital information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services, and National Security Systems. (Determination of the Chief Management Officer, https://open.defense.gov/Portals/23/Documents/FOIA/FOIA_Resources/10-19-2018_Determination.pdf)

DoDIN Approved Products List: Process used to test and certify products that affect communication and collaboration across the DoDIN and is an acquisition decision support tool for DoD organizations interested in procuring equipment to add to the Defense Information System Network (DISN) to support their mission. (Defense Information Systems Agency [DISA], https://aplits.disa.mil/processAPList.action)

East-West Traffic: Refers to activity between servers or networks inside a data center, rather than the data and applications that traverse networks to the outside world. (SDxCentral, https://www.sdxcentral.com/articles/analysis/east-west-encryption-security/2016/09/)

Edge Computing: Represents an emerging topology-based computing model that enables and optimizes extreme decentralization, placing nodes as close as possible to the sources and sinks of data and content. As a decentralized approach, it is a perfect complement to the hyperscale cloud providers' tendency towards centralization, where they take advantage of huge economies of scale. (Gartner, https://www.gartner.com/en/webinars/3846163/what-is-edge-computing-and-why-should-you-care-)

EINSTEIN: Serves two key roles in Federal Government cybersecurity. First, it detects and blocks cyber-attacks from compromising federal agencies. Second, it provides the Department of Homeland Security with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself. EINSTEIN has three phases: (1) EINSTEIN 1; (2) EINSTEIN 2; and (3) EINSTEIN 3A. EINSTEIN 1 and 2 detect potential cyber-attacks before they can enter the facility. EINSTEIN 3A detects and blocks many of the most significant cybersecurity threats. (CISA, https://www.cisa.gov/einstein)

Emerging Technologies: New, evolving, or innovative technologies. (NSTAC SGC Subcommittee Definition)

Enhanced Mobile Broadband: Focuses on a higher data rate, with a large payload and prolonged internet connectivity-based applications. (MDPI, *5G Ultra-Reliable Low-Latency Communication [URLLC] Implementation Challenges and Operational Issues with IoT Devices*, https://www.mdpi.com/2079-9292/8/9/981)

European Telecommunications Standards Institute (ETSI) Network Functions Virtualization (NFV) Working Group: Founded in November 2012 by seven of the world's leading telecom network operators, the ETSI NFV Working Group led the definition and consolidation for NFV technologies. (ETSI, https://www.etsi.org/technologies/nfv)

European Union Agency for Network and Information Security: Supports the development and implementation of the European Union's policy and law on matters relating to network and information security, and assists member states and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis. (European Union Agency for Cybersecurity, https://www.enisa.europa.eu/about-enisa)

Fast Failover: Process where the controller pre-establishes multiple paths for each source-destination pair in the related OpenFlow switches. When a link becomes faulty, OpenFlow switches can failover the affected flows to another path. (IEEE, https://ieeexplore.ieee.org/document/7510886)

Federal Information Processing Standards (FIPS): Standards and guidelines for federal computer systems that are developed by NIST in accordance with *the Federal Information Security Management Act* and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular government requirement. Although FIPS are developed for use by the Federal Government, many in the private sector voluntarily use these standards. (NIST, https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips)

Federal Risk and Authorization Management Program (FedRAMP): A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant Agency security assessments. (FedRAMP, https://www.fedramp.gov/faqs/)

Fifth Generation (5G): A future mobile network, whose specification has not fully been defined. It is expected to support 10 gigabits per second data rates and higher. Commercial 5G deployments are not expected until around 2020. (Newton's Telecom Dictionary)

Fourth Generation (4G): A successor of the third-generation standards. A 4G system provides mobile ultra-broadband internet access, for example to laptops with Universal Serial Bus wireless modems, to smartphones, and to other mobile devices. (International Center for Applied Studies in IT, http://icasit.gmu.edu/course-databases/technology-topics/4g-technology/)

Global Information Grid-Bandwidth Expansion (GIG-BE): Provides a worldwide, ground-based fiber-optic network that will expand IP-based connectivity and at the same time effectively and efficiently accommodate older, legacy command, control and communications systems. GIG-BE created an ubiquitous bandwidth-available environment to improve national security intelligence, surveillance and reconnaissance, and command and control information-sharing. To implement GIG-BE, DISA aggressively enhanced the existing end-to-end information transport system, the DISN, by significantly expanding bandwidth and physical diversity to selected locations worldwide. (Global Security, https://www.globalsecurity.org/intell/systems/gig-be.htm)

Groupe Speciale Mobile Association (GSMA): Represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. (GSMA, https://www.gsma.com/aboutus/)

High Assurance Internet Protocol Encryptors Interoperability Specification: Defines requirements for a modular suite of traffic protection, networking, and management features that provide secure interoperability between users, content repositories, and net-centric enterprise service. (Committee on National Security Systems, https://www.hsdl.org/?view&did=487795)

Information and Communications Technology (ICT): The full range of a device and applications that play a role in digital communication, ranging from monitors and cell phones to personal computers and storage devices. (SDxCentral, https://www.sdxcentral.com/resources/glossary/information-communication-technology-ict/)

ICT Supply Chain Risk Management: The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. (NIST SP 800-161)

IT: Equipment, processes, procedures, and systems used to provide and support information systems (computerized and manual) within an organization and those reaching out to customers and suppliers. (Newton's Telecom Dictionary)

IaaS: The capability to provision processing, storage, networks, and other fundamental computing resources to deploy and run arbitrary software, which can include operating systems (OS) and applications. (NIST SP 800-145)

Intelligence Community (IC): A group of Federal Government departments and agencies that collect, analyze, and deliver foreign intelligence and counterintelligence information to America's leaders so they can make sound decisions to protect the United States. (IC, https://www.intelligence.gov/)

Internet Engineering Task Force (IETF): An internet standards body that develops open standards through a community of network designers, operators, vendors, and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet. (IETF, https://ietf.org/about/)

IoT: A computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices (Techopedia, https://www.techopedia.com/definition/28247/internet-of-things-iot)

Internet Service Provider (ISP): A company that provides customers with internet access. Data may be transmitted using several technologies, including dial-up, digital subscriber line, cable modem, wireless or dedicated high-speed interconnects. An ISP is also known as an internet access provider. (Techopedia, https://www.techopedia.com/definition/2510/internet-service-provider-isp)

Interoperability: The ability of independent systems to exchange meaningful information and initiate actions from each other in order to operate together for mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility for use in services outside the direct control of the issuing assigner. (International Organization for Standardization Technical Committee 46/Subcommittee 9)

International Telecommunication Union (ITU): The United Nations specialized agency for ICT. Founded in 1865 to facilitate international connectivity in communications networks, ITU allocates global radio spectrum and satellite orbits, develops technical standards to ensure networks and technologies seamlessly interconnect, and strives to improve access to ICT to underserved communities worldwide. (ITU, https://www.itu.int/en/about/Pages/default.aspx)

Intrusion Detection Systems (IDS): Software that automates the intrusion detection process. (NIST SP 800-94)

Intrusion Prevention Systems: Software that has all the capabilities of an IDS and can also attempt to stop possible incidents. Also called an intrusion detection and prevention system. (NIST SP 800-94)

IP: A set of rules that dictate how data should be delivered over the public network (internet). Often works in conjunction with the transmission control protocol, which divides traffic into packets for efficient transport through the internet. (SDxCentral, https://www.sdxcentral.com/resources/glossary/internet-protocol-ip/)

Jitter: Variation in the delay of received packets. (Cisco, https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html)

Joint Interoperability Test Command (JITC): Provides risk-based test, evaluation, and certification services, tools, and environments to ensure joint warfighting IT capabilities are interoperable and support mission needs. (JITC, http://jitc.fhu.disa.mil/organization/aboutJitc/jitcAbout/index.aspx)

Joint Worldwide Intelligence Communications System (JWICS): Provides the Top Secret/Sensitive Compartmented Information (SCI) services, hardware, and software in direct support of Marine Corps SCI intelligence architecture. The program enables Marine Corps intelligence to access National intelligence data, services and assets in support of current and future operations of the Marine Corps Leaders. JWICS serves as the primary conduit for national-to-tactical SCI integration, network operations, specialized capabilities, remote production, exploitation, and dissemination across all intelligence domains. (The United States Marine Corps, https://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/JWICS/)

Layer 2: Refers to the second layer of the Open Systems Interconnection (OSI) Model, which is the data link layer. (Techopedia, https://www.techopedia.com/definition/16495/layer-2)

Layer 3: Refers to the third layer of the OSI Model, which is the network layer. (Techopedia, https://www.techopedia.com/definition/14825/layer-3)

Layer 7: Refers to the seventh and topmost layer of the OSI Model, or the application layer. Layer 7 identifies the communicating parties and the quality of service between them, considers privacy and user authentication, as well as identifies any constraints on the data syntax. This layer is wholly application-specific. (Techopedia, https://www.techopedia.com/definition/20338/layer-7)

Legacy Networks: The generic name assigned to any old network, which is rarely used today and not part of the Transmission Control Protocol/IP suite. Legacy networks are mostly proprietary to individual vendors. (Techopedia, https://www.techopedia.com/definition/25121/legacy-network)

Massive Machine Type Communications (mMTC): Focuses on providing connectivity to a large number of devices, but with low reliability. mMTC can provide long-range communication with energy efficiency and asynchronous access. Such features are very suitable for low power devices in a massive quantity. (MDPI, *5G URLLC Implementation Challenges and Operational Issues with IoT Devices*, https://www.mdpi.com/2079-9292/8/9/981)

Micro-Segmentation: This is a security technique that enables fine-grained security policies to be assigned to data center applications, down to the workload level. This approach enables security models to be deployed deep inside a data center, using a virtualized, software-only approach. (SDxCentral, https://www.sdxcentral.com/networking/virtualization/definitions/how-does-micro-segmentation-help-security-explanation/)

Microsoft Azure's ExpressRoute: A service that allows users to create private connections between Microsoft data centers and infrastructure on-premise or in a colocation facility. ExpressRoute connections do not go over the public internet, and offer higher security, reliability, and speeds with lower latencies than typical connections over the internet. (Microsoft, https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs)

Mobile Ethernet Forum (MEF): Provides a practical framework and roadmap for service providers and their vendors to embark on a transformation journey regardless of their starting point. MEF membership is over 200 companies. Member companies include Tier 1, 2, and 3 service providers, hardware and operational support system/orchestration software providers, test labs, test equipment and test software providers, actively contribute to key projects to reach our MEF 3.0 vision. (MEF, https://www.mef.net/about-mef)

Moore's Law: States that technology continually expands at an exponential and measurable rate. For example, Dr. Gordon Moore correctly theorized that from 1965 to 1975, the complexity of integrated circuits would grow from 60 to 60,000. Now all technological advances and increases in knowledge that happen exponentially is colloquially called Moore's Law. (Newton's Telecom Dictionary)

Multiprotocol Label Switching (MPLS): An underlying and overriding transport methodology for forwarding packet data over a network. MPLS assigns labels to data packets on ingress into the domain and forwards the data throughout the network based upon the label. (Defense Information Systems Agency, *Multiprotocol Label Switching, Global Packet Transport Rollout*)

N32 Interface: The N32 interface is used between the software engineering for parallel processing of a visited public land mobile network and a home public land mobile network in roaming scenarios. (ETSI, https://www.etsi.org/deliver/etsi_ts/129500_129599/129573/15.01.00_60/ts_129573v150100p.pdf)

Network Latency: Term used to indicate any kind of delay that happens in data communication over a network. Network connections in which small delays occur are called low-latency networks whereas network connections which suffers from long delays are called high-latency networks. (Techopedia, https://www.techopedia.com/definition/8553/network-latency)

Network Slicing: A type of virtual networking architecture in the same family as SDN and NFV, two closely-related network virtualization technologies that are moving modern networks toward software-based automation. (SDxCentral, https://www.sdxcentral.com/5g/definitions/5g-network-slicing/)

NIST Cybersecurity Framework: Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. (NIST, https://www. nist.gov/cyberframework/new-framework)

National Security and Emergency Preparedness (NS/EP) Communications: Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the national security and emergency preparedness (NS/EP) posture of the United States (47 Code of Federal Regulations Chapter II, § 201.2(g)). NS/EP communications include primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international), to include communicating with itself; the Legislative and Judicial branches; state, territorial, tribal, and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications further include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (NS/EP Communications Executive Committee based on Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions* [2012])

Networks: Information system(s) implemented with a collection of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary of Information Security Terms – NISTIR 7298 – Revision 2)

NFV: The decoupling of network functions from proprietary hardware appliances and running them as software in virtual machines. (SDxCentral, https://www.sdxcentral.com/networking/nfv/)

Node B: Term for a radio base station receiver. It provides radio coverage and converts data between the radio network and the radio network controllers. (Gartner, https://www.gartner.com/en/information-technology/glossary/node-b)

Northbound Interface (NBI): The interface to a component of higher function or level layer. The lower layer's NBI links to the higher layer's southbound interface (SBI). In an architectural overview, an NBI is drawn on the top portion of the component or layer in question and can be thought of as flowing upward, while a SBI is drawn at the bottom, symbolizing a downward flow. (Techopedia, https://www.techopedia.com/definition/29594/northbound-interface-nbi)

OAuth 2.0: The industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity, while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. (OAuth, https://oauth.net/2/)

Open Daylight Project (ODL): A modular open platform for customizing and automating networks of any size and scale. The ODL Project is a direct result of the SDN movement, with a clear focus on network programmability. It was designed from the outset as a foundation for commercial solutions that address a variety of use cases in existing network environments. (The Linux Foundation, https://www.opendaylight.org/)

Open Flow: Considered one of the first SDN standards, it originally defined the communication protocol in SDN environments to enable the controller to directly interact with the data plane of network devices, both physical and virtual (hypervisor-based), so it can better adapt to changing business requirements. (SDxCentral, https://www.sdxcentral.com/networking/sdn/definitions/what-is-openflow/)

Open Network Automation Platform (ONAP): Provides a comprehensive platform for real-time, policy-driven orchestration and automation of physical and virtual network functions that will enable software, network, IT and cloud providers and developers to rapidly automate new services and support complete lifecycle management. (The Linux Foundation Projects-ONAP, https://www.onap.org/)

Open Radio Access Network (O-RAN): Designed to enable next generation radio access network (RAN) infrastructures. Empowered by principles of intelligence and openness, the O-RAN architecture is the foundation for building the virtualized RAN on open hardware, with embedded AI-powered radio control, that has been envisioned by operators around the globe. (O-RAN Alliance, https://www.o-ran.org/)

Operational Technology (OT): Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. (Gartner, https://www.gartner.com/en/information-technology/glossary/operational-technology-ot)

Oracle Cloud's FastConnect: A network connectivity alternative to using the public internet to connect to Oracle Cloud Infrastructure and other Oracle Cloud services. (Oracle, https://www.oracle.com/cloud/networking/fastconnect.html)

OS: The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The OS sets the standards for all application programs. The applications communicate with the OS for most user interface and file management operations. (NIST, https://csrc.nist.gov/glossary/term/Operating_System)

OT-SDN: Compared to traditional SDN, OT-SDN uses static flows for proactive engineering of known network configuration.

Path Computation Engine: Computes optimized working and restoration paths, and signals dynamic configuration to the network elements (Ciena, https://www.ciena.com/insights/articles/Software-Defined-Control–Brought-to-You-by-the-Letter-C.html)

Policy Enforcement Points (PEP): A network device on which policy decisions are carried out or enforced. When a user tries to access a file or other resource on a computer network or server that uses policy-based access management, the PEP will describe the user's attributes to other entities on the system. Therefore, PEPs are usually specific to an application and cannot be re-used for different applications. (Certificate of Cloud Security Knowledge, https://ccskguide.org/policy-decision-points-policy-enforcement-points/)

Protocol: A set of rules and formats, semantic and syntactic, permitting information systems to exchange information (NIST Glossary of Information Security Terms – NISTIR 7298 – Revision 2)

Quality of Service (QoS): A set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which packets are handled, and the amount of bandwidth afforded to that application or traffic flow. (Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos)

RAN: Controls the transmission and reception of radio signals across cellular networks. Components of the RAN include a base station and antennas that cover a given region depending on their capacity. (SDxCentral, https://www.sdxcentral.com/5g/definitions/radio-access-network/)

Reliability: A measure of how dependable a system is once you use it. (Newton's Telecom Dictionary)

Resilience: The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (Presidential Policy Directive-8: National Preparedness)

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

SBI: A component's lower level interface layer. It is directly connected to that lower layer's northbound interface. It breaks down the concepts into smaller technical details that are specifically geared toward a lower layer component within the architecture. In SDN, the southbound interface serves as the OpenFlow or alternative protocol specification. It allows a network component to communicate with a lower level component. (Techopedia, https://www.techopedia.com/definition/29595/ southbound-interface-sbi)

Secret Internet Protocol Router Network: The worldwide Secret-level packet switch network that uses high-speed internet protocol routers and high-capacity DISN circuitry. (Military Factory, https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4771)

Security: A way of insuring data on a network is protected from unauthorized use. Network security measures can be software-based where passwords restrict users' access to certain data files or directories. This kind of security is usually implemented by the network operating system. Audit trails are another software-based security measure, where an ongoing journal of what users did what with what files is maintained. Security can also be hardware-based, using more traditional lock and key. (Newton's Telecom Dictionary)

Security Edge Protection Proxy (SEPP): A non-transparent proxy that sits at the perimeter of the public land mobile network (PLMN) network and enables secured communication between inter-PLMN network messages. The SEPP implements Transport Layer Security (TLS) protocols for all the service layer information exchanged between two Network Functions across two different PLMNs. (Oracle, https://docs.oracle.com/en/industries/communications/cloud-native-core/2.2.0/sepp_user_guide/intoduction.html#GUID-DD3D470E-5FF8-4779-B8E8-0FD42151D6A4)

Security Information and Event Management (SIEM): The term for software and services combining security information management and security event management. SIEM is an approach to security management that combines event, threat and risk data into a single system to improve the detection and remediation of security issues and provide an extra layer of in-depth defense. (Internal Revenue Service, https://www.irs.gov/privacy-disclosure/security-information-and-event-management-siem-systems)

Segment Routing: A flexible, scalable method for source routing. The source chooses a path and encodes it in the packet header as an ordered list of segments. Segments are identifier for any type of instruction. (Cisco: Introduction to Segment Routing, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-3s/segrt-xe-3s-book/intro-seg-routing.pdf)

Service-Based Architecture: An approach that promises to bring data center technologies like micros-service architectures and containers into 5G foundations. (SDxCentral, https://www.sdxcentral.com/resources/sponsored/downloads/interdigital-cloud-native-foundations-5g-networks/)

SDN: The separation of the control functions from the forwarding functions, which enables greater automation and programmability in the network. It is often paired with NFV, which separates network functions from hardware in for the form of virtual network functions (VNF) (SDxCentral, https://www.sdxcentral.com/networking/sdn/)

SD-WAN: A network that is abstracted from its hardware, creating a virtualized network overlay. Operators can remotely manage and quickly scale this overlay, which can span over large geographical distances. It is an application of SDN (SDxCentral, https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/)

Software Assurance Marketplace (SWAMP): Provides a national marketplace of continuous software assurance capabilities for researchers and developers. SWAMP aims to reduce the number of vulnerabilities deployed in new software systems. (DHS Office of Science and Technology, https://www.dhs.gov/science-and-technology/swamp)

Supervisory Control and Data Acquisition (SCADA): Refers to industrial control systems used to control infrastructure processes (e.g., water treatment, wastewater treatment, gas pipelines, wind farms), facility-based processes (e.g., airports, space stations, ships) or industrial processes (e.g., production, manufacturing, refining, power generation). (SCADA Systems, http://www.scadasystems.net/)

Third Generation Partnership Project (3GPP): Unites seven telecommunications standard development organizations to provide their members with a stable environment to produce the reports and specifications that define 3GPP technologies. (3GPP, https://www.3gpp.org/about-3gpp)

3GPP Technical Specifications Group Service and System Aspects Working Group 3 – Security (SA3): Performs analysis of potential threats to 3GPP systems. Based on the threat analysis, the working group will determine the security and privacy requirements for 3GPP systems and specify the security architectures and protocols. (3GPP, https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security)

Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS. (NIST SP 800-53, CNSSI 4009, Adapted)

Threat Environment: The online space where cyber threat actors conduct malicious cyber threat activity. (*An Introduction to the Cyber Threat Environment*, https://icclr.org/wp-content/uploads/2019/05/Intro-to-cyber-threat-environment-e.pdf?x37853)

Tier 1 ISP: A type of ISP that directly connects with and has access to the global internet backbone in a specific region under the settlement-free peering agreement, where the flow of information between one or more networks is exchanged voluntarily. (Techopedia, https://www.techopedia.com/definition/23819/tier-1-internet-service-provider-tier-1-isp)

TLS 1.2: This is the strongest form of TLS that is widely supported by modern browsers. (Federal Chief Information Officer, https://https.cio.gov/technical-guidelines/)

TLS 1.3: Secure socket layer/TLS creates a secure channel between a users' computer and other devices as they exchange information over the internet, using three main concepts: encryption, authentication, and integrity to accomplish this. Encryption hides data being transferred from any third parties. Authentication ensures the parties exchanging information are confirmed, while verifying the integrity of the data has not been compromised or tampered with. At a high level, this is accomplished using a handshake process. The client and server agree on an encryption key, which cypher to use during the session. After the handshake both endpoints have a symmetric key, and all subsequent transmissions are encrypted. TLS 1.3 speeds up the handshake process helping to prevent breaches of the server's key from being used to decrypt historical data. (Garland Technology, https://www.garlandtechnology.com/blog/what-is-ssl-and-tls-and-how-it-works-in-todays-security)

Trusted Internet Connection (TIC): Since its establishment in 2007, TIC has moved the Government from a period of uncontrolled and unmonitored internet connections to a controlled state, reducing the .gov domain's attack surface. (CISA, https://www.cisa.gov/trusted-internet-connections)

TIC 3.0: Expands on the original initiative to drive security standards and leverage advances in technology to secure a wide spectrum of agency network architectures. This new version of TIC is highly iterative, which means the guidance will better reflect modern processes and technological innovations compared to previous iterations of the program. TIC 3.0 recognizes shifts in modern cybersecurity and pushes agencies toward adoption, while recognizing their challenges and constraints in modernizing IT infrastructure. (CISA, https://www.cisa.gov/trusted-internet-connections)

Trustworthiness: The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. (NIST SP 800-39, CNSSI-4009)

Tunneling: A protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the internet, through a process called encapsulation. (Techopedia, https://www.techopedia.com/definition/5402/tunneling)

URLLC: Focuses on an ultra-responsive connection with ultra-low latency. The data rate is not expected to be very high in URLLC, but it does offer increased mobility. Potential applications of URLLC include industrial automation, autonomous driving, mission-critical applications, and remote medical assistance. (MDPI, *5G URLLC Implementation Challenges and Operational Issues with IoT Devices*, https://www.mdpi.com/2079-9292/8/9/981)

United Kingdom Code of Practice (CoP) for Consumer IoT Security: The aim of this CoP is to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world. (Gov.UK, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security)

Vendor Lock-In: The restricted or proprietary use of a technology, solution, or service developed by a vendor or vendor partner. (Techopedia, https://www.techopedia.com/definition/26802/vendor-lock-in)

VNF: Located at the core of NFV, VNFs handle specific network functions such as firewalls or load balancing. Individual VNFs can be connected or combined together as building blocks to create a fully virtualized environment. (SDxCentral, https://www.sdxcentral.com/networking/nfv/definitions/virtual-network-function/)

Virtual Local Area Network (vLAN) Tagging: A method through which more than one vLAN is handled on a port. vLAN tagging is used to tell which packet belongs to which VLAN on the other side. To make recognition easier, a packet is tagged with a vLAN tag in the Ethernet frame. Independent logical systems can be formed accurately with the help of the vLAN tagging inside a physical network itself (Techopedia, https://www.techopedia.com/definition/32105/vlan-tagging)

Virtual Private Network: An encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. (Cisco, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html)

White Box: A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing. (NIST SP 800-53A Revision 4)

Zero-Trust Architecture (ZTA): Provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. ZTA is an enterprise's cybersecurity plan that utilizes zero-trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero-trust architecture plan. (NIST SP 800-207, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf)

Zero-Touch Provisioning: Helps accelerate deployments based on faster, easier infrastructure installations, and associated configuration for reduced time-to-market and accelerated 5G revenues. Additionally, it eliminates manual configuration provisioning errors during the deployment of new transport equipment, ensuring that all of a user's sites are turned up rapidly and securely. (Ciena, https://www.ciena.com/insights/articles/uncovering-the-path-to-5g-connectivity-part-3-why-zero-touch-provisioning-ztp-is-critical-for-5g-success.html)

Appendix F: Bibliography

Abella, Alicia, AT&T, “AT&T’s Software-Defined Networking [SDN] Transformation” (Briefing to the President’s National Security Telecommunications Advisory Commitee [NSTAC] SDN Subcommittee, Arlington, VA, May 26, 2020).

“About Us. 2020.” The Federal Risk and Authorization Management Program (FedRAMP). FedRAMP, January 21, 2020. https://www.fedramp.gov/about/.

“Advancing SDNs: A Survey,” Institute of Electrical and Electronics Engineers (IEEE). IEEE, October 12, 2017, https://ieeexplore.ieee.org/document/8066287.

“Application Chaining.” Oracle. Oracle, https://docs.oracle.com/cd/E86291_01/docs.81/20170711_115004_m_dsr_fabr_help/concepts/c_dsr_help_fabr_application_chaining.html.

AT&T, “FirstNet Soars with Over 1 Million Connections and Launch of ‘FirstNet One’ – a Deployable Blimp – for Public Safety,” December 16, 2019, https://www.firstnet.com/community/news/firstnet-soars-with-over-1-million-connections.html.

—, “Fifth Generation [5G] for You.” AT&T, 2020, https://about.att.com/pages/5G.

Berthou, Pascal and Hakiri, Akram, “Leveraging SDN for 5G Networks: Trends, Prospects, and Challenges,” French National Center for Scientific Research- The Laboratory for Analysis and Architecture of Systems, https://arxiv.org/ftp/arxiv/papers/1506/1506.02876.pdf.

Boeckl, Kaitlin, et. al., “Considerations for Managing Internet of Things [IoT] Cybersecurity and Privacy Risks,” National Institute for Standards and Technology (NIST), June 2019, https://csrc.nist.gov/publications/detail/nistir/8228/final.

Borchert, Oliver, et. al., “Zero Trust Architecture,” NIST Special Publication 800-207, February 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.

Burger, Eric, Office of Science and Technology Policy, “SDN Technology Policy” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, March 5, 2020).

Bush, Terry, Ericsson, “NSTAC SDN Brief” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 28, 2020).

California Senate Bill Number 327-Chapter 886, “An Act to Add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, Relating to Information Privacy,” California Legislative Information, September 28, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

Chua, Roy, AvidThink, “State of SDN 2019” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 19, 2019).

“Communications Security, Reliability, and Interoperability Council.” Federal Communications Commission (FCC). FCC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

“COVID-19: How Cable’s Internet Networks Are Performing-Metrics, Trends, and Observations.” The Internet and Television Association (NCTA). NCTA, https://www.ncta.com/COVIDdashboard.

CTIA – The Wireless Industry Association, “U.S. Wireless Industry Contributes $475 Billion Annually to America’s Economy and Supports 4.7 Million Jobs, According to New Report,” CTIA, April 5, 2018, https://www.ctia.org/news/study-reveals-powerful-economic-impact-of-wireless-across-50-states.

—, “Wireless Industry Announces New Cybersecurity Certification Program for Cellular-Connected IoT Devices,” CTIA, August 21, 2018, https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program.

Danilowicz, Neil, Versa Networks, “NSTAC SDN Briefing” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 30, 2020).

Dano, Mike, “AT&T: SDN, Network Functions Virtualization (NFV) Helped Meet COVID-19 Traffic Demands,” LightReading, April 2, 2020, https://www.lightreading.com/cloud-native-nfv/atandt-sdn-nfv-helped-meet-covid-19-traffic-demands/d/d-id/758661.

Dassanayaka, Ranil, VMware, “The Role of Virtualization Platforms in Transforming Security” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, February 18, 2020).

Defense Information Systems Agency (DISA). “About DISA,” January 21, 2020. https://www.disa.mil/About.

Department for Digital, Culture, Media, and Sport, “Code of Practice for Consumer IoT Security.” Gov.UK, October 2018, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

Ericsson, “5G Security - Enabling a Trustworthy 5G System,” January 8, 2020. https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security—enabling-a-trustworthy-5g-system.

Entner, Roger, Recon Analytics, “Conversation around SDN” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, February 18, 2020).

European Union Agency for Cybersecurity (ENISA), “Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures,” ENISA, November 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

Fagan, Michael, et al., “Foundational Cybersecurity Activities for IoT Device Manufacturers,” NIST, May 2020, https://csrc.nist.gov/publications/detail/nistir/8259/final.

“Fifth Generation Supply Chain Working Group.” Alliance of Telecommunications Industry Solutions (ATIS). ATIS, 2020, https://www.atis.org/01_strat_init/5g-supply-chain/.

“First Responder Network (FirstNet) Authority Roadmap.” FirstNet. FirstNet, 2019. https://www.firstnet.gov/system/tdf/FirstNet_Roadmap.pdf?file=1&type=node&id=1055.

“FirstNet Nationwide Coverage.” FirstNet. FirstNet, January 20, 2020, https://www.firstnet.com/coverage.html.

“FirstNet: The History of Our Nation’s Public Safety Network.” FirstNet.FirstNet, https://firstnet.gov/about/history.

Fuetsch, Andre, “How a Software-Centric Network Keeps Business Customers Connected in a Highly Safe Manner,” AT&T Technology Blog, April 2, 2020, https://about.att.com/innovationblog/2020/04/anira.html.

General Services Administration (GSA). “GSA Background and History - Mission and Strategic Goals. January 21, 2020. https://www.gsa.gov/about-us/background-history/mission-and-strategic-goals.

Goldstein, Phil, “Why DISA Has Embraced SDN for the Pentagon,” FedTech, September 28, 2018, https://fedtechmagazine.com/article/2018/09/why-disa-has-embraced-sdn-pentagon-perfcon#:~:text=DISA%20announced%20its%20shift%20to,based%20on%20software-defined%20technologies%20.

Gottlieb, Andrew, Oracle, “Delivering Reliability and Quality of Experience with Failsafe Software-Defined Wide-Area Networks (SD-WAN) Technology” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 17, 2019).

Guo, Yang, National Institute of Standards and Technology (NIST), “Some Thoughts on SDN Security” (Briefing to the NSTAC SDN Subcommittee. Arlington, VA, December 3, 2019).

Hadley, Mark, Pacific Northwest National Laboratory, “SDN for Operational Environments” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, February 20,2020).

Hawkins, Stephen “Chris,” Laboratory for Advanced Cybersecurity Research “SDN” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 30, 2020).

Horner, Larry, Intel, “Securing the Network in the Age of Virtualization” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, March 10, 2020).

“Information and Communications Technology Supply Chain Risk Management Task Force.” Cybersecurity and Infrastructure Security Agency. Department of Homeland Security, March 5, 2019, https://www.cisa.gov/ict-scrm-task-force.

Jain, Raj, Washington University in St. Louis, “Challenges of SDN in National Security” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 10, 2019).

Kapko, Matt “Dish Firm on 5G Costs,” SDxCentral, February 20, 2020, https://www.sdxcentral.com/articles/news/dish-firm-on-5g-costs/2020/02/.

“Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.” NIST Computer Security Resource Center. NIST, February 2020, https://csrc.nist.gov/publications/detail/nistir/8276/draft.

Khalidi, Yousef, Microsoft, “Enabling and Securing Ubiquitous Compute from Intelligent Cloud to Intelligent Edge” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 16, 2020).

Kovac, Stephen, Zscaler, “Zscaler: Federal Platform” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, February 6, 2020).

Lemons, William and Richberg, James, Fortinet Federal, “SDN: A Security Original Equipment Manufacturer’s Perspective” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, March 5, 2020.

“Lifecycle Service Orchestration.” MEF, MEF, https://www.mef.net/lso/lifecycle-service-orchestration.

Martin, Adrian Belmonte, et al., “Threat Landscape and Good Practice Guide for SDN/5G Networks,” The European Union Agency for Network and Information Security, January 27, 2016, https://www.enisa.europa.eu/publications/sdn-threat-landscape.

Marty, Rita, AT&T, “SDN Best Security Practices” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, May 26, 2020).

Medin, Mark and Sirangelo, Mark, “Defense Innovation Board: Fully Networked Command, Control, and Communications Recommendations.” *Department of Defense*. October 25, 2019. https://media.defense.gov/2019/Oct/31/2002204194/-1/-1/0/DIB_FULLYNETWORKEDC3_RECOMMENDATIONS.PDF.

Membership Information.” O-RAN Alliance, https://www.o-ran.org/membership.

Moore, Gordon, “Cramming More Components onto Integrated Circuits,” Electronics, Volume 38, Number 8, April 19, 2965, http://www.monolithic3d.com/uploads/6/0/5/5/6055488/gordon_moore_1965_article.pdf.

“Moore’s Law.” Techopedia. Techopedia, June 14, 2012, https://www.techopedia.com/definition/2369/moores-law.

Morris, Iain “The Future’s Bright, the Future’s Open Radio Access Networks,” LightReading, June 28, 2018, https://www.lightreading.com/mobile/fronthaul-c-ran/the-futures-bright-the-futures-O-RAN/d/d-id/744294.

“Network Functions Virtualization 101 Networking Foundations Guide.” SDxCentral. SDxCentral, https://www.sdxcentral.com/networking/nfv/definitions/nfv-101-networking-foundation-guide/.

“Network Performance.” USTelecom. USTelecom, 2020, http://www.ustelecom.org/research/network-performance-data/.

NSTAC. *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, Washington, DC: NSTAC, September 3, 2019, https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_0.pdf.

NSTAC, *NSTAC Report to the President on Emerging Technologies Strategic Vision*, July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

Obraczka, Katia, University of California, Santa Cruz, “NSTAC SDN Briefing” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 19, 2019).

“Open Network Automation Platform.” Linux Foundation Project. Linux Foundation, https://www.onap.org/about.

Palmer, Matthew, SDxCentral, “Accessing Security Ramifications and Risks of Network Evolution to SDN” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 16, 2020).

Pankajakshan, Bejoy, Mavenir, “NFV-Driven Rise of SDN: Challenges and Opportunities” (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, February 6, 2020).

Rakuten, "A World First for 5G: Rakuten Mobile and NEC Deploy Groundbreaking Radios for New 5G Network," Rakuten, April 9, 2020, https://rakuten.today/blog/rakuten-mobile-partner-profile-nec.html.

Robuck, Mike, "AT&T on Target for Virtualizing 75% of its Network by 2020," Fierce Telecom, January 3, 2020, https://www.fiercetelecom.com/telecom/at-t-target-for-virtualizing-75-its-network-by-2020.

Rysavy, Peter, Rysavy Research, "Overview of SDN and Virtualization" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, December 10, 2019).

Ryland, Mark, Amazon Web Services, "Network Modernization in the Cloud Era" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

SDxCentral Staff, "How 5G SDN Will Bolster Networks," SDxCentral, October 31, 2017, https://www.sdxcentral.com/5g/definitions/5g-sdn/.

Shalita, Steven, Pluribus Networks, "Leveraging Next-Generation SDN to Improve Security and Transform Operations" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, March 3, 2020).

Simlot, Anil, CenturyLink, "Importance of SDN for a Service Provider" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 23, 2020).

Stolfo, Salvatore, Allure Security, "SDN: Producer and Consumer of Security" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 21, 2020).

"Trusted Internet Connections." CISA. CISA, March 16, 2010, https://www.cisa.gov/trusted-internet-connections.

Ward, David, Cisco Systems, "SDN and Virtualization Technologies in Communication Networks to Thwart Cyber Threats and Improve Security" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 7, 2020).

Zielinski, William, GSA, "SDN and Network Modernization with Enterprise Infrastructure Solutions" (Briefing to the NSTAC SDN Subcommittee, Arlington, VA, January 21).