BREAKING DEFENSE

In Focus:

Electronic Warfare and Sensors

UNDERWRITTEN BY

NORTHROP GRUMMAN


Joining forces to
change the future
of what's possible.
NG
NORTHROP GRUMMAN
ngc.com

Editor's Letter

BREAKING DEFENSE

Stop pretty much anyone at the Pentagon, and they'll be quick to tell you that the nature of warfare has changed in the last decade. Bombs, planes and tanks will always matter, of course, but it's the sensors, waveforms and code behind it all that will differentiate a well-armed force from a truly elite military.

When Breaking Defense launched this package, the idea was to tackle that complicated subject largely from an American perspective — but then Russia invaded Ukraine and the real world intervened. You'll see the topic of Russia's electronic warfare capabilities scattered throughout this collection, as analysts and Defense Department officials alike worked to study the use of EW on the modern battlefield in real time, including why the expected onslaught of Russian EW simply never seemed to materialize in Ukraine.

This collection is hardly the definitive word on sensors and EW capabilities in the Pentagon, but it will give you a sample of key issues that crossed the desks of service leadership from the first half of 2022. As always, you can check back at BreakingDefense.com for more on the topic — and everything else going on in the world of defense.

Aaron Mehta

Editor in Chief

Electronic Warfare and Sensors Table of Contents

BREAKING DEFENSE

Army progresses on electronic warfare revamp

Army systems to give soldiers EW and cyber options on the battlefield are inching towards reality.

Terrestrial Layer System-Brigade Combat Team design tenets are expeditionary to support the maneuver commander with electronic attack and offensive cyber warfare options to deny, degrade, disrupt, or manipulate enemy signals of interest and the targeted force. (Courtesy Photo Illustration via DVIDS)

By ANDREW EVERSDEN on April 25, 2022 at 8:03 AM

WASHINGTON: The US Army's electronic warfare portfolio is maturing with critical electronic warfare capabilities scheduled for fielding or prototyping in the next year.

The service is in the midst of a multi-year effort to rebuild its EW capabilities, after largely not investing in those platforms since the end of the Cold War. Through several new platforms, soldiers at the brigade level and higher will receive systems that will enable them to do electronic sensing and attack, as well as give commanders a better understanding of the electronic environment on the battlefield.

Closest to fielding is the Army's Electronic Warfare Planning and Management Tool (EWPMT), designed to allow a commander to better understand and visualize the electromagnetic spectrum on the battlefield during an operation. That should, in theory, lead to better planning choices and decisions on which EW system to apply to any given situation.

Ken Strayer, program manager for electronic warfare and cyber at Program Executive Office Intelligence, Electronic Warfare and Sensors, said that EWPMT is expected to request a full-deployment decision at the end of the current fiscal year with initial fielding scheduled for FY23. The initial plan is to upgrade units with earlier versions of EWPMT to the full kit.

"Up until EWPMT, we had no way to really understand and visualize the spectrum, whether that is the current environment from the commercial activity that's out, or our blue friendly communications and red enemy communications," Strayer told Breaking Defense. "Now a commander will be able to understand the environment and he'll be able to do mission planning so that when he's planning an operation he can understand how the spectrum and the terrain will be able able to impact his ability to that operation."

Strayer said that EWPMT will be used by brigades or higher formations initially, but noted that the requirements keep expanding. As the program moves forward, EWPMT will add new capabilities such as connecting to new sensors, completing new modeling and analysis, or add the ability to understand different parts of the electronic environment, Strayer said.

"[There's] a lot of demand for the capability out there— it's only growing," Strayer said.

Terrestrial Layer System

The Army is also working on a pair of systems called the Terrestrial Layer Systems that will deliver integrated electronic warfare and cyber capabilities to soldiers on the battlefield.

The TLS-Brigade Combat Team program will give soldiers integrated electronic warfare, cyber, and signals intelligence capabilities at the brigade level. The program is looking to integrate the platform onto Strykers, Armored Multi-Purpose Vehicles and, eventually, for infantry brigade combat teams.

Strayer said the program office is set to receive two of the early AMPVs as they come off the assembly line for testing.

In September, the Army chose Lockheed Martin to move forward with the Stryker configuration over Digital Receiver Technology, a Boeing subsidiary. The program office has a planned operational assessment in late FY23 that will provide data on the program's readiness to transition to production and fielding. For infantry brigades, the office is deciding whether soldiers need a vehicle-mounted system or a man-packable one.

"There's force structure growth. The Army is investing in new electronic warfare soldiers and they're heading out to the field. They need their equipment," Strayer said. (Notably, the layer system will include EWPMT on board.)

PEO IEW&S is also developing another electronic warfare system for Army formations larger than a brigade through a program called TLS-Echelons Above Brigade. That program has just started to get off the ground because the lapse in approved appropriations prevented new programs from beginning.

As the Army shifts back to divisions as the unit of action after decades of operating primarily at the brigade level, EW capabilities will be needed by higher-level formations such as divisions, corps or theater armies, as well as the service's multi-domain task force, which will need longer-range EW capabilities.

"You're talking about much longer ranges, different type of threat targets that we need to be able to sense and effect," Strayer said.

He said the program is in its "first phase," which will include concept development and initial design. That includes defining what the requirements are at each echelon and establishing the best technical approaches. Overall timelines for the program aren't clear yet, Strayer said.

"Depending on what our two competitive offers propose and what the Army decides they actually want to go out and prototype, [that] will drive the timelines," Strayers said, adding that testing will start in a few years.

As for the kit each echelon will receive, Strayer expects it's likely that different formations above brigade will receive different capabilities, but would likely have a "shared common core" with different sensors and effectors.

"There's some advantages in having one configuration for all in terms of cost of production, but we're learning that the specific targets and the ranges are different and that's going to necessitate that we have some different technologies onboard to get at the problem," Strayer said.

According to Strayer, the office is "very close" to awarding prototype agreements.

SpaceX beating Russian jamming attack was 'eyewatering': DoD official

"The way that Starlink was able to upgrade when a threat showed up, we need to be able to have that ability," said Dave Tremper, the Pentagon's director of electronic warfare. "We have to be able to change our electromagnetic posture, to be able to change very dynamically what we're trying to do without losing capability along the way."

A Ukrainian serviceman patrols on March 3, 2022 in Sytniaky, Ukraine, west of the capital. (Anastasia Vlasova/Getty Images)

By VALERIE INSINNA on April 20, 2022 at 4:29 PM

WASHINGTON: The US military's electronic warfare enterprise needs to take a page from SpaceX when it comes to responding to new threats, the Pentagon's director for electromagnetic warfare said today.

After SpaceX sent Starlink terminals to Ukraine in February in an apparent effort to help Ukraine maintain its internet connection amid war with Russia, SpaceX founder Elon Musk claimed that Russia had jammed Starlink terminals in the country for hours at a time. After a software update, Starlink was operating normally, said Musk, who added on March 25 that the constellation had "resisted all hacking & jamming attempts" in Ukraine.

Assuming Musk — famously something of a showboater in his public comments — is providing an accurate picture, a private firm beating back Russian EW attempts with software updates is the kind of thing that makes Pentagon EW experts pay attention.

"From an EW technologist perspective, that is fantastic. That paradigm and how they did that is kind of eyewatering to me," said Dave Tremper, director of electronic warfare for the Pentagon's acquisition office. "The way that Starlink was able to upgrade when a threat showed up, we need to be able to have that ability. We have to be able to change our electromagnetic posture, to be able to change very dynamically what we're trying to do without losing capability along the way."

Since Russia's takeover of the Ukrainian territory of Crimea in 2014, the Russian military has used electronic warfare extensively in Ukraine's Donbas region — often to great effect, using electromagnetic signals to uncover the positions of Ukrainian forces and disrupt equipment such as drones. However, the current conflict may be exposing the limits of Russia's EW capability.

Tremper noted that Russia' ongoing invasion deep into Ukraine is "a very different scenario" to earlier operations that were mostly contained on the border between Russia and contested regions of Ukraine.

"[When] you're trying to get to the center of that country, I think EW coordination and synchronization become very challenging. To get into those urban scenarios becomes even more complicated," he said. "And I think, what we're seeing in the Ukraine is a resistance, where the dependence on [the electromagnetic spectrum] isn't there."

Another challenge for the Russian military has been a lack of training and expertise — a failing that has been made painfully obvious even outside the realm of electronic warfare, with major embarrassments such as the sinking of the Russian warship Moskva, the Russian air force's inability to achieve air superiority against an adversary with far fewer combat aircraft, and continued logistics failures that have resulted in memes featuring Ukrainian farmers driving away with Russian tanks.

"I think we expected a much stronger EW presence," Tremper said. "Which isn't to say that it's not there, but I think the degree of coordination and synchronization of these types of operations is such that the undertrained operator will have a hard time pulling off those types of events successfully."

Brig. Gen. Tad Clark, the Air Force's director of electromagnetic spectrum superiority, prefaced his statements by acknowledging that he couldn't detail specifics about what the United States is gleaning about the Russian electronic warfare threat based on its activities in Ukraine.

However, he noted that those activities do more than simply provide information about Russia's technological capabilities — they also paint a picture about whether Russia has the capital necessary to execute that mission.

"We're learning a lot what Russia has been investing their money in, the sophistication and the reliability of their equipment, and.. their ability to execute that mission in a synchronized fashion," he said. "It gives us some insight of where certain countries are, where we are, where we need to be, and where we want to be."

Multi-domain operations demand multifunction sensors

presented by NORTHROP GRUMMAN

Emerging threats and complex challenges to situational awareness require a next generation of sensor systems.

Northrop Grumman's Digital Shadow, a virtual mission systems integration lab, provides the ability to correlate digital sensor representations with their physical design. Photo courtesy of Northrop Grumman.

By BREAKING DEFENSE on May 09, 2022 at 9:52 AM

With the Great Power competition, the threat against the US and its partners has moved to an extremely sophisticated stage where the US will meet near-peer challenges in numerous areas: long-range missiles, anti-access and area denial, remote targeting, command and control (C2), electronic warfare (EW), and cyber, to name several.

"Staying one step ahead on the battlefield calls for innovation in how our platforms and systems are developed, built, and acquired," said Roshan Roeder, vice president and general manager of the Airborne Multifunction Sensors division at Northrop Grumman Mission Systems. "Instead of the long design-build-prototype-test cycle that we've used in the past, we are realizing digital capabilities to validate designs prior to hardware builds, and we are implementing product lines based on broadband multifunction building blocks to accelerate our overall deliveries to the warfighter."

"To quickly and collectively observe, orient, decide and act (OODA) to address advanced threats, spectral agility and the use of multifunction sensors is the way of the future and a necessity. Using integrated capabilities across the overall electromagnetic spectrum decreases the adversary's ability to deny operations and enhances the reliability and timeliness of situational awareness. This type of multifunction capability allows our systems to leverage adaptive methods and AI to respond to the changing warfighting environment in ways never seen before."

Roles for multifunction sensors for EW, targeting, and C2

What is a multifunction sensor and how does it fit into the future battlespace and threat environment described above?

A multifunction sensor is an integrated system that consolidates multiple capabilities across the radio frequency (RF) spectrum – including communications, radar, electronic warfare, and intelligence, surveillance and reconnaissance (ISR) – into a single sensor.

This differs from multispectral sensors where two or more physically different systems, each sensing in its particular part of the spectrum, produce data that is fused together to create a more accurate picture of the target. Think of a multifunction sensor like a smartphone with multiple functions such as voice, text, camera, and navigation; the multifunction sensor includes many functions to satisfy different users and the data products must be highly reliable and secure.

"Depending on the requirement, we can provide higher-power multifunction sensors for larger platforms and different multifunction sensors with lesser size, weight, and power demands that are more appropriate for smaller, autonomous capabilities," explained Roeder. "To be more agile and innovative, we've built our multifunction sensors on a set of building blocks that are all sensors, which reduces the number of apertures and power needed for individual sensors."

"In addition, through the use of open-system architecture and software-defined networking we're able to easily adapt sensors to specific multi-mission needs and create actionable data at the speed of relevance to the services."

Multifunction sensors are especially suited to support future Joint All Domain Command and Control (JADC2) and multi-domain operations (MDO) to connect all five warfighting domains. That's because multiple sensors operating across multiple frequencies give commanders a higher confidence set of actionable data that can improve both targeting and the OODA loop for precision fires. This is needed for the DoD to enact its Joint Warfighting Concept that is founded on the ability to gain and maintain decision dominance.

"The beauty of a multifunction sensor is that it is a single system to do radar sensing, electronic warfare, and communications — all of the capabilities that are needed for decision dominance," said Roeder, adding that these sensors can have both passive and active capabilities in one system. Similar to the different apps on your cell phone, a multifunction sensor provides the information to support a variety of missions by giving responders a centralized set of information for better situational awareness.

Taking it one step further, there can be two, three or more multifunction sensors with those types of capabilities spread out across the threat environment. This would provide what Roeder calls "unprecedented situational awareness" for command and control in a multi-domain environment.

A new multifunction sensor to defeat complex, emerging threats

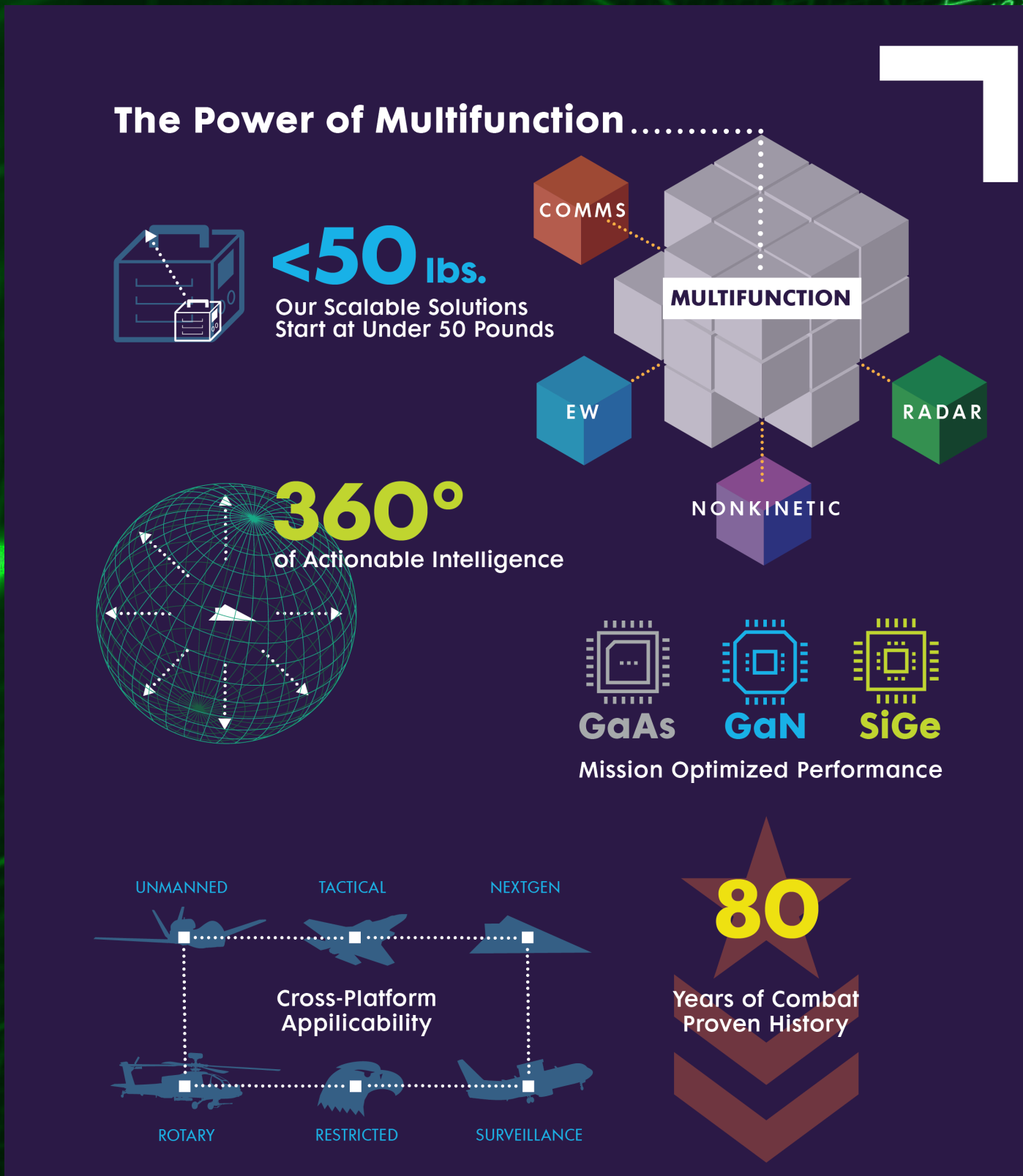
In mid-2021, Northrop Grumman Corporation delivered one of the most advanced multifunction sensors ever developed to the Air Force Research Laboratory (AFRL) and Defense Advanced Research Projects Agency (DARPA) for testing. Called the Arrays at Commercial Timescales-Integration and Validation (ACT-IV) system, it is based on an advanced multifunction digital active electronically scanned array (AESA).

The company calls the ACT-IV system a breakthrough in AESA performance and marks an important milestone in the nation's transition to digitally reprogrammable, multifunction radio frequency (RF) systems. ACT-IV is one of the first multifunction systems based on a digital AESA using the semiconductor devices developed by the DARPA Arrays at Commercial Timescales program.

"The details of ACT are exciting, though the benefits are what is important," said Roshan. "ACT technology enables agile multifunction systems, and our use of common ACT-based building blocks, supports rapid deployment of new capabilities to the warfighter."

These new apertures are based on common building blocks with RF energy on one side and digital data over fiber on the other side. Digital building blocks allow the aperture to instantaneously transform from an AESA Radar, to a passive ESM receiver, to a datalink, to a "SIGINT" machine.

An array of multiple software defined apertures can provide all of these capabilities at a large scale or simultaneously at the building block or groups of building block levels. This has a massive effect on platform size, weight, and power (SWAP) reduction, simplified logistics, and overall cost of ownership for the warfighters, equippers, and acquirers. Northrop Grumman is using these building blocks to develop product lines across the full RF spectrum to support a wide range of platforms on land, sea and air.



A multifunction sensor provides multiple capabilities and can seamlessly adapt to mission needs. Image courtesy of Northrop Grumman.

Designing multifunction sensors with digital engineering in open architectures

One of the key concepts of multifunction sensors is that they are digitally engineered for an open architecture environment that facilitates the building block nature of multifunction sensor development. This makes it easier to share data between different sensors and enhance the sensor's capabilities over time with new products and even another company's product because of its open system.

"Open architecture is the premise upon which we're building our developmental efforts," said Roeder. "Our architecture lets us take some of our best-of-breed products and enhance them with third-party processing, functional modes/waveforms, and networking capabilities to eliminate any concerns around vendor lock. That enables us to create a sensor, maybe beyond the means of what the requirements are now, utilizing third-party capabilities to enable different functions on that multifunction sensor."

Backing up these words, is a "Capability Development Kit," or CDK, that is already in place along with training sessions for third parties.
Building-block construction and open architecture break vendor lock, and are cost-effective ways to build economies of scale and reduce the cost for product design, development, and production. In that vein, Northrop Grumman has also devoted resources to understanding what drives cost in the supply base and focused its digital transformation on helping third parties synthesize the engineering lifecycle aspects of multifunction sensors, according to Roeder.

Key to the company's efforts in that respect is digital engineering. "Our deep understanding of the mission environment and threats allows us to take that experience and accurately model and analyze numerous, complex scenarios in the electromagnetic spectrum," said Roeder. "Our customers are sharing more and more information about their needs so we're able to run as many as 100,000 tests per night to validate changes in our system, predicated on real information and real data. It helps us enable the mission suite, optimize performance for the warfighter, and understand the technical performance that's needed to meet our customers' timelines and cost requirements."

Me and my (digital) shadow

To assist in the work of rapid iteration and assessment of multiple configurations of mission systems such as multifunction sensors and radar systems for fighter aircraft, Northrop Grumman has developed what it calls its "Digital Shadow" testbed, also known as a digital twin. This is a digital replica of its flying experimental aircraft testbed airframe and subsystems.

"The digital twin will serve as a multi-spectral integration platform to allow us to simulate current and future capabilities on the aircraft, and select that virtual test performance so we can correlate predicted sensor performance to actual performance," explained Roeder. "That further increases the fidelity and credibility of those digital representations. Using our Digital Shadow testbed is an iterative transformation for us."

The digital testbed, which is a virtual mission systems integration lab, provides the ability to correlate digital sensor representations with their physical design, further validating system and performance models and leveraging Northrop Grumman's large repository of collected data.

By creating a digital version of the aircraft and the onboard mission-system suites, the company can virtually configure, integrate, and fly scenarios and sensor combinations beyond the physical testbed limitations, increasing the breadth and scale of experimentation — reducing timeline and flight test costs, and ultimately extending mission capabilities for the warfighter to stay ahead of evolving threats.

"The digital environment lets us explore the huge test and performance space created by a multifunction system performing many functions on many threats across many frequencies and on many different platforms," said Roeder. "A digital system can traverse many more tests in a shorter amount of time than would be humanly possible in a flight. So these digital twins are a necessary part of the multifunction, multi-domain infrastructure of our future fighting forces."

Much like the cell phone has evolved to meet customer expectations, multi-domain operations are demanding an evolution in sensors in order to maintain spectrum superiority. Multifunction sensors can adapt to the mission need and scenario and dynamically support ISR, targeting, communications, electronic warfare and C2 requirements in a seamlessly integrated way. This will be necessary in defeating emerging threats in the complex and increasingly agile threat environment of MDO.

Army's Gray Eagle jamming pod program could expand to other aircraft

"Expanding the full deployment of MFEW and where it's going to end up long term, those are questions we're having within within the Army," an Army official told Breaking Defense.

The MFEW-AL system's purpose and ability is to create a clear picture, in real time, of the EMS in any given area it is flying over. (John Higgins/US Army)

By ANDREW EVERSDEN on April 18, 2022 at 8:50 AM

WASHINGTON: The US Army is updating the requirements for its Multi-Function Electronic Warfare-Air Large (MFEW-AL) program, as the service builds forces for multi-domain operations and pivots to operate in the vast distances of the Pacific.

The MQ-1C Gray Eagle-mounted jamming pod is expected to be an integral part of the Army's future electronic warfare arsenal, which it is trying to rebuild after deprioritizing EW after the Cold War. The Army zeroed out procurement funding in its fiscal 2022 budget request for the jammer, but it could be on track for a production decision later this year.

"There's a requirements update in the works based on what we've learned in terms of how the technology works, and what the right performance is," said Ken Strayer, program manager electronic warfare and cyber at PEO Intelligence, Electronic Warfare and Sensors. "Expanding the full deployment of MFEW and where it's going to end up long term, those are questions we're having within the Army."

The MFEW-Air Large pod, made by Lockheed Martin, is designed to provide brigade combat teams with offensive electronic warfare capabilities. Its original intent was for use by the service's combat aviation brigades, but as the service shifts to the Pacific, MFEW may meet new needs.

"With this concept of MDO, we're learning that MFEW does have an extended range and it can sense and effect in ranges that we believe are effective," Strayer said. "But we lack really the operational test data that proves that out."

Strayer said that the Army has tested MFEW-AL on other airborne platforms besides the Gray Eagle, but declined to go into specifics.

"We're proving out that it's really platform agnostic, as long as the platform can support the power and weight," Strayer said. "We have an opportunity to deploy it in a number of different configurations to get the right line of sight that you need to do the mission you need to do."

The Army cut $12.3 million in production funding for the program last year. In this year's budget request, Strayer said that the platform did receive money back to begin initial production. Strayer didn't provide a specific number, and the Pentagon has yet to release its justification books that detail what each program is asking for.

He said the budget will include funding to begin production capabilities, including long-lead time components and getting contracts in place. Strayer said that the limited user test is scheduled for early FY23; after the limited user test, the Army should have the data it needs to make a production decision.

The MFEW program experienced some delays due to the continuing resolution, he said, but with its authorized research, development, test and evaluation funds, the program office will be able to complete its development testing later this year. He said soldiers will test MFEW on Army ranges against "specific targets and specific ranges that have been called out in the requirement, as well as operational requirements."

The limited user test will include Army test and evaluation command, in addition to the Defense Department's director of operational test and evaluation. That will include "full operational threads" of the MFEW pod supporting a brigade.

"Their position has always been wait and see, we need to prove operationally that it's the right capability," Strayer said. "It's a big investment so this is the year that we need to prove it."

Electronic warfare and drone swarms: Here's the Army's plan for EDGE 22

"We'll basically be scrimmaging with our partners and allies," Maj. Gen. Walter Rugen.

An Area-I Air-Launched, Tube-Integrated, Unmanned System, or ALTIUS, is launched from a UH-60 Black Hawk at Yuma Proving Ground, Ariz., March 4 where the U.S. Army Combat Capabilities Development Command Aviation & Missile Center led a demonstration that highlighted the forward air launch of the ALTIUS. (Courtesy photo provided by Yuma Proving Ground)

By ANDREW EVERSDEN on April 11, 2022 at 7:45 AM

NASHVILLE, Tenn.: The US Army will be "working heavily" with electronic warfare and experimenting with large drone swarms as part of an upcoming sensor-to-shooter experiment in the Utah desert, according to a senior Army aviation official.

The US Army plans to include seven international allies for its second Experimental Demonstration Gateway Exercise that begins at the end of the month.

"We'll basically be scrimmaging with our partners and allies," Maj. Gen. Walter Rugen, director of the Future Vertical Lift Cross-Functional Team, said during his presentation at the Army Aviation Association of America conference in Nashville, Tenn.

EDGE is a risk reduction event ahead of Project Convergence, the Army's annual experiment in Arizona, during which the service ties disparate sensors and shooters together to test capabilities vital for multi-domain operations and Joint All-Domain Command and Control

Rugen said that EDGE 22 will focus on networks and interoperability as part of seven "key" exercise objectives. The exercise, Rugen said, will include two air assaults alongside allies. The Army plans to use electronic warfare, including electronic sensing and electronic attack, to enable the assault.

"We're gonna see tremendous amount of … electronic warfare, both electronic sense and electronic attack, and all that will begin to generate that decision dominance to set conditions for the air assault and set the conditions for the wet-gap crossing for our ground combat teams," Rugen said during his presentation.

The Army is also planning to experiment with multi-intelligence sensing capabilities, as well as EW for counter-UAS, at EDGE 22, but Rugen didn't get into specifics.

The FVL-CFT is expecting at least 20 other DoD organizations to participate, including several other program executive offices, the Army's ISR Task Force and the Artificial Intelligence Integration Center. Rugen's presentation showed that Italy, Germany, the Netherlands, Australia, France, Canada and the United Kingdom would participate.

The service is aiming to achieve more than 50 technology objectives, Rugen told reporters at a roundtable, but there will be seven "key" priority objectives for the exercise, including interoperability with allies and refining the network to enable the combined force.

"So if a German squad leader needs an emergency call for fire, you know, how do we do that in an effective manner in a fast, agile manner, back into the 82nd [Airborne Division] BCTs' [brigade combat teams] TAK [tactical assault kit] and TOC [tactical operations center]," Rugen told reporters during a media roundtable.

The EDGE venue will also host a drone swarm of around 30 Air Launched Effects, essentially mini-drones that can carry different payloads, which will demonstrate both classified and unclassified behaviors, Rugen told reporters.

Among the unclassified behaviors, the ALEs perform autonomous detect and identify of targets, communication in denied environments, provide lethal targeting and complete battle damage assessment. The two-star's presentation at the conference showed that the ALEs would also carry electronic warfare capabilities and enable cooperative search.

"We're just creatively working with what is the swarm need to do to be better than maybe what some of the cheap swarms that our adversaries are putting together," Rugen said.

EDGE 22 runs from April 25 to May 12.

Disrupting the 'critical linkage': What is the Navy's SEWIP?

After troubling Pentagon tester report, prime contractor Lockheed Martin says its working closely with the Navy to address the issues.

Cryptologic Technician Technical 2nd Class Ryan Smith, from Cave Creek, Ariz., conducts maintenance on an SLQ-32 electronic warfare suite aboard the Arleigh Burke-class guided-missile destroyer USS Halsey (DDG 97). (U.S. Navy photo by Mass Communication Specialist 3rd Class Jaimar Carson Bondurant)

By JUSTIN KATZ on April 04, 2022 at 1:33 AM

WASHINGTON: The electronic warfare capability scheduled for installation onboard several classes of Navy warships experienced multiple problems while in use on an aircraft carrier during testing in April 2021, leading Pentagon weapons testers to doubt whether it will meet key performance goals.

The capability, part of the Surface Electronic Warfare Improvement Program (SEWIP) Block 2, is planned for outfitting on Navy aircraft carriers and destroyers. But testing last year on the aircraft carrier Gerald Ford (CVN-78) showed the system reporting "extraneous contacts for the radio frequency emitters it detects" and misidentifying "non-radio frequency emissions as [anti-ship cruise missiles]," according to the Pentagon's chief weapons tester.

The specific issues experienced onboard the carrier were excluded from the annual testing report published by the Pentagon in January, but the issues were described in a different version of the same document labeled as "controlled unclassified information" and made public by the Project on Government Oversight.

Joe Ottaviano, an executive at Lockheed Martin, the prime contractor delivering the block 2 version of the system to the Navy, said in a statement to Breaking Defense that the issues raised in the Pentagon's report were already known to the company. "As part of an ongoing engineering services contract for SEWIP Block II, we routinely assess the system's functionality and performance so that we can proactively find, fix and improve the system before problems arise," he said.

"The DOT&E report highlights several findings that we are aware of and are working in close partnership with the Navy to address and have addressed these findings," he continued.

As of press time, a Navy spokesman did not respond to questions from Breaking Defense for this report.

Fighting On The Electronic Seas

SEWIP is one of the Navy's premiere electronic warfare capabilities programs and versions of its chief system are already on almost every surface ship in the fleet. Given the issues the new weapons tester reports brought to light and the Navy's nascent plans to install the next block of SEWIP systems onto destroyers in the near future, Breaking Defense thought it was a good time to explain what SEWIP brings to the Navy's fight. But first, what's electronic warfare?

Electronic warfare, or what the Pentagon now more often calls the electromagnetic spectrum, uses electromagnetic or directed energy to accomplish one of three goals, according to Brian Hinkley, a retired Navy captain with more than two decades of experience as an electronic countermeasures officer: electromagnetic attack or jamming an adversary's systems, defensive measures to protect personnel or protect equipment from getting jammed and electronic support which focuses on surveillance and identifying sources of electromagnetic energy.

SEWIP, then, is the Navy's overarching program to incorporate various EW capabilities into its ships.

"SEWIP will give us better capability to sense the environment," said Hinkley, who also serves in leadership positions with the Association of Old Crows, a non-profit organization focused on EW, and is an executive at the services provider Amentum. "It'll give us a better capability to jam incoming missiles in the maritime domain."

But SEWIP is also the source of some confusion for navy observers, as Capt. Jesse Mink, one of the officers overseeing SEWIP for the Navy, explained during his presentation at the Surface Navy Association's annual symposium earlier this year.

"A lot of folks call it SEWIP… But I want to make sure you understand that SEWIP is the program. We don't install SEWIP onboard ships," he said. "We install versions of SLQ-32."

AN/SLQ-32, often pronounced as "slick 32," is the chief system the SEWIP program has incrementally upgraded since 2002. The program has subsequently been divided into blocks since its inception with a different prime contractor for each block.

The blocks are further divided to denote certain capability differences, but in general, Lockheed Martin is the prime contractor for block 2, the version cited in the weapons tester report, and Northrop Grumman is producing block 3, which will bring new electronic attack capabilities to the fleet. General Dynamics and Lockheed Martin have been the prime contractors for various iterations of the legacy block 1 SLQ-32. (There is also a "lite" versions of block 2, designed to be more modular.)

A fourth SEWIP block exists on paper but mostly serves as a bookmark for undetermined future upgrades the Navy will seek following its own research and development.

While SEWIP as a program has only been around since 2002, historically EW has proven itself to be a decisive capability during armed conflict. Some forms of communications jamming have been present in military operations going back for more than 100 years ago, Hinkley said.

"He who had the communications and had the ability to pass that information, whether it was to people or to weapon systems, that was the critical linkage. So anyone that could disrupt that linkage was given an advantage," he said. In most every armed conflict "everybody proves time and again that you have to control the EMS for almost all military operations to be successful."

Moving forward, the Navy is in the process of installing SLQ-32V(7) — the capability associated with SEWIP Block 3 — onboard a Flight IIA Arleigh Burke-class destroyer.

"This [SLQ-V(7)] is revolutionary in its ability to do electronic attack for surface warfare," Mink, the Navy officer partly responsible for the SEWIP program, said. "We've never had this capability afloat before."

In the meantime, though, it remains to be seen how the problems in block 2 may postpone the system from getting its final green light from the Pentagon's development and test community.

Why hasn't Russia used its 'full scope' of electronic warfare?

"The Ukrainians still have good command and control over their forces in the field in ways that the Russians actually don't have," Pentagon press secretary John Kirby told reporters last week.

A Ukrainian soldier takes part in a 2017 live-field exercise. Despite Russia's overwhelming military edge, Ukraine has maintained its C2 capabilities. (US Army/ Anthony Jones)

By ANDREW EVERSDEN and JASPREET GILL on March 28, 2022 at 4:55 AM

WASHINGTON: Russia's full-scale invasion of Ukraine is now a month old, and Ukraine's stiff resistance has exposed wide issues with Russia's perceived military dominance. While Russia's military challenges are pervasive, one surprising situation sticks out to puzzled experts: the apparent lack of widespread use of advanced electronic warfare capabilities.

At the beginning of March, a senior defense official said that the Russian military had yet to use its "full scope" of EW, but stated that "we do have indications that in some places they have used EW to their advantage, particularly in jamming, at a local level." Weeks later, the Pentagon still assesses that Ukrainian forces retain command and control of their military.

"The Ukrainians still have good command and control over their forces in the field in ways that the Russians actually don't have," Pentagon press secretary John Kirby told reporters on March 22.

That is not what many experts expected to happen, given Russia's well-documented buildup of advanced electronic warfare platforms and its proven use in the 2014 invasion of eastern Ukraine's Donbas region.

"I would have, prior to the invasion, assessed that Ukrainian logistics and command and control would be hampered, that UAVs would be targeted, quite extensively, and that they would struggle to coordinate a response against the Russian forces," said Sam Cranny-Evans, a C4ISR research analyst at the London-based think tank Royal United Services Institute.

One of the reasons the Russians haven't been able to use the full range of EW capabilities is because the Ukrainians are fighting an "irregular" war than what Russia's EW systems are designed to challenge, said Bryan Clark, a senior fellow at the Hudson Institute. They're dispersed, operating in much smaller units and using a combination of Western-supplied radios that the Russians aren't necessarily able to detect easily.

He added that emissions from Ukrainian forces using their cell phones are also being caught up in other civilian emissions, making it harder for Russian forces to find Ukrainians in the forest of electromagnetic spectrum emissions.

Laurie Buckhout, a retired Army colonel who specializes in EW, told Breaking Defense that the non-contiguous battlefield could be impacting Russian decision-making on its electronic warfare capabilities. For example, in 2014 the battlefield had an obvious forward line of troops that allowed for the Russian military to jam without impacting their own communications. That's made more difficult without a distinct forward edge and Russian forces trying to surround multiple cities.

"When you're [the Russia military] trying to get into Kyiv and you're trying to surround the city and there's people all around you …you need to be a little more careful and more surgical," Buckhout said. "So you're not going to see some of the broadband, high range stuff that you saw the first time into Ukraine … because you've got now your own troops in that area."

Russian military advances in Ukraine have largely stalled amid fierce Ukrainian resistance and significant logistical issues, including lack of fuel or getting stuck in the mud. For example, Buckhout said that Russia's airborne EW system, like a helicopter with an EW payload, is only valuable if there is a capable ground attack.

"If you wanted to blind and deafen your enemy when you were about to go after him with heavy armor, you would have a helicopter up then," Buckhout said. "But if your armor's bogged down in mud or soldiers are surrendering or giving up their vehicles because they're out of fuel, you're not going to put your helicopters up to support that, because there's not going to be a heavy armor attack. Why put your asset up there for it to be taken down if there's not an operation worthy of it happening on the ground?"

What's Being Missed?

Another question is how observers know that the Russian forces aren't using electronic warfare — particularly given that it's an invisible capability. Cranny-Evans explained that just because it's not being observed, in part because "good EW" is very targeted, doesn't mean it isn't happening.

"You try and find a specific radio and you jam that specific radio, or you jam a number of radios in an area. You don't take down everything because you need it as well," Cranny-Evans said. "So I'm very reticent to say that we haven't seen it because it's not observed. And B, the Ukrainians will be the last to admit that they're having problems communicating."

According to a 2017 report from the International Centre for Defence and Security, Russia's EW portfolio is geared toward challenging NATO communications, radars, unmanned aerial vehicles and other sensors. For Sergey Sukhankin, a senior fellow at Jamestown Foundation, Russia's lack of extensive use of its EW capabilities is showcased by Ukraine's success using Bayraktars and other types of killer drones.

Ukrainian drones have "managed to derail at least part of the supplies of fuel and other important commodities, and basically, Russia was unwilling or unable … to deal [with] it," Sukhankin said.

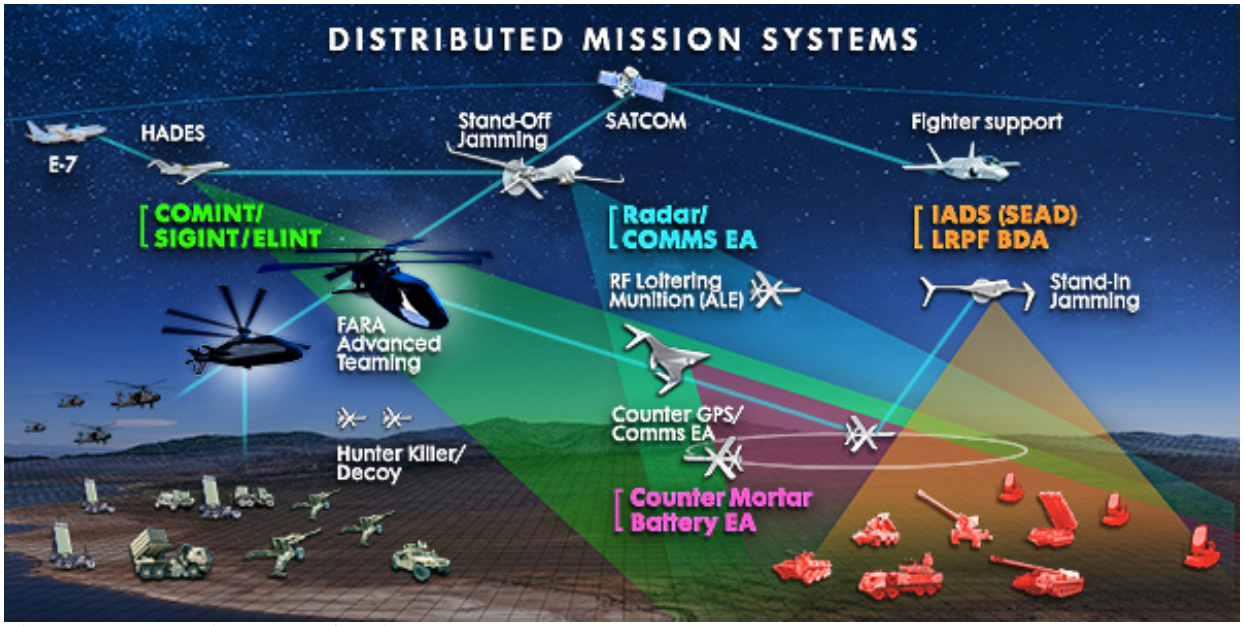
However, experts said Russia will likely increase its use of electronic warfare as the war progresses. Clark said the Russia military is "adapting and learning" to new radios used by Ukrainian forces and how they can be jammed.

"So I think what we're going to see in the EW world is just a steady increase in the use of EW by Russian forces, because at this point, the EW capabilities that they have… been using in the past are mostly designed around ground force operations," Clark said. "I think you'll see more and more of that, especially the use of UAVs because I think early on they were reticent to use a lot of their UAV-based EW systems because the Ukrainians had a bunch of these air defense systems [and] stinger missiles."

New tools for electronic warfare: multispectral operations and mission-adapting sensors

presented by NORTHROP GRUMMAN

Multispectral operations are the response to a dynamic world where hostile nations have well known and advanced capabilities in EW and cyber.



Distributed mission systems graphic courtesy of Northrop Grumman.

By BREAKING DEFENSE on April 29, 2022 at 11:25 AM

Joint All Domain Command and Control (JADC2) is usually described in terms of playing offense: the OODA loop, the kill chain, and sensors to effectors. Defense is inherent in the "C2" part of JADC2 but it's not what comes to mind first.

To use a football analogy, it's the quarterbacks that get the attention but it's the teams with the best defense — against both the run and the pass — that usually make it to the championship.

In the world of electronic warfare (EW), think of the electromagnetic spectrum as the playing field and the battle playing out upon it being waged both offensively through tactics such as targeting and spoofing and defensively through what's known as countermeasures.

The military uses the electromagnetic spectrum — essential, yet invisible — to detect, deceive and disrupt the enemy while protecting friendly forces. As enemies become more capable and threats more complex, controlling the spectrum is increasingly critical.

"What has happened over the last few decades is that processing power has greatly increased," explained Brent Toland, sector vice president and general manager for the navigation, targeting and survivability division, Northrop Grumman Mission Systems. "That allows one to create sensors where you can have increasingly broad, instantaneous bandwidth for much faster processing and greater awareness. Further, in a JADC2 context, this enables distributed mission solutions that are more effective and more resilient."

Large Aircraft Countermeasures (LAIRCM), one of Northrop Grumman's IRCM systems, protects against infrared-guided missiles. It has been installed on more than 80 aircraft types. Shown above is a CH-53E installation. Photo courtesy of Northrop Grumman.

Because the processing is all digital, signals can be adapted in real time at machine speeds. From the targeting side, that means that the radar signal can be adapted to make it harder to detect. From the countermeasures side, the response can also be adapted to better counter the threat.

Beating back the swarm with dynamic countermeasures

The new reality of electronic warfare is that greater processing ability makes the battlespace increasingly dynamic. For example, both the U.S. and its adversaries are developing concepts of operation for swarms of unmanned aerial systems that increasingly have sophisticated EW capabilities. In response, countermeasures must be equally advanced and dynamic.

"The swarm generally is performing some sort of sensor mission such as EW," said Toland. "When there are multiple sensors flying on different air platforms and, perhaps, even space platforms, you are in an environment where you need to defend yourself against detection from multiple geometries."

"It's not just facing forward into an air defense system. All around you there are potential threats now. If they're communicating with each other, then countermeasures also need to rely on multiple platforms to help commanders assess the situation and offer up effective solutions."

Such a scenario is at the heart of JADC2, both offensively and defensively. An example of distributed systems conducting distributed EW missions would be a crewed Army platform with RF and IR countermeasures working in conjunction with an uncrewed Army platform with Air Launched Effects that is also performing some part of the RF countermeasures mission. This multi-ship, crewed-uncrewed configuration gives the commander multiple geometries in which to sense and defend than is possible when all the sensors are on a single platform.

"In an Army multi-domain-operations environment, you could readily see where they are absolutely going to need to have awareness all around themselves in terms of the threats that they will be immersed in," said Toland.

It's a capability that the Army, Navy, and Air Force all need for multispectral operations and electromagnetic spectrum dominance. That requires broader bandwidth sensors with advanced processing capabilities to control much larger swaths of spectrum.

Multispectral operations fuse data from multiple EW sensors

To conduct such multispectral operations, it will be essential to begin employing what's known as mission-adapting sensors. Multispectral refers to the electromagnetic spectrum, including a range of frequencies that cover visible light, infrared radiation, and radio waves.

Targeting, for example, has historically been done with radars and electro-optical/infrared (EO/IR) systems. So multispectral in a targeting sense would be a system that can use broadband radar and multiple EO/IR sensors, such as digital color cameras and multi-band IR cameras. The system would have the ability to switch back and forth between the sensors to gather more data, by using different parts of the electromagnetic spectrum.

LITENING is an electro-optical/infrared targeting pod capable of imaging at long ranges and sharing data securely through its two-way, Plug-and-Play data links. U.S. Air National Guard photo by Staff Sgt. Bobbie Reynolds.

Also, multispectral doesn't imply that a single targeting sensor has a combined capability in all areas of the spectrum, to use the example above. Rather, it is the use of two or more physically different systems, each sensing in its particular part of the spectrum, with the data being produced by each individual sensor fused together to produce a more accurate picture of the target.

Toland described the power of multispectral capabilities through the lens of countermeasures.

"On the survivability side, you're obviously trying not to be detected or targeted. We have a long history of providing survivability in the infrared and radio frequency portions of the spectrum, with effective countermeasures for both."

"You want to be able to detect if you are being acquired by an adversary in either portion of the spectrum, and then be able to provide the appropriate counter technique as needed — whether that be RF or IR. Multispectral becomes powerful here in the sense that you're relying on both and can choose which is the appropriate part of the spectrum to use, as well as the appropriate techniques to counter the attack. You are assessing the information from both sensors and determining which is the most likely to protect you in this situation."

Artificial intelligence (AI) plays an important role in fusing together and processing the data from two or more sensors for multispectral operations. AI helps to thin and sort the signals, culling out the signals of interest and providing an actionable recommendation of what the best course of action is.

The AN/APR-39E(V)2 is the next step in the evolution of the AN/APR-39, the radar warning receiver and electronic warfare suite that has been protecting aircraft for decades. Its smart antenna detects agile threats over a wide frequency range, so there's nowhere in the spectrum to hide. Photo courtesy of Northrop Grumman.

In a near-peer threat environment, there is going to be a proliferation of sensors and effectors, with many threats and signals coming at US and coalition forces. Presently, known EW threats are stored in a database of mission data files that identify their signatures. When an EW threat is detected, the database is searched at machine speed for that particular signature. When the stored reference is found the appropriate countermeasure techniques are applied.

It's a certainty, however, that the US will face never-before-seen EW attacks (similar to Zero Day attacks in cybersecurity). This is where AI will step in.

"In the future, as the threats become more dynamic and change, and they are no longer able to be categorized, AI would be extremely helpful to identify what appears to be a threat that your mission data file would not recognize," said Toland.

Conclusion

Multispectral operations and mission-adapting sensors are the response to a changing world where potential adversaries have well known and advanced capabilities in EW and cyber.

"The world is changing rapidly, and the shift of our defense posture toward near-peer competitors has heightened the urgency of us employing these new, multispectral systems in order to engage distributed systems and effects," said Toland. "This is the near future of electronic warfare."

Staying ahead in this era calls for fielding of a new generation of capabilities and enhancing the future of EW. Northrop Grumman's expertise in electronic warfare, cyber, and electromagnetic maneuver warfare spans all domains — land, sea, air, space, cyberspace and the electromagnetic spectrum. The company's multispectral, multifunction systems give warfighters superiority across the spectrum and allow for faster, more informed decisions and ultimately mission success.

Satellite jamming 'normal' by militaries during conflict, not peacetime: State Dept. official

Airmen from the 4th Space Control Squadron take a picture in front of the Counter Communications System Block 10.2 on March 12, 2020 at Peterson AFB, Colorado. (U.S. Air Force/Andrew Bertain)

By THERESA HITCHENS on March 21, 2022 at 12:15 PM

WASHINGTON: The Russian military's jamming of GPS signals and communications satellites in Ukraine is considered by the US government as essentially a routine wartime activity, according to a senior State Department official.

Judging from actual real world actions during recent conflicts around the globe, Washington and Moscow appear to be on the same page with this issue — a good thing for avoiding conflict between the two nuclear powers. But there may be a growing disconnect between the two sides on the question of satellite interference outside of direct conflict, with a senior Russian official earlier this month making the surprising claim that doing so is an act of war.

During a March 17 virtual conversation at the National Security Space Association, Eric Desautels, acting deputy assistant secretary for emerging security challenges and defense policy in State's Arms Control, Verification and Compliance bureau, explained that the US military has its own jamming capabilities for use in conflict zones.

"For example, the United States has our own communications jammer known as the CCS system," he said. "We think that jamming is probably a normal part of conflict."

CCS is the Space Force's Counter Communications System, a mobile communications satellite jammer built by L3Harris and first fielded in 2004. The system has been upgraded routinely over the last 20 years, with the latest upgrade, called Block 10.2, declared operational in March 2020.

In the current conflict, Russian forces actively have been jamming GPS signals in Ukraine as they attempt to advance. In addition, a senior Ukrainian cybersecurity official this week suggested that a Feb. 24 cyber attack on commercial communications provider Viasat, which provides Internet connectivity in Ukraine and Europe, was part of an organized Russian cyber campaign against his country's forces.

Reuters quoted Victor Zhora as saying that the attack, which shut down thousands of satellite receivers across Europe, "a really huge loss in communications in the very beginning of war." While Zhora said the attack has yet to be formally attributed to Moscow, "we believe that Russia is attacking not just with missiles and with bombs, but with cyber weapons."

While jamming Ukraine's systems will certainly not be welcome by Ukraine or its supporters, it appears that in the US view, those actions are just part of any basic military engagement.

Jamming and hacking satellite capabilities in peacetime, however, is an entirely different matter — and the subject of planned UN discussions seeking to create norms for military activities in space, he said.

When employed outside a theater of conflict, the US considers satellite interference to be "irresponsible" and potentially dangerous — strong disapproval, but a far cry from calling it an act of war.

"Jamming in peacetime that disrupts activities of civilians — for example, Russia's jamming of GPS during the Trident Juncture exercise off of Norway that caused aircraft … to be unable to use GPS — that is an irresponsible behavior," Desautels said.

For that reason, he said, the US wants to raise the issue of jamming of GPS receivers, as well as of satellite command and control, during the upcoming meetings of the UN Open Ended Working Group (OEWG) On Reducing Space Threats. "If you lose control of your satellite, that makes it a hazard to other satellites," he explained. "And so there's a lot of work that can be done on all of these various cyber attack methods, jamming methods, that we look forward to having discussions on in the Open Ended Working Group."

Peacetime (or what passes for it): Just Say No

Contrast Desautels' remarks to those of Dmitry Rogozin, the head of Russia's space agency Roscosmos, earlier this month, and a disconnect seems to appear.

Reuters reported on March 2 that Rogozin, who has a history of hyperbolic statements and over-the-top tweets, told Russia's Interfax News Agency that "Offlining the satellites of any country is actually a casus belli, a cause for war."

Up to now, there has been no indication that any country seriously considers satellite interference as a legal act of war that allows an armed response. Under international law, a casus belli is a justification that a nation is being threatened, and thus has a right to self-defense.

Instead, Russia, China, the US and Iran (and most likely others) have used GPS and/or satcom jamming for both political and military purposes in what is at least technically peacetime. (For a good primer on the extent of such activities, see Secure World Foundation's annual Global Counterspace Capabilities report.) This suggests that nations see reversible satellite interference as acceptable under what is know as customary international law, or in essence, real-world practice.

Which is precisely why the US, and the United Kingdom that sponsored the effort to launch the OEWG, want it to be on the table during the upcoming discussions.

And as far as electronic warfare in conflict zones, Russian forces practice it routinely. The Russian military has frequently jammed GPS in Eastern Ukraine since the Crimean conflict in 2014, according to experts inside and outside the US government, as well as in Sryia.

Desautels said that the OEWG is now set to begin May 9, although it remains unclear whether it will actually happen due to the ongoing war. As Russian aircraft are now banned from landing in either the US or Europe, he explained, Moscow may try to block the meeting from going forward by arguing that Russian diplomats from the Foreign Ministry will be unable to attend.

In fact, the May 9 date for the launch of the first OEWG session is the result of Russia's attempts to derail the talks during a preparatory meeting last month; the original plan was for Feb. 14-18 in Geneva, Switzerland. Russia's invasion of Ukraine was initiated on Feb. 23.

Desautels stressed that the OEWG discussions are important to the United States as it seeks to promote more stability in military space relations — an effort the Pentagon is fully behind.

As first reported by Breaking Defense, Secretary of Defense Lloyd Austin last July issued a first-ever unclassified policy memo committing the US military to five overarching "tenets" to guide DoD space operations in peacetime. And one of those tenets states: "Avoid the creation of harmful interference."

Meanwhile the National Security Council is leading an inter-agency effort to put more flesh on the bones laid out by Austin and years of declarations by US government officials. That work, Desautels said, is still ongoing and covers a number of complex issues, such as how to ensure that any agreements don't prevent tests of missile defense systems.

Russia and China, on the other hand, have been been less than supportive of the UN discussions, voting against the establishment of the group. That said, several Western diplomats have told Breaking Defense that Beijing has been less belligerent in the run up to the discussions (as well as parallel efforts taking place in Vienna to establish guidelines for best practices for space activities), and has shown willingness to seriously engage on the issues.

Desautels kept a hopeful tone in his remarks last week, but cautioned that the May meeting is the first in a two-year process that will run through 2023.

"This is going to be one of the first times where we really sit down with countries and start talking about these norms of responsible behavior," he said. "So, the first meeting in May will most likely be focused very much on background information — what is the outer space environment; what are the security threats in the environment what is the existing legal regime in the environment — so that we can raise the level of education."

Army races to research new electronic warfare tech, on offense and defense

"The electromagnetic spectrum is not officially a domain, but operations on the electromagnetic spectrum are critical in order to realize the different phases of the multi-domain operations," said one Army researcher.

Sgt. Jessie Albert, an electronic warfare specialist with the 25th Infantry Division, trains on the Wolfhound Radio Direction Finding System at Schofield Barracks, Hawaii, on April 11, 2018. (Staff Sgt. Armando R. Limon/US Army)

By ANDREW EVERSDEN on March 15, 2022 at 4:45 AM

WASHINGTON: As the Army revitalizes its electronic warfare systems after years of neglect, the service's researchers at the C5ISR Center said they are developing several technologies that will make EW soldiers more effective on the battlefield, even if they can't talk much about the tech specifically.

Instead, several Army researchers told Breaking Defense about the challenges they're hoping to overcome: They need resilient EW systems that can stretch over greater distances to get close to enemies (or automated options if the link breaks), ways to sniff out enemy electromagnetic signatures that can reveal battlefield data and potential EW targets, and, finally, methods to know if an EW attack — generally a silent, explosion-less technical assault — did what it was supposed to do to enemy systems.

This is all in service of, and integrated into, the Army's new warfighting concept known as multi-domain operations. The concept of MDO is how the Army plans to fight as part of the joint force against an adversary who can contest the US military across land, sea, air, space and cyber.

"The electromagnetic spectrum is not officially a domain, but operations on the electromagnetic spectrum are critical in order to realize the different phases of the multi-domain operations," said Jeff Boksiner, senior research scientist for electronic warfare technology at the center. "[EW] will have different roles depending on where you are within the MDO just because MDO is defined by not just the phase operation, but also by the operational distances."

Electronic warfare can be used to interfere with enemy communications systems, interrupting their ISR, battlefield maneuvers and target acquisition processes. To develop the electromagnetic superiority the service needs, Boksiner said, the Army will need to use automation and machine learning to more quickly process battlefield information and alleviate cognitive burden on soldiers. He added that automation could also be used used to coordinate EW effects on the battlefield. Information overload, as Breaking Defense has previously reported, is a primary challenge in multi-domain operations.

To help deal with the greater distances, particularly envisioned by experts if the US ever has to take on China in the Pacific, the researchers at the C5ISR Center are also considering the possibilities of high-altitude platforms and distributed sensors, mixing sensors that are close to the enemy with ones that are far away, or a "layered" portfolio of battlefield capabilities.

"When we look at our traditional approaches things … for a while, have been done from really from a standoff perspective," said Joe Plishka, integrated offensive electronic warfare branch chief. "But approaches that focus more on a layered approach — capabilities at different layers — are certainly something that we have to consider going forward in our research portfolio."

In one specific example, the C5ISR researchers are diving into photonic signals processing, a complex method of rapidly processing signals. Boksiner added that they are also exploring atomic sensors, though that type of technology is still in the early research stage and years off.

The mix of sensors at different locations on the battlefield will also help the Army's with its deep maneuvers and deep fires as it transitions back to large-scale combat operations, but that comes with distance limitations for radio frequency waves. Therefore, researchers are looking at how to maintain connection with dispersed sensors to overcome distances.

The researchers are fiddling with how to "get some of these capabilities to be autonomous, either through some network connection where we can maintain communication with them or in some free autonomous mode for them to be effective if we can't establish some type of communication link," said Bill Taylor, cyber technology division chief at the C5ISR Center.

But while the Army is trying to ensure its own networks and communication lines stay up, it also wants to be zeroing in on the enemy using their electronic "emissions." Ultimately, the service wants to be able to identify what EMS emissions are associated with different formations and weapon systems, in order to understand what they're doing on the battlefield and ultimately predict their next move.

One of the challenges for the Army's science and technology community, according to Taylor, is that the EMS spectrum is "very dense," and adversary systems operating in different frequency bands and ranges make them difficult to track.

"Our ability to be able to detect those RF emissions, sense them, understand them at a rapid speed at the pace of operation is challenging," Taylor said.

Another area of research is how to provide battle damage assessment when the Army conducts an EW attack on the enemy. The invisible nature of the electromagnetic spectrum makes it challenging for commanders to see if an attack impacted its intended target. Taylor there's no "smoking hole in the ground or some destroyed equipment" to physically show a commander the result of an attack.

"Giving commanders that are not familiar with the use of electronic warfare as a means of fires the confidence that these capabilities are key tool in their tool chest of capabilities to provide challenges to the adversary and operation is something that we want to make sure that we can provide," Taylor said.