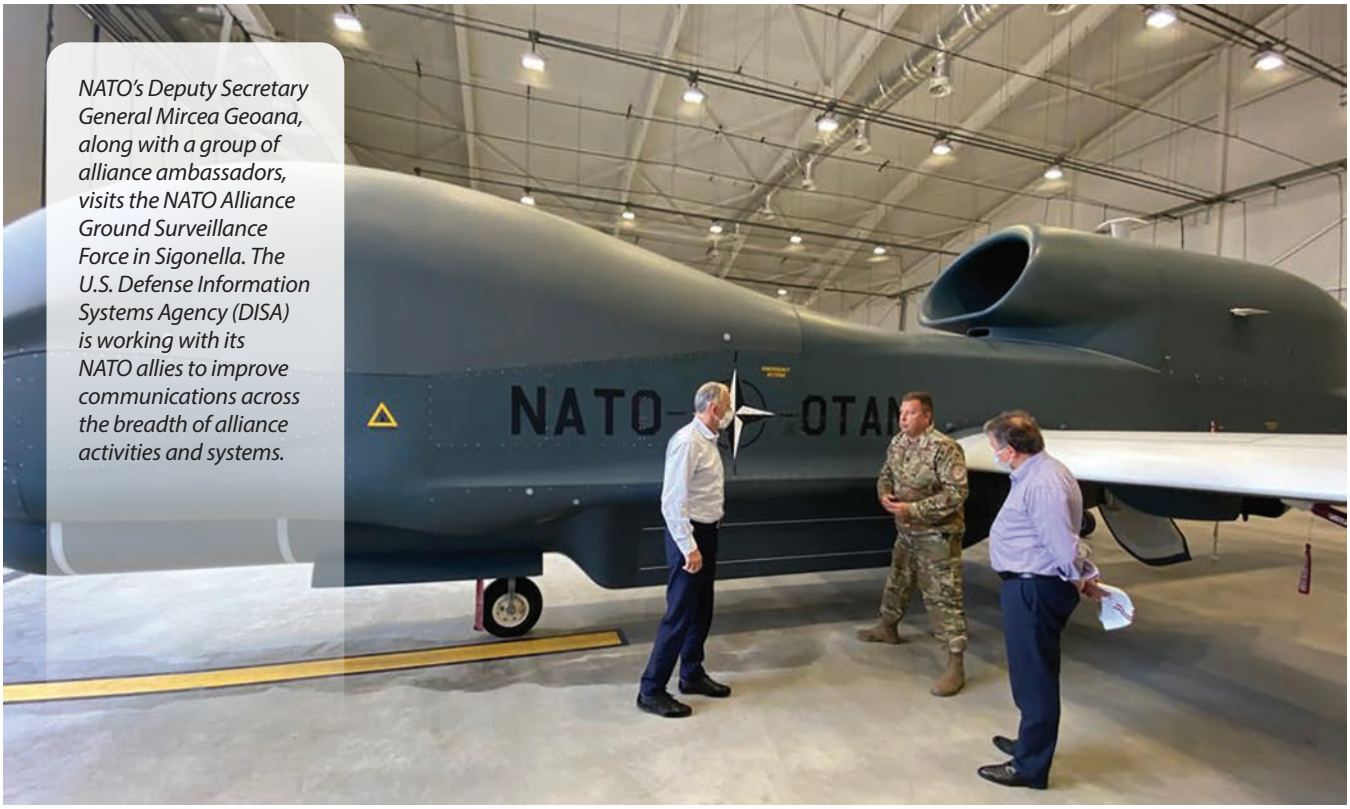


NATO

NATO's Deputy Secretary General Mircea Geoana, along with a group of alliance ambassadors, visits the NATO Alliance Ground Surveillance Force in Sigonella. The U.S. Defense Information Systems Agency (DISA) is working with its NATO allies to improve communications across the breadth of alliance activities and systems.

DISA Looks Heavenward for Cyber With NATO

Space is a top priority in work with international partners.

BY ROBERT K. ACKERMAN

The battle for cyberspace may hinge on outer space as experts expand the digital frontier. The leading U.S. military communications organization is working with partners in NATO to exploit and dominate space communication systems with an eye to hurling defense systems into an advanced technology future.

John R. Kahler, chief of the Defense Information Systems Agency (DISA) NATO Field Office, offers that space is the biggest challenge facing DISA and NATO in cyber. Its characteristics of being open and available offer both opportunities and vulnerabilities. He believes that NATO nations will embrace space just as they did the Internet.

Kahler elaborates that the space arena, particularly satellites, is vital to cyberspace. "We are beginning to expand in many different areas in space itself." However, he also warns that adversaries are pursuing the same goals in this key area. "Technology today is not like it was yesterday, where you were limited by the knowledge of availability of what's out there. We have to be very front-moving with respect to space and our activities."

He continues that NATO is working in several different areas that relate to the space realm. Big data, wireless technologies and other capabilities are active among NATO nations, and the alliance is putting together working groups to accommodate those technologies accordingly. One key is the adoption of standards for space cyber links. Defining the requirements for industry partners will establish the necessary alignments to pursue vital areas for advanced technologies, he says.

Kahler offers that DISA is leading the way for NATO in cyber. "DISA is the tip of the spear for NATO cybersecurity," he declares. "There is no doubt about it. DISA sets the gold standard; it is the organization to emulate." The agency has field offices around the globe with a dispersed workforce interconnected in a giant network.

"Not only is that cybersecurity workforce reaching out and protecting our defenses in our military, but they are

also helping our alliance partners do the same across the board in a collaborative effort," he emphasizes.

Kahler states that DISA's cyber base is the best in the world. "DISA's technical capabilities are second to none," he maintains. Yet, he emphasizes that the flow of technology between DISA and NATO is two-way. He cites a talented workforce aligned with academia and industry that creates a synchronization among global technology and that workforce.


DISA

John R. Kahler is the chief of the DISA NATO Field Office.

That same approach benefits and applies to all NATO members. One advantage to working with NATO is that 30 nations are focused on the same goal, Kahler observes. This large community allows multiple capabilities to be leveraged from industry, scientists and academia throughout the alliance.

Other nations have lessons learned that can benefit alliance members and DISA, he adds. The information shared through standards development, cyber working groups and capability teams "makes a difference" in NATO cyber readiness. "Each nation brings to the table a different perspective and a different view—a different culture, a different way and a different approach to dealing with cyber.

"Together, they form a very strong alliance against hazards associated with cyber," Kahler states.

The DISA office works through NATO's mechanisms, he continues. The alliance's collaborative effort is shared by all the nations through different boards, one of which is the Consultation, Command and Control (C^3) Board. This board defines standards, which are moved to the capability panels when they are identified as requirements. The DISA office provides subject matter expertise to alliance members. "We bring the full breadth of DISA's knowledge and technology to that table, and so we share that with our mission partners to help define those requirements and those standards," he offers. "That provides a significant capability."

And identifying areas for standards that align with cybersecurity are vital, he continues. Topics such as asset management, service management and cloud technologies stand out. Expanding networks under a single standard is ripe for solutions, which is being borne out as NATO implements its federated network. This network is aligned with risk reduction and vulnerability mitigation, and it represents a significant way forward, Kahler says.

"That technology and the direction in which NATO is going is largely based on a lot of the things that DISA already has put out there and put in place," he adds. "That alignment between DISA and its lessons learned and those technologies are feeding over into the NATO alliance, and so our partners are using them. NATO is really using that to their benefit moving forward."

The U.S. support of the C^3 Board includes high-ranking U.S. officials attending its meetings, Kahler adds. This complements the DISA field office that is located in the middle of that activity. The board's process is "very structured and very formal," he says, and it opens up technologies "in a very neutral way." The board defines the requirements, which are fixed because they are standards. Once the standards are defined, the Standardization Agreement (STANAG) is finalized and industry partners can enter the bidding process. A vendor that presents the best opportunity to meet the STANAG standards is selected for the contract.

Dealing with NATO from a U.S. perspective is a challenge, Kahler allows. He works with DISA from his post overseas, which faces the tyranny of distance. On the other hand, the NATO Communications and Information Agency in which his DISA office is embedded is very similar to DISA, he offers. Both groups perform the same function for their respective parent organizations, the U.S. Defense Department and NATO. Also, the NATO agency and DISA are willing to share capabilities for the betterment of both. That willingness is not always present with individual countries in Europe, he notes.

"Being in this position, you really get to see the relationship and impact that DISA has on its mission partners, particularly over here in NATO," he points out. "We have 30 nations working together and leveraging those lessons learned and resources that DISA provides—and being able to share that at a central location." The agency also is able to reach back to its own resources in the United States and apply them around the globe.

One of the biggest assets NATO offers DISA is the willingness to work collaboratively toward a single goal, he


NATO

Students from Dutch universities engage in a rapid design challenge aiming to develop faster and more innovative routes to delivering technologies to NATO. DISA, through its office in NATO, works with European industry and academia to develop standard communications technologies that will advance capabilities across the alliance.

elaborates. "That's very refreshing to see that occur when you go to a meeting of 30 different nations focused on interoperability in communications."

He continues that each nation brings its own technological capabilities, and they are different. But technology today is becoming ubiquitous, especially with many U.S. industries working in Europe through their own presences, in some cases collaboratively. NATO has established a working group of industry partners, which Kahler describes as unique. Companies from the United States and Europe focus on requirements that emerge from the C^3 Board, such as with 5G.

DISA's work with its industry partners domestically sets the standard for how it aims to help introduce commercial innovation into NATO systems, Kahler says. For example, the agency brought industry partners to the table to help define the future of 5G. That model made its way to the European Union (EU), which now has a 5G working group that incorporates the same concept. "That's a significant move forward and a great example of using something that we've moved toward in a collaborative way for the betterment of the entire EU itself," he observes.

At a higher level, the United States has disagreed with some of its European allies over the use of the Chinese firm Huawei for 5G development, with U.S. officials concerned over security vulnerabilities that might be present in the Chinese technology. Kahler offers that these disagreements are not affecting the use of 5G in NATO, as the partners are still working collaboratively on 5G requirements and are examining all options in capabilities. In the end, it may come down to multiple vendors all having a piece of the system.

NATO approached industry partners from all over the world for a plan for expanding 5G. These partners came to the working group, and they've made progress, Kahler reports. Other recent working group efforts have focused on cloud technology, he adds.

• • • — • —

To share or comment on this article
go to http://url.afcea.org/April22

contact: Robert K. Ackerman, signalnews@afcea.org

Automated Cyber Defense at Speed Is Manageable

XDR and MDR can shorten the time between attack and detection.

Extended detecton and response (XDR) offers crticial collective monitoring of identity management, intrusion sensors, firewall and cloud applications.

PopTika/Shutterstock

BY PAUL BECKMAN

In today's cyber environment, the attack surface grows exponentially day after day with no sign of slowing. With the near-geometric growth of applications, the signal-to-noise ratio has been amplified into the stratosphere. The result: The hunt for timely and important context in system and network telemetry is like trying to find a particular needle in a sea of needles.

Equally challenging is the "dwell time" of attacks—the period between initial penetration and the point of detection/eradication. In 2020, the average global dwell time was 56 days. That means that an attacker had nearly two months inside a network on average before being discovered.

Two excellent approaches to these challenges are extended detection and response (XDR) powered by artificial intelligence (AI) and managed detection and response (MDR). Both shorten dwell time by quickly detecting and responding to penetrations.

XDR is the next step beyond conventional endpoint detection and response (EDR). Nir Zuk, chief technology officer and co-founder of Palo Alto Networks, first coined the term "XDR" and introduced the concept. Today, he describes XDR as "the future of detection and response."

XDR adds collective monitoring of critical areas such as identity management, intrusion sensors, firewall and cloud applications and many more and ties all of it together. XDR ingests data from a myriad of security products and appropriately correlates the telemetry data intelligently, accurately and with automated response across all data types at speed.

The XDR AI engine looks for behaviors from all the telemetry data ingested throughout the network in real time and finds anomalous patterns of behavior that would otherwise go undetected. When the AI engine determines that something is a security risk, the response phase can automatically remediate the issue by responding to the relevant security devices, depending on the configured

Blue Planet Studio/Shutterstock

Dwell time can be significantly reduced by XDR and managed detection and response by quickly finding and responding to penetrations.

playbook. This can include blocking an IP address at the firewall, quarantining a user at the switch port or blocking a domain on the mail server to mitigate risk.

There is just one downside: XDR with AI doesn't necessarily come cheap.

One alternative is third-party MDR that leverages XDR's ability to integrate, automate and provide an enhanced threat-monitoring detection and response service at a reasonable price, which works 24/7 to significantly reduce cyber-attack dwell times.

The quality of an MDR service depends on its ability to incorporate extended detection and response visibility that includes network traffic analysis, visibility tools and analysis of security log data. Today, MDRs fall into three capability groups:

Base Level Services: This includes proactive threat hunting, investigation and response services.

Managed EDR Services: Here, the MDR provider is managing the EDR client and providing base-level services.

Advanced Services: These span incident response as a service as well as the deployment of traditional "boots on the ground" personnel to assist with incidents.

With the cyber risks at hand, the advanced approach is always the best because it provides insight into what's happening on a network that would otherwise be difficult or impossible to do manually. For organizations that don't have the manpower or expertise to take on XDR themselves, Managed service security providers that offer MDR are a smart solution.

• • • — • —

Paul Beckman is vice president and chief information security officer at ManTech.

ManTech is sponsoring AFCEA International's annual The Cyber Edge writing contest, open to thought leaders and subject matter experts in the military, government, academia and industry. This year's contest theme is" Emerging Technologies in the Cyber Realm." Three authors will win monetary prizes and will have their articles published in SIGNAL *Magazine. Top prize is $5,000; second prize is $2,000; and third prize is $1,000.*

To share or comment on this article go to http://url.afcea.org/April22

contact:
signalnews@afcea.org

Courtesy Photo, 1st Special Forces Group (Airborne)

MPE must support rapid decision making from the strategic to tactical level. At the cutting edge of coalition operations, a Green Beret with the U.S. Army's 1st Special Forces Group (Airborne) clears a room alongside Royal Thai Army soldiers during Cobra Gold 21.

Strengthening Alliances Is Critical for Tackling Shared Challenges

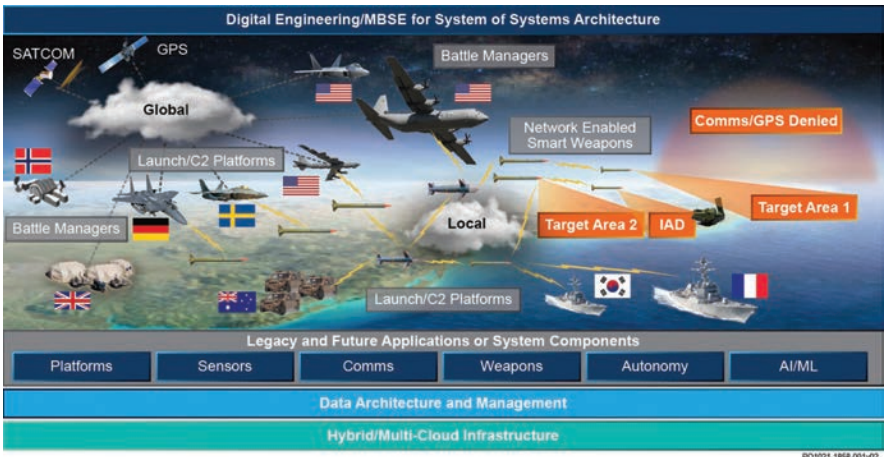
An enterprise-level mission partner environment is needed for JADC^2.

BY KIRK NILSSON

Today, more than ever, combatant commands, joint task forces, service components and supporting agencies need the mission partner environment to deliver the same capabilities envisioned for the U.S. Defense Department's Joint All-Domain Command and Control concept. With two near-peer competitors dominating the defense strategy, the need for an enterprise-level mission partner environment has never been greater for promoting security cooperation while maintaining military readiness. As Cliff Fegert, former director of the Mission Partner Capabilities Office noted, "With two near peers, we do not have the luxury of preparation time, and we must have allies/partners to deter or win."

In the Indo-Pacific area of tesponsibility, recent headlines only further highlight current and emerging threats to a free and open Indo-Pacific region. Advancements in hypersonic weapons, nuclear weapons technologies testing established treaties and regimes, and aggressive territorial posturing challenging international norms pose a greater threat to regional peace and stability. Strengthening alliances and partnerships into a capable, combined and joint all-domain force is critical for deterrence or decisive action across the spectrum of shared challenges.

Synchronizing the independent, if not disparate, efforts of the Defense Department, services, combatant commands and coalition partners to deliver a Joint All-Domain Command and Control (JADC^2)-capable mission partner environment (MPE) that is both effective at the speed of war and cost-efficient is challenging. It is also essential. The current practice of allowing combatant commands or service-centric solutions sets conditions for higher risk in any future near-peer fight. Some of the most significant challenges to achieving the future state of MPE (and JADC^2) include providing system of systems (SoS) interoperability across coalition and joint forces, ensuring enterprise-to-edge connectivity for global users and enabling data-centricity for accelerated decision



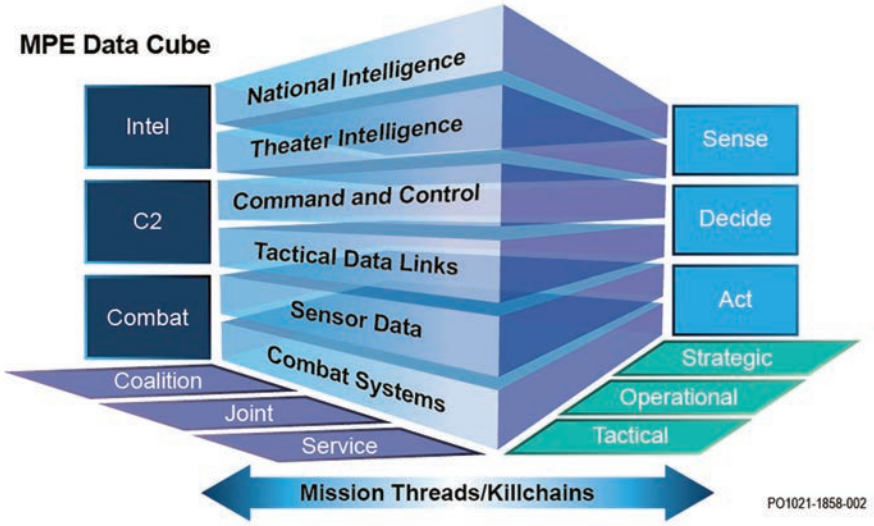
making. The solutions to these challenges must provide highly available, resilient and global access across multiple classification levels, with assumptions of denied, degraded, intermittent or limited bandwidth environments.

The Defense Department's JADC² strategy will facilitate better solutions to unlock the power of data, fundamental for any command and control (C²) modernization efforts. Yet stronger alignment and synchronization from strategic and operational levels are required to accelerate decision advantage for coalition warfighters. This is reflected at the strategic level with the recent establishment of the Defense Department chief digital and artificial intelligence (AI) officer, who is charged with leading efforts to improve data-centricity, AI and digital solutions across the Defense Department. This should also help drive service and combatant command-acquisition efforts toward joint interoperability standards and open architecture solutions needed to implement the JADC² and MPE reference designs, consistent with the Federated Mission Networking framework.

By design, the JADC² strategy captures the need for a compatible MPE with the inclusion of line of effort (LOE) 5, Modernize Mission Partner Information Sharing. Lt. Gen. Dennis Crall, USMC, director, Command, Control, Communications and Computers/Cyber, and chief information officer, Joint Staff, J-6, described the MPE aspect of the JADC² strategy as, "We are building in a mission partner environment as part of the organic conversation, not as an afterthought or a bolt-on later … We expect it to be a little more challenging, but we also know that we need it."

Ongoing service and combatant command efforts contribute significantly to JADC² and specific aspects of MPE. These include the Air Force Advanced Battle Management System, the Army's Project Convergence, the Navy's Project Overmatch and the Data-Centric Information Domain that is enabling the U.S. Central Command Partner Environment. However, these efforts tend to be discrete activities not fully synchronized under a centralized plan and indicative of the substantial risk to the future state of an MPE. The current distributed approach to building MPE capability outside a centralized Defense Department acquisition program provides great flexibility but dilutes direction and resource authority.

An option is to adopt campaign planning, the proven approach to keep complex, multifaceted efforts on track to achieve a strategy's future state objectives across combatant commands and services. JADC² and MPE would clearly benefit from the development of a functional campaign plan, potentially directed by the chairman of the Joint Chiefs of Staff, to translate strategic JADC² and MPE guidance into activities executable by the services and combatant commands. The Mission Partners Capabilities Office (MPCO), charged with executing the secretary of the Air Force's responsibilities as executive agent for the MPE, could coordinate the development of the campaign plan to organize, integrate, execute and assess significant MPE activities or capabilities supporting the JADC² strategy.



The MPCO is responsible for designing, implementing, operating and sustaining a Defense Department-wide enterprise-level capability that supports joint and multinational warfighting functional information-sharing requirements with mission partners. In addition, the MPCO evaluates, recommends

prioritization and incorporates requirements, capabilities and solutions for the integration and evolution of C² and intelligence information-sharing capabilities in a coalition environment.

The MPCO also serves as the office of primary responsibility of the JADC² strategy LOE 5 to reinforce synchronization of JADC², Federated Mission Networking and MPE efforts. The MPCO's material solution envisioned for MPE at strategic to operational levels is the secret and below releasable environment (SABRE). SABRE will federate combatant command or service component mission networks, such as the U.S. Central Command's Partner Environment that was demonstrated at Bold Quest 2021, and the U.S. Indo-Pacific's MPE, to be delivered through the joint warfighting network known as Indo-PACNET.

The MPCO is working to integrate and operationalize a prototype, SABRE v1.0, into a fully functional Defense Department zero-trust architecture cloud. SABRE will utilize identity, credential and access management and data labeling/tagging to achieve logical separation of data managed through enterprise-level data-centric security-based access controls. SABRE will also be the Defense Department cloud-based instantiation of a Federated Mission Networking-compliant MPE enterprise. The delivery of SABRE's initial operational capability is a key component of the future state MPE and will help synchronize MPE across the data, technical and human enterprise LOEs of JADC².

The MPCO is also charged with developing metrics and comparison benchmarks for overall MPE implementation and performance to determine specific areas for improvement. This role may be of equal, if not greater importance, than providing the operational SABRE.

The MPCO, as the implementing arm of the U.S. Air Force executive agent, should be fully resourced to develop and manage an MPE campaign plan. The plan would set the baseline and provide the road map for Defense Department agencies, services and combatant commands to organize, integrate, test, execute and assess MPE capabilities supporting the JADC² strategy. The plan should be resource-informed, similar to combatant command campaign plans, constrained by the availability of resources and authorities and future requirements based on ongoing operations and planned activities. Services and CCMDs should develop supporting plans, and any partner nation-specific MPE objectives could cross-walk into the country-specific security cooperation section of the associated combatant command campaign plan.

Photo by Petty Officer 2nd Class Arthur Rosen

MPE must support secure access and sharing of information across public, controlled unclassified and classified levels. Demonstrating critical coalition maritime capabilities, the U.S. Navy destroyer USS Benfold *conducts replenishment-at-sea with JS* Towada*, a replenishment ship of the Japanese Maritime Self-Defense Force in the Philippine Sea.*

The future state MPE will likely draw upon three foundational capabilities: 1) mission engineering, digital engineering and model-based systems engineering for SoS architecture; 2) data-centric architecture and data management; and 3) a hybrid/multicloud infrastructure. These should be LOEs as part of the MPE campaign plan and be included as requirements in future MPE acquisition efforts.

For the mission engineering LOE, the Defense Department's mission integration management construct and technical sub-element of mission engineering would help drive the MPE campaign plan to deliver end-to-end MPE services mission-based engineered outputs. Mission engineering considers mission threads, which define the execution sequence of how systems, people, data, methods, tactics, timing and interfaces interact to achieve mission objectives. The MPE campaign plan should include a mission engineering LOE to direct development, management and repositories of MPE mission threads to facilitate services and combatant commands efforts.

Synchronizing SoS across applicable national and international data standards, dozens of mission threads and hundreds of applications or services within or supporting the MPE ecosystem is exceptionally complex. Standardized implementation of digital engineering and model-based systems engineering practices, tools and processes mitigate the complexity and facilitate decision making. The mission engineering LOE should include digital engineering and model-based systems engineering objectives with clear standards and implementation milestones.

The data management LOE is critical to provide coalition warfighters with decision advantage against near-peer adversaries. It must guide

the rapid evolution of the MPE into a data-centric enterprise. Established within a federated global data fabric, the MPE data-centric enterprise must manage the volume, variety, velocity and variability of data from diverse and growing sources available to coalition warfighters. The desired outcome for a data-centric enterprise is for seamless data feeds to all relevant coalition mission applications in all security domains to support unified action.

The MPCO can accelerate a data-centric enterprise by leveraging the ongoing work of the services, combatant commands and industry. The data management LOE should provide specific objectives and milestones for how data is collected, tagged, secured, enriched, visualized, analyzed, automated and distributed to authorized MPE user workstations or mobile devices.

Key milestones of the data management LOE should include implementing identity, credential and access management, attribute-based access control and a zero-trust architecture, such as the Defense Information Systems Agency Thunderdome project. Data must be accessible from traditional local area networks and wide area networks, as well as mobile communication or radio access technologies like 5G.

User experience in the data-centric approach is also important to MPE users, and the applications and automations that support users need to improve dramatically. There must be a revolutionary shift in user experience supported by machine learning (ML) and AI to more effectively share with mission partners.

The cloud LOE should guide the adoption of the evolving global cloud capabilities needed to provide coalition forces with assured data in times of infrastructure degradation. Cloud integration will occur at enterprise, regional and tactical levels. The complexity of implementing high levels of utility, performance, security and resiliency across hybrid and multiple cloud environments poses significant challenges. Resource constraints dictate that MPE cloud efforts capitalize on current or near-term Defense Department/service cloud offerings and leverage best practices for enterprise and expeditionary use cases.

MPE cloud LOE should continue to leverage the Defense Department Cloud Strategy, Defense Department Outside the Continental United States (OCONUS) Cloud Strategy and Joint Warfighting Cloud Capability objectives. It also must establish specific policy objectives and milestones for the MPE cloud to support information sharing with coalition partners. These objectives would provide the road map for how the enterprise will federate and control hybrid/multicloud approaches across multiple security domains, with access to any network or global infrastructure for the data needed to meet mission requirements.

The 2018 National Defense Strategy states, "We will strengthen and evolve our alliances and partnerships into an extended network capable of deterring or decisively acting to meet the shared challenges of our time." In the four years since, this objective remains a work in progress. While the Defense Department has undertaken unparalleled efforts to implement JADC^2 and MPE, these are complex, transformational endeavors requiring continued leadership by all MPE stakeholders. The department will not rapidly deliver a JADC^2-capable MPE with an ad hoc approach. The U.S. Air Force/Mission Partner Capabilities Office, empowered by the chairman of the Joint Chiefs of Staff and Joint Staff and in support of the other services and combatant commands, should develop an MPE campaign plan to guide resourcing and implementation decisions.

Finally, the Defense Department cannot achieve this MPE transformation alone. Collaboration with mission, coalition, industry and academic partners is critical to implement best practices and resolve the challenges faced by coalition warfighters as they defend nations every day.

• • • — • —

Kirk Nilsson is a senior programs director for the Army and Missile Defense unit of the Integrated Defense Solutions business area within the Intelligence & Security sector of BAE Systems and a retired U.S. Army Special Forces colonel with over 30 years of service and extensive experience working with allied, coalition and partner nation forces during military operations and security cooperation activities.

To share or comment on this article go to http://url.afcea.org/April22

contact:
signalnews@afcea.org