Military Cyber Affairs

Volume 4
Issue 2 *Technological Challenges in Cyberspace*

Article 3

December 2020

Three Emerging Innovative Technologies Required for Cyber Operations to Execute Commander’s Intent at Machine Speed

Andrew Stewart
andrewst@cisco.com

Three Emerging Innovative Technologies Required for Cyber Operations to Execute Commander's Intent at Machine Speed

Erratum

Format changes (various)

Three Emerging Technologies Required for Cyber Operations to Execute Commander's Intent at Machine Speed

Andrew Stewart

Abstract

Decision advantage for the DoD and Combined Cyber Operations results from the secure, seamless, and rapid maneuver of data and information. In the DoD's 2018 Artificial Intelligence Strategy, the DoD recognized that it must, "put in place key building blocks and platforms to scale and democratize access to AI. This includes creating a *common foundation* of shared data, reusable tools, frameworks and standards, and cloud and edge services."[1] More than ever, integrated, adaptive cyber operations provide the means of maneuver for data to enable DoD's decision advantage-based goals. To support this vision, the integrated implementation three innovative cyber technologies must be rapidly realized across DoD Networks in order to execute cyber operations according to Commander's Intent—at machine speed

Getting Information to the "edge" is what makes DoD competitive and provides advantage. The word "edge" in this context reflects the distributed individual platforms, sensors, and people who comprise the scale and scope of today's globally networked DoD operations. That edge is creating the demand to access data and consume information as never before, and a greater need for more innovation to support DoD cyber operations on the DoD Information Network (DODIN). At the heart of the need for innovation is an increased demand for data and information, as well as the size and scale of networks and networking exploding without a proportionate growth in the IT resources to support today's cyber operational demand. If the network continues to grow exponentially and must function as the medium of maneuver for the data that provides DoD decision advantage to the edge, then the DoD must deploy revolutionary innovations to reinvent the network as an integrated platform for cyber operations—across the enterprise and to the edge and implemented natively as hybrid multicloud-ready.

Three innovative, next-generation networking technologies, integrated tightly together, offer the opportunity for DoD to provide revolutionary cyber operations capabilities across the DODIN and produce improved, data-enabled mission results. The scalable and seamless integration of: (1) advanced identity management, (2) software-defined networking, and (3) hybrid multicloud capabilities provides a Commander's Intent-driven Cyber Platform implemented in a zero trust architecture that operates at machine speed and ensures decision advantage for the DoD.

1. Three Imperatives for the Integrated Emerging Technology Cyber Platform

Imperative 1.

The Department of Defense's (DoD) recently released Artificial Intelligence Strategy and supporting documents describe and direct how DoD must take

[1] Department of Defense (DoD), Summary of the 2018 Artificial Intelligence Strategy, Feb. 2019, 7.

immediate action to realize the benefits of AI across tactical, operational, and strategic levels. These strategy and policy directives have launched a set of initiatives to enable data as a new "force in being" that will enhance decision making and drive superior operational outcomes across DoD's missions. Accordingly, each of the DoD Service Components (and much of the Federal Government) have launched "Digital Transformation Initiatives" in order to "harness the power of data" to drive faster, more efficient decision making in order to enhance their mission outcomes. Implementing an intent-driven Cyber Platform is a necessity for any organization's digital transformation efforts. Although the implementation of novel data strategies and new data-science algorithms are absolute necessary conditions for the Department to achieve these goals, DoD must undertake the essential implementation of integrated, emerging networking capabilities to ensure that its network, the DODIN—a warfighting platform—can guarantee the sufficient conditions to operate as a secure, agile, and Commander's-Intent informed Cyber Platform that provides the medium of maneuver for data.

Imperative 2.

Simultaneous to AI/ML-driven digital transformation efforts in the Federal government, DoD and Government agencies are deliberating on the tenants of a Zero Trust Architecture in order to protect data, infrastructure, and networks from growing digital threats. DoD must adopt a zero trust network architecture based on a "verify and never trust" approach. Assuming attackers and malicious insiders will penetrate threat-centric defenses, applying the zero trust approach to the Cyber Platform requires that security must extend throughout the network, not just at the perimeter. The original tenets of a zero-trust network center around the following elements:

- Software Defined Networking and Identity, Credential, and Access Management (ICAM) are essential Zero Trust components;
- Eliminate network trust. Assume that all traffic, regardless of location, is threat traffic until it is verified (authorized, inspected, and secured);
- Segment network access. Adopt a least-privileged strategy and strictly enforced controls so users have access only to the resources needed to perform their job; and,
- Gain visibility and analytics. Continuously inspect and log all traffic both internally and externally, using real-time protection capabilities, to monitor for malicious activity.[2]

The American Council for Technology-Industry Advisory Council (ACT-IAC) recently published the industry-recognized Zero Trust Maturity Model depicted in Figure 1. The ACT-IAC report provides a guide for implementing a Zero Trust Architecture based on the tenants above and recommends that agencies must move beyond the weaknesses of the traditional hub-and-spoke network model and implement strong identity management with software defined

[2] American Council for Technology-Industry Advisory Council (ACT-IAC), "Zero Trust Cybersecurity Current Trends," April 2019, 7

wide area network (SD-WAN) capabilities in an architecture that is based on a logically defined "Control Plane/Data Plane model."3

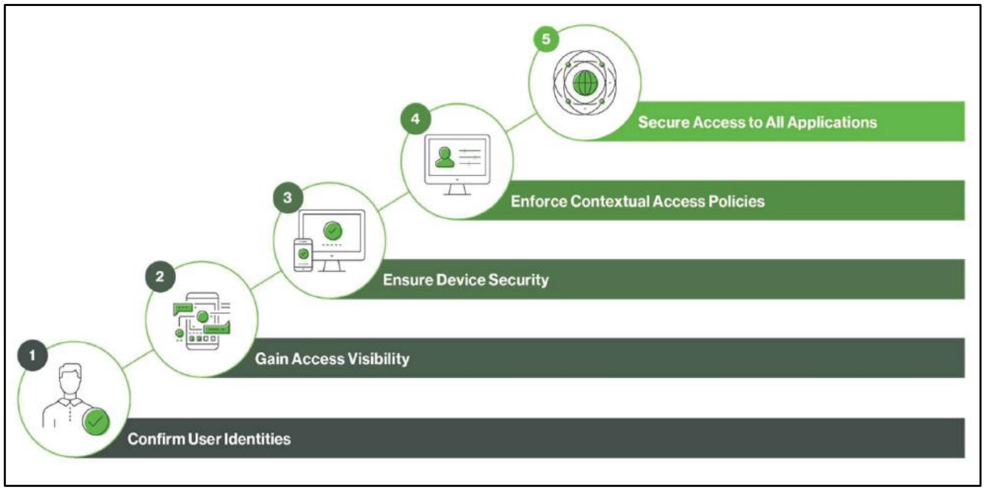

Figure 1 - Zero Trust Maturity Model from ACT-IAC

Imperative 3. Operating the network as a warfighting platform requires a machine-speed platform that can execute mission based on Commander's Intent. Commander's Intent "is the commander's clear and concise expression of what the force must do and the conditions the force must establish to accomplish the mission."4 Commander's Intent is applied through controlling actions and maneuver orders to units of action, according to the units' specific capabilities. Likewise, the network platform must apply policy and controlling actions, at machine speed to users and devices to satisfy Commander's Intent for the Cyber Platform. Admiral Robert Willard's famous article on the art of command and control provides a concise list for exerting controlling actions which are as relevant to physical units of maneuver as they are to implementing network policy and actions on the Cyber Platform:

- Maintain alignment with the operational mission.
- Provide situational awareness in the framework of the agreed-upon common operational picture.
- Advance the plan on the timeline and adjust to deviations accordingly.
- Comply with procedure to achieve standardization and effectiveness.
- Counter the enemy and be responsive to emerging intelligence, surveillance and reconnaissance.
- Adjust apportionment of assets and resources, including time.

[3] ACT-IAC, 11

[4] Joint Publication 3.0, October 2018, II-7

Thus, executing Commander's Intent for the network means exerting controlling actions through procedures and automated policy that includes controlling actions that:

- Provision of all devices at scale per respective functions and mission outcomes.
- Exercise centralized management – informed by threats and extreme visibility of all network flows and devices.
- Handle network authentication, granular access control, and rapid device discovery.
- Conduct continuous monitoring and enforce policy
- Execute protective segmentation orders when necessary to counter threats.
- Make adjustments for optimal performance across network, devices, and applications.

Therefore, there exists an immediate data-driven need for DoD to implement a Cyber Platform established on a zero trust architecture through the scalable and seamless integration of the emerging technologies of (1) advanced identity management, (2) software-defined networking and (3) hybrid multicloud capabilities. Such a Commander's Intent-driven Cyber Platform operates at machine speed and ensures decision advantage for the DoD.

1.1. The Cyber Platform: Data-Driven Operational Requirements

Connecting data across cyber terrain from the edge, datacenters, and through multi-cloud environments, the Commander's Intent-driven Cyber Platform provides integrated networking, security and distributed computing that empowers all DoD mission sets—across all domains. Realizing the operational advantage of accelerated and data-informed decision cycles, requires a secure decision infrastructure, or Cyber Platform, that understands mission intent and implements agile data maneuver and distribution schemas, at scale and speed, via software-defined, intent-based networking capabilities. Software-defined, intent-based networking recognizes the relationship between users, data, machines, devices and applications and can seamlessly and securely connect them across strategic, operational, and tactical decision environments with machine-speed agility.

In DoD's global cyber operational environment, this revolutionary Cyber Platform provides the means for the infrastructure fabric to effortlessly adapt to mission needs across the DoD cyber terrain: from where the data is (data lakes, operational platforms, and/or distributed sensors); to where the compute resources reside (datacenters, clouds, and/or edge nodes), and respond to mission constraints (latency, data sovereignty/classification, and/or mission resiliency). Thus, the Cyber Platform's intelligent, software-defined networking capabilities automatically prioritize, maneuver, and ensure the security of the data to the required, dynamic and contextual computing resources and services. Informed by mission priorities, intent-driven and woven together with interlaced mission threads and infrastructures, the Cyber Platform operates as an intelligent mission fabric that automatically orchestrates networking, distributed resources and services to deliver data, computing at scale, and computing point-of-need at the time of need—across edge, data centers, and multicloud cyber terrain.

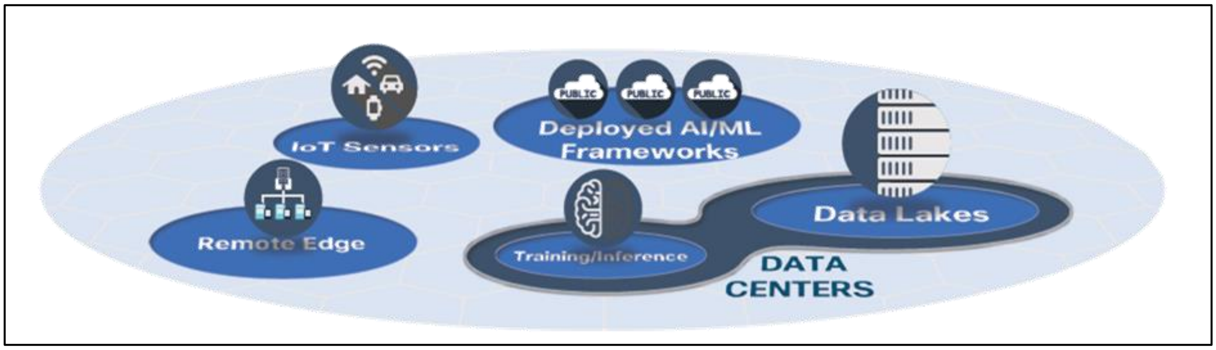

Figure 2 - Integrated Data Environments

An understanding of the operational characteristics of the edge, data center, and multicloud environments is critical to understand how to exploit the data in each of these environments, consider key characteristics of each environment, and, how to apply the requisite innovative technologies to the Cyber Platform across these environments. Section 2 will describe the requisite technologies in detail.

1.2. The Edge Environment

The edge is characterized by two key attributes:

1. The accumulation of large amounts of data coming from an exploding number of operational technology (OT) devices that have intermittent-to-pervasive connectivity via mobile or wireless networking (WiFi, 5G, LoRa, etc); and

2. The need for agility for speed of decision and action through the rapid synthesis of the data. For operational decision making, the key element of the successful use of this data will be connecting the data to edge computing (or, fog computing) which is computing power placed near the creation of the data to provide real-time analysis and action. In fact, both the edge and cloud environments share "data-center-like" functional needs for compute and processing; however, it is the data gravity derived from OT-like devices and the need for agility that differentiates the edge environment from the cloud and data center environments.

In order to tap into this data for mission outcomes, OT devices must be reliably connected, secured and managed through dynamic, profound Identity Management capabilities and software-defined networking. With secure, policy-enforced network flows established from trusted devices, the Cyber Platform can extract, compute and move data from Operational Technology (OT) systems to the most optimal applications and/or services where the data can be unlocked to create value. This includes not only meeting the requirements for speed of decision making at the edge; but also, means the Cyber Platform can move edge-derived data—via a transport-aware software-defined architecture—in order to enrich higher-echelon data models and algorithms in the data center and/or cloud environments. New insights and models from the data center or cloud environments that are refined by the latest edge-derived data are then delivered back to the edge to enhanced agile decision making.

1.3. The Data Center Environment

The DoD AI Strategy recognizes that AI-enabled capabilities at the forward edge, "will require the Department to put in place key building blocks and platforms to scale and democratize access to AI."[5] Modern hyperconverged infrastructure delivers the integrated capabilities of networking, computing power, and data storage combined with the flexibility that DoD requires for the development and deployment of AI/ML algorithms. Innovations for computing and networking in the data center are compatible with smaller formfactor hyperconverged edge nodes. Together, these contribute to the democratization of AI/ML by enabling enterprise environments to run powerful analytics and models seamlessly on infrastructure that is recognized and understood by the Cyber Platform. Providing command and control for the network's data maneuver paths, the Cyber Platform provides the means to realize scalable adaptability, programmability, and manageability to power AI/ML applications at any scale and over any cyber terrain location. Enabled by software-defined networking, advanced identity management, and extreme workload visibility, the Cyber Platform automatically provides operational management simplicity, application agility and security into and out of the data center – to any workload, to any location, or to any cloud. Cyber Platform multicloud capabilities further extend automation, management, and security by fully integrating with their respective cloud platform (XaaS) services environment.

1.4. The Multi-Cloud Environment

Securely moving data and/or an AI/ML model and its associated dependencies from a development environment to a cloud cluster can be an involved process and the dynamic management of such a complex ecosystem can be equally dauting. The multicloud-enabled Cyber Platform brings together infrastructure, security, management, open APIs, containers, and tools to create a consistent and secure environment across on-premises data centers and across multicloud environments. Rapid deployment and management of AI/ML applications in the cloud can be made possible via containers which allow developers to quickly, easily, securely and consistently deploy and monitor container clusters across local environments and across public clouds.

As DoD consumes more multicloud services, the Cyber Platform must automatically identify performance trends to right-size resources across clouds and data centers. With these integrated capabilities, DoD can deploy and incorporate new AI/ML applications quickly into cloud-based analytical environments; securely connect them to data lakes; and enrich models with data supplied by the edge – all using an integrated multicloud management platform that demystifies the orchestration of this complex ecosystem. By dynamically expanding to multicloud environments according to mission need and demand, DoD can adaptively streamline the consumption of multiple services securely and do so with speed and agility.

[5] DoD AI Strategy, 7

2. Integrated Technologies – Vision

The intent-driven network provides DoD the medium of maneuver for the data that provides decision advantage to the DoD. A Commander's Intent-driven network is made possible through the tight integration of three emerging capabilities for advanced user/device identity, software-defined networking, and native-multicloud technologies. These capabilities allow for a revolution in operations for the DODIN to be realized as a DoD Cyber Platform that delivers integrated network operations with visibility, agility, and security on a zero trust architecture. Least privilege access, intent-driven policy is applied to every OT device, all users and devices, and on each and every workload through an advanced approach to identity management and access control – enabled by the integration of dynamic identity with software-defined networking and native multicloud capabilities.

As required to implement a zero trust architecture, software defined networking provides granular access control and logical micro segmentation by weaving layers of network into a policy-driven fabric that understands and automatically implements and enforces Commander's Intent for cyber operations. Consistent with the essential Zero Trust Control Plane/Data Plane model, as shown in Figure 3 below, software defined networking provides the means to form abstraction layers in the network to reduce the complexities of managing individual devices and enhance security by interlacing a fabric of only those connections that are authorized per Commander's Intent. Software defined networking capabilities will be described in greater detail in Section 2.2; however, in the context of identity management and policy enforcement, understanding the Zero Trust Controller Layer is most critical.

Akin to the "Trust Engine" described in the ACT-IAC Zero Trust guide[6], in the Controller Layer, the Identity Engine and both Control Platform systems work together to form an abstraction layer that understands and executes Commander's Intent for network operations. This policy-to-task automation removes the complexities and dependencies of manual implementation across many network devices and protocols. All of the "identity" and "policy" services are provided by the Identity Engine. All of the "base" and "fabric" automation services are provided by the NCP, and all of the "analytics" and "assurance" services are provided by NDP. These three subsystems form the "software defined" aspect of the overall networking solution. Each subsystem is responsible for managing its respective part of the solution, and for exchanging contextual information with the others. In the Controller Layer, these three subsystems work together to deliver a fully automated Commander's Intent-driven, closed-loop management system for devices on the network.

[6] ACT-IAC, 14

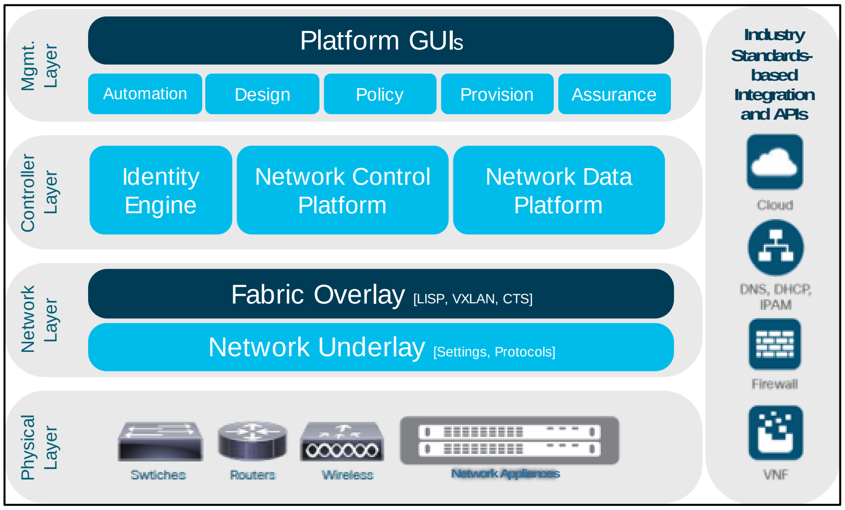

Figure 3 - Software Defined Networking Layers (adapted from[8])

Description of the Layers in Figure 3

- Physical Layer: Contains the hardware elements, such as routers, switches and wireless platforms, interfaces and links, and clusters or virtual switches, as well as server appliances.
- Network Layer: Contains the control plane, data plane, and policy plane elements that make up the network underlay and fabric overlay.
  - The network underlay is analogous to a typical Layer 2/Layer 3 network and is most closely associated with the physical layer, but with a simplified focus on transporting data packets between network devices for the (logical) overlay.
  - The fabric overlay is a mostly a logical (tunneled) network that virtually interconnects all of the network devices (to form a "fabric") and this abstracts the inherent complexities and limitations of the (physical) underlay.
- Controller Layer: As described, contains the software system management and orchestration elements and associated subsystems, such as automation, identity, and analytics.
- Management Layer: Contains the elements that users interact with, such as Graphical User Interfaces (GUIs), as well as APIs to control and interface with network devices and services.[7]

With this architecture in place, "the zero trust model can assert that every single flow on the network is authenticated and expected. Hosts and network devices can drop traffic that has not had all of these components applied, significantly reducing the likelihood of sensitive data

[7] Cisco Systems Inc, "Software-Defined Access 1.0," 2018, 3

leaks. Additionally, by logging each of the control plane events and actions, network traffic can be easily audited on a flow-by-flow or request-by-request basis."[8]

Going beyond the "local network environment," software-defined networking becomes absolutely essential for enterprise networking and translating Commander's Intent to public and private cloud clouds. "Cloud orchestration is the use of programming technology to manage the interconnections and interactions among workloads on public and private cloud infrastructure. It connects automated tasks into a cohesive workflow to accomplish a goal, with permissions oversight and policy enforcement."[9] Critical to executing Commander's Intent into such multicloud environments, through orchestration, the Cyber Platform can integrate checks for security and compliance by leveraging its profound understanding of identity and workload authorizations. Thus, the Cyber Platform must be a natively realized as a hybrid multicloud from inception to command and control a more dynamic infrastructure. This is critical to serve DoD mission needs related to data-driven outcomes when using existing DoD infrastructure and when, as required, expanding to multicloud services to meet new or more demanding mission needs on call.

As discussed, DoD must leverage its vast amounts of data to drive mission outcomes. In their quest for digital transformation, organizations across the Federal Government are rewriting their mission strategies to appropriately leverage cloud-delivered technologies where cloud-delivered capabilities make the most sense. Digital transformation efforts require the transformation of yesterday's data center—formerly defined by static workloads confined to specific infrastructure silos—to an extended, dynamic data environment that supports hybrid multicloud environments in which any workload can be provisioned anywhere and can scale on demand according to data and application needs. Software defined networking "solutions can provide a powerful framework for hosting and adding value to cloud automation solutions, which provide higher level workflow and process automation services, and rely on the underlying software defined framework to program, provision, and configure infrastructure nodes."[10]

Hence, to meet digital transformation needs, it is not a question of whether expanding consumption of hybrid multicloud solutions will be necessary, it is a question of how to best integrate the right capabilities in the most optimal way to support mission outcomes. Software defined networking and advanced identity management provide the means for the Cyber Platform to seamlessly expand to these services with integrated security via a zero trust architecture.

The need to enable the speed and pace of innovation required for cloud technologies to deliver on mission objectives means DoD will need a multicloud ready Cyber Platform built for data. One that:

- Extends from the edge to the cloud
- Integrates with every cloud

[8] ACT-IAC, 12

[9] TeachTarget, https://searchitoperations.techtarget.com/definition/cloud-orchestrator

[10] Kinghorn, Gary and Underdahl, Brian, Software Defined Networking for Dummies, (New Jersey: John Wiley & Sons, Inc.), 2015, 21

- Protects everyone
- Connects the right data, to the right user, on the right device at the right time
- And automates it all.[11]

In summary, the vision for an intent-driven Cyber Platform that provides DoD the medium of maneuver for the data to provide DoD decision advantage is realized from the tight integration of these three emerging technologies—advanced user/device identity management, software-defined networking, and native-multicloud capabilities. The next sections explore each emerging technology in greater detail; however, it is the deliberate close integration of these individual capabilities that delivers this vision for a Cyber Platform built on a foundational zero trust architecture.

2.1. Advanced Identity Management

Advanced identity management coupled with the software-defined networking control plane (introduced above and discussed in the next section), provides the means to implement granular micro-segmentation at scale and speed, and enables an automated network fabric that allows operational technology (OT) devices (or, "devices without users") and users and devices (abbreviated: users/devices) to connect more easily and more securely. As discussed in Imperative 3 above, in the physical world, Commander's Intent is applied through controlling actions via the orders process, according to each unit's specific identities and defined capabilities. For DoD cyber operations, the network must also be able to apply policy to users and devices – based on their individual capabilities and assigned missions – with full knowledge of how they are connected to the network, and their allowed functions – automatically, at scale and speed.

The decision criteria for individuals to access to data in the DoD is usually based on: (1) identification and authentication—does the individual have the proper credentials for identification? and (2) authorization – is the individual authorized to access the data, or "do they have the need to know?" The intent-driven Cyber Platform takes the same approach for the identity of all OT devices and users/devices that attempt to connect to the network. This challenge/authentication process is not a single event; rather, using dynamic context and identity authentication, the Cyber Platform, applies least privilege access principles continuously challenging and authenticating every user/device every time a data access decision must be made, at machine speed.

Establishing the identity of every device on the network has historically been a challenge for the DoD. As a result of NDAA legislation, all DOD Components were required to implement a Comply-to-Connect (C2C) Framework. Rightly so, these efforts focus on the automatic detection and identification of all devices in order to comprehensively obtain an accurate inventory of all devices on DoD networks and enforce endpoint health compliance and facilitate remediation. Although the C2C framework remains a necessary first step for complete visibility of all network devices and enforcing their health – and, per zero trust objectives, doing so *before **any** network connection and access to data is granted* – a more comprehensive

[11] Michaelides, Nick, "Cloud Ready Networks for Government: Connecting Everyone and Everything," https://blogs.cisco.com/government/cloud-ready-networks-for-government-connecting-everyone-and-everything, July 2019

implementation of user/device identity must be implemented to satisfy the zero trust imperative. In order to fulfill the necessary and sufficient conditions for a zero trust model user/device identification and logical segmentation of compliant endpoints, a more dynamic approach to user/device identity based on role and function of the user/device is required. Expanding beyond the initial, necessary network access control (NAC) functions, such an approach to identity provides the functions necessary to enforce comprehensive authentication and authorization for every IOT device and user/device as described for the "Trust Engine"[12] in the Zero Trust model. Hence, with a deep understanding of every IOT device and user/device identity integrated into the controller layer of the network, the Cyber Platform constantly applies granular network access controls and enforces those policies based on a profound understand of those profound identity characteristics – doing so adaptively, with as much dynamic operational context as possible; not one time, but every time a data access decision is made. Thus, Commander's Intent for the network is applied through network policy controlling actions, via the control plane, according to each user/devices' specific identities and defined capabilities – based on their individual capabilities and assigned missions. These policies are applied ***before*** network connection/access is granted with full knowledge of how they are connected to the network, their compliance and capability status, and their allowed functions. This is executed automatically, at scale and speed with no manual CLI or SSH/SNMP calls to the physical layer to make the required dynamic access changes; and, simultaneously, intent-informed hosts and network devices automatically drop traffic that has not had the requisite trust components applied.

Just as important, Commander's Intent based controlling actions must be applied and enforced to every application workload across the edge, datacenter, and especially including connections between containers or hypervisors in the cloud. Application data flow in today's modern networks flow across edge, datacenter and multicloud environments and number in the millions of flows per second. Users and devices must be able to access data and workload beyond their local environments—including those that are delivered from internet-delivered multicloud services. A software defined networking approach allows for the implementation of a Software Defined Perimeter (SDP) that "comports with zero trust by maintaining a default-deny posture for every transaction. Policy is defined by user and context . . . reduc[es] risk below that of micro-segmentation alone. The risk of unauthorized lateral movement is eliminated because all transactions are assessed the same way they occur inside or outside the enterprise firewall."[13] Combined with a profound understanding of the identity of users/devices on the network, the integrated Cyber Platform automatically maps out device workloads and implements application whitelisting across all environments and over millions of flows per second ("machine speed") according to Commander's Intent. This SDP-approach "creates a protective barrier around high value enterprise applications and data access" that "protect[s] application infrastructure against existing and newly emerging cyber threats," blocking them dynamically, by "only allow[ing] access from devices registered to authenticated users which is a key zero trust element."[14]

Hence, augmented by dynamic network context and coupled with authentication mechanisms, advanced identity management enables the Cyber Platform to assign granular

[12] ACT-IAC, 14

[13] ACT-IAC, 22.

[14] ACT-IAC, 22.

attributes about users, devices, and workloads to assign and enforce micro-segmentation policies based on zero trust access. These policies are logically applied and executed per Commander's Intent via a software-defined network.

2.2. Software-Defined Networking

Software-Defined Networking is a programmable network architecture that provides software-based access, policy and segmentation from the edge of the network and across the enterprise. The above introduction to Section 2 and Figure 3 provided the fundamentals on how the abstraction layers function in a modern software defined network. This section focuses on how this emerging technology enables the Cyber Platform and interreacts with advanced identity management and multicloud technologies. Modern software-defined networking provides multiple benefits for cyber operations:

- Reduction in complexity with automated services;
- Scaling in size and scope – including Operational Technology (OT) with segmentation;
- Constant monitoring and collection of network telemetry and flows;
- Actionable insights from network information; and
- Automated actions to enforce policy or recommendations for new policies.

As discussed, advanced identity management operating in the controller layer (see Figure 3) provides all of the identity and policy services for the physical layer and network layer. Automated identification and profiling of network devices and endpoints is accomplished via the Commander's approved policies and mechanisms—e.g.: AAA/RADIUS, 802.1X, and others. However, the identity engine continues to collect and apply the contextual information shared from NDP, NCP, and via industry-standard APIs across the Cyber Platform (e.g.: to/from active directories, firewalls, cloud instances, IPAM services, etc.). From this dynamic information constantly being gleaned by the identity engine, the controller layer places the profiled endpoints into the correct security-defined group and enforces micro-segmented device access per Commander's Intent-driven policy for each IOT device, user/device, and workload—automatically at speed and scale.

The dynamic identity information is provided, to the management layer so that the Cyber Platform can create, enforce, and manage mission-defined group-based access policies across the entire global enterprise and extend those policies into multicloud environments. Compared to traditional inflexible network management systems, modern software defined networking solutions provide an entirely different approach to managing networks that is more powerful, efficient, and flexible. Rather than requiring an administrator to touch every device, this approach provides programmatic software control from an out-of-band central point that is no longer restricted to the limits of the network management system and does not require knowledge of the command line interface (CLI) of the network switches and other devices. Centralized policy repositories make the intent-based policies much easier to change and audit. Distributing those policies to the entire network or cloud infrastructure from a central spot also saves time and provides operational agility and flexible options (e.g.: network maneuver, enact network wartime modes, execute segment isolation, etc.) compared to updating network nodes one at a time.[15] Because the policy model is based on industry-standard APIs, it supports multi-vendor and multiple device types; thus, it can easily incorporate multiple types of switches, routers, security solutions, Layer 4 through 7 services, and so on.[16]

Thus, the management layer abstracts all of the complexities and dependencies of the other layers and provides the "pilot" (administrator) of the Cyber Platform with a heads-up display ("HUD") that contains the GUI tools and workflows to easily manage and operate the entire Cyber Platform integrated with a common operating picture ("COP") of the entire network. This level of abstraction provides the tools to logically define the network and enforce intent-driven policies as required for a zero trust architecture. These tools include network settings – e.g.: network servers (such as DNS, DHCP, AAA, etc.), device credentials, IP management, and wireless settings; network profiles – e.g.: define LAN, WAN, and WLAN connection profiles (such as SSID) and applying them to multiple sites; network physical hierarchy – means of transport, physical location, operating environment, etc.); and network image management. The outcome of these capabilities results in the realization of an operational network "order of battle" with an integrated "network COP" that enables operations to be orchestrated via GUI on a single pane of glass (or, "network HUD") that can automatically provision and deploy the Cyber Platform's underlay and overlay networks with speed, scale and agility.

2.3. Hybrid Multi-Cloud

Finally, DoD must implement innovative networking technologies that enable the edge and enterprise through **hybrid multi-cloud ready capabilities**. The network platform must be multi-cloud-enabled and ready to expand to cloud-delivered capabilities on demand – with security, identity management and visibility throughout. DoD cyber operations must be more dynamic compared with those of the past—the edge must be able to stand on its own and, when required, intuitively know when, where, and how to securely connect to hybrid clouds across the enterprise. A multi-cloud-enabled edge and enterprise must be capable of connecting across a Commander's Intent-driven, application-centric infrastructure with a pervasive security model and executed at speed. For DoD, the ability to dynamically expand to a multicloud environment is a game changer. Cloud-hosted applications and data can be linked to real-time incoming data—identifying alerts that both reduce operational risk and expose opportunities to increase operational effectiveness. These opportunities for DoD include ensuring the availability of critical information; securing mission networks; streamlining logistics and sustainment; increasing situational awareness in the battlespace; and enhancing quality of life for Soldiers, Sailors, Airmen, Marines, and their families.[17]

Traditional hub-and-spoke network architectures were designed to support consolidated applications and services hosted in centralized demilitarized zones (DMZs) and data centers. This approach forces the backhaul of internet traffic through the DMZ, creating inefficient traffic routes that increase the distance between end user and application. With an ever-growing influx

[15] Kinghorn and Underdahl, 11

[16] Kinghorn and Underdahl, 11

[17] Cisco Systems, Inc., Cloud-Ready Networks, "What Successful Cloud Adoption Means for Defense Agencies," 2019, 3

of data and devices and the need to rapidly apply this data for decision making, the DoD data environment is pushing timeworn hub-and-spoke networks beyond their limits. The realized data-enabled Cyber Platform must provide agile capabilities that support the required edge-to-cloud shift of DoD mission demands. Additionally, the combination of security, complexity, and cost arising from the rigidity the old hub-and-spoke approach makes this architecture impracticable on a large scale nor does it comport with the requirements for a zero trust architecture as described in the ACT-IAC zero trust approach. "That weakness of the traditional hub-and-spoke network model lies in its architecture. Crossing the chasm from trust to distrust via a firewall is inherently risky. Instead, zero trust no longer distinguishes between 'inside' and 'outside' the network perimeter."[18] As discussed in relation to establishing a software defined perimeter (SDP), "the traditional infrastructure firewall perimeter 'castle and moat' approach is not sufficient. The perimeter must move closer to the data in concert with micro-segmentation to strengthen protections and controls."[19] Thus, working together, advanced identity, software defined networking and multicloud technologies extend the SDP all the way to users and devices accessing data and workloads beyond their local environments—especially, to those that are delivered from internet-delivered multicloud services.

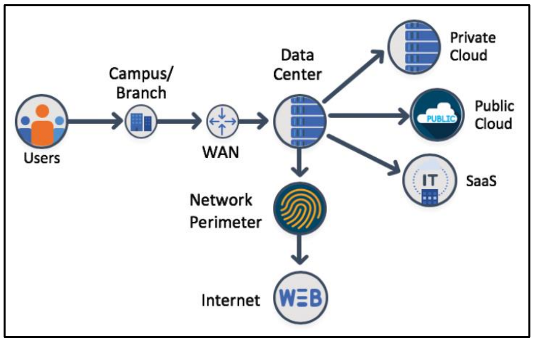

Figure 4 - Timeworn Hub and Spoke

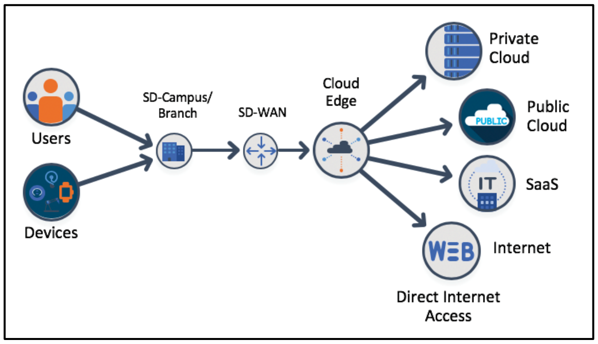

Figure 5 - Software Defined, Zero-Trust Architecture

Finally, by providing a software defined networking enabled WAN (SD-WAN) architecture that integrates routing, security, centralized policy, and orchestration, this approach enables DoD enterprise and remote edge users to securely connect to applications and available services wherever they exist through a transport-aware approach (e.g., MPLS, cellular, broadband). Software defined networking and cloud orchestration measure the performance of cloud applications across all transport paths. For each path, the fabric computes a quality-of-experience score that gives the Cyber Platform pilots (administrators) visibility into application performance. The software defined technology can make real-time decisions about the best-performing path between the edge and the cloud application. Thus, software defined networking technology addresses the bandwidth and performance issues related to cloud-hosted applications, so DoD can extend a secure footprint across hybrid multicloud environments – on demand and with agility. This architecture delivers: predictable application experience using multiple hybrid

[18] ACT-IAC, 3

[19] ACT-IAC, 9

datalinks; zero trust network security and segmentation; integrated security; seamless multicloud expansion and XaaS optimization; centralized management with zero-touch provisioning; and a highly scalable automated solution able to deploy to thousands of locations.[20]

With a Commander's-Intent driven software defined networking approach, intent-translated policy automatically ensures a predictable end-user experience for hybrid multicloud-hosted applications and supports a seamless, hybrid multicloud architecture with simplified operational experience, integrated security, and rich network performance analytics.

3. Conclusion

Implementing an intent-driven Cyber Platform is a necessity for any organization's digital transformation efforts. The Commander's Intent-driven Cyber Platform enables cyber operations at machine speed to empower decision makers with data-driven insights across all of DoD's missions. The close integration of emerging technologies in (1) advanced identity management, (2) software defined networking, and (3) hybrid multicloud capabilities enable the Cyber Platform to understand and execute Commander's Intent at machine speed. Implementing these capabilities across edge, data center, and multicloud environments, will provide DoD with a platform that provides the means of maneuver for data and, thus, endows a "*common foundation* of shared data, reusable tools, frameworks and standards, and cloud and edge services" required to "democratize access to AI"[21] and win the day with decision advantage.

Biography

Andrew D. Stewart, CAPT, USN (Ret.) served as the Assistant Chief of Staff for Operations (N3) and Maritime Operations Director (MOC-D) at Fleet Cyber Command/U.S. TENTH Fleet. He also served as the Commanding Officer and Program Manager at the Navy Cyber Warfare Development Group (NCWDG). He is a graduate of the Sellinger School of Business, Loyola University Maryland, the Naval Postgraduate School Monterey, CA, the United States Naval Academy, the National Defense University, and the Naval War College. He is currently a strategic programs manager at Cisco Systems, Inc. where he implements strategies to support innovative cyber solutions across the Federal Government.

[20] Cisco, "Cloud Ready Networks," 5

[21] DoD, 7