# SOAR

STATE-OF-THE-ART REPORT (SOAR)
FEBRUARY 2023

CSIAC-BCO-2023-351

# EDGE COMPUTING AND COMMUNICATIONS OVER UNTRUSTED TRANSPORT

*By Alok Chawla, Randy D. Bishop, and Danielle Tarino*
*Contract Number: FA8075-14-D-0001*
*Published By: CSIAC*

*This Page Intentionally Left Blank*

SOAR

STATE-OF-THE-ART REPORT (SOAR)
FEBRUARY 2023

# EDGE COMPUTING AND COMMUNICATIONS OVER UNTRUSTED TRANSPORT

ALOK CHAWLA, RANDY D. BISHOP, AND DANIELLE TARINO

# ABOUT CSIAC

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a U.S. Department of Defense (DoD) IAC sponsored by the Defense Technical Information Center (DTIC). CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001 and is one of the three next-generation IACs transforming the DoD IAC program: CSIAC, Defense Systems Information Analysis Center (DSIAC), and Homeland Defense & Security Information Analysis Center (HDIAC).

CSIAC serves as the U.S. national clearinghouse for worldwide scientific and technical information in four technical focus areas: cybersecurity; knowledge management and information sharing; modeling and simulation; and software data and analysis. As such, CSIAC collects, analyzes, synthesizes, and disseminates related technical information and data for each of these focus areas. These efforts facilitate a collaboration between scientists and engineers in the cybersecurity and information systems community while promoting improved productivity by fully leveraging this same community's respective knowledge base. CSIAC also uses information obtained to generate scientific and technical products, including databases, technology assessments, training materials, and various technical reports.

State-of-the-art reports (SOARs)—one of CSIAC's information products—provide in-depth analysis of current technologies, evaluate and synthesize the latest technical information available, and provide a comprehensive assessment of technologies related to CSIAC's technical focus areas. Specific topic areas are established from collaboration with the greater cybersecurity and information systems community and vetted with DTIC to ensure the value-added contributions to Warfighter needs.

**CSIAC's mailing address:**

CSIAC
4695 Millennium Drive
Belcamp, MD 21017-1505
Telephone: (443) 360-4600

| **REPORT DOCUMENTATION PAGE** | *Form Approved OMB No. 0704-0188* |
|---|---|

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

| **1. REPORT DATE**<br>February 2023 | **2. REPORT TYPE**<br>State-of-the-Art Report | **3. DATES COVERED** |
|---|---|---|
| **4. TITLE AND SUBTITLE**<br>Edge Computing and Communications Over Untrusted Transport | | **5a. CONTRACT NUMBER**<br>FA8075-14-D-0001 |
| | | **5b. GRANT NUMBER** |
| | | **5c. PROGRAM ELEMENT NUMBER** |
| **6. AUTHOR(S)**<br>Alok Chawla, Randy D. Bishop, and Danielle Tarino | | **5d. PROJECT NUMBER** |
| | | **5e. TASK NUMBER** |
| | | **5f. WORK UNIT NUMBER** |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**<br>Cybersecurity & Information Systems Information Analysis Center (CSIAC)<br>SURVICE Engineering Company<br>4695 Millennium Drive<br>Belcamp, MD 21017-1505 | | **8. PERFORMING ORGANIZATION REPORT NUMBER**<br>CSIAC-BCO-2023-351 |
| **9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**<br>Defense Technical Information Center (DTIC)<br>8725 John J. Kingman Road<br>Fort Belvoir, VA 22060 | | **10. SPONSOR/MONITOR'S ACRONYM(S)**<br>DTIC |
| | | **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** |

**12. DISTRIBUTION/AVAILABILITY STATEMENT**
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**
Today's "gray zone" battlefield has become increasingly digital. The fielding of "edge" sensors, processing tools, and ubiquitous transport—coupled with global cloud infrastructures—is transforming data collection, exploitation, and sharing, driving rapid decision-making at the speed of relevance. Adversaries actively target U.S. communications, making it difficult for operators to use untrusted infrastructures securely and surreptitiously. Securely exfiltrating data from contested networks into U.S.-owned networks at operational tempos remains a significant technical challenge and requires developing technologies that allow us to do so unimpeded. Future technical solutions must enable us to route, rapidly secure, and obfuscate data while preventing the adversary from detecting, intercepting, or exploiting critical information. These technologies must also allow secure and covert communications between operators' smartphones, end-user devices, and local commercial cellular, Wi-Fi, Bluetooth, and navigation satellite sources.

**15. SUBJECT TERMS**
edge computing, cloud computing, obfuscation, secure computing, contested networks

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. TELEPHONE NUMBER** *(include area code)* |
| U | | | UU | 48 | Vincent "Ted" Welsh |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | | 443-360-4600 |

**Standard Form 298 (Rev. 8/98)**
Prescribed by ANSI Std. Z39.18

**ON THE COVER:**
*(Source: Shutterstock)*

# THE AUTHORS

## ALOK CHAWLA

Alok Chawla works at the software security company Code-X, which provides the U.S. Department of Defense (DoD) with vital communication security and novel Intelligent Machine Authentication™. He spent over 28 years in the information technology industry, with the past 12 years focused on cloud and mobile security, and worked at several software security companies, where he delivered new security solutions. He was the former Chief Enterprise Architect at the Health Resources & Services Agency, where he led the cloud strategy for the Agency and adopted the Department of Homeland Security's Continuous Diagnostics Mitigation program. Mr. Chawla is completing his B.S. in information systems at the University of Maryland.

## RANDY D. BISHOP

Randy D. Bishop is the Vice President of Code-X. Before working at Code-X, he held several executive positions in industry, the federal government, the U.S. Air Force, and the U.S. National Laboratory complex. He is a former special agent in the federal government and the U.S. Air Force, with over 30 years of experience in cybersecurity and counterintelligence. Mr. Bishop earned a B.A. in criminal justice from Columbia College and completed the Post Graduate Intelligence Program at the National Intelligence University.

## DANIELLE TARINO

Danielle Tarino is the founder and Chief Operating Officer of Code-X and a leading national expert in privacy and confidentiality. Before Code-X, she held multiple executive positions in national nonprofit organizations and the federal government. During her tenure with the government, she was responsible for developing innovative public health technology and privacy software, government-wide privacy and confidentiality regulatory activities, and a myriad of assignments across communities affected by narcotics and substance use. Ms. Tarino holds a B.A. from Rutgers College and an M.A. from Georgetown University. She is currently receiving her MBE at the Harvard Medical School Center for Bioethics.

# ABSTRACT

Today's "gray zone" battlefield has become increasingly digital. The fielding of "edge" sensors, processing tools, and ubiquitous transport—coupled with global cloud infrastructures—is transforming data collection, exploitation, and sharing, driving rapid decision-making at the speed of relevance. Adversaries actively target U.S. communications, making it difficult for operators to use untrusted infrastructures securely and surreptitiously. Securely exfiltrating data from contested networks into U.S.-owned networks at operational tempos remains a significant technical challenge and requires developing technologies that allow us to do so unimpeded. Future technical solutions must enable us to route, rapidly secure, and obfuscate data while preventing the adversary from detecting, intercepting, or exploiting critical information. These technologies must also allow secure and covert communications between operators' smartphones, end-user devices, and local commercial cellular, Wi-Fi, Bluetooth, and navigation satellite sources.

# ACKNOWLEDGMENTS

The authors would like to thank the following individuals for their contributions to the report:

- Joseph Cole—Senior Operations Manager/ Program Manager, KeyLogic Associates
- Dustan Hellwig—Founder/Chief Strategy Officer of Chesapeake Technology International
- Joel Hewett—Scientific and Technical Subject Matter Expert, KeyLogic Associates
- Gregory Nichols—Corporate Quality Manager/ Public Health Expert, KeyLogic Associates
- John A. Wilcox—former Director of Communications Systems (J6) and Chief Information Officer, U.S. Special Operations Command

# EXECUTIVE SUMMARY

The world's current geopolitical posture places the U.S. military in a precarious operational position, better known as the "gray zone," or "Phase 0," where deployed U.S. forces maneuver just short of armed conflict. Moreover, the battlespace is increasingly digital, where data and its usage are the new weapons. This new dynamic requires capabilities at and from the tactical "edge" of the battlespace, such as sensors, data processing, and secure communications, including over untrusted or uncontrolled transport infrastructure.

The "edge" is a military term that refers to forward military operations, usually within denied, disconnected, intermittent, and limited (D-DIL) environments. The rapid exploitation of critical operational information to be filtered out of raw data allows for better analysis and strategic decision-making. The U.S. Department of Defense's strategy for multidomain command and control heavily depends on connected and distributed sensors, including smart devices like smartphones, tablets, phablets, smartwatches, smart glasses, and other personal electronics. These sensors collect massive amounts of data, which can be difficult to share among operators. Another limitation is reliance on data centers in the continental United States. However, when combined with artificial intelligence technologies, they can be transformed into edge-computing systems, allowing faster and more efficient data exploitation.

While edge computing can be an effective tactical tool, it becomes unhelpful unless information stored and exploited at the edge can be shared quickly and securely. Tactical edge operators frequently deal with limited bandwidth and constraints on size, weight, and power, as well as the ever-present threat of detection by adversaries. Also, operators may have to depend on different communications capabilities, such as satellite or wireless communications provided by local telecommunications companies. New technologies for transporting critical information to, across, and from the edge are coming online at a rapid clip, almost daily. Examples include fifth generation mobile networks, software-defined wide area networking, and a growing constellation of commercial satellites.

However, adversarial groups actively target U.S. interconnected systems, making it challenging to communicate securely and surreptitiously over untrusted and commercial transport infrastructure as it attempts to synchronize with friendly systems. Consequently, the ability to securely exfiltrate data from contested networks into U.S.-owned networks at a speed and quantity sufficient to support intelligence or operational needs represents a significant technical challenge. Indeed, a requirement exists for technologies that decrease the detection, amount, and vulnerability of data exfiltrated by U.S. operators from the forward-contested environment. These technologies should also enable secure communications between operators' smartphones, end-user devices, and local commercial cellular, Wi-Fi, Bluetooth, and navigation satellite sources. Future solutions route large volumes of obfuscated data securely, making it more difficult for analysts to detect specific markers and deny adversary detection by denying analysts access to the information.

*This Page Intentionally Left Blank*

# CONTENTS

# CONTENTS, *continued*

# SECTION 01 INTRODUCTION

The world's current geopolitical posture places us in a precarious operational position, better known as the "gray zone," or "Phase 0," where our deployed forces maneuver just short of armed conflict [1]. The U.S. Department of Defense (DoD) describes Phase 0 (Zero) as "Joint and multinational operations – inclusive of normal and routine military activities – and various interagency activities performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends or allies" [2].

Moreover, the battlespace is increasingly digital, where data and its usage are the new weapons. As Figure 1-1 illustrates, this new dynamic requires capabilities *at and from* the tactical "edge" of the battlespace, such as sensors, data processing, and secure communications, and sometimes over untrusted or uncontrolled transport infrastructure. The fielding of "edge" communications, sensors, and processing tools, coupled with cloud computing and infrastructure (including untrusted systems outside the continental United States [OCONUS]) [3],

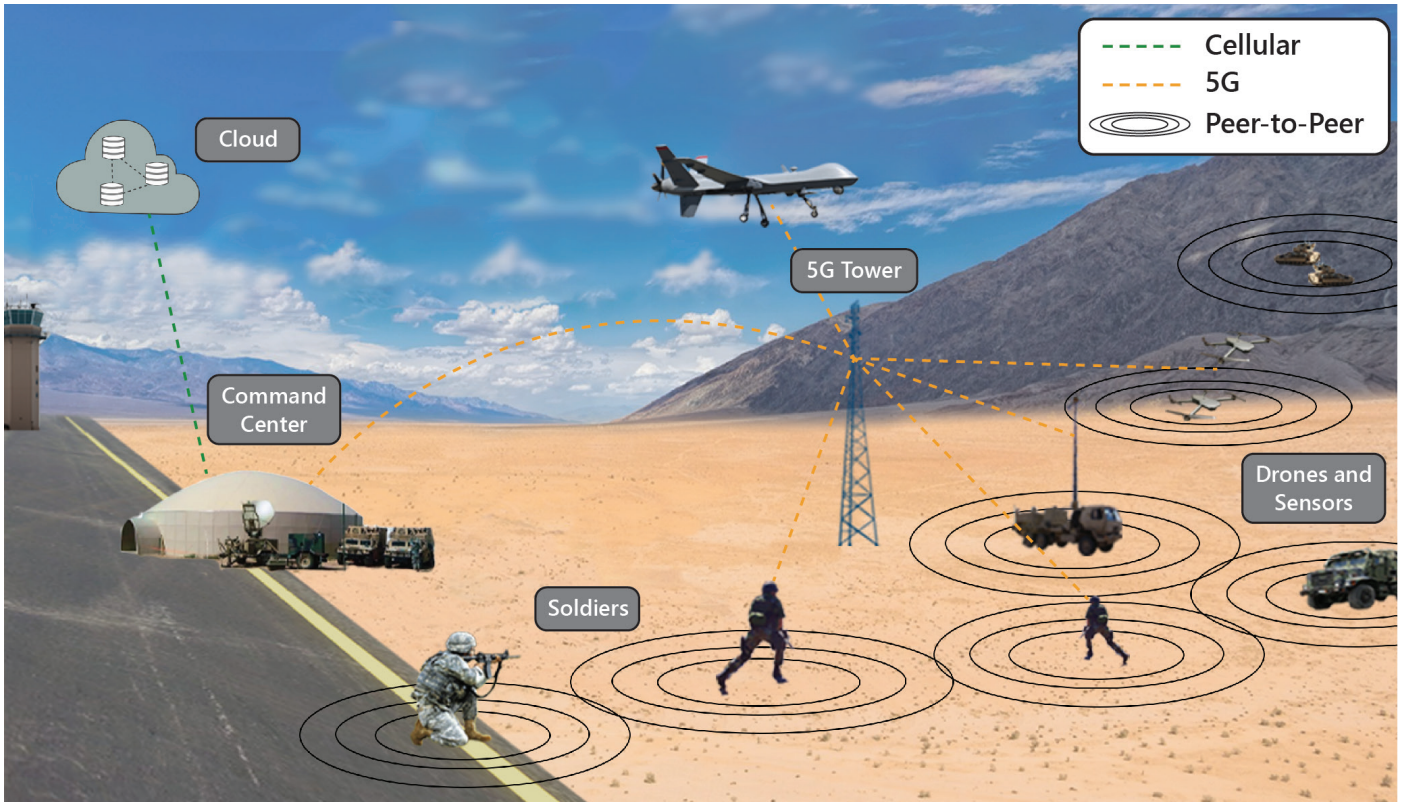


Figure 1-1. Example of a Multidomain Command and Control (C2) Environment *(Source: CSIAC).*

is transforming the speed and scale of data collection and exploitation, enabling rapid decision-making [4]. As described by a mathematician at the National Institute of Standards and Technology (NIST), "Edge computing is an emerging architecture, which extends the Cloud computing paradigm to the edge of the network, enabling new applications and services, including Internet of Things (IoT)" [1].

However, securely exfiltrating or transferring valuable data from edge environments and networks into U.S.-owned networks at a speed and quantity sufficient to support intelligence or operational needs represents a significant technical challenge. The need for low or no probability of detection further exacerbates this challenge. Advancing global telecommunications technology and reach presents both challenges and opportunities. As U.S. military elements integrate advanced technologies into edge operations, our adversaries likewise respond. These adversaries actively target U.S. smart devices to capture and exploit identifying information and other metadata. Even with traditional, highly secure encryption, a skillful adversary can make it very difficult for operators to communicate within and through untrusted infrastructure securely and surreptitiously.

Over the past 18 months, several prominent government research centers have recognized the need to identify data communications capabilities that employ all available local, regional, global, and space-based networks. These technologies must also enable secure communications between operators' smartphones, end-user devices (EUDs), and local commercial cellular, Wi-Fi, and navigation satellites while simultaneously enabling data to be rapidly routed, secured, and obfuscated. Further, these capabilities must travel through trusted and untrusted communications while hiding in plain sight and through untrusted indigenous infrastructure and service providers. Data obfuscation, i.e., making data "invisible" or appearing as "uninteresting" traffic, must be provided resiliently and function in networking environments that may be unreliable and untrustworthy. By preventing analysis, cross-correlation, and the adversary's ability to detect specific data markers, the DoD can prohibit the adversary from employing "cyber kill chains," compromising critical communications or data.

Though no solution can provide all these requirements, several technologies have succeeded in providing some of these capabilities with varying degrees of success. Encryption methodologies (Type-1 cryptography) remain the standard for highly sensitive data; however, they are costly and require very specific types of hardware to enable their use. For this, the National Security Agency (NSA) Commercial Solutions for Classified (CSfC) program allows commercial solutions to deliver security for classified data. However, CSfC and Type-1 products have typically approached security through different forms of cryptography and have not addressed how to obfuscate data. Forward-deployed or contested areas can be problematic for Type-1 devices, as sending and protecting them in these regions may take time. Without the ability to obfuscate data communication, using an encrypted channel is highly visible to our adversaries. It provides them with the knowledge that someone is present and the possible location of where the traffic originated.

# SECTION 02 EDGE OPERATIONS

For the first time, the National Defense Strategy released in October 2022 recognizes and predicts "an escalation of competitors' coercive and malign activities in the 'gray zone' " [5]. The gray zone may not be war, but without boots on the ground and persistent "stare" at the tactical environments, miscalculations and unintended escalation could lead to one. For example, China's activities in the South China Sea and Russia's annexation of Crimea are considered gray zone activities. Without context and current intelligence, they could rapidly lead to open hostilities.

Historically, U.S. forces went to war in a complex environment that was not only unknown but unknowable and constantly evolving, meaning that we could not anticipate who, where, and with whom we would fight. Achieving awareness requires continual intelligence preparation of the battlefield and "operating environment and providing early indication and warning" [6]. U.S. Special Operations forces (SOF) and other forces conduct gray zone initiatives for several purposes. They conduct intelligence, surveillance, and reconnaissance operations to improve our understanding of the operating environment, shape adversary perceptions by creating doubt in their ability to achieve their military objectives, and effect unattributed actions. These activities serve several nonexclusive purposes, such as situational awareness (SA) and intelligence preparation of the battlefield [7]. Ultimately, U.S. forces strive to disrupt adversarial infrastructure, logistics, C2, and mobilization advantages while reinforcing our own.

To achieve their mission, edge-computing platforms are a central component of gathering, analyzing, and disseminating data. As shown in Figure 2-1, which depicts the layers of the edge-computing ecosystem, the various tiers are deconstructed into the following:

- Edge Sensors and Chips: Where data is initially collected. Edge sensors can be anything from a temperature monitoring IoT device to heart rate monitoring devices worn by soldiers.
- Edge Devices: Edge devices with compute and storage capabilities may also include edge sensors. These devices can process and analyze the data they collect or the data sent to them from edge sensors. Edge devices range from a smartwatch to an unmanned aerial drone collecting image data.
- Edge Infrastructure: Edge infrastructure seeks to bring immense compute and storage capabilities closer to where the data is collected. By doing so, the goal is to reduce latency and processing data without solely relying on a centralized collection point. To centralize operations, data centers in several geographic locations or highly mobile devices that can communicate reliably can be deployed.
- Centralized Cloud: This term, which denotes the "cloud," is the most understood. It is a virtualized data center that stores and processes vast amounts of data, including mission-critical systems that analyze all the collected data. In the edge-computing

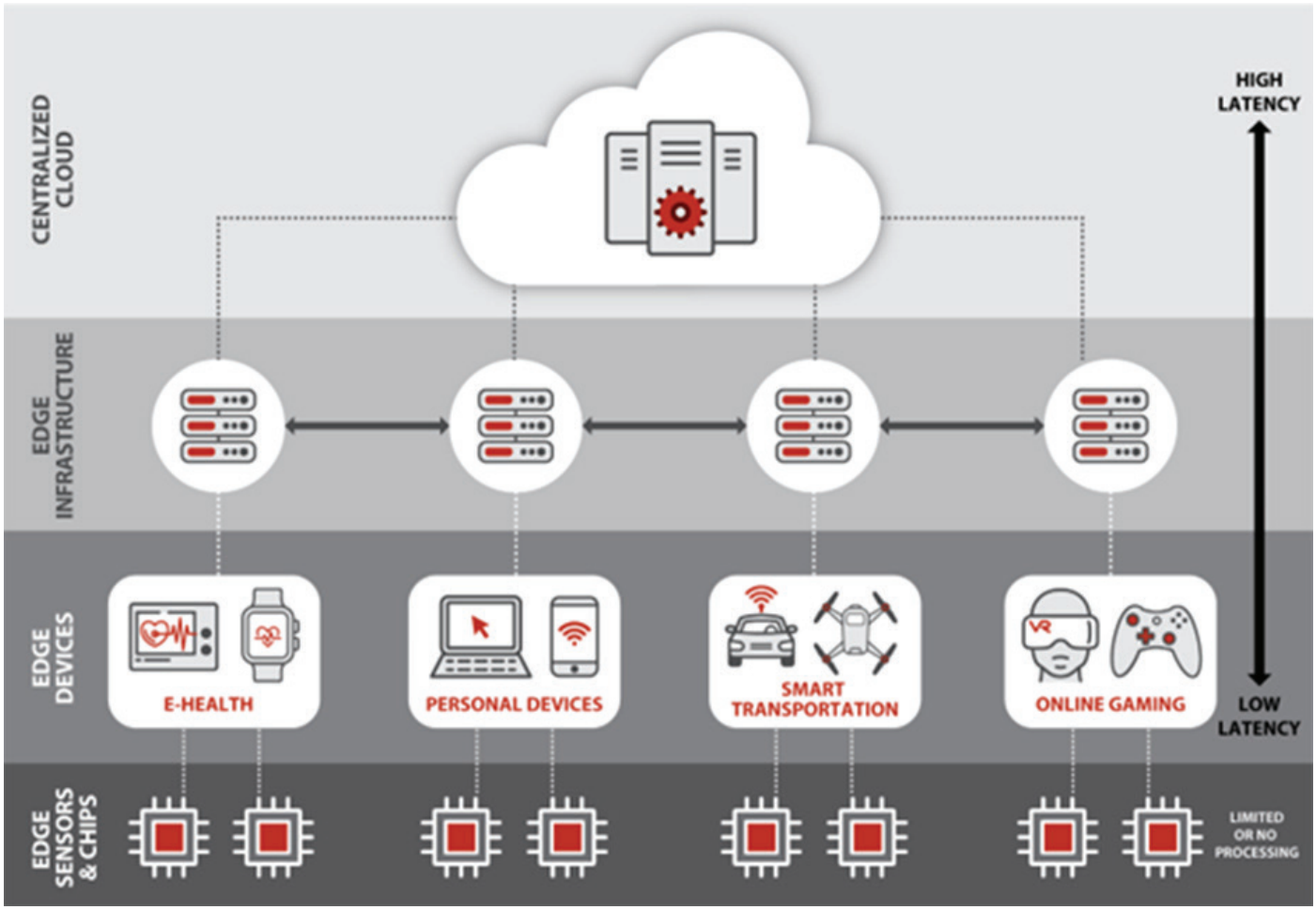


Figure 2-1. Hierarchy of Edge Computing *(Source: CSIAC).*

paradigm, the centralized cloud serves as the tier where data is stored in archives and analyzed against historical data to help continue to refine mission goals.

In March 2022, the Deputy Secretary of Defense signed the Joint All-Domain Command and Control (JADC2) Implementation Plan [8]. JADC2 is the newest DoD effort to enable the Joint Force to "sense," "make sense," and "act" on information across the entire spectrum of conflict, including gray zone edge operations. The JADC2 plan, as depicted in Figure 2-2, acknowledges the critical role that automation, artificial intelligence (AI), predictive analytics, and machine learning (ML) play in delivering data via a resilient network environment, even when contested. Chairman of the Joint Chiefs of Staff Gen. Mark Milley said, "This is about dramatically increasing the speed of information sharing and decision making in a contested environment to ensure we can quickly bring to bear all our capabilities to address specific threats" [8].

For several reasons, the momentum toward JADC2 is relevant to edge operations and communications. Simultaneous with the signing of the Implementation Plan, the DoD published an unclassified summary of its JADC2 Strategy [9]. In the Strategy, the DoD commits massive investments in technologies and program capabilities (across each service branch) that directly support armed conflict and gray zone operations. The Strategy lays out the following six guiding principles delivering materiel and nonmateriel capabilities:

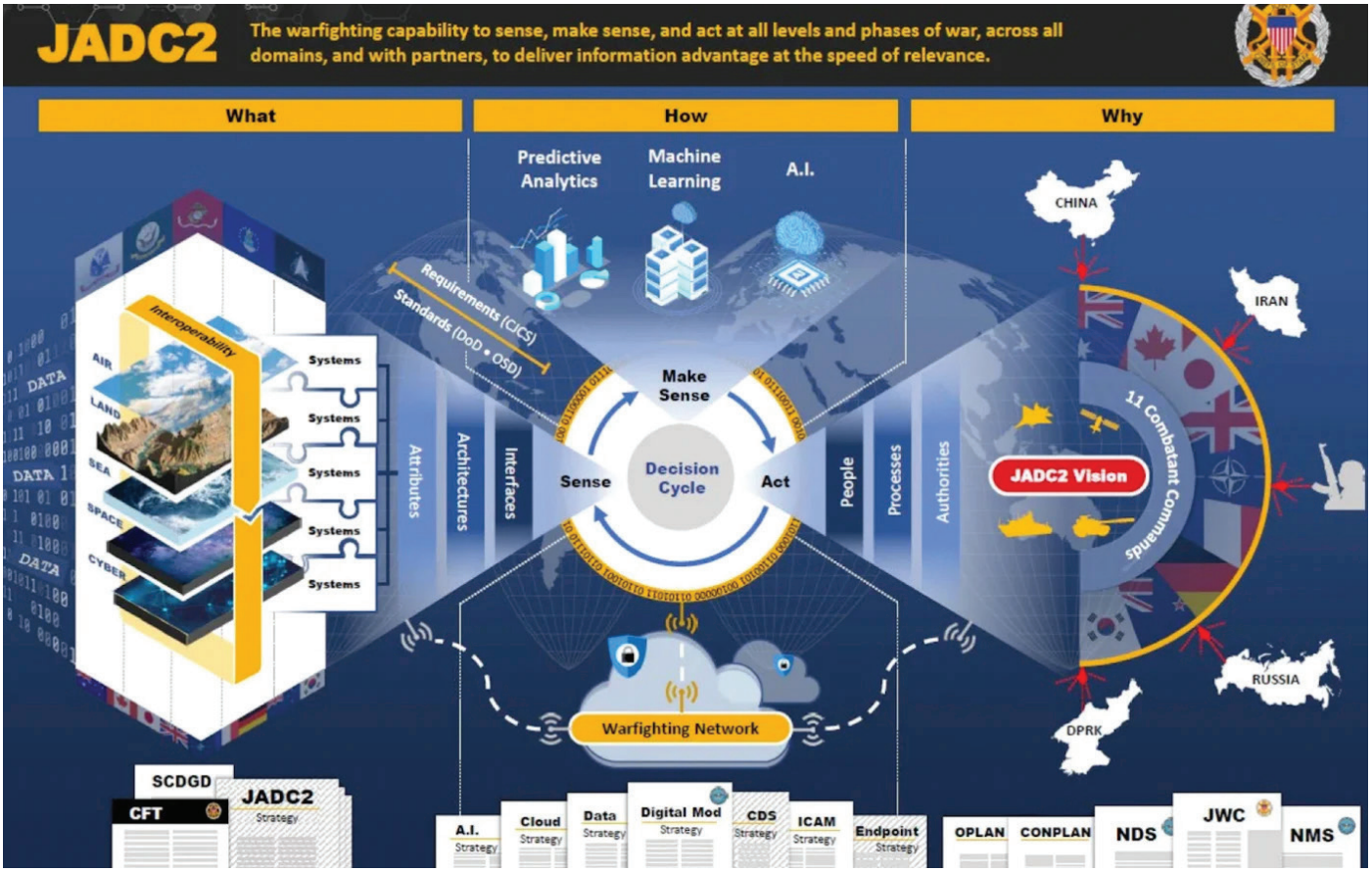


Figure 2-2. JADC2 Placemat *(Source: DoD [9]).*

1. Information sharing capability improvements are designed and scaled at the enterprise level.
2. Joint Force C2 improvements employ layered security features.
3. JADC2 data fabric consists of efficient, evolvable, and broadly applicable common data standards and architectures.
4. Joint Force C2 must be resilient in degraded and contested electromagnetic environments.
5. Department development and implementation processes must be unified to deliver more effective cross-domain capability options.
6. Department development and implementation processes must be executed at faster speeds.

Collectively, each of the JADC2 principles directly supports and enhances edge operations and is being tested continually by the Combatant Commands across several world regions, including the Indo-Pacific Command, Northern Command, Southern Command, and European Command. For example, in 2021, the U.S. military services conducted Project Convergence 2021 (PC21), the second annual joint exercise to establish an experimental global network to develop integrated capabilities across all services. According to a Congressional Research Service report [10], PC21 examined several scenarios, including the following:

- Test joint all-domain SA and incorporate space sensors in low earth orbit.
- Conduct a joint air-and-missile defense engagement in response to an enemy missile attack.
- Conduct a joint fires operation as the force transitions from crisis to conflict.

- Conduct a semiautonomous resupply mission.
- Conduct an AI and autonomy-enabled reconnaissance mission.

According to PC21's after-action reports, the demonstrations were successful, and the subsequent annual exercise, Project Convergence 2022 (PC22), continues to demonstrate several additional features. Significantly, PC22 added some critical elements that recognize the importance of unfettered access to the electromagnetic spectrum environment (see Figure 2-3). Another area explored during PC22 was signature management, or control, and reducing the detectability of visual, infrared, radar, and sound electromagnetic emissions. While many specific tests were classified, the technologies were not; many were commercially available technologies repurposed for the test environments.

Figure 2-3. U.S. Soldiers Assigned to 2nd Battalion, 20th Field Artillery Regiment, Work With the Autonomous Multidomain Launcher, on a Palletized Load System Using a Remote Interface Unit *(Source: DVIDS [11]).*

# SECTION 03 CURRENT TECHNOLOGY

Forward-edge operations include the ability to collect, analyze, filter, and securely transport data (sensor data, drawings, photos, text, and video) across myriad transport and cloud backbones, ultimately to a secure enclave for processing, exploitation, and dissemination (PED). These activities serve multiple purposes, including SA, intelligence preparation of the battlefield [7], and precursors to direct action such as counterdrug or insurgency operations or to coordinate and synchronize tactical, operational, and strategic fires targeting capabilities [12]. Each is employed to help determine mission variables such as enemy/adversary, terrain, weather, and civil considerations.

John A. Wilcox, former Director of Communications Systems (J6) and Chief Information Officer at the United States Special Operations Command (USSOCOM), recently stated that the current threat environment only solidifies the need for more significant enhancement and adoption of tactics that leverage edge-computing capabilities [13]. In his estimation, the following are two primary objectives that edge computing enables for the DoD:

1. Decision superiority, or the ability to make decisions inside the enemy's thought cycle, is enhanced by using edge computing by enabling and empowering U.S. SOF operators to make immediate sense of collected data.
2. Edge computing allows continuous operations through a disconnected, interrupted, and low-bandwidth (DIL) environment. Operators and soldiers constantly find themselves in a D-DIL environment; the ability to maintain momentum with continuous operations is a crucial objective using edge computing.

## 3.1 DATA COLLECTION AND PROCESSING

One of the primary reasons behind the DoD's interest in edge computing is that raw data is not intelligence. Raw data is rarely actionable. With the growth of military sensors, the volumes of data collected can overwhelm an analyst's ability to turn it into meaningful intelligence and insights. The rise of more sensors and IoT devices has brought about a need for computational tasks to be carried out without relying on transporting data back to a central data center. The computational ability at the edge is crucial to avoid enormous bandwidth demands and enhance the speed and reliability of results.

Moving to an edge operations model addresses some of these critical areas of weakness. Because sensors collect massive amounts of data, the ability to analyze and filter that data and ensure secure transport of information through an all-domain transport infrastructure is critical to successful edge operations [5]. Leveraging AI or ML technology at the edge allows for the analysis of data and immediate filtering and prioritization of events that may be deemed critical to the mission. When employed, analytics at the edge mitigate bandwidth, latency issues, and data encryption overhead.

Many industries view the power of edge computing as the ability to aggregate and analyze vast amounts of data closer to the logical edge of an enterprise network. When coupled with AI/ML technology, this ability allows immediate processing of large data sets. With properly trained AI/ML algorithms residing at the edge, only data relevant to the mission or business use case can traverse the enterprise network to a centralized processing area. For many use cases, such as monitoring the national electricity grid in the United States, edge computing provides geographically dispersed processing points that are physically closer to the sensors with which they communicate. IoT devices, from something as simple as a temperature sensor to something as complex as a wireless-enabled land mine, do not have the storage space or processing power to analyze the data they collect. However, once aggregated at an edge-computing node, AI/ML algorithms can quickly analyze data from groups of IoT devices and provide immediate outputs to users.

With the advent of edge computing, a new area of research has emerged regarding how best to use and secure the vast amounts of data collected by mobile devices. In the broadest terms, edge computing brings computational resources, connectivity resources, and data storage closer to the data's generation point. Mobile devices have finite limits on the amount of computational power and data storage they can house; however, their ability to collect immense amounts of data has no such limits. With increasingly complex and powerful edge-computing capabilities, a new method to address mobile device limitations requires greater exploration.

Advances in purpose-built edge devices and cloud computing could help transform where and how fast data is collected, analyzed, and acted upon in forward-operating environments. Cloud service providers (CSPs) like Amazon Web Services (AWS) and Microsoft have created military-focused, ruggedized hardware components to provide mobile edge-computing services. These devices, shown in Table 3-1, are built for military

Table 3-1. Edge-Computing Devices

| Device Name/Vendor | Storage Specification | Weight (lb) | Capabilities |
|---|---|---|---|
| AWS Snowball Edge | 28–78 TB | 49.7 | AWS Snowball Edge has multiple configurations based on need. Edge-optimized computes edge-optimized storage or edge-optimized storage with compute. Devices with computing onboard also support AI/ML capabilities. Each device is highly portable, designed to be rugged, and runs on multiple communication formats. |
| Microsoft Azure Data Box Edge | 80 TB | <50 | Data Box Edge is for data storage and transfer to cloud computing, battery-powered, and light. Further, Data Box Edge possesses AI-enabled edge-computing capabilities that allow users to analyze, process, and transform the on-premises data before uploading it to the cloud. |
| Performance Defense Edge 5G-X | 256 GB solid-state drive | Unknown | Ruggedized, edge device capable of multiple communication methods, such as satellite communications (SATCOM), fourth generation (4G)/5G, Wi-Fi, and wired ethernet. Hardened devices, including the hardware-based root of trust and red/black architecture design. Offers open-platform AI/ML environment to meet DoD needs. |

applications, providing AI/ML-enabled edge-computing capabilities at the tactical edge, with the ability to process and analyze data before uploading the information to the cloud. Other vendors, such as Performance Defense, have created edge appliances that work directly with natively available fifth generation (5G) wireless signals to allow for a truly mobile edge-computing node.

As edge capabilities mature, AI/ML-enabled processing tools could be applied in forward areas or on-site, rapidly generating actionable intelligence for operators and decision-makers. When paired with advanced sensors and communications platforms, human collectors equipped with edge devices could push into harsh, high-risk, or denied areas for sensitive collection missions and transmit time-sensitive data in close to real-time. AI, coupled with edge computing, has been the topic of much research, primarily because to harness the best and realize the benefits of computing at the edge, AI represents the best means to process and automate the analysis of vast amounts of data. However, as Dustan Hellwig (Director and Chief Strategy Officer, Chesapeake Technology International) has shared [14], much research is still needed on securing AI/ML algorithms from attack vectors that seek to mislead and incorrectly train the algorithms. False data sets specifically designed to train AI/ML incorrectly have already been seen in use by our adversaries. It is logical to assume the accelerated increase in such attacks as edge-computing adoption grows.

As detailed in a recent webinar hosted by the Cybersecurity & Information Systems Information Analysis Center (CSIAC) regarding the resiliency of AI systems, emerging AI countermeasures (adversarial AI) continue to grow, with similar goals to traditional countermeasures, i.e., evading detection and diluting the effectiveness of AI capabilities. The following three direct adversarial AI attacks occur with high frequency [15]:

1. Poisoning Attack: Focused on polluting training data to skew decision boundary and model behavior, thus lowering AI accuracy.
2. Evasion Attack: Engineered adversarial inputs to produce misclassified results, thus avoiding detection while not alerting on misclassification of data.
3. Model Inversion Attack: Reconstructing the model (direct AI attacks) via constant probing or building an AI proxy model to discover training data characteristics, thus providing adversaries with insight into how the AI model is constructed.

The recommended countermeasure defenses for any attack are as follows [15]:

- Data sanitization of baseline traffic ingested by AI.
- Leverage differential privacy methods to obfuscate data.
- Integrity checking of data being ingested/evaluated by AI.
- Identification and removal of bot-generated data (i.e., untrusted bots or rogue network nodes in edge-computing use cases).

AI nodes deployed at the edge of a computing network may not have the same protections as nodes within an enterprise network. AI sitting at the edge of computing nodes may be exposed to each of the attack vectors because they lack this protection. Capabilities that provide data provenance and the ability to trust sensors deployed in contested areas are needed to enable edge-computing capabilities. As John A. Wilcox noted, "The most significant hurdle to the continued adoption of edge computing for U.S. military use is the accuracy and trustworthiness of data outputs. Research on protecting the data's provenance and securing the AI/ML algorithms must continue in earnest" [13].

Edge computing and AI/ML applications can help speed the process of sensitive site exploitation of captured enemy materials. These advances shorten the PED cycle for intel-driven tactical operations, which require ever-faster processing speeds and resilient storage capabilities—all achieved while reducing power consumption. Some of the largest chip manufacturers, like Intel and NVIDIA, have engineered chipsets that bring AI to edge computing. Hewlett Packard Enterprise (HPE) and NVIDIA have partnered to bring AI/ML to the cloud through HPE GreenLake, via a new set of cloud offerings in the HPE cloud [16].

Other CSPs like AWS and Azure have developed standalone, security-hardened, edge-computing devices with embedded AI/ML capabilities; for example, many include Advanced Encryption Standard (AES) 256 encryption and possess the capacity to hold up to 100 TB of data. Allowing for data capture using such devices, CSPs seek to transfer the computing edge to their cloud or closer to the data-processing site. Niche companies are also continuing to bring additional capabilities to the growing area of edge computing. BrainChip, an American startup leader in edge "on-chip" processing and computing, has partnered with semiconductor startup SiFive to bring optimized AI/ML chips to the market. These developments focus on the performance, ultra-low power consumption, and on-chip learning needed for advanced neural networking processor architecture explicitly designed for edge-computing use cases [17]. Continued research and development need to occur in natural language processing and convolutional neural networking, as they are two of the critical technologies to enable AI and ML at the edge.

AI-enabled tactical forensics tools assist in processing massive amounts of digital materials from captured devices, filtering and extracting prioritized data, such as names, phone numbers, or images of specific people. Automation tools and integrated APIs can then dispatch specific data to specific receivers in the intelligence-operations cycle, enabling more profound analysis and immediate action by operators. Many industries provide valuable lessons on edge-computing adoption and the successful automation types. From manufacturing to supply chain streamlining, edge-computing components have started to be deployed at the industrial-terminal level, allowing just one terminal to interface with a wide array of machines. They are removing machine-specific terminals and observing an increase in the workforce's broader training while decreasing downtime due to terminal issues.

As John A. Wilcox discussed, a significant industry to watch and learn from is the continued development of smart cars and autonomous driving capabilities [13]. These vehicles require constant communication with edge-computing capabilities as they exchange sensor data back and forth from nodes at the edge enabled with 5G communications. Edge computing extends into virtual machines and container services, which virtualize software layers and allow DevOps teams to build virtual machines and containers optimized to run at the edge. Software specifically written to run on edge-computing resources allows the developer to use edge devices' unique hardware infrastructure and streamline their applications. Additional use cases include edge processing radio frequency (RF) signaling between U.S. smartphone EUDs and commercial cellular, Wi-Fi, Bluetooth, and navigation satellite sources.

## 3.2 DATA TRANSPORT

### 3.2.1 Edge Communications

Mobile technology remains at the forefront of how military and intelligence community (IC) personnel communicate and gather information. John A. Wilcox contends that communication between every team member, regardless of where deployed, requires minimal access to voice and data communications [13]. This data communication is central to enhancing SA and C2 across the battlespace or forward-deployed environments

where SOF operators may find themselves [18]. Wilcox further states that developing new form factors other than mobile devices that allow SOF operators to connect to and use edge-computing capabilities is vitally important for their continued evolution and adoption and being agile and having extreme mobility in the next conflict is vital to be victorious. Soldiers and SOF operators must be able to move quickly and deploy into extremely contested, D-DIL environments but communicate, gather information, and send that data back to CONUS-based systems for processing. However, as the amount of data sent back to these systems continues to grow, we face the arduous task of securing that data, ensuring its provenance, and bearing the sheer cost of transmitting that amount of data as an ever-increasing burden.

USSOCOM widely uses handheld software-defined radios (SDRs) to provide a means of communication that can be upgraded in the field with new waveforms and software without additional hardware. There are several types of devices, with varying uses already available and used by the DoD. One of the newest and most used SDRs, the Falcon IV AN/PRC-163 Next Generation Tactical Communications built by L3Harris Technologies, provides a dual-channel SDR supported by the tactical, scalable MANET (Mobile Ad Hoc Network)-X (TSM-X) waveform. The clear advantage of such a mobile device is that using the MANET waveform allows SOF operators to create a single mesh network with up to 200 nodes across a battlespace [18].

The U.S. Air Force-developed Android Team Awareness Kit (ATAK) system is an example of such a mobile device. ATAK is a government off-the-shelf (GOTS) device that has been in service for several years in real-world combat zones. It is used by conventional Warfighters and SOFs for tactical data collection, analytics, and visualization—all while operating in real-time at the edge. ATAK operators can identify "blue force" friendly operators while simultaneously seeing potential adversary activity, depending on the data feeds programmed at the time. It can also be downloaded to a commercial off-the-shelf (COTS) Android device or tablet and provided to partner forces without disclosing sensitive hardware [19].

Communications at the edge involving C2 and other classified data require strong security measures. Cross-domain solutions (CDSs) address the need to enable communication between disparate systems that may also sit inside incompatible security domains. CDS technology aims to allow different security domains to exchange data while eliminating the need for time- and resource-intensive, advanced data filtering [20]. A CDS solution, coupled with an edge-computing solution, offers a secure path to enable the sharing of insecure data collected at the edge across different security domains in rigid, forward-deployed environments. CDS technologies must constantly evolve and be subject to new and constantly changing cyberthreats. Yet, at the same time, these devices can also use programmable rule sets that allow the filtering of information, allowing individual messages or data fields within the message to be passed, blocked, or changed. IC and DoD communities currently use CDS solutions on the market. However, only those meeting the NSA and National Cross Domain Strategy Management Office (NCDMSO) Raise-The-Bar cybersecurity guidelines are suitable for use in gray space engagements. Table 3-2 lists several CDS solutions that meet these criteria and could provide a valuable integration point for securing and enabling communication between trusted and untrusted domains, with the extensive and highly unsanitized data collected at the edge.

To ensure the DoD can adequately access communications and computing gear, NSA established the CSfC program. CSfC is an integral part of their commercial cybersecurity strategy to quickly ensure ready access to commercial technologies. The program intends to provide a second option to Type-1 cybersecurity designation, the long-standing designation for NSA-certified

Table 3-2. Comparison of System and Architecture Characteristics of Two CDSs

| CDS | Architecture Characteristics | System Characteristics |
|---|---|---|
| General Dynamics Tactical Cross Domain Solution [21] | • NCDSMO-compliant filters<br>• Authorized for both Secret and Below Interoperability and Top Secret and Below Interoperability applications | • Low size, weight, and power (SWaP) and cost, rugged, tamper-resistant form factor<br>• Hardware-enforced domain separation<br>• Encrypted storage of rule sets and audit logs<br>• Separate high and low data ports |
| Collins Aerospace SecureOne Multiple Independent Levels of Security tactical CDS [22] | • Unified Cross Domain Services Management Office baseline certification is in the process<br>• Simultaneous Top Secret through Unclassified data protection in one channel and one step | • Designed for tactical embedment with SWaP usage<br>• Low-latency communications<br>• Scalable support for multiple decentralized systems and security enclaves |

equipment. The NSA defines Type-1 products as "cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA-approved algorithms used to protect systems requiring the most stringent protection mechanisms" [23]. Type 1 is also commonly used when describing the cryptographic suite (algorithm) used within a Type-1 product. AES 256 is an example of NSA-approved, Type-1 encryption. This type of encryption has now seen wide adoption in the commercial realm, with products such as Apple iPhones now using AES-256 crypto to secure data on Apple devices. While Type-1 products have long been the standard for securing data at rest and in transit, they have some drawbacks. The speed of deployment, ease of use, cost of specialized training (for Type-1 devices), and burden of risk to secure such devices (both physical security and cybersecurity risks) can be issues for some mission goals. Hence, NSA created the CSfC program to allow stakeholders in the DoD, IC, and military services to use its vetted and approved commercial solutions [24].

NSA has provided capability packages that are reference architecture packages for commercial vendors to build and design products that comply with CSfC guidelines and achieve NSA certification. Only products that have obtained this NSA certification will be permitted within the CSfC program. For a commercial product to participate in the CSfC program, each product component must be CSfC approved. CSfC technologies encompass radios, computers, and other items typically carried by U.S. forces into the field and at the edge of battle. NSA defines these systems as national security systems and thus requires robust encryption techniques. Standard protocols like Internet Protocol Security (IPsec), Secure Shell (SSH), Transport Layer Security (TLS), Datagram TLS (DTLS), and Hypertext Transport Protocol Secure (HTTPS) provide encryption and two-way authentication to secure sensitive data. The NSA-approved Commercial National Security Algorithm suite provides cryptographic requirements to securely use these protocols [25].

When the U.S. military deploys its communications equipment to the edge, it must consider communications security a key component. Achieving unified communications, including voice, video, instant messaging, and collaboration

tools, has significantly transformed the modern battlefield. However, this has also introduced some vulnerabilities. Encryption is introduced into the communications channels and edge devices to mitigate many of these vulnerabilities. The NSA CSfC program offers quick access to IPsec, SSH, TLS, DTLS, and HTTPS and the equipment that employs them. In addition, using CSfC devices vs. Type-1 devices mitigates the risk of highly guarded hardware/software technology from falling into the adversary's hands. The loss of a CSfC device, such as a Samsung Galaxy S20 Tactical Edition smartphone (edge device), can be tolerated, whereas the loss of a Type-1 device cannot.

Regardless of the physical makeup of the devices and networks operating at the edge, several guiding principles make any edge-computing architecture viable and successful. In addition to the fundamentals, such as security (confidentiality, integrity, and availability), defense technology analysts at Booz Allen Hamilton have described four of them as follows [26]:

1. Open Architecture Design. Open architecture allows for flexibility and portability over the long term, with the ability to create new connections and innovate with ease.
2. Focus on Connectivity. The power of edge computing comes from the effects of the network—the more people and things that communicate at the edge, the more influential the coalition or total platform becomes, underscoring the importance of mesh networks and working in disconnected states.
3. Prioritize Interoperability. Interoperable platforms in the modern digital battlefield can lay the foundation for edge computing, which creates a force multiplier and benefits from network effects. Much of this arsenal was designed and purchased to operate and communicate within a vertical system.
4. Integrate in Design. Edge computing requires a forward-looking and enterprise mindset toward integration. Integration into older systems (like Link 16 and Link 22) requires consideration when creating value through a mesh network to realize the value of edge computing.

### 3.2.2 Zero Trust Architecture

The industry consensus is turning to a zero trust model to ensure security in the cloud, regardless of the type of cloud infrastructure used and whether the application is internal or external. A 2020 report published by NIST titled "Zero Trust Architecture" (Special Publication 800-207) [27] describes the following seven primary tenets of zero trust:

1. All computing resources, assets, and data sources are considered resources.
2. All communication is secured, regardless of the location of the devices involved. Security means that no trust is automatically assumed based on network location, as every device or asset must submit an access request and be verified by some form of authentication, whether it sits inside or outside the security boundary of a system.
3. Resource access is granted on a per-session basis. Users, devices, and services are granted the minimum necessary access required. Only one resource is granted access at a time; additional resources require explicit authentication.
4. Dynamic policy determines resource access based on device health, configuration, location, and behavioral attributes.
5. Continuous diagnostics and mitigation is a set of practices and technologies that monitors the integrity and security posture of all devices and applications within an enterprise boundary. Assets outside the boundary may have more tightly controlled access based on security posture.
6. Authentication to any resource is never inherited. Users, devices, or services must authenticate every resource they require for any function.

7. The agency or enterprise collects as much information as possible on the current state of all network infrastructure, assets, and data communication to monitor, maintain, and improve the overall security posture.

The DoD released the Zero Trust Reference Architecture (ZT RA) guide in July 2022. Much like the NIST Zero Trust Architecture (ZTA), the DoD ZT RA has the following five basic tenets [28]:

1. Assume a hostile environment.
2. Presume a breach has already occurred.
3. Never trust; always verify.
4. Scrutinize explicitly.
5. Apply unified analytics.

Drivers for implementing and adopting the DoD ZT RA stem from the Director, Operational Test & Evaluation. The fiscal year (FY) 2021 Annual Report details that although cybersecurity is the most common survivability problem in the DoD, the suite of cybersecurity capabilities intended to protect the DoD Information Network was ineffective in defending against cybersecurity threats [27]. As network boundaries become more fluid, multicloud environments, hybrid cloud, and/or virtual private network (VPN)-accessible legacy cybersecurity approaches that focus primarily on perimeter defenses and detection of intrusion after a cyber incident have proven to be ineffective. Hence, on 22 November 2022, the DoD released the DoD Zero Trust Strategy and Roadmap [29], which details the following four high-level and integrated strategic goals that define the future for ZTAs within the DoD:

1. Zero Trust Cultural Adoption – All DoD personnel are aware, understand, are trained, and committed to a zero trust mindset and culture and support integration of ZT.
2. DoD information Systems Secured and Defended – Cybersecurity practices incorporate and operationalize zero trust in new and legacy systems.
3. Technology Acceleration – Technologies deploy at a pace equal to or exceeding industry advancements.
4. Zero Trust Enablement – Department- and component-level processes, policies, and funding are synchronized with zero trust principles and approaches.

Zero trust cannot be implemented by a single solution or platform that can be purchased; however, with well-integrated products and implemented and well-defined policies, it is a security framework that seeks to protect critical assets, regardless of the security boundaries of deployed systems. Through the integration of multiple products to meet the pillars and capabilities described in the DoD ZT RA, a zero trust architecture can be achieved. The DoD ZT RA defines the most critical aspects of the ZT RA as pillars, which are key focus areas for implementing zero trust controls. The DoD ZT RA defines capabilities as the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means (technology and policy) to perform a set of activities [29].

The zero trust architecture provides explicit security guidelines for how edge computing can be secured and used effectively in CONUS and OCONUS. The DoD developed ZT RA to secure systems, regardless of security boundaries; it has become an essential reference framework to enable truly secure edge computing. As data traverses through an unknown number of public and private clouds, how data is secured and validated and its provenance protected remain among the most critical factors accelerating cloud-computing adoption. The DoD stated that it will adopt a zero trust architecture by 2027 [20]. Research and development of solution sets that can meet the core tenets of the DoD ZT RA continue to evolve and need further development to make the true implementation of zero trust a reality.

### 3.2.3 MANETs

Telecommunications and computing networks have changed significantly since the 1980s. Changes have evolved from introducing and adopting 4G mobile networks to the current construct of 5G networks. 5G on orthogonal frequency-division multiplexing (OFDM) modulates a digital signal across several channels to reduce interference and uses the new 5G New Radio (5G NR) air interface alongside OFDM principles. The use of the new 5G NR air interface will enhance current OFDM signals and deliver greater scalability and flexibility. 5G also uses broader bandwidth technologies, such as sub-6 GHz and millimeter wave (mmWave) [30], and dramatically enhances the mobile network's speed, scale, and availability. It expands the current electromagnetic spectrum usage, where frequencies at 300 GHz and below are typically used to transmit information for cell phones, television, radio, satellite communications, and the Global Positioning System [31]. What makes 5G a marked improvement over 4G is that it can operate in both lower bands (e.g., sub-6 GHz) as well as mmWave (24 GHz and up), which provides extreme capacity, multi-Gbps throughput, and low latency [30]. 5G plays a central role in the DoD's Electromagnetic Spectrum Superiority Strategy. With the advent of 5G, the DoD has recognized that competition and security incidents on the electromagnetic spectrum have increased sharply [32].

5G can enable faster data speeds and higher capacity than previous generations of mobile networks, especially in the higher spectrum. The higher speed and spectrum allow the DoD to provide its military forces with a highly connected, resilient battlefield network that gathers and ingests large amounts of data from edge sensors or edge-computing platforms. With faster data transport and more nodes to communicate simultaneously, 5G promises to increase SA in active conflicts and the gray zone. It also provides new layers of security built directly into the mobile network, so implementing the zero trust architecture may be possible. This fact alone has made 5G a pivotal ingredient to any edge-computing strategy.

The zero trust policies discussed in Section 3.2.2 establish an understanding that our adversaries have already penetrated our networks, stolen data, and exploited DoD systems. This has created an urgency to develop new policies and security capabilities that emphasize the need to adapt current cybersecurity strategies. As previously mentioned, the traditional perimeter or "castle wall" defense is insufficient to secure the DoD global enterprise, which supports millions of users, many of whom require access to DoD networks outside traditional boundaries, such as at the tactical edge [33].

In the late 1980s, the DoD began conducting research and development activities into smaller, more efficient radio and computer network technologies, which currently stand as precursors to the modern-day MANET. The DoD and others began to standardize network routing protocols with the advent of smaller (and more powerful) laptop computers and broader network-scale communications. These advances led to the development of Bluetooth and, eventually, the Wireless Local Area Network (WLAN), which led to the development of MANET [34].

MANETs are small systems of mobile devices, such as laptops, radios, vehicles, and Wi-Fi equipment, which form a temporary and flexible network without the overhead of administrative and support systems required by traditional networks. One unique aspect of MANET is that the network determines how to communicate, selecting among radio or electromagnetic signals or even routing messages over the internet. One of the benefits that a MANET provides to the DoD is its adaptability in range and applications, both of which can change and move with the force it supports based on changing environments and mission parameters. Today, we use MANETs to relay communications services beyond the range

of a single radio. The service data rate delivered to an individual in a MANET drops to a small fraction of the radio's capability. However, when MANETs grow, the traffic is divided into the number of users served by the networks.

As with all network designs, a MANET can take many forms or typologies. Some emerging examples in the DoD MANET class are the Vehicular Ad Hoc Network (VANET), the Intelligent VANET (InVANET), the Services and Protocol for Advanced Networks (SPANs), and the Flying Ad Hoc Networks (FANETs). VANETs, as the name implies, are a collection of wireless technologies designed to communicate between vehicles and fixed nodes. This architecture enables novel capabilities via "multihop" dissemination over long distances (see Figure 3-1). The VANET operates a moving node able to relay communication across long distances while remaining challenging to pinpoint, thus remaining more secure than fixed points. InVANETs can integrate several ad hoc networks, including over Wi-Fi and Bluetooth, and offer significant redundancy and resilience. SPANs employ Wi-Fi, Bluetooth, and cellular systems to create peer-to-peer systems without relying on cellular networks or wireless access points (WAPs). Also, by design, any node in a SPAN can leave and join a network without causing disruption. Finally, FANETs are very useful in unmanned aerial vehicle (UAV) communications, especially in a machine-to-machine (M2M) mode where the UAV squadron can communicate and coordinate without a fixed WAP. However, at least with FANETs, nodes must connect with a ground control station, navigation, and C2 satellite [34].

Another type of MANET developed and fielded by the U.S. Army is the Secure Wireless Campus-Wide Local Area Network (CWLAN). The new MANET derivative is designed to improve resiliency and is simple to set up, use, and take down (which increases mobility and unit security). Similar to the MAN-CC, CWLAN enables the use of CSfC software-based secure internet protocol router and leverages commercial nonsecure internet protocol router and foreign partner coalition networks. Several other characteristics relate to MANET's applicability to the tactical edge. They are as follows:

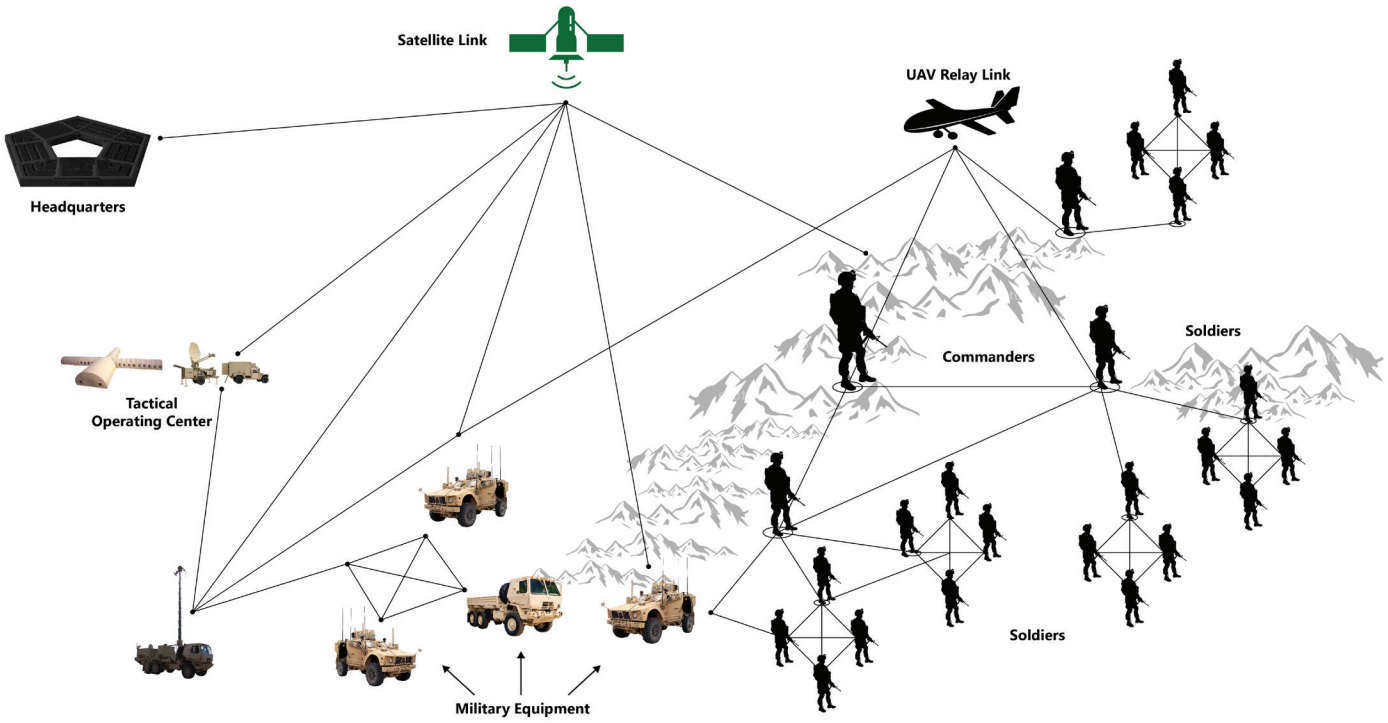


Figure 3-1. Depiction of the DoD Warfighter Information Network - Tactical *(Source: CSIAC).*

- Due to the design of MANETs, they offer a robust C2 network among forces, commanders, and, when appropriate, the local citizenry without physical infrastructure. Without a central management node, the MANET is resilient and agile by design and is not necessarily affected by physical or digital attacks.
- MANETs are also very flexible in the communication protocols they can support, including internet, radio, and electromagnetic signals.
- Due to this flexibility, MANET can support different data types, adapting to signal strength and speed and the requisite distance of communications and allowing data sharing over various geographical spaces, including in urban, remote, and contested areas.
- Finally, MANET can take advantage of 5G upgrades on the fly, allowing the DoD to exploit all the benefits of enhanced 5G networks while simultaneously adapting to lower 4G and third generation (3G) environments.

While MANETs are increasingly part of the edge-computing environment, they are still a developing capability. Only a few companies currently offer mature MANET technologies for military use. That is not to say that traditional communications companies are not getting into this market space, but the entry stakes are high due to stringent military requirements and testing standards. The following are some examples of companies that are developing and fielding MANET in military systems [34]:

- Silvus Technologies is a U.S. company developing multiple-in multiple-out (MIMO) communication technology to transmit high-fidelity video, voice, and data under challenging conditions. MIMO designs its devices so that "when a packet is transmitted into the channel, it is transmitted on more than one antenna, and when it comes out of the channel, it is received on multiple antennas" [35, 36]. Since 2011, Silvus has developed a commercial product line of MANET radios and has been working with the DoD to improve their SWaP characteristics and functionalities.
- Bittium is a Finnish company focusing on developing SDR radios for IoT, VANET, and handheld radios for on-the-move edge operators, while also offering a unique SA for small units to share back to main MANET headquarters elements [37, 38].
- Thales is a French multinational company with heavy involvement with DoD and SOF units worldwide. Since 2000, Thales has focused on Big Data, AI, cybersecurity, and connectivity in D-DIL environments. Thales has developed a widely used small, rugged form factor radio for tactical C2 units on the move at the edge [39].
- TrellisWare Technologies is a privately held U.S. company that features multiple waveforms, such as the TSM-6 waveform, which provides interoperability, scalability, and networking in tactical communication environments. TSM-6 supports an infrastructureless, nonrouting MANET that performs reliably in harsh RF environments. TrellisWare is also the prime developer of the Warrior Robust Enhanced Network-Narrowband (WREN-NB) waveform for the U.S. Army. The WREN TSM commercial waveform provides the DoD with the ability to run Sensitive But Unclassified and Secret and Below using NSA Type-1 crypto. In technical development testing conducted by the U.S. Army's Project Manager Tactical Radios, the WREN TSM waveform was successfully ported into both Manpack radio variants. Technical testing of this commercial waveform was successful in creating multiple networks, with over 93 nodes, including testing multihop network topology to allow communication in obstructed areas [40].

Edge-computing and MANET operators have myriad and unique applications and systems, some using proprietary technical standards and

protocols, which can make interoperability difficult. The DoD addressed the challenge by introducing a technology that automatically translates and seamlessly connects multiple platforms. The System-of-Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) allows one application to transmit data or instructions into its technical library, which identifies and translates that message into the recipient system standards language. The STITCHES toolchain enables M2M communications and can integrate C2 and fires platforms quickly, which is critical for MANET-enabled electromagnetic spectrum operations. Initially developed by the Defense Advanced Research Projects Agency (DARPA), the U.S. Air Force later adopted STITCHES to establish tactical networks via self-writing software. The JADC2 concept uses this premise to solve critical and complex battlefield networking challenges. We must enable the commanders to link data from unrelated systems and connect "every sensor and every operator" [9, 41].

As the MANET concept has evolved, there has also been a concurrent move to develop a capability that more precisely considers the D-DIL environment that forward-deployed forces may endure at the tactical edge. Over the last few years, the DoD National Spectrum Consortium and the U.S. Army's Program Executive Office for Command, Control, and Communications-Tactical have worked to develop the "MANET for Congested and Contested Environments" (MAN-CC) to deliver a MANET for congested and contested environments [35]. Employing COTS field radio networking along with high-throughput physical layer processing, an intuitive user interface, and well-vetted hardware and software, the MAN-CC system enables three novel improvements over traditional MANETs. These include CSfC-certified encryption for the protected transmission of Secret information, antijam capabilities in the MANET waveform to conduct operations in a congested and contested electromagnetic spectrum, and a spectrum sensor application-specific integrated circuit for RF-based SA. MAN-CC highlights the DoD's effort to identify and employ commercial capabilities, including CSfC equipment, into its MANET strategy addressing D-DIL environments.

### 3.2.4 Challenges to MANET Use

While each of the different manifestations of MANET is promising, several challenges exist. These challenges include cybersecurity, low probability of intercept/low probability of detection (LPI/LPD) concerns, signal strength, network error detection and remediation, and the potential for encrypted and unencrypted communications to coincide. Because MANETs are mainly wireless networks, they are susceptible to external interference and cyberattack. For the same reason, in CSfC-equipped MANETs, no assurance is given against LPI/LPD, which can cause severe operations security (OPSEC) problems for ongoing operations. While encryption protects the contents of the communicated data, it does not prevent an adversary from detecting the fact that it is encrypted—which reveals that it is likely of high importance. Most encryption techniques tend to have a uniform or unique distribution of data sets or values. The unique properties are significant because an adversary may key in on the fact that the communications traffic is encrypted and then use that fact to identify the source and destination of the communications, thereby discerning the purpose of the communication. Communication discernment is crucial in D-DIL environments when edge forces intend to stay "quiet" or undetected until extraction. MANET systems focus on the ability to create highly mobile secure networks using encrypted waveforms. Obfuscation is not a requirement of these products, as they primarily seek to secure data communication. However, in doing so, they also provide our adversaries with a way to detect and locate these systems.

An example of this challenge is that the People's Republic of China (PRC) has signaled its intent to become nonreliant on foreign technology. To achieve this, the PRC has focused its policies recently on becoming the global leader in AI,

quantum communications, high-performance computing, 5G mobile networks, biotechnology, and advanced materials and manufacturing. PRC involvement in 5G implementation has pushed the United States and allied nations to develop denial capabilities within U.S.-manufactured communications equipment and infrastructure assets [42]. At the same time, the 2022 Russian invasion of Ukraine amply illustrates the importance of having access to secure networks, or at least the ability to communicate securely regardless of the network [43].

### 3.2.5 Controlled Cloud Infrastructure

Cloud usage continues to grow, with the largest market share belonging to AWS, followed by Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure. AWS and Azure have recently made concerted investments into research and development and new cloud offerings designed to use and harness edge-computing capabilities. Because both CSPs have Federal Risk and Authorization Management Program-accredited data centers and DoD and federal government-specific cloud enclaves to house impact-level (IL) 4 and 5 applications and workloads, they have become the apparent market leaders to providing cloud infrastructure services to the DoD.

Edge computing has become synonymous with CSPs, as it has become a natural extension of how these widely distributed networks function. As more devices, especially IoT ones, continue to flood the market, the need for quick and reliable processing of multithreaded data continues to grow. At the same time, the need for even faster processing of the data these connections provide has grown as connections grow. The burgeoning demand for edge computing from many industries has led to a demand for edge computing from many industries, such as automotive, industrial, energy, and internet streaming services. Using the cloud to host edge-computing infrastructure provides the most flexible and cost-effective method for many industries. The ability to rapidly deploy and elastically expand edge-computing resources as needed has made the cloud the most attractive and technically feasible location for the edge.

The term "edge computing" has vastly different meanings for commercial practitioners vs. the specific needs of DoD operators. As Dustan Hellwig explained, "The DoD-specific computational edge use case spans from the grey hull, or small deck of a U.S. Navy vessel… to small Special Operations group" [14]. Regardless of the "edge" environment, CSPs understand that the military requirements driving edge computing are directly linked to how well they can provide computational and storage power in austere environments (where data bandwidth and signal loss can quickly occur). As Frank Paterra, Senior Manager of Edge products at AWS (and the inventor of the "Snow" family of products) has stated, this requirement is what has led AWS to research and develop highly available, highly portable, and secure solutions like the AWS Snowball [44]. The AWS Snowball is a member of the Snow family of devices, offering computing resources to collect and process data at the edge. These devices include the Snowball, the Snowcone, and an additional man-portable device planned for release in 2023. The Snowcone is a small (4.5 lb), rugged, encrypted, edge-computing and data-migration device. It is also rack mountable and can be checked as luggage on an airline or carried and delivered by a drone. It has up to 14 TB of storage and can be used wirelessly as part of a MANET or other network configuration.

Several commercial computing products have been developed that meet military specifications. Examples of these products include Microsoft Azure Data Box and AWS Snowball. With the Azure Stack Edge device, Microsoft seeks to enable running applications and leveraging hardware-accelerated AI and ML solutions to analyze and filter data at the edge. Azure Stack Edge and Azure Data Box are available in the Azure government cloud. They have received DoD IL6 accreditation for Azure government Secret, enabling capabilities that allow

for preprocessing data at the edge, thus allowing decision-making in DIL or even disconnected environments [45].

Performance Defense has built the Edge 5G-X device to provide edge-enabled AI/ML using an array of communication lines, such as 4G/5G, Wi-Fi, SATCOM, and traditional wired ethernet. Unlike Snowball and Data Box, the Edge 5G-X device is a highly customizable COTS solution, designed and hardened with the highest security considerations, including red/black architecture and hardware-based root of trust capabilities.

The ability to provide a mobile, security-hardened, ruggedized device that contains storage, computing, and multiple communication capabilities (via 4G/5G, SATCOM, or the cloud) is vital to bringing edge computing to contested, forward-deployed areas. The Snowball, Azure Data Box, and the Edge 5G-X are all examples of how to enable edge-computing capabilities in contested and DIL environments. By enabling AI/ML processing on these hardened devices, large volumes of data are no longer required to transit back to a centralized processing arena. These devices provide a new level of mobility and agility to U.S. military forces, regardless of the type of communication links available.

### 3.2.6 Untrusted OCONUS Cloud Infrastructure

Employing the OCONUS cloud infrastructure during deployed operations presents both challenges and opportunities. OCONUS cloud infrastructure use is much like CONUS cloud, except for the geographical location of the physical data centers that house the OCONUS clouds. However, many integration points are needed to make the OCONUS infrastructure as secure and reliable as the CONUS infrastructure. Boundary cloud access points and voice cloud access points must be appropriately implemented at all classification levels to allow OCONUS cloud infrastructure to communicate securely with the Defense Information System Network [3]. Unlike in the CONUS cloud infrastructure, another key difference in the OCONUS cloud needs is that due to the geographical location of the OCONUS cloud infrastructure itself (data centers, network circuits, etc., physically located in foreign territory), disconnected users/Warfighters must have access to enough data without the reliability and availability of the CONUS cloud. It is reasonable to assume that in large OCONUS areas, D-DIL environments become prevalent, thus requiring users to transfer data rapidly and securely to edge-computing resources while not revealing their location to our adversaries.

Competitive operations require continued access to information sources and producers, applying untrusted OCONUS infrastructure surreptitiously with information assurance. If accomplished securely on these untrusted networks, forward-deployed forces can rapidly produce, communicate, and consume significant amounts of information and thus allow the Warfighter to securely reach back to CONUS infrastructure to access data repositories, analytical technology, and automation engines (including those equipped with AI/ML capabilities). Any solution to do so should securely make the most of indigenous assets. It should also seamlessly synch, when possible, with CONUS assets.

Multicloud and hybrid cloud models provide the most highly available and effectively distributed solution to build and house cloud applications and infrastructure. However, this approach also introduces security concerns. The increasing complexity of cloud, multicloud, and hybrid network environments—combined with the rapidly escalating and evolving nature of adversary threats—has exposed the lack of effectiveness of traditional network cybersecurity defenses. Identity management across multicloud and hybrid cloud models relies on a shared or distributed directory of authorized users and machines. This vulnerable technique reveals administrative burdens and exploits security gaps. Another challenge is maintaining encryption throughout

end-to-end communication in multicloud environments. As data moves from one cloud to another, how encryption is enforced and maintained has been cumbersome and expensive.

Traditional perimeter-based network defenses with multiple layers of disjointed security technologies have been unable to meet cybersecurity needs due to the current threat environment. As the NIST guidance for zero trust details, trusting any communication or asset just because it has passed through a perimeter-based defense is no longer sufficient to protect data and assets from cyberattacks.

### 3.2.7 Challenges to Secure Communications From the Edge

The basic architecture underlying edge-computing capabilities, regardless of its application, is composed of the following three layers:

1. Cloud Services Layer: Primarily used for data storage and large volumes of computing power.
2. Edge Servers/Nodes Layer: Serves as computational power placed geographically close to devices or nodes that communicate directly with the edge servers/nodes. This layer itself is composed of devices with various functions commonly deployed in a hierarchal manner. Higher computing/storage devices sit closer to the Cloud Services Layer, while devices that function as access points or data aggregators sit closer to the Edge Devices Layer.
3. Edge Device Layer: Composed of sensors, arrays, actuators, or IoT devices. This list can include mobile devices with embedded sensors that gather data or sensor arrays that may sit on forward-deployed assets. Regardless of their form factor, most devices in this layer do not have the storage capacity or computing capacity to correlate and analyze the data they gather effectively.

Various risks become apparent when looking at the many use cases for mobile edge computing and become increasingly pronounced considering the use of military and intelligence applications. Despite the existence of well-established security frameworks, such as NIST SP 800-53 Rev. 5 ("Security and Privacy Controls for Information Systems and Organizations" [46]) or the "Cloud Controls Matrix (CCM)," [47], no frameworks encapsulate all three layers of a mobile edge-computing system. This exposure leaves the Edge Devices Layer and Edge Servers/Nodes Layer particularly exposed to cyber-focused attacks.

Edge servers have been deployed globally as hardware and software, whether located in a commercial cloud in a foreign country or onboard a forward-deployed vessel or aircraft. As these systems must collect, correlate, and analyze the data sent from many sensors/devices, they house large amounts of data that our adversaries may want to destroy, corrupt, or manipulate to decrease the effectiveness of intelligence-gathering activities. As noted by a 2020 Center for Strategic & International Studies brief [4], "The same technological tools augmenting U.S. intelligence will empower and embolden foreign intelligence rivals—namely China and Russia—in detecting, denying, disrupting, and deceiving U.S. intelligence collection efforts."

*This Page Intentionally Left Blank*

# SECTION 04 RELEVANT DOD RESEARCH EFFORTS

The DoD's budget request for the fiscal year 2022 provides insight into several efforts to address the need for technology supporting edge operations and secure communications [48]. The authors identified current research underway across the DoD, and this section covers some of those leading-edge projects undertaken by the DoD. Examples of relevant projects are summarized in the next sections and categorized as Analytic Support, Decision-Making Support, or Secure Computing and Communications Support. The project description and commentary also provide an overview of its applicability to future edge-computing capabilities.

## 4.1 DEFENSE THREAT REDUCTION AGENCY (DTRA)

### 4.1.1 Edge Computing for AI/ML Based in Forward-Deployed Cell Phones and Associated Equipment – Current Project [49]

**Description:** DTRA is attempting new innovative ways to improve C2 for deployed forces by leveraging standard equipment and technologies. This project involves GOTS/COTS cell phones' ability to increase compute capabilities to create virtual processing networks for secure processing to the edge, possibly adding advanced AI/ML for the end user. Adding AI/ML capabilities closer to the edge ensures timely C2 and intelligence sharing more rapidly and efficiently, leading to a reduction of overhead, which improves SWaP and LPI/LPD.

**Category:** Analytic Support, Decision-Making Support

**Applicability:** As GOTS/COTS communication devices like the Android Tactical Assault Kit are more frequently deployed to gray zone environments, exploiting improved compute and quality with novel analytic capabilities improves C2 and data collection sharing.

## 4.2 U.S. ARMY

### 4.2.1 ConnextEdge: A Hierarchical Framework for Resilient Edge Analytics – Current Project [50]

**Description:** On behalf of the U.S. Army, this project focuses on integrating sensor data with AI analytics at the edge. As part of the DoD strategy for a future Internet of Battlefield Things, this effort may enable improved SA and C2 in D-DIL environments, enabling local analytic decisions about myriad sensor data. Also, by considering SWaP realities, agile decisions can be made on where and how to process data at networked or edge devices.

**Category:** Analytic Support, Decision-Making Support

**Applicability:** This capability, if successful, enables powerful compute and analytic algorithms at edge devices to perform timely analysis on critical sensor-derived and other data, as well as ensures continuity of operations in disconnected situations.

#### 4.2.2 Context-Aware Networking and Cybersecurity for Resilient Networking – Past Project [51]

**Description:** This three-year project focused on two main topics—context-aware networking and cybersecurity for resilient networking. Network resilience is the network's ability to continue operating during an adversary attack. The author assessed the findings of the cybersecurity portion of the project, which focused on enhancing the security of tactical networks in the presence of dynamic and sophisticated adversaries. The research also addressed moving target defense (MTD), a proactive approach to cybersecurity that increases the complexity and uncertainty for the attacker by dynamic changes to the attack surface. While the project was not conclusive, it created several derivative projects within the Army that are underway today.

**Category:** Secure Computing and Communications Support

**Applicability:** The applicability of this research strongly suggests that MTD and network obfuscations clearly support MANET environments and deployed forces in D-DIL environments. Network obfuscations are also extremely helpful during gray zone engagements by denying the adversary the ability to detect operations, providing LPI/LPD.

### 4.3 U.S. AIR FORCE

#### 4.3.1 Softward-Defined Multiaccess Edge Collaboration Platform – Current Project [52]

**Description:** This U.S. Air Force research project combines COTS equipment (Android/iOS) and software, such as edge-computing and group collaboration apps (video, audio, chat, and file sharing), with AI/ML to enable video analytics. The resulting platform would exploit current smart devices' abilities to operate in D-DIL environments, such as poor or no wireless connectivity or limited network bandwidth.

**Category:** Analytic Support, Decision-Making Support

**Applicability:** If successful, this platform could be deployed autonomously in austere and D-DIL environments, allowing edge video analytics in a timely fashion.

### 4.4 OFFICE OF THE SECRETARY OF DEFENSE

#### 4.4.1 Secure Edge Computing With Encrypted Neural Networks – Current Project [53]

**Description:** This project envisions employing homomorphic encryption (HE), a type of encryption that allows the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form in deployed neural networks. Neural networks are AI-driven computer nodes that process data like the human brain through an ML process called deep learning. HE is highly secure and prevents most types of cyberattacks, which may ensure the protection of neural networks without leakage of classified or sensitive data. This research has several challenges due to incompatibilities between HE and neural network learning algorithms. Also, HE-encrypted neural networks would not operate well on current edge-computing systems due to SWaP issues.

**Category:** Analytic Support, Decision-Making Support

**Applicability:** If successful, this capability would allow advanced AI/ML analysis of encrypted data at the edge, significantly improving edge C2 and SA.

### 4.5 DARPA

The most relevant DARPA research projects are summarized next and categorized as Analytic Support, Decision-Making Support, or Secure Computing and Communications Support. The project description and commentary also provide an overview of its applicability to future edge-computing capabilities.

### 4.5.1 Guaranteeing AI Robustness Against Deception (GARD) – Current Project [54]

**Description:** The GARD program is developing techniques to defend against deception and other adversarial attacks on AI/ML systems. GARD addresses the need to defend against deception attacks, whereby an adversary inputs engineered data into an ML system intending to cause the system to produce erroneous results. Deception attacks can enable adversaries to take control of autonomous systems, alter conclusions of ML-based decision support applications, and compromise tools and systems that rely on ML and AI technologies.

**Category:** Analytic Support, Decision-Making Support

**Applicability:** Current techniques for defending AI/ML have proven brittle due to a focus on individual attack methods and ineffective methods for testing and evaluation. Techniques developed under the GARD program address the current limitations of defenses and produce ML and AI systems suitable for use in adversarial environments.

### 4.5.2 Secure Handhelds on Assured Resilient Networks at the Tactical Edge (SHARE) – Past Project [55]

**Description:** DARPA was looking for technologies that enable single, smart devices to consolidate and process several different security levels and then share the resultant data across unsecured commercial networks, including cellular, Wi-Fi, satellite, and other communications platforms.

**Category:** Secure Computing and Communications Support

**Applicability:** Forward-deployed Warfighters must have multiple laptops or devices approved to communicate at various classification levels. The vision of SHARE is to develop software that moves the management functions of multiple security levels from a handful of data centers down to trusted, handheld devices on the tactical edge.

### 4.5.3 Memory Optimization (MemOp) – Current Project [56]

**Description:** The MemOp program is developing technology to optimize memory transactions in large-scale computing systems. Distributed data centers with high-speed interconnected and customizable hardware, including graphics processing units and field-programmable gate arrays, are being used to achieve greater efficiency and improved processing performance.

**Category:** Analytic Support

**Applicability:** MemOp is exploring new memory architectures that fully leverage emerging customizable hardware to deliver computing services reliably and at a reduced cost. The technologies developed in this program enhance efficiency and improve performance for large-scale and edge-computing systems.

### 4.5.4 Resilient Anonymous Communication for Everyone (RACE) – Current Project [57]

**Description:** The RACE program is developing cryptographic and communication obfuscation technologies to enable anonymous, attack-resilient mobile communications within a network environment.

**Category:** Secure Computing and Communications Support

**Applicability:** RACE is developing a mobile phone application and distributed systems that provide a secure message-passing service by combining advanced distributed system tasking with communication protocol encapsulation methods. The system maintains confidentiality, integrity, and messaging availability while preventing large-scale compromise of the system.

### 4.5.5 Dispersed Computing – Past Project [58]

**Description:** The Dispersed Computing program was developing techniques to distribute computing tasks across network computing elements to enable more efficient utilization of enterprise and internet-based storage, processing, and networking resources. This program was developing a dispersed computing architecture that results in more efficient utilization of storage, processing, and networking resources.

**Category:** Analytic Support, Secure Computing, and Communications Support

**Applicability:** With Dispersed Computing technology, the network becomes the cloud, performing effective and efficient computations. Enterprises and internet-based information technology service providers are increasingly adopting the cloud model, with data storage and computer processing concentrated in large data centers. Employing the cloud model brings economies of scale and cost savings to storage and processing but creates problems for the network and latency-sensitive applications due to the need to backhaul data to (often distant) data centers.

### 4.5.6 Brandeis – Past Project [59]

**Description:** The Brandeis program created the capability to dynamically, flexibly, and securely share information while ensuring that private data may be used only for its intended purpose.

**Category:** Secure Computing and Communications Support

**Applicability:** Brandeis technologies can resolve the tension between maintaining privacy and being able to tap into the massive value of data. The U.S. military is increasingly involved in operations requiring highly selective data sharing with a heterogeneous mix of allies, coalition partners, and other stakeholders. Brandeis technologies work with virtualization, cloud computing, and software-defined networking technologies, now widely used in civilian and military environments.

### 4.5.7 Data Privacy for Virtual Environments (DPRIVE) – Current Project [60]

**Description:** The DPRIVE program enables data privacy at the user and application level by developing new hardware accelerators to achieve acceptable computational times.

**Category:** Secure Computing and Communications Support

**Applicability:** The program plans to provide strong privacy protections at the tactical edge with no more than one order of magnitude penalty in computation time and enable robust privacy at the enterprise level with no more than three orders of magnitude penalty over unencrypted processing. The program enables the development and deployment of these hardware accelerators to edge-computing devices where power and time are at a premium, as well as enterprise computing facilities where the amount and sensitivity of the data require increased protection.

### 4.5.8 Generating Communication Channels to Operate (GeCCO) – Current Project [61]

**Description:** DARPA recently announced the GeCCO project, which seeks to enable secure communications for military applications in permissive environments by using a flexible communications architecture to deploy virtual network services to preserve privacy by preventing pattern-of-life analysis. GeCCO aims to identify novel technology and solutions that allow secure communications across commercial and untrusted channels while maintaining privacy and preserving OPSEC protocols among and between U.S. and partner nation military forces operating at the edge.

**Category:** Secure Computing and Communications Support

**Applicability:** Today's distributed operations across the globe require a small logistical footprint to enable collaboration with mission partners while still preserving the privacy of communications. GeCCO overcomes this challenge by enabling the secure use of widespread cellular networks to reduce the logistical burden of deploying military systems. It uses virtualization and software programmability to create the network services needed to preserve privacy while improving the quality of service compared to today's tactical radio networks.

*This Page Intentionally Left Blank*

# SECTION 05 COMMERCIAL/ MARKET RESEARCH

## 5.1 ARCHON

Archon is a CSfC-trusted integrator that offers several product lines in the security sector. Archon provides obfuscation capabilities through the CAMO product. Archon CAMO provides covert attribution management and orchestration by masking an asset's identity, location, and destination. CAMO utilizes a VPN-based, multihop technology to make it more difficult for adversaries to identify CSfC enclaves by making IPsec VPN traffic look like other types of traffic, such as a video-streaming service. CAMO then routes traffic through a multihop path created exclusively for the current session. Archon CAMO randomly selects servers from hundreds of private and popular commercial services worldwide for each session. The options include major hosting providers like AWS and VPN providers like NordVPN. At each hop, a VPN server is spun up just for the duration of the session. CAMO can also exclude countries or regions from the multihop route created.

Archon believes that network obfuscation and managed attribution solutions are essential because encrypting data before sending it over the open internet is not secure enough. An adversary might not be able to view the data. However, by seeing that it is encrypted and where it is coming from, the adversary can easily extrapolate that (1) this is important and (2) this person is important. CAMO's obfuscated VPN service adds an extra layer of protection by making IPsec VPN traffic look like another type of traffic, such as a YouTube video or an IP camera stream. It provides a means to hide traffic from adversaries looking for encrypted traffic as a countermeasure in their cyber kill chain.

Unlike other network obfuscation services, Archon CAMO can create and break down a new dynamic connection monthly or daily. Archon can set up new locations for network nodes on the fly, whereas other obfuscation services on the market set up an initial network and maintain the same network connections. The ability to significantly randomize the network over which communication and data transport occurs is vital to maintaining anonymity and data obfuscation [62].

## 5.2 CODE-X

Code-X is a secure communications platform that enables operators to manage how machines, processes, and components engage with each other. Code-X facilitates zero trust security between operators' smartphones, EUDs, and local commercial cellular, Wi-Fi, Bluetooth, and navigation satellite sources. Using patented Network Watermark™ and Intelligent Machine Authentication™ technology, Code-X provides a new form of identity management that enables the zero trust framework. It disrupts adversary detection and allows operators to communicate in contested environments that lack high-throughput communication pathways. Code-X technology allows communications across more low-bandwidth network links and synching stored data sets post mission. It also enables large volumes of signaling

data to be rapidly routed, secured, and obfuscated—preventing analysis and cross-correlation of specific data markers that indicate conventionally encrypted activity by adversaries.

Code-X, a 100% lightweight software engine smaller than most photo files, is a security solution that employs five unique dimensions that all work simultaneously. The system allows communications to remain covert and prevent the cyber "kill chain" so that even if an adversary could detect the traffic, it would appear mundane, and no usable data could be detected.

Code-X leverages the following dimensions in its secure communications platform: Fractionalization, Multipathing, Network Watermark, Intelligent Machine Authentication, and Measurement of Change.

## 5.3 TELOS

Telos Ghost is a shared or dedicated network-as-a-service (NaaS) that provides network obfuscation and managed attribution for cybersecurity and enable security operations. It approaches cybersecurity by stating, "The best way to protect people, assets, and information on the network is to prevent them from being seen in the first place" [63].

Telos Ghost is a virtual obfuscation NaaS that allows an enterprise to obfuscate communications and transactions over the internet by leveraging dynamic internet protocol (IP) routing and management attribution. It complements and enhances the technical security stack of organizations by providing an additional layer of security on top of VPNs, endpoint protection, and frameworks, such as zero trust network access and secure access service edge.

Telos Ghost uses encryption and proprietary-based mesh algorithms for dynamic IP routing among cloud transit nodes to perform the following [62]:

- Obscure and vary network pathways to prevent adversaries from tracking users and information.
- Use multiple layers of encryption to protect information and remove the source and destination IP addresses to eliminate network paths back to the source.
- Enable users to manage their technical and nontechnical persona to disguise their identity and location.
- Hide critical network resources using cloaked capabilities for email, storage, applications, and unified communications.

*Note: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. government and shall not be used for advertising or product endorsement purposes.*

# SECTION 06 CONCLUSION

This report contends that the future U.S. military Warfighter requires the technological devices and capability to conduct analytics at the edge and securely and surreptitiously transmit the resulting data to decision-makers, all while located in a D-DIL setting and during contested digital network environments. Edge computing is a valuable new and emerging capability for the DoD, with in-depth research and development being conducted individually and cooperatively across industry, academia, and DoD research institutions. Edge computing has the potential to enhance Warfighter communication and operations capabilities across untrusted networks or cloud infrastructure.

The need for better communication obfuscation and secure, concealed data exfiltration at the edge of a network is lacking adequate attention considering the tools needed by the Warfighter in an austere environment. Most equipment and transport technologies today rely on standard NSA-approved CSfC encryption protocols, which exacerbate network and SWaP overhead and illuminate data traffic, making it susceptible to cyber "kill chain" attacks. Encrypted traffic is easily detected and can potentially expose the location of forward-deployed assets. These limitations also undermine sensitive-edge OPSEC in gray zone environments.

Edge computing and data transmission to or from Warfighters remain an active area of research and development in the near term. As John A. Wilcox has noted, "This is one of the most critical areas of needed research; edge communications systems must focus on reducing transmission signatures to gain LPI/LPD" [16]. Consequently, edge communications systems must focus on reducing their signature to gain improved LPI/LPD. Reduction is through digital obfuscations, "beamforming," or other novel techniques to make it more difficult for adversaries to use their signals intelligence capabilities to detect, find, and fix U.S. forces [64].

A recent U.S. Air Force research request for edge operations is an example of future expectations in the area. The Air Force requested high frequency (HF) radio modernization to replace legacy HF radios, which have reached obsolescence and require increased capacity modernization. HF modernization provides an alternate means of communication when satellite communications are unavailable due to natural and manufactured disruptions. The new technologies must incorporate 3G/4G automatic link establishment and comprehensive band features and, most importantly, possess LPI/LPD features. These airborne radios must keep pace to guarantee C2 interoperability [48].

Furthermore, the Defense Modernization and Prototyping program within the Office of the Under Secretary of Defense for Research and Engineering recently sponsored a technology demonstration and experimentation collaboration request for information from industry, named Thunderstorm 22-2 [65]. The event focused on improving battlespace management in contested

environments. Quantifying the provenance and pedigree of signals (data integrity) and optimizing SA and communications (decision-making) were of primary interest. These topics specifically addressed facilitating an LPI/LPD (data and OPSEC) and ensuring reliability in D-DIL environments.

The computing environment for edge military and intelligence operations requires rapid, secure, and automated relocation of containers from the enterprise to and across the edge and back. Further, connectivity, capacity, available processing, and mission needs are critical to this scalable and dynamic network. Eventually, distributed and covert container management solutions, along with the described data science pipeline, allow easy relocation of compute and analytic processing to the location (or locations) where it is best hosted for the required mission and concept of operations. To help address vulnerabilities and secure data, the DoD depends on the standard and approved cybersecurity. Information security approaches for edge computing and communications include firewalls, VPNs, proxies, and physical and logical separation of networks. Data and system obfuscation can significantly mitigate these problems by masking users and data in transit or by adding complex techniques to obscure IP addresses, user identity, and source and destination data to make any recovered information unusable.

# REFERENCES

1. Marbukh, V. "Towards Efficient Offloading in Fog/Edge Computing by Approximating Effect of Externalities." IEEE INFOCOM 2018 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), https://doi.org/10.1109/INFCOMW.2018.8406835, April 2018.
2. U.S. DoD. *Joint Operation Publication 5-0: Joint Planning.* Joint Chiefs of Staff, https://grugq.github.io/resources/jp5_0.pdf, 11 August 2011.
3. U.S. DoD. "Outside the Continental United States (OCONUS) Cloud Strategy." Office of the DoD Chief Information Officer, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-OCONUSCloud Strategy.pdf, 26 May 2021.
4. Katz, B. "The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection." CSIS brief, Center for Strategic & International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20713_Katz_CollectionEdge_v4_WEB%20FINAL.pdf, July 2020.
5. U.S. DoD. "2022 National Defense Strategy of the United States of America." Washington, DC, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, October 2022.
6. U.S. Army Training and Doctrine Command Pamphlet 525-3-1. *The U.S. Army Operating Concept: Win in a Complex World 2020-2040.* https://usacac.army.mil/sites/default/files/publications/Army%20Operating%20Concept%202014%20%28TP525-3-1%29.pdf, October 2014.
7. U.S. Department of the Army. *ATP 2-01.3, Intelligence Preparation of the Battlefield.* Washington, DC, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31379-ATP_2-01.3-001-WEB-4.pdf, March 2019.
8. U.S. DoD. "DoD Announces Release of JADC2 Implementation Plan." Press release, Washington, DC, https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/, 17 March 2022.
9. U.S. DoD. "Summary of the Joint All-Domain Command & Control (JADC2) Strategy." Washington, DC, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF, March 2022.
10. Feickert, A. "The Army's Project Convergence," Congressional Research Service, IF11654 (Version 6), https://crsreports.congress.gov/product/pdf/IF/IF11654/6, 2 June 2022.
11. MacKown, C. Project Convergence 2022 at Fort Irwin, CA (image 22 of 22). Photo ID 7494334, Defense Visual Information Distribution Service (DVIDS), https://www.dvidshub.net/image/7494334/project-convergence-2022, 31 October 2022.
12. U.S. DoD. *Joint Publication 3-09: Joint Fire Support.* Joint Chiefs of Staff, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf, 10 April 2019.
13. Chawla, A., and J. Wilcox. Personal communication, 29 November 2022.
14. Chawla, A., and D. Hellwig. Personal communication, 23 November 2022.
15. Bastian, N. "Evaluating the Resiliency of AI Systems: An Overview of Adversarial AI." CSIAC webinar, https://csiac.org/wp-content/uploads/2022/02/Bastian_CSIAC-Webinar-Adversarial-AI_MB-edits_2.pdf, 17 May 2022.
16. Hewlett Packard Enterprise. "HPE and NVIDIA Accelerate I.I. From Edge to Cloud." https://www.hpe.com/us/en/solutions/artificial-intelligence/nvidia-collaboration.html, accessed 27 December 2022.
17. Army Technology. "BrainChip Advances A.I. and ML to Edge Computing." https://www.army-technology.com/research-reports/brainchip-advances-ai-and-ml-to-edge-computing/, 2 May 2022.
18. White, A. "Special Operations Tactical Communications." DefenseMediaNetwork, https://www.defensemedianetwork.com/stories/special-operations-tactical-communications/, 27 May 2020.
19. U.S. Air Force Research Laboratory. "Tactical Assault Kit (TAK)." https://afresearchlab.com/technology/information-technology/tactical-assault-kit-tak/, accessed 27 December 2022.
20. Lopez, C. T. "DOD Releases Path to Cyber Security Through Zero Trust Architecture." https://www.defense.gov/News/News-Stories/Article/Article/3229211/dod-releases-path-to-cyber-security-through-zero-trust-architecture/, 28 November 2022.
21. General Dynamics Mission Systems. "Tactical Cross Domain Solution (TACDS)." https://gdmissionsystems.com/products/cross-domain-solutions/tacds-tactical-cross-domain-solution, accessed 5 December 2022.
22. Collins Aerospace. "Data Flow Security." https://www.collinsaerospace.com/-/media/CA/product-assets/marketing/s/secureone/secureone-mils-tactical-cds-ms-

# REFERENCES, *continued*

datasheet.pdf?rev=c50d1d90a80f4e9f85ea9e9bbec44d00, accessed 6 December 2022.

23. Committee on National Security Systems. CNSS Instruction No. 4009. https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf, 26 April 2010.
24. NSA. "CSfC Frequently Asked Questions (FAQs)." https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/faq/#General, accessed 7 January 2023.
25. NSA. "Deploying Secure Unified Communications/Voice and Video over I.P. Systems." Cybersecurity Technical Report PP-21-0827, Version 1.0, https://media.defense.gov/2021/Jun/17/ 2002744054/-1/-1/1/CTR_DEPLOYING%20SECURE%20VVOIP%20SYSTEMS.PDF, 15 June 2021.
26. Lee, K., G. Dupier, and J. Pisano. "How the U.S. Military Is Using Edge Computing." Booz Allen Hamilton, https://www.boozallen.com/s/insight/blog/how-the-us-military-is-using-edge-computing.html, accessed 27 December 2022.
27. NIST. "Zero Trust Architecture." NIST Special Publication 800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final, August 2020.
28. Denman, T. "Zero Trust – The Time Is Now." CSIAC webinar, https://csiac.org/wp-content/uploads/2022/09/Denman-ZT-Presentation-CSIAC-July-2022-v-3.pdf.
29. U.S. DoD. "Department of Defense Releases Zero Trust Strategy and Roadmap." News release, https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/, 22 November 2022.
30. Qualcomm. "Everything You Need to Know About 5G." https://www.qualcomm.com/5g/what-is-5g, accessed 28 December 2022.
31. Lopez, C. T. "New Spectrum Strategy Reveals DOD's Plan to Master Airwaves." U.S. DoD, https://www.defense.gov/News/News-Stories/Article/Article/2404027/new-spectrum-strategy-reveals-dods-plan-to-master-airwaves/, 3 November 2020.
32. U.S. DoD. "Department of Defense Electromagnetic Spectrum Superiority Strategy." Washington, DC, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_ SPECTRUM _SUPERIORITY_STRATEGY.PDF, October 2020.
33. U.S. DoD. "DoD Zero Trust Strategy." Office of the Chief Information Officer, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf, 7 November 2022.
34. Kaplan, M., A. Corrente, and E. Montalti. "An Overview of MANET Technologies: Advantages and Disadvantages in the Military." Finabel, Brussels, https://finabel.org/wp-content/uploads/2022/10/48.-An-Overview-of-MANET-Technologies-Advantages-and-Disadvantages-in-the-Military.pdf, October 2022.
35. Silvus Technologies, Inc. "Silvus Technologies and Information Assurance Specialists Team to Deliver Classified Data Protection on MANET Radio Networks Using NSA Commercial Solutions for Classified (CSfC)." Los Angeles, CA, https://silvustechnologies.com/wp-content/uploads/2019/05/20190520-Silvus-IAS-CSfC.pdf, 20 May 2019.
36. Silvus Technologies, Inc. "Introduction to MIMO." https://silvustechnologies.com/why-silvus/technology/introduction-to-mimo/#:~:text=MIMO%20stands%20for%20Multiple%2DIn,is%20received%20on%20multiple%20antennas, accessed 28 December 2022.
37. Bittium. "Company Overview." https://www.bittium.com/about-bittium/facts-figures/company-overview, accessed 28 December 2022.
38. Bittium. "Tactical Communications." https://www.bittium.com/tactical-communications/%20tactical-manet, accessed 28 December 2022.
39. Thales. "U.S. Soldiers Rely on Thales for Tactical Command and Control Communications." https://www.thalesgroup.com/en/united-states/press-release/us-soldiers-rely-thales-tactical-command-and-control-communications, 27 January 2021.
40. Bailey, K. "Commercial Waveforms Provide Flexibility for the Army's Manpack Radios." https://www.army.mil/article/238077/commercial_waveforms_provide_flexibility_for_the_armys_manpack_radios, 12 August 2020.
41. Clark, C. "ACK, STITCHES and the Air Force's Networking Hopes." Breaking Defense, https://breakingdefense.com/2021/07/ack-stitches-and-the-air-force-networking-hopes/, 20 July 2021.
42. U.S. DoD. "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress, 2021." Office of the Secretary of Defense, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF, November 2021.
43. Treverton, G. F., and P. Esfandiari. "Will the Ukraine War Reshape the Internet?" CSIS commentary, Center for Strategic & International Studies, https://www.csis.org/analysis/will-ukraine-war-reshape-internet, 20 October 2022.

# REFERENCES, *continued*


44. Chawla, A., and F. Paterra. Personal communication, 16 December 2022.
45. Brown, E. "Accredited for Azure Government Secret: Azure Stack Hub, Azure Stack Edge, Azure Data Box." Microsoft, Azure Government, https://devblogs.microsoft.com/azuregov/accredited-for-azure-government-secret-azure-stack-hub-azure-stack-edge-azure-data-box/, 13 October 2021.
46. NIST. "Security and Privacy Controls for Information Systems and Organizations." NIST Special Publication 800-53, Rev. 5, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, September 2020.
47. Cloud Security Alliance. "Cloud Controls Matrix (CCM)." https://cloudsecurityalliance.org/research/cloud-controls-matrix/, accessed 28 December 2022.
48. U.S. DoD. "Defense Budget Materials – F.Y. 2022." Office of the Under Secretary of Defense (Comptroller)/CFO, https://comptroller.defense.gov/Budget-Materials/Budget2022/, accessed 28 December 2022.
49. SBIR.gov. "Edge Computing for AI/ML Based in Forward Deployed Cell Phones and Associated Equipment." https://www.sbir.gov/node/1965541, accessed 16 November 2022.
50. SBIR.gov. "ConnextEdge: A Hierarchical Framework for Resilient Edge Analytics." https://www.sbir.gov/sbirsearch/detail/1930275, accessed 16 November 2022.
51. Chan, K., E. Graves, K. Marcus, T. Moore, J. Perazzone, L. Scott, A. Swami, A. Toth, G. Verma, and P. Yu. "Context-Aware Networking and Cybersecurity for Resilient Networking (Summary Technical Report, Oct 2017–Sep 2020)." U.S. Army Combat Capabilities Development Command, Army Research Laboratory, 29 September 2022.
52. SBIR.gov. "Software Defined Multi-access Edge Collaboration Platform." https://www.sbir.gov/sbirsearch/detail/1939971, accessed 14 December 2022.
53. SBIR.gov. "Secure Edge Computing With Encrypted Neural Networks." https://www.sbir.gov/node/1971101, accessed 14 December 2022.
54. Draper, B. "Guaranteeing A.I. Robustness Against Deception (GARD)." DARPA, https://www.darpa.mil/program/guaranteeing-ai-robustness-against-deception, accessed 6 January 2023.
55. Schurgot, M. R. "Secure Handhelds on Assured Resilient networks at the tactical Edge (SHARE)." DARPA, https://www.darpa.mil/program/secure-handhelds-on-assured-resilient-networks-at-the-tactical-edge, accessed 14 December 2022.
56. U.S. DoD. "DoD FY 2023 Budget Estimates." https://www.darpa.mil/attachments/U_RDTE_MJB_DARPA_PB_2023_APR_2022_FINAL.pdf, p. 13, April 2022, accessed 15 December 2022.
57. Baron, J. "Resilient Anonymous Communication for Everyone (RACE)." DARPA, https://www.darpa.mil/program/resilient-anonymous-communication-for-everyone, accessed 22 November 2022.
58. DARPA. "Dispersed Computing (Archived)." https://www.darpa.mil/program/dispersed-computing, accessed 22 November 2022.
59. Baron, J. "Brandeis." DARPA, https://www.darpa.mil/program/brandeis, accessed 7 January 2023.
60. Jacobs, B. "Data Protection in Virtual Environments (DPRIVE)." DARPA, https://www.darpa.mil/program/data-protection-in-virtual-environments, accessed 7 January 2023.
61. Schurgot, M. R. "Generating Communication Channels to Operate (GeCCO)." DARPA, https://www.darpa.mil/program/generating-communication-channels-to-operate, accessed 7 January 2023.
62. Archon. "Covert Attribution Management and Orchestration." https://www.archonsecure.com/obfuscates-vpn, accessed 9 January 2023.
63. Telos. "Telos Ghost." https://www.telos.com/wp-content/uploads/pdf/Telos-Ghost-brochure.pdf, accessed 9 January 2023.
64. Hoehn, J. R., J. C. Gallgher, and K. M. Sayler. "Overview of Department of Defense Use of the Electromagnetic Spectrum." R46564, Congressional Research Service, https://sgp.fas.org/crs/natsec/R46564.pdf, updated 10 August 2021.
65. U.S. Naval Postgraduate School. "Thunderstorm Technology Demonstration and Experimentation." https://nps.edu/web/slamr/thunderstorm, 14 September 2020.

# EDGE COMPUTING AND COMMUNICATIONS OVER UNTRUSTED TRANSPORT

*Alok Chawla, Randy D. Bishop, and Danielle Tarino*

CSIAC-BCO-2023-351