2021-12-21

Mosaic Warfare Networks Can Serve Naval Expeditionary Forces

Jasper, Scott; Hollingshead, Travis

AFCEA

Scott Jasper and Travis Hollingshead, "Mosaic Warfare Networks Can Serve Naval Expeditionary Forces", SIGNAL Magazine, 1 January 2022.
https://hdl.handle.net/10945/68622

Marine Corps Tactical Systems Support Activity trains Marines on networking on-the-move. Th
Sky Laron, Marine Corps Systems Command Lan

Mosaic Warfare Networks Can Serve Naval Expeditionary Forces

THE CYBER EDGE

January 1, 2022

By Dr. Scott Jasper and Master Sgt. Travis Hollingshead, USMC

Preserving the information advantage poses a significant challenge.

A new concept is necessary to maneuver forces, potentially with small and scalable autonomous organizations operating independently of one another. The concept, called Expeditionary Advanced Base Operations, is being explored and instituted for Naval Expeditionary Forces to fight in this manner. The challenge is in defending expeditionary networks in a mosaic warfare distribution to avoid the big problem of information advantage loss faced in a recent wargame.

CYBER ALERTS

- AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities
- AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus
- AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

A wargame of the new Joint Warfighting Concept last October witnessed U.S. forces losing access to digital networks almost immediately. Right from the beginning of the conflict, ubiquitous information was not available as it had been for the past 30 years. A brutal loss to an aggressive red team convinced Gen. John Hyten, USAF, vice chairman of the Joint Chiefs, to scrap foundational concepts that have guided the military. Gen. Hyten explained that "with significant long-range fires coming at us from all domains, if you're aggregated and everybody knows where you are, you're vulnerable."

When Gen. David H. Berger, USMC, commandant of the U.S. Marine Corps, disseminated the Force Design 2030 directive in March 2020, his vision depicted a significant change in how naval expeditionary forces will operate in the future. Marine units are shifting focus from the counterterrorism fight to renewed power competition, where Marines are expected to enable maritime competition and deterrence, including by detection of adversarial aggression. A central part of this shift in supporting the National Defense Strategy is operating in contested environments with organic mobility and dispersion. Stand-in forces will persist inside an adversary's threat range and facilitate a larger naval campaign. According to Force Design 2030, they will generate "technically disruptive, tactical stand-in engagements" with low signature platforms and payloads to "confront aggressor naval forces." To achieve this revolutionary vision, Marines are experimenting with the Expeditionary Advanced Base Operations (EABO) concept through the creation of Expeditionary Advanced Bases (EABs) for small groups of Marines to distribute and engage a competitor seeking to counter U.S. forces.

EABO includes what Gen. Berger refers to as "sweeping changes" in Marine Corps tactics by adding advanced sensors and various automated and autonomous armed platforms. These capabilities will integrate targeting data between sensors paired with lethal capabilities or single-mission platforms operating in networked swarms with complementary capabilities. The growing number of digital communications and networked devices depicts a need for organic cybersecurity competencies for managing and defending critical systems. However, the current manning structure of the new Marine Littoral Regiment (MLR) does not include significant cybersecurity expertise. Meanwhile, testing of EABO capabilities is already underway, such as the firing of a new anti-ship missile system during the Navy's Large-Scale Exercise 2021. The acceleration of numerous capabilities and foundational doctrine outlined in the **Annual Update to Force Design 2030** shows the need for naval expeditionary forces to defend their mosaic warfare networks against emerging cyber threats while operating in contested environments.

The Defense Advanced Research Projects Agency concept of mosaic warfare combines functional characteristics of different platforms, like ceramic tiles in mosaics, to make a larger force package. Small and scalable systems dynamically source effects from across an array of options based on shifting mission demands. Mosaic warfare enables a new form of maneuver by connecting unmanned systems with existing or emerging capabilities in creative and evolving combinations. Marine Corps stand-in forces will be able to converge these capabilities from multiple domains to create what Gen. Berger testified to Congress this year as "the virtues of mass without concentration." His envisioned capabilities include anti-ship Naval Strike Missiles fired from the unmanned Remotely Operated Ground Unit for Expeditionary Fires; the mobile Light Amphibious Warship; and long-loiter aerial reconnaissance by medium-altitude, long-endurance Group 5 unmanned aerial systems (UAS). The MLRs will be networked with existing F-35 capabilities and, in the future, with advanced munitions and an array of unmanned systems to enhance deterrence.

These platforms and payloads will provide Marines with dependable and expendable mosaic systems available for integration or independent deployment. The connection of autonomous platforms through digital means will support the fast-moving and flexible aggregation of capabilities. While the flexibility of these connections allows for the rapid dissemination of data and communications across multiple systems, it also provides a potential strategic vulnerability. Ensuring systems are fortified against bad actors requires diligence. Mosaic operational principles could be applied to defend networked EABO capabilities within the cyber domain. The pioneering thinker on the topic, Lt. Gen. David A. Deptula, USAF (Ret.), heralds mosaic warfare as a way of war that "leverages the power of information networks, advanced processing and disaggregated functionality."

The operational necessity for connecting capabilities in austere environments will require a sophisticated network architecture to consolidate and integrate (such as the F-35 or various UAS platforms), which also provide opportunities for adversaries to target. Connections through short- or long-range radio frequency (RF) transmissions require direct connections for operational

synchronization, which introduces additional risk to mission execution. Based on the dynamic nature of military operations, RF-enabled connections are necessary for integrating the various systems and ensuring adequate command and control. Long-range RF connections such as satellite communications (SATCOM) relays enable the dissemination of data across extensive areas but require large and expensive equipment, which may be difficult to use with mobile systems such as UAS platforms.

SATCOM relays may not necessarily meet the bandwidth and throughput levels necessary for system interoperability. 5G telecommunication towers provide adequate throughput/bandwidth and can be designed small enough for use at the squad level, but may prove challenging to achieve the level of interoperability desired based on limited range (approximately 1500 feet) due to use of millimeter wave signals. Similar issues arise with 802.11 Wireless Access Points and Bluetooth connections as both accompany limitations with security, bandwidth, throughput and range. Expeditionary networks desired require authentication, encryption and frequent transmissions to ensure kill chain fluidity. Establishing these connections launches networked systems operating as mosaic tiles toward an intended purpose or mission.

Options for ubiquitous connectivity are developed daily through existing and emerging technology. While deploying forces to foreign locations, connecting to local communication backbone networks is an option if adequate security and throughput are available. Even so, these types of connections are unlikely to be available for operations in austere environments such as underdeveloped regions or hazardous areas.

Establishing digital networks that remain disconnected from conventional connections are necessary for EAB use. One method for implementation is the F-35, where its digital capabilities create similar expeditionary digital networks that may be leveraged to coordinate actions across multiple ground or air platforms. Separately, 5G mobile connections are part of the EABO experimentation occurring at Marine Corps Air Station Miramar for integration at the squad level. Both connectivity mechanisms will enable the fluidity for dynamic connections based on mission needs and operational requirements. But further development and testing of these two types of digital connections require additional evaluation and field testing during operational use. Regardless of the connection mechanism, the EABO digital connections require decentralized management of integrated systems to enable the type of autonomy desired. However, these interconnections create key cyber terrain and potential vulnerabilities through ubiquitous connections, presenting significant risk without adequate cybersecurity mechanisms in place.

Based on Marine Corps Doctrinal Publication **1-4 Competing**, released in December 2020, Marines will leverage Defensive Cyberspace Operations to counter adversary encroachments and attacks in the cyber domain. This is intended to “name and shame” adversarial actions attributed to a suspected organization. However, the isolated networks used in EABO must not be investigated independently. Cloud-based analytics for enterprise-wide analysis of malicious activities, telemetry data and indicators of compromise targeting EABO networks could be utilized to consolidate and evaluate intrusion events. If the EABs included a cybersecurity system such as a Security Information and Event Management (SIEM), intrusion investigations could be automated to enhance the effectiveness of their defense. System log consolidation with analytic display generated through a SIEM for exporting suspicious activity to a cloud-based storage mechanism would allow for a broad view of malicious activity across multiple dynamically networked devices. But these logs would be limited to only those capabilities with connectivity to the EAB, and the SIEM will enable only consolidated analytics without any threat enrichment data. Although this capability would enhance the ability of a local information technology (IT) specialist, it would require constant attention and a more than novel level of cyber expertise to be effective.

Enabling broad-range analysis of malicious activity through the use of preconfigured logic, artificial intelligence (AI) and machine learning (ML) may assist in protecting critical systems from nation-state-sponsored cyber actors. Including a security orchestration, automation and response (SOAR) platform as an enterprise-level analytic consolidating all expeditionary network event data would enhance localized threat analysis, automate the response to the intrusion and minimize the onsite cybersecurity resource requirement. Enriching SIEM data with threat intelligence automating response options for immediate action against malicious activity provides a customizable defense measure that can be modified based on observations of global nefarious cyber activity. These options may be configured for automated human-in-the-loop actions (a prompt to notify the IT specialist an action is recommended), human-out-of-the-loop actions (preconfigured logic executes

a response action on behalf of the IT specialist) and notifications of activity (occurring within a defended network).

The integration of ubiquitously connecting capabilities as tiles in a mosaic empowers small and scalable platforms for expeditionary missions in contested environments. Even so, these interconnected systems create systemic vulnerabilities by the nature of their connectivity. Not only does this provide potential opportunities for a cyber actor to access EAB systems, but it also may enable adversaries to counter Naval Expeditionary Force operations. The need for a cyber defense strategy that incorporates layered and automated security modules supporting resistant and resilient cyber infrastructure must be considered a priority. The current methods for protecting similar networks may not be adequate for defending from future cyber threats by adversaries operating within the same contested environments as the naval expeditionary forces of the future.

Through the application of the mosaic warfare concept, EAB digital networks can become a force multiplier for aggregating capabilities within a dynamically changing target environment. The interconnectivity and adaptability of EAB networks when applying the mosaic warfare concept provides the Marines with capability resiliency and reliability. In the event that one tile is compromised, other tiles are able to support the mission through the networked connectivity used for command and control. Further enhancements concerning the effectiveness of this interconnectivity will occur through the use of automated capabilities.

While the use of AI and ML within military networks is a promising concept, secondary and tertiary effects of their integration remain clouded by uncertainty. The integration of both capabilities into tactical and strategic level networks is necessary for quickly processing the large amounts of data collected through various advanced sensors while making operationally relevant recommendations to the appropriate decision makers. Though this is an appropriate desired end state for future military networks, Marines will need opportunities to gain familiarity with their functionality before adequate trust can be established and maintained. Meanwhile, other forms of automation can augment EAB digital networks through offensive and defensive options. Not only does this enhance the effectiveness of cyber operations from within the EAB, but it also maximizes the operational opportunity for Marines in a fluid and shifting environment.

Dr. Scott Jasper is a senior lecturer in the National Security Affairs Department at the Naval Postgraduate School and the author of Russian Cyber Operations: Coding the Boundaries of Conflict by Georgetown University Press.

Master Sgt. Travis Hollingshead, USMC, is an active-duty cyberspace chief (1799 MOS), a recipient of the 2020 AFCEA Copernicus Award, and a current applied cyberspace operations student at the Naval Postgraduate School in Monterey, California.

Departments: Cyber

RELATED CONTENT:

The Cyber Edge autonomous systems cyber

Share Your Thoughts:

Your name

E-mail

The content of this field is kept private and will not be shown publicly.

Comment *

- No HTML tags allowed.
- Web page addresses and e-mail addresses turn into links automatically.
- Lines and paragraphs break automatically.

More information about text formats

Notify me when new comments are posted

All comments Replies to my comment

I'm not a robot

reCAPTCHA
Privacy - Terms

Save

Select Language