National DEFENSE

NATIONALDEFENSEMAGAZINE.ORG

Marine Corps Restructuring Makes Early Progress

The Pentagon's Push For Electric Motors

TACTICAL VEHICLES

Industry Gears Up For JLTV Competition: Round Two

FEBRUARY 2022

$6.99US $7.99CAN

02>

0 74470 68499 2

The Business and Technology Magazine of NDIA

DELIVERING
ON TARGET

Precision munitions guidance proven to withstand 20,000g shock

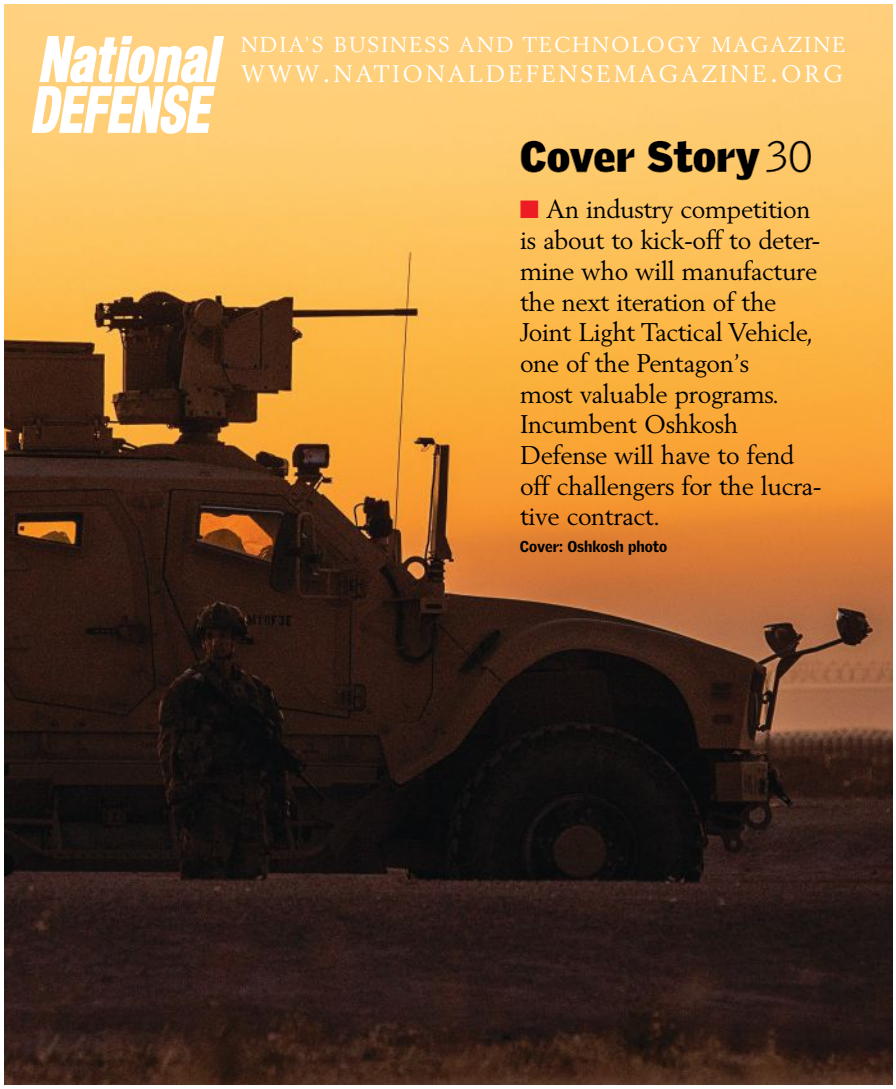
Our Atlantic Inertial Systems' compact, gun-hard guidance technology delivers increased precision for many munition types. Ultra-reliable performance in the most challenging environments.

collinsaerospace.com/gnc

Collins Aerospace

FEBRUARY 2022 VOLUME CVI, NUMBER 819

National DEFENSE
NDIA'S BUSINESS AND TECHNOLOGY MAGAZINE
WWW.NATIONALDEFENSEMAGAZINE.ORG



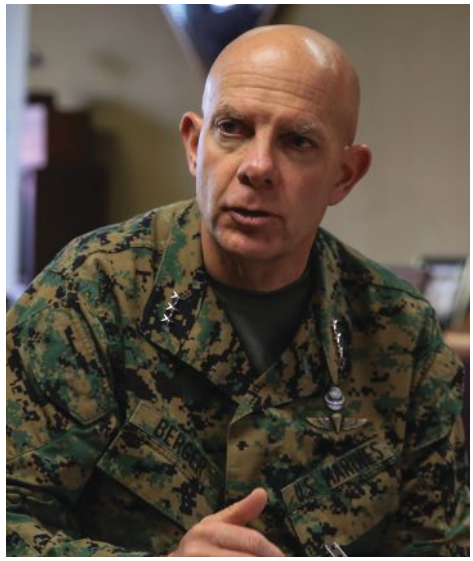
Cover Story 30

An industry competition is about to kick-off to determine who will manufacture the next iteration of the Joint Light Tactical Vehicle, one of the Pentagon's most valuable programs. Incumbent Oshkosh Defense will have to fend off challengers for the lucrative contract.

Cover: Oshkosh photo

Military Vehicle Electrification 33

To combat climate change, the Defense Department wants to transform its fleet of non-tactical vehicles by procuring EVs. For its tactical platforms, the military is exploring hybrid-electric technologies, with the long-term goal of moving to fully electric systems.



Marine Corps Restructure 24

Marines are reorganizing for an era of great power competition in the Indo-Pacific region. While the initiative has seen early successes, the next year or two will be critical in determining the fate of the effort says the service's top officer.


3


6


8


10

VIEWPOINTS

FEATURES

DEPARTMENTS

National DEFENSE
FEBRUARY 2022
VOLUME CVI
NUMBER 819

EDITOR IN CHIEF
Stew Magnuson
(703) 247-2545
SMagnuson@NDIA.org

CREATIVE DIRECTOR
Brian Taylor
(703) 247-2546
BTaylor@NDIA.org

MANAGING EDITOR
Jon Harper
(703) 247-2542
JHarper@NDIA.org

SENIOR EDITOR
Yasmin Tadjdeh
(703) 247-2585
YTadjdeh@NDIA.org

STAFF WRITER
Meredith Roaten
(703) 247-2543
MRoaten@NDIA.org

EDITORIAL ASSISTANT
Mikayla Easley
(703) 247-9469
MEasley@NDIA.org

National Defense
2101 Wilson Blvd., Suite 700
Arlington, VA 22201

BPA WORLDWIDE

National Defense (ISSN 0092–1491) is published monthly by the National Defense Industrial Association (NDIA), 2101 Wilson Blvd., Suite 700, Arlington, VA 22201–3060. TEL (703) 522–1820; FAX (703) 522–1885. **Advertising Sales:** Kathleen Kenney, 2101 Wilson Blvd., Suite 700, Arlington, VA 22201–3060. TEL (703) 247–2576; FAX (703) 522–4602. The views expressed are those of the authors and do not necessarily reflect those of NDIA. **Membership rates** in the association are $40 annually; $15.00 is allocated to *National Defense* for a one-year association basic subscription and is non-deductible from dues. Annual rates for NDIA members: $40 U.S. and possessions; District of Columbia add 6 percent sales tax; $45 foreign. A six-week notice is required for change of address. Periodical postage paid at Arlington, VA and at additional mailing office. **POSTMASTER:** Send address changes to National DEFENSE, 2101 Wilson Blvd, Suite 700, Arlington, VA 22201–3060. The title *National Defense* is registered with the Library of Congress.

The Selfless Service of the 54th Massachusetts Regiment

■ Service to our great nation takes many forms, but in all forms, it requires a selflessness of spirit, recognizing the best outcome for the organization may not provide the best outcome for an individual.

In early 1863, a few months after President Abraham Lincoln's signing of the Emancipation Proclamation, Massachusetts Gov. John Andrews oversaw the raising of the first U.S. military unit comprised primarily of Black soldiers, the 54th Massachusetts Volunteer Infantry Regiment. Andrews expected he could recruit a regiment of free Black men, despite knowing all eligible volunteers had likely experienced slavery in a way that a reasonable person could assume would make potential recruits reluctant to serve.

Despite lacking sufficient Black citizens in the state, Massachusetts got enough volunteers to establish both the 54th and 55th Massachusetts Regiments when volunteers from across the northern states and Canada traveled to the Bay State to enlist. At their first opportunity, Black men from a wide variety of backgrounds answered the call to service.

Library of Congress artwork

They answered the call in early 1863 during some of the Union's darkest days. They answered the call wanting to fight, yet not knowing if the U.S. government would allow them into combat. They answered the call despite knowing they could not serve in commissioned officer or command positions. They answered the call knowing they would have to sublimate their egos to achieve a greater objective — defense of the principles upon which the United States was founded.

Since they could not serve as commissioned officers or commanders, Andrews recruited Col. Robert Gould Shaw to lead the new regiment. The governor requested Shaw transfer from the 2nd Massachusetts Regiment, with which he saw action at the Battle of Cedar Mountain and was injured during the Battle of Antietam. Reluctant at first, at least partly because he did not want to leave his friends in the 2nd, Shaw eventually agreed to serve in the new organization. Shaw came to admire his unit, believing they would acquit themselves with distinction if allowed to do so.

Initially they were not allowed to do so. From late May through mid-July, the 54th was primarily given manual labor duties.

However, they persevered. Their first action was a skirmish, the Battle of Grimball's Landing. They then served as the vanguard of the Union attack on Battery Wagner outside of Charleston, South Carolina, leading the attack against a highly fortified position with ample guns and ammunition. Union forces failed and the 54th suffered more than 40 percent casualties including the death of Shaw.

Despite the failure, the 54th demonstrated great courage and initiative during the attack, highlighted by Sgt. William Carney. After the regimental color bearer was killed, Carney grabbed the colors before they hit the ground and moved to the front of the attack. When it became clear the Union could not overcome the Confederate defenses, he retreated under fire and was injured multiple times. Despite his injuries, he refused to relinquish the regimental colors to another Union soldier, feeling only a member of the 54th should have the honor of bearing his unit's flag. For his actions during the battle, in 1900 Sgt. Carney became the first Black man awarded the Medal of Honor.

Despite their valor, the government treated the men of the 54th Massachusetts poorly. Recruited with a promise of the same pay as white soldiers, the government initially offered $10 per month instead of the $13 received by white troops. So, the men of the 54th Regiment fought for 18 months without pay. Refusing to accept lesser pay for equal work, their families suffered as the men risked their lives for the Union. However, the soldiers took a principled stand, likely knowing they would set a precedent for all future Black service members; they refused to accept anything less than what they earned.

The success and impact of the 54th Massachusetts was not foreordained. When Andrews called for volunteers, he did not know if he would get enough recruits for the regiment. When Shaw and the other white officers began training the Black soldiers, who came from different backgrounds with different education, training and experience, they did not know if they could create a cohesive combat unit. And no one can know prior to combat how any individual or group of individuals will react under fire.

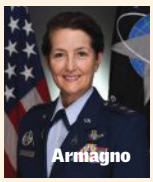
The 54th Massachusetts Volunteer Infantry Regiment established a standard of selfless service that provides an example for all U.S. military units. Service requires selflessness, with a focus on the mission, to ensure the principles upon which our nation is founded endure.

After the war, Charles W. Eliot, Harvard's president, praised the regiment, saying: "The Black rank and file volunteered when disaster clouded the Union cause. Served without pay for 18 months till given that of white troops. Faced threatened enslavement if captured. Were brave in action. Patient under heavy and dangerous labors."

Their selflessness and courage demonstrated Black units could fight as effectively as white units. The men of the 54th were pathfinders for Buffalo Soldiers and Tuskegee Airmen and are among the great examples of selflessness of service that mark the men and women who served our nation with honor and distinction. ND

Retired Army Maj. Gen. Jim Boozer is executive vice president and retired Air Force Col. Rachel McCaffrey is vice president of membership and chapters at NDIA and executive director of Women In Defense.

UP FRONT COMPILED BY STEW MAGNUSON



Space Force Has Big Plans for Year Three

■ After celebrating its second birthday in December, Space Force officials have ambitious plans for year three.

In 2022, the service plans on "really putting our tires on the track and just really moving out and delivering the things that we've been thinking about and working on and designing," said **Lt. Gen. Nina Armagno**, director of staff at Space Force headquarters.

For example, the service intends to release force design concepts for missile warning and missile tracking in 2022, she said at a Washington Space Business Roundtable event.

Additionally, the Space Force plans to continue standing up the service's headquarters.

"We have about 300 people and that's less than half of what we need to be a full, functioning headquarters here in the Pentagon," she said. "We're going to stay lean, agile and mission focused, but we need more than 300 people to do it."

The service will also grow in terms of capability as it brings Army, Navy and Marine Corps members into the force and some of their space systems into the fold, she noted.

Japan, Australia Deepen Defense Cooperation

■ Prime Ministers **Scott Morrison** of Australia and **Fumio Kishida** of Japan signed a Reciprocal Access Agreement to deepen military cooperation in the Indo-Pacific and "ensure the preservation of the international rules-based order."

The pair signed the agreement during a virtual ceremony after holding talks about a rising China and how to further the goals of the Quadrilateral Security Dialogue, a group of four nations with similar goals that includes the United States and India, according to press reports.

"The Australia-Japan RAA will establish standing arrangements for the Australian Defence Force and the Japan Self-Defense Forces to facilitate cooperative activities such as joint exercises and disaster relief operations, including those of greater scale and complexity, while improving the interoperability and capability of the two countries' forces," a statement from the Australian prime minister's office said.

Europe, Africa Want to Partner with U.S. on JADC2

■ As the services flesh out the Pentagon's joint all-domain command and control effort, allies and partners are eager to get involved, according to an Air Force leader.

Gen. Jeff Harrigian, commander of U.S. Air Forces in Africa and Europe, said allies are essential to the process of enabling information sharing on the tactical edge, also known as JADC2.

Now that programs like the Air Force's Advanced Battle Management System are taking off, he said other nations are asking how they can work with artificial intelligence and machine learning to become "contributors to where we go together in the future."

"JADC2 without our partners is a non-starter in the neck of the woods that I work in," he said at a Mitchell Institute event. "We need them to contribute to how we do this."

To achieve air dominance, international and U.S. armed forces will need to create "a shared understanding of the environment," which will enable rapid joint decision making, he said.

Pentagon Targets Data Quality Over Quantity

■ As the Defense Department works to harness the power of data, it is moving away from the notion that quantity is more important that quality, said **David Spirk**, the Pentagon's chief data officer.

"At the department we're … making a transition to a conversation about data quality and our ability to deliver that data to the warfighter, decision maker or platform and in a repeatable, testable manner," he said during a media roundtable.

While great power competitor China has a glut of data that it collects from its citizens, that doesn't mean it has a leg up in the development of information dominance systems.

"I don't necessarily see China having an advantage over us," he said. "China has an ability to ... leverage that data in an autocratic state that we will always guard against, because that's not our American values." *— Reporting by Stew Magnuson, Yasmin Tadjdeh and Meredith Roaten*

FURTHER READING

"AI and the Future of Disinformation Campaigns Part 2: A Threat Model," *By the Center for Security and Emerging Technology*

■ Part one of this two-part report compiled by a team of five researchers at Georgetown University's Center for Security and Emerging Technology did an excellent job of mapping out exactly how organizations engage in information warfare to divide and conquer populations.

Part 2 looks at future trends, including the application of artificial intelligence and machine learning to disinformation campaigns.

The future is now, unfortunately: "Our findings show that the use of AI in disinformation campaigns is not only plausible but already underway," the authors wrote.

There are several new software programs emerging from China that can generate "natural language." Easily spotted fake social media posts written in "anguished English" may soon be a thing of the past.

Private "disinformation for hire" organizations using advanced computing are also an emerging trend.

The report includes several recommendations for inoculating populations against fake news, deep fakes and other means to create unrest, and for governments to actively defend against this gray zone warfare.

They include: developing a common operating picture that feeds an early warning system for disinformation campaigns; raising public awareness of such campaigns; and enabling the media to report on fake news without enhancing its message.

However, "the ultimate line of defense against automated disinformation is composed of discerning humans on the receiving end of the message," the report said.

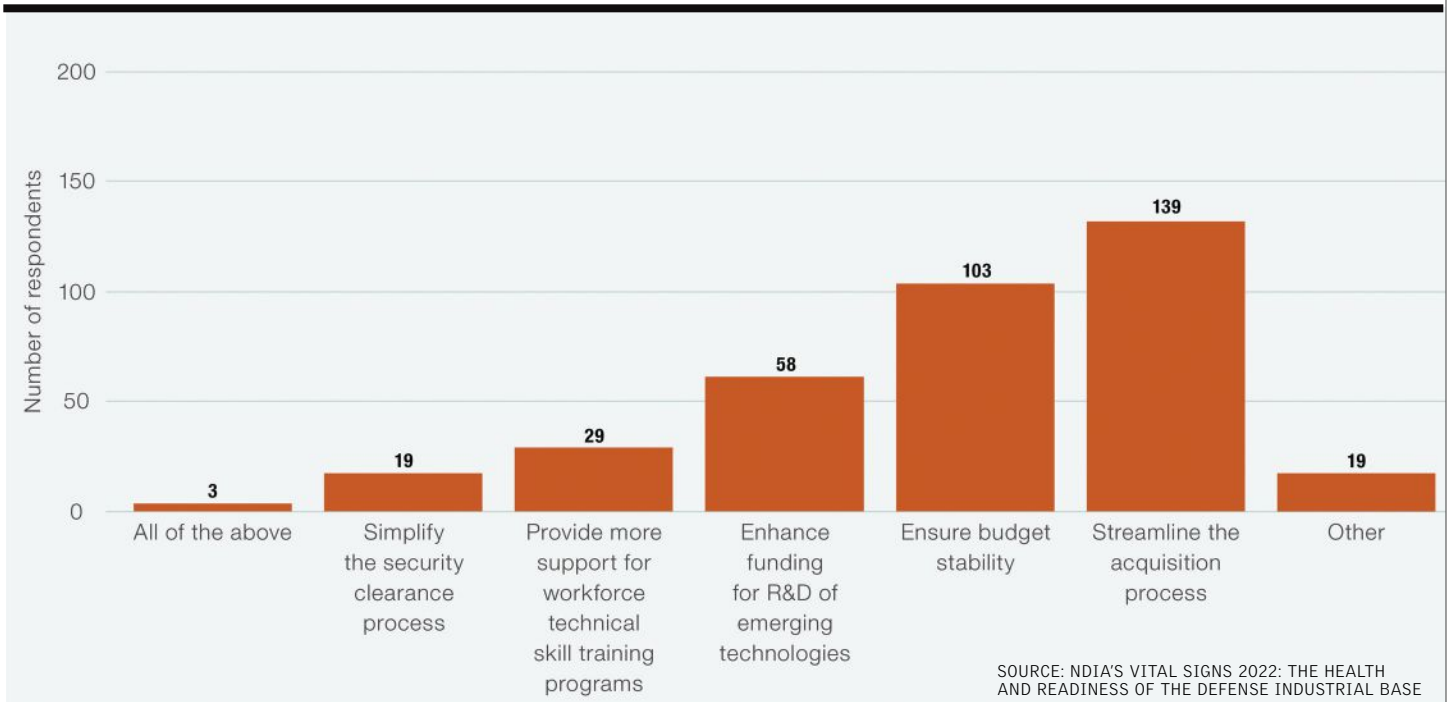
— Stew Magnuson

For more on information warfare, see page 20.

Defense Dept. photos

By The Numbers

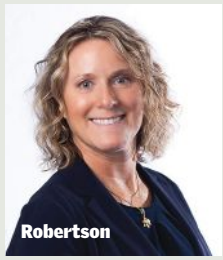
The Most Important Thing the Federal Government Can Do to Help the Defense Industrial Base Is?



SOURCE: NDIA'S VITAL SIGNS 2022: THE HEALTH AND READINESS OF THE DEFENSE INDUSTRIAL BASE

Hello, Goodbye


Aboulafia


Robertson


Samms

■ After 32 years, aerospace analyst **Richard Aboulafia** has left The Teal Group. He has moved on to be managing director at AeroDynamic Advisory, an Ann Arbor, Michigan-based consultancy.

Raytheon Intelligence and Space named **Kristin Robertson** as president of its Space and C2 strategic business and **Brad Tousley** to serve as president of subsidiary Blue Canyon Technologies, which specializes in space systems. Robertson most recently served as vice president and general manager of autonomous systems at Boeing. Tousley came from Raytheon's Advanced Concepts and Technology division, and served as president of Raytheon BBN Technologies.

The Army Combat Capabilities Development Command created a new chief technology officer position and named **Charneta Samms** as its first CTO. Samms most recently was the chief of plans and programs at the Army Research Laboratory.

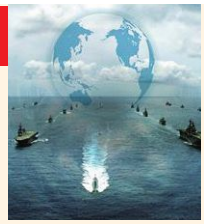
Mick Golson has been appointed president and COO of Orlando-based military and first responder training and simulation company ECS. The Air Force veteran had been an executive at the company since 2014.

The Navy conducted a joint ground-breaking and ribbon-cutting ceremony for the first purpose-built and co-located facilities for unmanned maritime vehicle testing. It is located at Naval Surface Warfare Center Port Hueneme Division, at Naval Base Ventura County in California. The facilities will accommodate testing, evaluation, and technology demonstration for extra-large undersea robots and unmanned surface vessels.

Rocket Lab USA Inc. is acquiring SolAero Holdings Inc., a supplier of space solar power products and precision aerospace structures, for $80 million in cash.

SolAero's acquisition adds 425 personnel to Rocket Lab's total headcount, which now totals more than 1,100 employees. ND

Coming Soon


NDIA image

■ With a goal of bringing more Indo-Pacific coverage to our readers, the magazine will be sending a correspondent to the Singapore Airshow, Feb. 15-18 and the Pacific Operational Science and Technology Conference organized by NDIA, March 7-10, in Honolulu, Hawaii.

Closer to home, NDIA's Tactical Wheeled Vehicles Conference returns to Norfolk, Virginia, Feb. 28 to March 2. Read NationalDefenseMagazine.Org online for breaking news from these major events. ND

The Meanings of 'Attritable' and 'Expendable'

■ Think of a typical family car or SUV and put an average price on it. How about a nice round number for the purposes of this article — $25,000.

A typical American family doesn't have that kind of cash sitting around. Most have to finance the purchase.

Then there are those Americans who can tool around in high-end sports cars — the kind you see pulling up to casinos in James Bond movies. The absolute lowest priced Lamborghini currently available runs about $211,000, according to *MotorTrend*.

Spending that much on such a vehicle for the average American taxpayer is the stuff of fantasies.

Compare that to the price of a Joint Light Tactical Vehicle. The last time the government published an average price for the U.S. military's workhorse non-combat vehicle was 2015. It totaled $365,000 back then, and it would be higher now adjusting for inflation.

The public's perception of the cost of military platforms may be increasingly relevant as the Pentagon continues on the path of swapping out manned for unmanned aircraft, ships, submarines and ground vehicles.

Military leaders and thinkers have been tossing the terms "low cost" and "attritable" around to describe some of the platforms, as new warfighting concepts take hold such as swarming drones, loyal wingman and manned-unmanned teaming.

The Mosaic Warfare concept in air warfare, for example, calls for multiple robotic jet fighters to accompany a piloted jet that serves as a quarterback. The robo-jets are stripped down aircraft that might serve only one function such as sensing or shooting, or even be a decoy meant to be targeted.

They would present multiple dilemmas for the enemy, who would have five targets to defeat instead of one. Those four other jets are often described in PowerPoints presentations as "attritable," but what exactly does this word mean?

What does "low cost" mean to a public that has to make monthly payments on a $25,000 car?

The first immediately observable thing about "attritable" is as one types it, Microsoft Word's spellcheck gives it a red underline, meaning it doesn't even recognize it. Going to Google, a search reveals few references to the word outside of these warfighting concepts.

This pegs "attritable" as pure military jargon.

Participants at defense conferences who see the word used in presentations no doubt understand it, but do members of Congress and the general public?

The root word, "attrition." Sure. Easily understood.

As an adjective, "attrit-able" is literally "able to undergo attrition."

One of the Google references noted that it is not synonymous with the word "disposable," but I have yet to hear a military leader at a presentation emphasize that point.

In fact, the word used in a cavalier way — and as described in these warfighting concepts — may easily be misunderstood as "disposable."

Further muddying the picture is another often used term by military leaders: "expendable." That is better understood as meaning something that can be lost without much impact.

So, what can be lost with little impact: a $1 million aircraft, $5 million, or $20 million? What's the threshold?

And — getting back to that typical family car that costs $25,000 — the fact that the military wants to populate the battlefield with platforms that cost about the same as the most expensive Lamborghini, about $500,000, and upwards, might shock lawmakers and their constituents alike — especially if they believe such systems are perceived as throwaways.

Meanwhile, the public doesn't hear much about the "multiple dilemma" concept for robotic systems. It isn't what's being sold. It's the cost of saving lives.

Moviegoers back in 2009 first saw this in action during the opening scene of the Academy Award-winning film, *The Hurt Locker*. They saw an explosive ordnance disposal robot travel down a dusty road in Iraq to disarm a roadside bomb while its operator stood back at a safe distance.

An off-the-shelf medium-sized EOD robot back then cost about $125,000, not counting maintenance and sustainment costs. Calling them "disposable" was perfectly fine. No one ever questioned the cost-benefit of using EOD robots then, or now, because they saved lives and limbs. They were a triumph and a "good news" story for the military technology community.

But "taking warfighters out of harm's way" is just one of many reasons why military leaders want to proliferate robots enabled with artificial intelligence and machine learning on the battlefield.

Marine Corps Commandant Gen. David Berger foresees battlefields with a variety of robotic systems aiding troops.

He was asked at a media availability last year what "expendable" means and where the thresholds were for a robot that was low cost enough to be destroyed without anyone caring. He admitted that he didn't have all the answers yet, but this was the path the Corps was on.

"We're going to have to get comfortable with throwaway things," he said.

He used helicopters as an example. An unmanned low-cost rotary-wing aircraft could be used to transport supplies on the battlefield. He asked: How many sorties could it do in a cost-effective way before it would be considered expendable?

Some of the questions are "moral and ethical," he noted.

What if that low-cost unmanned helicopter was transporting casualties "MASH-style" when lives are at stake?

"If it's faster to get an unmanned platform there and pick you up, are we OK with that? Where we're headed in is an area where we haven't gone to before," Berger said.

Meanwhile, when it comes to explaining the direction the U.S. military is going with robotic systems to the public, leaders should take care to explain exactly what "attritable," "expendable," "disposable" and "low-cost" means. ND

iStock illustration

Best and the Brightest Forge a Way Ahead

NDIA created the Emerging Technologies Institute with the overarching goal of delivering critical new technologies into the hands of our warfighters. To do that, it is very clear that there is a list of technologies that will have, and in many cases are already having, a transformative impact on the future of warfare.

But it isn't enough to merely advocate for those broad technology areas; equally important is focusing the Defense Department's precious research-and-development dollars on the right projects that will have the biggest payoffs.

Not every idea in artificial intelligence, or directed energy, or even hypersonics, will make sense from a practical standpoint, or even from an operator's point of view. Every dollar spent on bad science or a dead end is a wasted dollar that could have been spent on something more useful.

That is why it is important to be skeptical, in a scientifically rigorous way, of even the most promising-sounding ideas. We need to take risks; and indeed, America's willingness to invest in high-risk, high-payoff science has been one of the keys to our scientific and technological prowess. But there is a difference between investing in risky ideas and things that are just plain dumb.

In her classic book *Imaginary Weapons*, author Sharon Weinberger explored the world of Pentagon science, including an examination of how fringe ideas sometimes get funded by mainstream defense organizations. Though her work is full of comedic elements, including descriptions of actual half-baked research projects that a well-educated high-school physics student would have recognized as absurd, it carries the somber warning that there is at times a "fuzzy line between heartfelt conviction and obsessive delusion."

Weinberger highlights defense programs that had very little scientific grounding but were still funded at significant levels, showing that when credentialed experts raised concerns they were often ignored.

In sorting through the myriad proposals and pitched concepts, the Defense Department must be able to separate the proverbial wheat from the chaff, zeroing in on the most promising ideas and avoiding the ones that are infeasible, impractical, or downright impossible.

This creates an extremely difficult challenge: err on the side of being too conservative and a scientific portfolio can stagnate; but allow bad science a foothold and that portfolio becomes significantly diminished in both quality and impact. That is why we need to populate the ranks of defense program managers and scientific leaders with the best and brightest minds.

Our people making research investment decisions and guiding the defense research enterprise must themselves have the technical prowess to enable sound scientific reasoning. Fortunately, the department has attracted a cadre of extremely talented professionals in places such as the Air Force Research Laboratory, Office of Naval Research, Army Research Laboratory and DARPA, to name a few. Maintaining the quality of that workforce and ensuring that top students in our colleges of engineering and science consider careers in national defense mut be a priority.

This includes not just bench scientists working in Defense Department laboratories and industry, but acquisition professionals and senior scientific leadership at the highest levels in the services and the Office of the Secretary of Defense, including civilians and those in uniform.

And having attracted those credentialed scientists and engineers, it is important that we retain them with appropriate recognition and by creating career paths that encourage their contributions. Sadly, this last point is something that could be greatly improved across the department.

Finally, it also means that the Defense Department must bring in outside expertise, with the various review boards and expert panels, as well as the federally funded and university affiliated R&D centers, and rely upon their observations and recommendations. And though it may sound self-serving, independent organizations such as the Emerging Technologies Institute can play an important role in helping to formulate a path ahead.

On the topic of hiring the best and the brightest, I am absolutely delighted to announce that by the time you read this column Dr. Arun Seraphin will have joined ETI as its deputy director. Seraphin is a Massachusetts Institute of Technology-educated PhD in material science, who has worked on the staffs of both the House and Senate, and had a leadership role in the White House office of science and technology policy. He has had a profound impact on nearly every element of Defense S&T, with a special focus on the workforce and small business.

Please join me in welcoming Arun to ETI and the NDIA family, and look forward to his future contributions to this column. **ND**

Dr. Mark J. Lewis is the executive director of NDIA's Emerging Technologies Institute.

BUDGET MATTERS

BY JON HARPER

Lawmakers Defying Public Opinion on Defense Spending

The recently passed 2022 National Defense Authorization Act green-lit a 5 percent boost in military expenditures, despite recent polling indicating that nearly two-thirds of Americans believe the federal government has been spending too much or about the right amount on the armed forces.

The bill, which was signed into law in December by President Joe Biden, authorized $768 billion for the Pentagon and defense programs administered by other agencies, although Congress has yet to pass a full-year appropriations bill that would provide the actual funding.

However, a poll conducted in November by the Ronald Reagan Presidential Foundation and Institute indicated the public isn't clamoring for plus-ups in military spending.

"A plurality (39 percent) think the U.S. government spends about the right amount on defense, whereas roughly equal percentages think it spends too little (27 percent) or too much (26 percent)," according to the Reagan National Defense Survey.

"When asked what the highest priority for increased funding should be, the military ranks fifth as a priority at 11 percent, behind healthcare (23 percent), border security (17 percent), education (15 percent), and infrastructure (14 percent)," it added.

There are partisan differences when it comes to defense spending, the survey found. About 42 percent of Republicans say Uncle Sam spends about the right amount, 11 percent too much, and 42 percent too little. About 45 percent of Democrats say it spends too much, 37 percent the right amount, and 13 percent not enough.

Notably, the passage of the 2022 NDAA came as Democrats held power in the House, Senate and White House.

The Reagan Institute poll also looked at threat perceptions. Concerns about cyberattacks topped the list at 88 percent.

Additionally, a whopping 85 percent of respondents are concerned about violence as a result of political division in the United States. The poll was conducted about 10 months after the Jan. 6 assault on the Capitol.

"When asked if they think the greatest threats we face come from outside of the country or from within the country, 41 percent think they come from within, which is up 5 points since February 2021," the survey noted. "Another 30 percent believe we face equal threats at home and abroad, which is also up 5 points since February. Only one in four (25 percent) think the greatest threats come from outside the country."

House Armed Services Committee Chairman Rep. Adam Smith, D-Wash., believes he knows why many Americans aren't on board with increases in military funding.

"There's a whole lot of reasons, but two rather important ones are No. 1, the spectacular amount of money that the Pentagon with the able help of Congress, fully admit, has wasted over the course of the last 20 years," he said in December at the Reagan National Defense Forum in Simi Valley, California.

He added: "No. 2 is there is an increasing number of people in this country on the left and on the right who look at the rest of the world and say, 'What are we doing? … China's not our problem, OK. I'm worried about my infrastructure. I'm worried about my education. I'm worried about my health care. You know, we just spent 20 years in Afghanistan and all that money and all those lives, and I got what for that?'"

The Defense Department needs to do a better job spending the money it gets, and policymakers need to do a better job explaining why the United States needs a robust military, according to Smith, who voted for the NDAA.

The Biden administration had requested just a 1.6 percent boost in Pentagon funding in 2022, significantly less than the NDAA authorized.

Going forward, Air Force Secretary Frank Kendall said Biden will submit budgets that he thinks can meet the national security needs of the United States. However, the administration wants more flexibility in how it spends defense dollars.

The Pentagon has been pushing lawmakers for permission to retire older systems and invest more money in modernization and new capabilities.

"We've got to be allowed to make some changes," Kendall said at the Reagan forum. "That's what we're going to have to have if we're going to deal with the threat that we're confronting now, particularly with China." ND

iStock illustration

Data Reveals Big Drop In U.S. Arms Sales

■ Implemented cases of foreign military sales and direct commercial sales of weapon systems to international customers by U.S. manufacturers plummeted last year, according to data released in December by the Biden administration.

While analysts had already been tracking a significant decrease in the value of announced potential sales, government statistics also show a drop in cases that made it to implementation.

For fiscal year 2021, the Defense Security Cooperation Agency executed $34.81 billion in implemented arm sales cases, including: $28.67 billion funded by U.S. allies and partners under the State Department's Foreign Military Sales program; $3.8 billion under the Foreign Military Financing program; and $2.34 billion under the Defense Department's Foreign Assistance Act and Building Partner Capacity programs.

Meanwhile, direct commercial sales of equipment by U.S. industry to foreign buyers totaled $103.4 billion, the agency announced.

Combined, the numbers add up to $138.21 billion.

In comparison, FMS and DCS totaled $50.78 billion and $124.3 billion in 2020, respectively, for a combined total value of $175.08 billion.

"Final FMS/DCS numbers for FY '21 … were down significantly," at 31 percent and 17 percent year-over-year respectively, said the Cowen Washington Research Group in an email to industry.

Those numbers are also way down from 2019, when FMS totaled $55.4 billion and direct commercial sales reached $114.7 billion.

"We're surprised by the magnitude of the drop, which suggests FMS/DCS sales will be a headwind for large-cap defense primes" with a significant international customer base in the near future, the email said.

The Biden administration has been approving arms deals at a much lower rate than the Trump administration, which made weapons exports a major pillar of its defense and economic policies.

The Biden team appears to be less gung-ho, as some observers anticipated.

"Under this administration, the United States will insist on adherence to our agreements on the use of U.S. origin defense equipment by U.S. allies and partners, compliance with the law of armed conflict, and respect for human rights," the Defense Security Cooperation Agency said in a statement.

"The United States will take appropriate measures in cases where the U.S. government concludes that violations have taken place. This administration will not approve arms transfers where we believe there is significant risk of diversion, civilian harm, or misuse," it added.

The Biden team's more selective FMS policy could mean a reversion back to levels of sales on par with those seen during the Obama administration, according to the Cowen email. "That appears to be what's happening." ND

iStock illustrations

Study: U.S. Underinvesting in 6G

■ The United States is behind the curve when it comes to fostering the next generation of communication technologies, according to a new study.

Much of the U.S. government's focus has been on 5G tech. The Defense Department is investing more than $600 million in these capabilities as it moves to integrate them into the military.

However, officials and other observers are also looking at what comes next. In 2021, the Biden administration committed to spending $2.5 billion on 6G, but a new report by the Center for a New American Security said it needs to do more.

"6G technologies will bring more than just improved data transmission speeds. Communications technology forms the conduit of societies, implicating future economic competitiveness, military strength and geopolitical influence," said the report, "Edge Networks, Core Policy: Securing America's 6G Future."

Uncle Sam is in a long-term competition with China, it noted. 6G, like 5G, is a dual-use technology and will be part of Beijing's military-civil fusion strategy, according to the study.

The nation's telecommunications companies "will almost certainly work with China's defense industry on pilot 6G projects. U.S. policymakers should anticipate that China will be as ambitious with 6G as it has been with 5G," it added.

"The case for developing policy on 6G, informed by lessons from the 5G rollout, is clear," the report said. "Delaying steps that other countries have already taken … will hurt American competitiveness and technology primacy. U.S. policymakers in the White House, Congress, and relevant departments and agencies should engage in proactive, affirmative, and collaborative efforts to ensure U.S. leadership in next-generation wireless technologies."

The authors recommend the U.S. government take a number of steps to lay the groundwork for the next generation of communications capabilities, including: crafting a long-term strategy and roadmap; expanding research-and-development funding; exploring opportunities for additional R&D funding through research grants, tax credit and financial support; establishing more test beds; and opening additional experimental spectrum licenses to accelerate R&D efforts.

Policymakers should also: promote the development of new 6G use cases by using the purchasing power of the federal government; create a security fund and look at providing financing support and technical assistance to "strategic partners" for the deployment of secure and trusted 6G networks; and help create a "multilateral digital development bank" in partnership with export credit and export finance entities in allied nations, the report said. ND

NEWS BRIEFS

BY MIKAYLA EASLEY AND MEREDITH ROATEN

Norwegian Startups Eye U.S. Defense Market

Some of Norway's most innovative companies are looking to break into the U.S. defense market with help from Silicon Valley.

Hacking 4 Allies — a program run by the Norwegian-American Defense and Homeland Security Industry Council — recently announced the selection of eight companies to participate in the program. The effort aims to generate investments, research-and-development funding, and contracts for startups to enter both military and civilian markets in the United States and Norway.

Peter Newell, CEO of Silicon Valley-based BMNT Inc., which is helping lead Hacking 4 Allies, told *National Defense* the two countries have mutual problems within their defense and commercial sectors.

"Because of Norway's unique positioning, it's easier to recognize the problem for what it is in Norway, and then find and identify where that problem presents itself in the United States," he said.

Eight startups based in Norway will be trying to put their products into the hands of defense personnel both in Washington and Oslo to solve the nations' shared obstacles. The products each company specializes in are diverse — including artificial intelligence, electronic blank ammunition, cybersecurity solutions and robotics.

Norway's defense industrial base is extremely niche compared to the rest of the world, explained Torbjorn Svensgaard, CEO of the Norwegian Defence and Security Industries Association. The country's specialized technologies could fill gaps in larger defense markets such as the United States, he said.

During the selection process, Tore Helland, senior advisor at the Norwegian Defence Research Establishment, said each startup's product was evaluated based on whether it could be beneficial to both U.S. and Norwegian defense sectors.

"I think that makes the companies selected … a mixture of the personalities needed to succeed," he said. "They have the technology that is interesting and can be used, and they now have a market that is bigger than their regional market."

The program will largely take place at BMNT's H4XLabs facilities, a business accelerator that works one-on-one with clients and helps them enter the U.S. market. The Norwegian Defence Research Establishment and the Norwegian-American Defense and Homeland Security Industry Council will also be involved in increasing the chosen companies' presence in the United States.

The groups will teach the companies how to find opportunities in the United States and strengthen the relationship between Norway's industry and the U.S. economy, according to a news release.

A key element of the program will be helping startups navigate the complex Pentagon acquisition process by "attacking the bureaucracy that prevents innovation," Newell said. The organizations want to help companies find a variety of pathways into the market, including with other transaction authority agreements, he said.

"It's yin and yang — we're working both sides of the fence," Newell said. "At this end, we're making sure they're highly qualified candidates with [products] with problems attached to them that are worth the time. At the same time, we're working with the government to make sure its platform is adequately built to actually be a better partner with them." **- ME**

iStock illustration

AI to Reduce Litter Swaying During Helicopter Rescues

■ Artificial intelligence may soon assist the Army with critical helicopter rescue missions.

Colorado-based company Vita Inclinata Technologies sold 15 rescue systems to the Army at the end of 2021 to undergo trials at the Aeromedical Research Lab in Fort Rucker, Alabama. The attachment will make emergency rescues safer and easier for soldiers, said Derek Sikora, chief technology officer and co-founder of Vita.

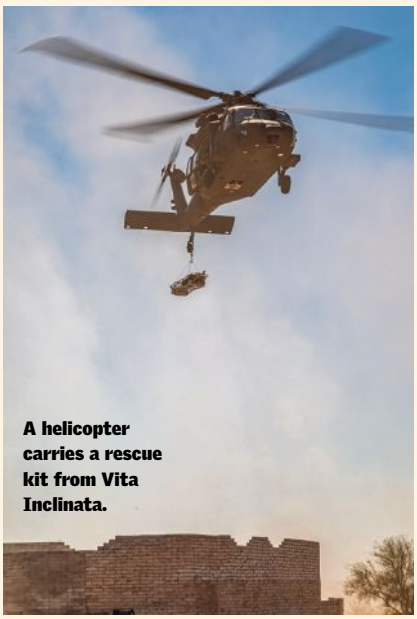
The system is made up of a rescue litter and a battery-powered hoist that attaches to rotary-wing aircraft. The hoist uses sensors and computers running algorithms to determine the best action to reduce the spin, swing and sway of items it is carrying.

Being lifted into the air by a helicopter is not easy, Sikora said. Rotary-wing platforms — which often weigh 15,000 to 20,000 pounds — hover off the ground and generate buffets of air that easily push and pull what is hanging below them.

Typically, "it's this complex situation that requires this person on the ground, coordinating with the person on the line and … also coordinating with the aircraft," Sikora said. "It's just complexity that doesn't need to be there."

With Vita's system, all a soldier has to do is flip a switch, Sikora said. This also means the device is relatively easy to train on for operators. However, there is also a manual option for the system.

Air rescues can be dangerous. While hovering, helicopters are at their most exposed in contested environments, so speed and accuracy matter, Sikora explained.



A helicopter carries a rescue kit from Vita Inclinata.

"If you can reduce the time that an aircraft is hovering … that is just game changing for how we get our warfighters out of a combat situation," he said.

The Army has been working with Vita on the system for more than three years with a cooperative research and development agreement that allowed the company to garner feedback directly from warfighters, Sikora said.

Now, the service wants to ensure the systems can withstand the harsh environments soldiers operate in through trials such as high-altitude and maritime testing, he said.

Army National Guard units and active duty combat aviation brigades will also evaluate the systems.

The technology is also headed abroad. The company sold one system to a defense organization in Japan and is in talks with rescuers in Australia and Europe, Sikora said. **- MR**

Vita Inclinata photo, TeleDyne FLIR image

Augmented Reality Tech Maps Chem-Bio Threats

■ Future warfighters could know where chemical, biological and radiological threats are located without ever stepping foot on the battlefield.

Teledyne FLIR announced it won a $15.7 million contract in December to develop augmented reality software that can pinpoint chemical, biological, radiological and nuclear, or CBRN, threats and map them for the military. The contract was awarded by the U.S. Defense Threat Reduction Agency's Joint Science and Technology Office.

For reconnaissance and decontamination missions, a remotely operated vehicle would first move through an area where hazardous materials may be present and collect data using sensors, said Jeremy Walker, the director of science and technology for the company's Pittsburgh location.

That data is then digitally registered and used to create an AR display of the area that highlights dangers, he added.

"As they're moving through that space, they're seeing these heat maps of where things were detected and what they are," Walker said. "Once that data is captured by that tip of the spear reconnaissance mission, then many other subsequent users … can use that data to do their mission better."

The mapping and AR technology will be integrated into the military's Tactical Assault Kit suite of tools, which could be a mobile phone or tablet. Mixed reality headsets, like the Integrated Visual Augmentation System, are also an option, Walker said.

"All those people farther back don't necessarily have to have sensors in their hand to know where the threat is to be able to do their work," he said. "You've got this tool that helps people intuitively interact with it so they can keep their hands free to do other things."

As it develop the technology, Teledyne FLIR's Pittsburgh lab will be looking to work with existing and new partners in augmented reality and 3D-mapping spheres to help build the software, he said. **- ME**

SAIC Emphasizing Digital Engineering for JADC2

As the Pentagon moves forward with its effort to connect the military's sensors, shooters and command elements into a single network, industry partners want to lead the way with digital engineering.

Information technology company Science Applications International Corp. demonstrated how digital engineering could be used for the military's joint all-domain command and control concept, also known as JADC2, during the National Training and Simulation Association's most recent annual Interservice/Industry Training, Simulation and Education Conference.

The demo highlighted how digital engineering strategies can allow the military's decision makers to act more quickly and efficiently against threats, said Jeff Raver, business development director of SAIC's naval business unit.

Digital engineering is an integrated approach that uses models and other computer resources to execute traditional engineering tasks, from design to experimentation of products.

SAIC's digital demonstration featured a simulation of how JADC2 could operate using digital engineering strategies. As an example, it depicted a coordinated effort between U.S. Space Command and high-altitude satellites, drone technologies and a Navy submarine to identify and eradicate a threat, Raver said.

By leveraging digital engineering, users have the ability to quickly ensure different types of data are configured and referenced together so that they can be communicated effectively between systems and organizations, he explained. It can also speed up the validation of data and the resolution of discrepancies in information.

The company is under contract with the Air Force and Navy to advance each branch's respective versions of the network.

While he acknowledged that transitioning to more digital-focused engineering can come with a high price tag, Raver said a more cost effective option is possible.

"This doesn't have to be an all or nothing," he said. "Our customers can implement elements of the digital engineering solutions incrementally that would allow them to sort of move down this pathway to advance toward the more digital environment without having to bite off the entire elephant all at once."

However, Raver predicted that soon the term "digital engineering" will disappear from the lexicon.

"Digital engineering is going to become engineering," he explained. "This idea of using legacy, paper-based, disconnected systems for engineering solutions and complex environments — it's just not going to be sustainable." **- ME**

Army to Ramp Up Testing For Cyber Weapons

As the Army sharpens its cyber capabilities, the service is planning to increase its capacity for training and simulation at its facilities across the nation.

Task orders for the National Cyber Range Complex support contract will start dropping shortly, according to BAE Systems, one of the companies that was selected for the contract.

The firm is helping the Army look toward the future, including initiatives such as joint all-domain command and control, or JADC2, said Dan Snowdall, a program manager at BAE.

JADC2 is the Pentagon's ongoing effort to connect sensors and shooters at the tactical edge. That connection will give the military decision dominance — but not if the flow of data is exposed to cyber attacks, Snowdall said.

"If you don't start at the impetus of a weapon system … and seeing that weapon system is protected, then you're going to build something that's going to be vulnerable and will always be vulnerable going forward," he said.

The National Cyber Range Complex "will consist of an integrated and interoperable constellation of facilities designed to enable the planning and execution of large-scale, complex and distributed cyber training and evaluation, training and mission rehearsal events," according to the Army's program executive office for simulation, training and instrumentation.

The contract will enable cyber event planning, design, engineering, execution and infrastructure maintenance at centers that host the simulated cyber network.

Two Estonian defensive cyber operators train on the National Cyber Range during U.S. Cyber Command's CYBER FLAG 21-1 exercise.

Increased testing and training for U.S. cyber forces means that leaders will have more trust that their equipment can withstand cyber attacks, Snowdall said.

The military has grown more concerned with cyber threats in recent years. For example, the SolarWinds hack that exposed government organization's data prompted the Defense Department to hold its largest ever multinational cyber exercise in November.

Though the company has not yet received specific directives for the contract, Snowdall said BAE Systems' approach to the Army's solution is holistic and uses model-based engineering.

"When we start something, we're going to model it up," he said. "We're going to test it and do iterative steps throughout to ensure that at the end, we're actually answering that customer requirement."

The contract supports four new facilities for the cyber complex including in Orlando, Florida, and Charleston, South Carolina, according to PEO STRI. **- MR**

SAIC image, Defense Dept. photo

Pentagon Shakes Up AI, Digital Bureaucracies

■ In December, Deputy Secretary of Defense Kathleen Hicks made waves when she issued a memo announcing the creation of a new key role that would report directly to her: the chief digital and artificial intelligence officer.

The individual selected for the position — which was slated to become effective Feb. 1 — will oversee three critical Pentagon offices: the Joint Artificial Intelligence Center, Office of the Chief Data Officer and Defense Digital Service. As of press time, the Pentagon had not announced who had been chosen for the role.

"The department has made significant strides in unlocking the power of its data, harnessing artificial intelligence and providing digital solutions for the Joint Force," Hicks said in the memo. "Yet stronger alignment and synchronization are needed to accelerate decision advantage and generate advanced capabilities for our warfighters."

The official in the new position, also known as CDAO, will be responsible for strengthening and integrating data, AI and digital solutions within the Pentagon, Hicks said. The office is expected to reach full operating capability by June 1.

Officials and experts say the move will help the Pentagon accelerate its adoption of AI and other digital technologies.


Kathleen Hicks

"It's going to allow us that stronger alignment to really accelerate into the future in a more formal manner," the Pentagon's Chief Data Officer David Spirk said during a media roundtable hosted by George Washington University's Project for Media and National Security in January. "I don't view it as a bureaucracy — if anything, I think the establishment of this activity knocks down some bureaucratic walls because it puts all of us under one vision."

The shakeup shows that the Pentagon is doubling down on a data-driven future and ensures that today's focus on data management isn't just a passing fad, he said.

Retired Air Force Lt. Gen. Jack Shanahan, former head of the Joint Artificial Intelligence Center, said the creation of the position is a natural evolution for the Defense Department.

"This is the next important step of three different organizations that have been working toward similar ends, but not always aligned as closely as they could have been," he said. "Not only are the three organizations interrelated, they are intertwined in that they all deal with the same big problems the department has with software, with data, with AI, with emerging technologies."

Shanahan — who retired from the Air Force in 2020 and is now an adjunct senior fellow at the Center for a New American Security — said there is an opportunity to create fewer administrative burdens within the Pentagon, especially for Hicks who had three disparate organizations reporting to her.

The individual who is selected will have the opportunity to make an enormous difference for the department, he added.

"It's never about one person, but the person who they select will have to have the trust and confidence of not just the deputy, but the secretary of defense, the chairman [of the Joint Chiefs of Staff], the vice chairman, the services and the combatant commands," Shanahan said. "It's a really important decision."

Rather than go with a three-star general — as the Pentagon did with its appointments for the JAIC, including Shanahan and his successor Marine Corps Lt. Gen. Michael Groen — for the role, the department should pick someone that has exceptional technology credentials and experience in Silicon Valley, Shanahan suggested.

"You're trying to take a Department of Defense — which is a hardware company from the industrial age — and begin this massive transformation into a software company in a digital age," he said. "That requires someone that understands how you do this in the commercial world."

However, the Pentagon will also need a deputy CDAO that understands very well how the bureaucracy of the Defense Department works.

"It is hard work as I learned over and over again in my time in the Pentagon, to work through budget battles, to work through processes, to work through human capital issues," he said. "You need someone that can work that system, that knows people in the inside of the building that can walk the corridors, meet and greet people and say, 'This is what we really do.'"

Right off the bat, the CDAO will have a lot on their plate, Shanahan noted. On day one, the official will need to take a survey of what's out there and what still needs to be done in the department, he said.

They will find that "we still have a whole lot of work to do," Shanahan said. "Where does it begin? We treat AI as a single thing. Sometimes we treat it as sort of magic dust — it's not. It requires a lot of work across what we call the 'AI stack.' And there are so many elements that have to be addressed."

Critical to the success of the new officer will be obtaining the right authorities from Congress, he noted.

"It's going to take some real groundwork behind the scenes with staffers and members to get it right," he said. If lawmakers understand "that the only way you get this right is putting the authorities and responsibility in the form of one person, they will do it. It may be hard work to get there, but I think what you will see is they're willing to do it because it's that important." **ND**

Defense Dept. photo

Innovation Does Not March — It Calls Cadence

■ "No answers exist in these walls." This is a mantra taught in the National Science Foundation's Innovation Corps, or I-Corps. The statement seems simple, but its gravity is profound. The I-Corps program teaches academics and entrepreneurs about lean startup techniques and how they can be used to de-risk a startup long before years and millions of dollars are spent.

The lessons from I-Corps along with many others from the lean startup community are prescriptive for modern defense innovation and acquisition, and may provide insights for the Army and the broader military acquisition ecosystem.

Perhaps the first lesson is that innovation should solve a problem. A cynical view might suggest that deploying a new weapon system has nothing to do with a Silicon Valley lean startup method. One might argue that weapon systems hold to their own unique ecosystems and purpose. However, abstract away all the complicating factors and the naked problem remains. The magic of modern innovation frameworks reveals itself when one views the weapon system as a response to a customer problem, which in this case happens to be a military problem.

Given the recent surprise launch of the Chinese hypersonic delivery platform, it is with a sense of irony that in the technology innovation ecosystem, a breakout success is called "escape velocity." However, this term based on the U.S. lunar program suggests the mindset in the civilian innovation ecosystem.

Escape velocity is the concept that the innovation, either through its merit or execution, cannot be matched by market forces, competitors, or otherwise. This approach allows for groundbreaking innovation, the revolutions in innovation that are "capital-I innovation" and give such a profound advantage that the competition sees it as insurmountable.

Now consider a specific application such as long-range precision artillery fire. The customer, the battlespace owner, has several problems to solve. It needs to effectively engage the adversary earlier and before the adversary can engage the battlespace owner. Further, the owner needs precision, owing to the economy of force principle. This problem set is not new. Rather it is one any commander would be familiar with. For example, Mehmed the Conqueror would have faced it as he aimed his large artillery at the fortified walls of Constantinople. This advent represented a capital-I Innovation: reliable fortification defeat by artillery.

Over time, innovators and foundries met this defend-attack problem set with larger cannons, thicker walls, new powder formulations and angular defenses, to name a few. This model of incremental innovation carried cannon development forward for nearly 450 years until another capital-I Innovation occurred with the French development of the hydro-pneumatic recoil mechanism. This innovation changed combat going forward. Commanders could quickly and accurately put more rounds on target than ever before and reliably mount guns on moving platforms. This innovation led to further developments in long-range precision fires and armor that were never possible previously.

This changed the face of battle as we know it today.

While the battlespace evolved considerably between the two advents, both represented capital-I Innovation and shaped subsequent combat. Both had problem sets that commanders and innovators solved by applying newly available practices enabled by technology. When asked what the problem set was for both cases, it is likely a commander would have stated it was indeed long-range precision fires. Neither invention would have likely existed if the innovators had not integrated practices and technologies outside of their known military capabilities. They did not invent something completely from nothing. Rather, they synthesized a novel application — in this case a military application. Innovation did not march, but rather, called cadence, and commanders had no choice but to listen.

Regardless of what lean innovation framework defense innovators employ, there is a common element in all civilian frameworks that is instructive to follow. All frameworks take this problem-back approach to understand and empathize with the customer problem. Whether it is called "jobs to be done," "unique value proposition," or simply "problem," it does not matter.

It is the empathy with the customer problem that matters — getting into their workspace and feeling the customer problem firsthand. It requires humility of the innovator to understand that their solution may not solve the problem.

To pose a solution and seek a problem is called solution fitting and rarely solves the issue as effectively as a pure problem-back approach.

These frameworks abstract the problem away from the known constraints. Abstraction like this allows for innovators to look at the problem set without the anchors or distractors of what has been done before. This helps overcome the status quo bias. Innovation can occur with a status quo bias, but it tends to be incremental and safe — no reason to disrupt what was done in the past. However, for capital-I Innovation the status quo bias must be minimized.

As Steve Blank wrote in *The Startup Owner's Manual* and Dan Olsen highlighted in *The Lean Product Playbook* — and now wholly incorporated in the I-Corps program — there are no answers in these walls. To really understand a problem, innovators must talk to customers. What does that mean for the Army and defense? Who is the customer?

Defining the customer is not easy. First, it is important to understand what a customer is. In the classic definition, it is one who will exchange something of value for a product or service. In defense applications this definition is not quite as straightforward. One could argue that it is the taxpayer that is the ultimate customer for defense, but that simplifies the definition too much in a military problem set context.

Perhaps commanders are the customer, as they are the ones interested in the outcomes produced by a weapon system. For purposes of defense applications, the definition becomes

iStock illustration

broader as it likely includes the soldiers deploying, sustaining and using the weapon systems. Together they all make part of the chain that realizes the value of the weapon system and outcomes that the taxpayer desired for the nation's military might.

In applying the "no answers exist in these walls" mantra, it is these customers that innovators need to be talking to and understanding their problems. The innovator should look for ways to address their problems in an integrated approach, because no warfighting function exists in a world unto itself. These customers understand the problem set at a visceral level that no PowerPoint slide deck can capture in a headquarters briefing room.

The unique aspect of defense and battlefield applications complicates the lean approach of understanding the customer problem and delivering a solution.

Nearly every new practice enabled by technology has long-chain effects, whether supply or command and control. Defense innovators need to be sensitive to ripple effects and solve the problems that arise from new innovation, whether incremental or capital-I Innovation. Here, history is instructive. Even the great recent innovators like Steve Jobs and Elon Musk did not single-handedly solve all the long-chain problems introduced by their innovation. That is the purpose of a team.

Getting out and talking to customers is revealing. Innovators will quickly learn if customers share their perceptions of the problems and, more importantly, the ground truth. It allows innovators to test hypotheses and pivot before costly investment into systems or ventures goes too far.

The soldier touchpoint for any program is a revealing moment that often comes too late as a defense system developer found when a soldier asked why the test system could not be as easy to use as the soldier's phone.

Defense innovators should take these modern innovation frameworks to heart and engage their customers as early and as often as is feasible.

Talking to customers is as much art as it is science. Henry Ford famously quipped, "If I had asked people what they wanted, they would have said a faster horse." Whether apocryphal or not, it drives the point that innovators must take customer feedback as directional, not as a destination.

Applying data science to customer interviews and looking for the underlying themes and messages are how many big tech firms guide product innovation. The call center has become these companies' greatest data mine for insights because it concentrates the problems customers are dealing with. A defense innovator may find the dining facility or wash racks equally productive.

Unlocking value through innovation is not easy. There are whole virtual communities in high-tech dedicated to innovation and lean product development. This community of practice approach may be instructive for defense innovation.

Innovation is stubborn and refuses to give up its secrets to those not willing to work hard, and innovation certainly does not march upon order. Rather it must be cultivated.

The defense industry and the military services can learn a valuable technique in talking with the customer to understand the customer problem deeply. That will lead to innovation and developing solutions that solve those problems more quickly than happens today.

For when innovation calls cadence, we all march. **ND**

Maj. Ray K. Ragan serves as an Army Reserve officer, with combat tours in Iraq and the Philippines and multiple mobilizations around the world. He currently is an innovation officer with the Army 75th Innovation Command and leads the Arizona Tech Scouting Team.

Viewpoint BY GENTRY LANE

Major Cyber Attacks Not the 'New Normal'

■ Cyberspace is the only warfighting domain in which daily degradation of critical assets is tolerated. This tolerance is not born out of willful indifference, but out of willful engagement in a losing battle due to lack of strategic response.

The scale and scope of advanced persistent threat-perpetrated aggression is beyond existing surveillance and incident response capabilities of any one nation. Despite America's technical advantage and consequential fighting force, it is and will always be outnumbered in the cyber domain. However, "always outnumbered" is not necessarily a decisive disadvantage. Military history is replete with smaller forces overcoming larger ones to achieve mission success.

The imbalance of power should be the leading factor when evaluating engagement strategies, but this is not currently the case. Instead, priority is given to triaging obvious insufficiencies in lieu of developing a viable asymmetric battle strategy. This approach yields stopgap solutions, piecemeal strategy and continued unencumbered success for adversaries.

Despite doctrine issued from both the Defense Department and the White House, the United States does not have a cohesive, sustainable strategy to efficiently deter nation-state aggression nor to adequately defend critical assets.

"Persistent engagement" and "defend forward," the two pillars of the current cyber national security strategy, are lines of effort unviable as standalone strategies. While both gambits yield intermittent efficacy in shaping adversary behavior, there are limits to their effectiveness. Given the escalating sophistication and scale of malicious cyber actors, scaling these lines of effort in a sustainable way is not possible.

Unfortunately, effort and budget continue to be allocated to the low hanging fruit and triage initiatives: establishment of norms and redlines for adversaries who flout international humanitarian law; initiatives that only incrementally increase the cybersecurity workforce; innovation programs that yield few results; and vague vows to increase resiliency. These initiatives fall short of the kind of strategic thinking and cohesive, sustainable, strategy development that the current situation requires.

These efforts are misaligned because the objective is unclear. The desired end-state has yet to be defined in the context of comprehensive strategy.

Further confounding the disorganization is a lack of consensus on the current state of affairs. There is no doubt among adversaries that they are each engaged in effective, active conflict on American soil, yet American authorities are still discussing where on the conflict continuum cyberattacks rank.

Adversaries are fighting — and winning — and we can't decide if we're in cooperation, competition, or conflict. The disconnect is stark.

The ultimate authority for strategy development is nebulous given the number of military, law enforcement, civilian, homeland security and diplomatic stakeholders who have equity in the cyber conflict at hand. Defense leaders articulate disparate goals. "Collective defense," "integrated deterrence" and "strategic stability" are neither aligned nor have they been built out beyond catchphrases into comprehensive strategies. Responsibility and negligence for the lack of a fully developed strategy lay somewhere, but it isn't clear where.

Regardless of who leads a strategic response, resilience and defense alone are inadequate. Even the most viable defense strategies necessitate prolonged engagement in a resource-intensive battle to maintain a status quo in which the best outcome is a condition of precarious security. This begs the questions of what exactly are the desired ends and what are we willing to sacrifice to achieve them? A defeat strategy has a high likelihood of escalating into traditional armed conflict and a coercion strategy is de-escalatory, but there is currently no authority engaged in the composition of this unprecedented and complicated effort.

To reset security conditions that favor the United States and its allies, conflict resolution must occur and result in a condition in which the nation is not restricted to a persistently defensive posture.

However, as in any conflict, the adversary has a vote in the direction of this current one. For the major threat actors, cyber aggression is a highly effective way to achieve their mission of degrading U.S. power and economic and institutional stability. It is reasonable to assume that they do not desire resolution and prefer to continue offensive operations.

De-escalation via coercion is a viable strategy for conflict resolution with favorable conditions. Taxonomic classification divides coercion into two main types: compellence and deterrence. Compellence requires a significant direct action or credible threat of action — which in this case could be singular or combined consequential military, economic, or diplomatic actions — that compel the adversary to abandon their U.S.-targeted offensive cyber operations. Compellence could be perceived as provocative by the major threat actors and yield an unintentional escalatory response. Given the high level of economic and trade entanglement with China — and Russia's historic volatility and perceived willingness to engage in kinetic conflict — compellence is not a viable resolution strategy for the current cyber conflict.

Deterrence also can be delineated into two types: "deterrence by punishment" and "deterrence by denial." Both forms are de-escalatory by nature because they are collaborative and afford the adversary agency. Deterrence by punishment presents a credible threat of strong punishment to deter the adversary from taking an unwanted action. The clumsy, unco-

ordinated efforts currently in place are the application of deterrence by punishment. The full gamut of punishments — such as sanctions, public naming/shaming, criminal prosecution and tacit threat of an armed response — have been applied, but they have done little or nothing to deter a state of persistent aggression.

Deterrence by denial deters unwanted aggression by rendering adversary offensive operations impossible or unlikely to succeed, thus negatively impacting the adversary's cost-benefit calculus and prompting prioritization of other opportunities with higher likelihoods of success.

But the application of deterrence by denial in the cyber domain manifests differently than it does in traditional warfighting domains. Deterrence by denial on land, air and sea often rely on a level of impenetrability that is neither practical nor achievable in the cyber domain. The attack surface in cyberspace is simply too big, too complex and too dynamic to adequately secure without impeding the free flow of information or denying the right to reasonable privacy.

Effective deterrence by denial in cyberspace may eschew impenetrable resilience and permit the breach of lines of defense, but reliably denies operations at some point in the kill chain before mission success can be achieved.

Deterrence by denial has never been applied in the cyber domain, nor has any cohesive battle strategy. The value in the de-escalatory nature and also the collaborative aspect of deterrence by denial cannot be underestimated in multinational conflict resolution. Allowing the adversary agency to determine and decline engagement by their own volition is key to sustainability. Without adversary buy-in, sustaining the achieved ends is precarious.

The unique features of this nascent warfighting domain — an ephemeral, binary battlefield that traverses all other warfighting domains as well as civilian, governmental and international environments — offer advantages and constraints that have yet to be studied, let alone tested. As the primary architect and provider of internet infrastructure, the United States has inherent advantages. Full strategic, tactical and operational exploitation of these advantages is essential in the development of strategy, but this knowledge remains siloed among operational teams in intelligence agencies and far from the offices where military strategy development occurs.

Understanding the gaps in technological capabilities required to achieve coercion is crucial. Currently, there are no commercial off-the-shelf or government-bespoke solutions that reliably deny mission success. Timely, deep situational awareness over civilian critical infrastructure is currently unavailable to any security authority. The lack of traditional visibility and latency in determining conclusive attribution is an adversary advantage that can and must be removed.

None of these deficits are technologically insurmountable, but without understanding and acknowledging that these capabilities are required for cyber conflict resolution, resources for their realization will never be prioritized. Nor will these capabilities be valued or recognized as essential when they do appear.

While the adversary's capabilities are advancing, their capacity is subject to constraints. Aggregate analysis of advanced persistent threat behavior over time shows an intentional focus on critical infrastructure assets and the software supply chain that affords access, indicating limited capacity that necessitates prioritization.

Adequate surveillance and incident response capabilities for the several hundred-thousand public and private entities that comprise critical infrastructure is possible, but the programs in current use are deficient. The technology that powers them is clumsy and verging on outdated. And the programs themselves are subject to suspicion by the assets they are meant to protect. It's essential that authorities instill confidence and engender trust in civilian sector partners to successfully execute a conflict response. The current government-provided monitoring technology, and slew of fusion centers and collaboration centers, have done little to engender trust and continue to deliver subpar results for both private and public stakeholders.

The impunity which adversaries currently enjoy is not a permanent feature of the cyber domain. Major cyber attacks on civilian assets do not have to be the new normal, nor can they be without significant compromise to the American way of life. Lack of stability in the cyber domain undermines power projection in all warfighting domains and standing in the liberal world order. Lack of domain dominance hinders the ability to strike at the time and place of America's choosing in all warfighting domains. The risk of intentional or inadvertent catastrophic failure of critical functions or significant compromise to force readiness is too high.

Until a clear end is defined, authorities are deconflicted, and the myopic focus on triage is eschewed in favor of resources allocated toward the composition of a viable coercion strategy, adversaries will continue to exploit the disorganization and draw the United States further into a quagmire of resource attrition. This current level of aggression is not sustainable and certainly on an escalatory trajectory. A cohesive, sustainable, equitable, coercion strategy that leverages all diplomatic, informational, military and economic institutions and elements of power, creates a coalition of allies, implements viable technology, and aligns incentives for private sector collaboration that are required to resolve the current state of conflict.

Perpetual cyber conflict engagement is futile, expensive and does not yield a secure end-state. And further pursuance of misaligned, Sisyphean efforts is not in the best interest of the country. ND

Gentry Lane is the CEO and founder of ANOVA Intelligence, a venture-backed cyber national security software company. She is also a fellow at the Potomac Institute for Policy Studies, a visiting fellow at the National Security Institute at George Mason University's Antonin Scalia Law School, represents the United States on a NATO science and technology panel and is a consultant with NATO Allied Command Transformation.

iStock illustration

Silicon Valley Takes on the 'Valley of Death'

BY JON HARPER

SIMI VALLEY, Calif. — The commercial technology sector wants to help the U.S. military acquire new capabilities. But if the Pentagon doesn't change the way it does business soon and help innovators bring their products across the "Valley of Death," they will go belly up or walk away, industry and military leaders are warning.

The Defense Department has launched a slew of initiatives in recent years aimed at expanding its innovation base and bringing startups and nontraditional companies based in Silicon Valley and elsewhere into the fold. But there's a problem — promising technologies still often fail to move beyond the research-and-development phase and into large-scale procurement. The phenomenon is known in defense acquisition circles as the Valley of Death.

The problem — and the need to fix it — was front and center at the recent Reagan National Defense Forum, the annual confab of national security elites in Simi Valley, California.

"Let's face it. For far too long, it's been far too hard for innovators and entrepreneurs to work with the department, and the barriers for entry into this effort to work with us in national security are often too steep — far too steep," Secretary of Defense Lloyd Austin III said during his keynote address.

"Let's say some great California startup develops a dazzling way to better integrate our capabilities. All too often, that company is going to struggle to take its idea from inception to prototype to adoption by the department," he added. "We call this syndrome the Valley of Death, and I know that many of you in this room are painfully familiar with it."

The phenomenon deters some innovators from ever trying to do business with the Pentagon, he noted.

Undersecretary of Defense for Research and Engineering Heidi Shyu said there isn't a dearth of high-tech firms that want to work with the military.

"Looking around in terms of number of companies, I don't see a shortage of innovation. Where I see the problem is they get seed money to develop designs and prototypes, and they die on the vine, because our acquisition system is too rigid," she said during a panel at the forum.

As an example, Shyu noted her recent visit to a small business in Santa Monica, California, working on what she dubbed a "superb product."

"They said, 'We're running out of money,'" Shyu recounted without identifying the company. "I said, 'Hello, you're just telling me today? You think I have a bank account I can open up and give it to you tomorrow?'"

"That's the problem," she continued. "They have venture capitalists that are interested in putting funding in them [but only] if they have production contracts. So, it's the Valley of Death. They have a design, the prototype won't be ready for another year and a half, right? So I'm … trying to figure out how I can find them some money to bridge them over."

There are two key metrics for assessing the Pentagon's relationship with the national security innovation base, said Air Force Chief of Staff Gen. Charles "CQ" Brown Jr. One is access to innovators, and the other is the ability to transition desirable capabilities into large-scale production.

"The access is actually pretty decent and pretty good. So, a lot of dialogue and discussion. But the transition is where we fail and fall really short," he said.

There's a lot of excellent innovation on one side of the Valley of Death. "We just can't get it to the other side of the valley and scale it," he added.

In recent years, the Pentagon has ramped up its use of other transaction authority agreements after Congress passed legislation in 2015 and 2016 encouraging their use. OTAs are intended to cut through bureaucratic red tape associated with the Defense Department's more traditional acquisition processes and facilitate rapid prototyping and follow-on production. The total value of OTAs awarded in 2020 topped $16 billion, according to decision science company Govini.

However, production OTAs account for just a tiny fraction of total OTAs awarded, according to the Center for Strategic and International Studies. The vast majority are for R&D and prototyping.

Additionally, projects initiated under the Small Business Innovation Research program, which Austin said the Pentagon is "doubling down" on to help small companies work with the department, often struggle to find funding after they reach the end of their SBIR Phase 2 contracts because they are not connected to a program office, officials have noted.

Nevertheless, the Pentagon has had some successes in helping nontraditional firms get their technologies across the Valley of Death. For example, in 2020 the Defense Innovation Unit — which is based in Silicon Valley and has outposts in other commercial tech hubs around the country — facilitated the transition of 11 successful commercial prototypes to other Defense Department agencies for large-volume procurement. From its inception in 2015 to 2020, the organization successfully transitioned a total of 26 commercial solutions, according to DIU.

But much more needs to be done, industry insiders say.

"Time is running out with Silicon Valley," warned Katherine Boyle, general partner at venture capital firm Andreessen Horowitz, also known as a16z, which is based in the region.

"After five years of DoD saying, 'We

want to work with the best startups,' we have, at most, two years before founders walk away and private capital dries up. And many, many startups will go out of business waiting for DoD to award real production contracts," she said in a tweet storm when the Reagan National Defense Forum kicked off.

"Experienced founders and investors know that until you have a production contract, these [other awards] are … little door prizes," she added.

Billions of dollars in venture capital have gone to defense-focused companies, but the Defense Department is dropping the ball, according to Boyle. That has implications for the workforce.

"Early-stage startups are waiting, and many will languish after getting OTAs and pilot contracts that felt real but weren't," she said. "While investors will give a handful of these companies the benefit of the doubt, you're going to see talented, hard-working teams go bankrupt and head back to Facebook and Google."

To address the problem, the Pentagon needs to award production contracts to "the most important startups with the teams who've proven they can build,"

she said. "These don't have to be big contracts. But they have to be real production contracts that show founders and investors that DoD is serious."

The Defense Department also needs to change the "culture" of procurement, Boyle said, noting that acquisition officers face blame if they bet on a startup and it doesn't pan out. Instead, officials should be incentivized to work with venture-backed startups that can create technologies that warfighters need, she argued.

iStock photo-illustration

The Pentagon can't continue with business-as-usual as adversaries roll out new high-tech capabilities, Boyle warned.

"The future of American national security depends on us finding a way to solve this procurement crisis," she said.

Joe Lonsdale, co-founder and managing partner at venture capital firm 8VC, said investors need to see results if they are going to keep bankrolling companies that are trying to work with the military.

"There's a lot of money that has gone to work in the venture capital ecosystem the last three, four, five years, in part inspired by a lot of these smaller programs that have helped get things going," he said.

Investors want to know "is this an area where people can actually make money?" he added. "A lot of people have a lot of minor work. And so far, we haven't seen the big wins. … It is a critical moment to figure this out."

Contributing to the problem is what Lonsdale described as a "lack of courage" in the Defense Department when it comes to picking winners and losers in the commercial tech sector.

Brown said the Pentagon needs to select some key programs and shepherd them across the Valley of Death to encourage organizations in the innovation ecosystem.

"When they get to the other side of the valley, we've got to continue to nurture them to show some success because if we don't do that, then I really believe all that venture capital is just going to walk," he said. "They're going to find someplace else to go."

Marine Corps Commandant Gen. David Berger said he is already hearing anecdotal stories of companies bailing.

"Two of the CEOs that I know that I talked to, I asked them, 'How's it going you guys?' They said, 'It's bad,'" Berger told reporters at the forum. "They're going to take their money and go do commercial stuff because they can't see where the return on investment is going to be. … That worries me."

Shyu said problems associated with the Pentagon's planning, programming, budgeting and execution process, known as PPBE, is hindering the department's ability to quickly deliver promising capabilities to warfighters.

Her office is planning to conduct a rapid joint experimentation campaign with products from innovators that combatant commanders are interested in. The hope is that they can move to rapid fielding. But in the past, that has been a challenge because "there's no transition budget," she said.

"Let's say the [combatant commands] love that capability and they want it. … Well, I have to go back to the service and say, 'Did you POM for that?'" Shyu said, referring to the program objective memorandum that lays out multi-year plans for resourcing projects.

The 2022 National Defense Authorization Act recently passed by Congress directs the establishment of a new commission tasked with comparing the PPBE process of the Defense Department with similar processes of private industry, other federal agencies and foreign nations, and making recommendations for improvement.

In the meantime, Shyu is asking for some "bridge funding" to get systems across the Valley of Death, although she didn't disclose how much money she's seeking.

"This is something that I've got to work internally within the DoD and I've got to work with the Hill because they want to … count every penny that we have," she said.

Rep. Ken Calvert, R-Calif., ranking member of the House Appropriations defense subcommittee, has a plan to mitigate the Valley of Death.

"The U.S. government has been a lousy partner, quite frankly," he said. "We get companies and we waste their time … and then we're wondering why we're not getting the technologies we want."

Calvert wants to create a new "innovation fund" through the appropriations process.

"Start out, say, with about $100 million, and then we can pick a number of people that we want to succeed and get them through that Valley of Death where they can actually get to procurement," he explained.

"I'm going to work with my friends on both sides of the aisle and the Senate" to set up the fund, he added. "I'm hoping that we can do that as soon as possible." ND

U.S. Still Playing Catch Up In Information Operations

BY STEW MAGNUSON

It has been more than 20 years since 9/11, when the United States acknowledged that it had allowed its once formidable information warfare and strategic messaging capabilities to lapse into a state of decline.

At the time, al-Qaida was proving on a daily basis that it could effectively use modern day tools such as the internet to spread its anti-Western propaganda. The U.S. government had little capacity to counter radical Islam's messages after allowing its skills to atrophy at the end of the Cold War.

Two decades later, the Joint Chiefs of Staff's point man on cybersecurity and information operations said little progress has been made.

"I'm not sure how much has changed, other than we continue to watch … our adversaries demonstrate tremendous competence in this area," Marine Corps Lt. Gen. Dennis Crall, director of command, control, communications and computers/cyber and chief information officer, Joint Staff, J6, said at the National Defense Industrial Association's Special Operations/Low Intensity Conflict conference held in Washington, D.C.

The last decade has only seen the problem worsen as social media grew in popularity and was then used by Russia to interfere in U.S. elections.

Rep. Mikie Sherrill, D-N.J., said, "We used to do this quite well. This was our mission — winning hearts and minds across the world. That's how we fought the Cold War. That's how we fought communism. And the reason we were so effective at it, quite frankly, is because here at home, we understood it. It was very clear to me growing up that living behind the Iron Curtain would be really the worst of all worlds."

Gavin Sundwall, a career foreign service officer in the office of policy, planning and resources for public diplomacy at the State Department, said, "The competition is fierce. Other actors, China, Russia, Iran are actively competing for control of information environments, and they're well funded. They're putting a lot of money into it precisely because — in the big scheme of things — it's low cost."

Sundwall, who recently served in Australia as minister counselor for public affairs and leader of strategy and affairs, saw firsthand how China was spreading its message throughout the region.

"This is low cost, high value for them," he added.

A State Department strategic resource review recently concluded that U.S. global competitors China and Russia combined invested significantly more than the United States in the competition for public influence, Sundwall said.

Russia spends approximately $1.3 billion annually on broadcast media and strategic communications. China's annual public influence investments exceed $10 billion, "and this is in addition to their robust disinformation and misinformation operations," he said of the two countries.

The State Department's total budget for all public diplomacy and public affairs efforts was $1.44 billion in fiscal year 2021, including funding for cultural and educational exchange programs, as well as public diplomacy programs at U.S. missions abroad, a State Department spokeswoman said.

The terms "information warfare," or "information operations" includes military information support operations that are carried out by special operators.

Sometimes still referred to as "psychological operations," or psy-ops, these specialists use various means to influence local populations or leaders to help combatant commanders achieve certain results on the battlefield.

Strategically, information operations are used by governments to influence populations or other governments.

"Disinformation campaigns" — normally the realm of intelligence agencies — are covert efforts to intentionally spread false or misleading information, according to a policy brief by the Center for Security and Emerging Technology titled, "AI and the Future of Disinformation Campaigns."

Whether it is the State Department, Special Operations Command or the Defense Department, no single agency "owns this space," Sundwall said.

As for the military, Congress mandated that the Defense Department designate a Joint Force provider and Joint Force trainer in the information operations space and build a strategy, Crall said.

"We are grossly late," he said. "It's time to do it now, rather than talk about it, and appreciate and think about it. We need to act," he said.

Combatant commanders too often think of information operations as an afterthought, he said.

"We understand kinetic operations very well. Culturally, we distrust some of the ways that we practice information operations," he said. The attitude is to "sprinkle some IO on that."

Information operations need to be used — as commanders do in kinetic operations — to condition a battlefield, he added.

Special Operations Forces are optimally positioned to lead in this space, but that doesn't mean that it's a SOF-exclusive activity, Crall said. It should be done with military partners, allies and the intelligence community, he said.

"If I were to pick a place to really be the genesis to move this, I would be looking to our special operators to do

that," Crall said.

Sundwall said Special Operation Command's psychological operations specialists should be empowered to take on these challenges as part of the government's interagency information operations.

"We're not as effective when conversations don't take place early on to shape the local environment. And then the train has kind of left the station," he said.

"I've seen it work really well. I've also seen it work not so well," he added.

The State Department has "a robust interagency presence in this space. And we're stronger when we work together," Sundwall said.

The State Department's 183 missions overseas, the ambassadors, their country teams and their communication professionals are a strength that the department brings, he said. "And when they work hand in glove with SOCOM, great things can happen," he added.

Crall said the focus should be on geographical combatant commanders and local experts. Messages shouldn't be crafted in an office in Washington, D.C.

"Do you understand that environment? Do you speak the native language? Do you speak the number of dialects in that area? Do you understand anthropology, religion, history when it comes to context? Many of our messages that sound righteous to us fail miserably when introduced to very specific populations during different times," he said.

Who knows that audience better than those in the region — the combatant commanders, the ambassadors who are there and their staffs, and the intelligence community station chiefs, he added.

Meanwhile, Crall has seen a sharp decline in information operations skills in the military. Those who honed their craft at the end of the Cold War have retired.

"I've said goodbye to them years ago. They've gone on to their second careers, and many of them now are gone. We don't build information experts who have deployed and have experience in areas like we did even a decade ago," Crall said.

Both Crall and Sundwall said if the United States is to take on formidable opponents such as China and Russia in the war of ideas, it can't be done "on the cheap."

Crall said: "This requires an investment. It requires a purposeful investment with a real stable organization, and structure behind it. If it's a pickup game … and it's sporadic and it's not continuous, I think it is where we run into trouble," he said.

Sherrill said, "It's an area where I think we're lagging a little bit, and we really need to do more."

It was appropriate to focus on counterterrorism messaging, but that came at a cost, she said. And that was letting major rivals move ahead in the information operations space.

"I think of it twofold," she said. One is to make sure the American people don't buy into the disinformation campaigns state actors such as Russia are propagating.

The other is U.S. strategic messaging.

"How can we promote our ideals abroad? And how can we make sure that we are winning the war of ideas, and enforcing what we need to do without going into a hot war? ... How are we going to win those, vis-a-vis Russia and China?" she asked.

Crall said some of the needed investment in information operations can go toward technologies such as artificial intelligence.

"What can help us in this is automation. When it comes to looking at content, scoring content, sentiment, everything that's happening out in the web, we can really benefit from a thin AI layer on top of this," he said.

But there are no shortcuts when it comes to cultural expertise. There should always be a human in the loop when making decisions, he added.

Meanwhile, adversaries are beginning to use AI to craft messages, Crall said.

The CSET policy brief said AI and machine learning are poised to amplify disinformation campaigns that are used by state and non-state actors to "shape global opinions, sow chaos and chip away at trust."

Crall said: "A lot of that works. It's not perfect. It doesn't pick the right audience. It's not always constructed properly. And there are obvious things. But as they go, what they're doing, unfortunately, is they're learning. And those machines are learning. And they're getting smarter."

Sundwall said: "We can't do this on the cheap. … We need to get bigger, more robust presence. We need to be able to find ways into conversations with audiences that matter, wherever they're taking place." ND

iStock illustration

The U.S. Coast Guard patrols for illegal fishing activity.

U.S. Fishing for Defense Tech To Protect International Waters

BY MEREDITH ROATEN

The Coast Guard and Navy are exploring new technology and partnerships to protect fisheries from Chinese theft.

Illegal, unreported and unregulated, or IUU, fishing is a growing problem across the world, but particularly in the seas traversed by Chinese ships, according to officials.

Advanced military technologies such as high-resolution radars, spy satellites and data-sharing software is needed to tackle the problem, experts said.

While Beijing has publicly talked about cracking down on illegal fishing, the nation has one of the worst records of state-sponsored fishing crimes in international waters, said Whitley Saumweber, director of the Center for Strategic and International Studies' Stephenson Ocean Security Project.

China is "obviously high on the list … when talking about state-sponsored IUU and the way that they use it as both a tool for … economic purposes, but also increasingly for the purposes of influencing bilateral relationships," Saumweber said during the CSIS Ocean Security Forum 2021 in December.

Coast Guard Commandant Adm. Karl Schultz pointed to vessels carrying Chinese flags that have been spotted off the coasts of countries in South America. More dialogue is needed with Beijing to ensure the government's rhetoric around tackling illegal fishing matches its actions.

"This is the space where maybe we can shape those behaviors and show by demonstrated action what is responsible flag state behavior," Schultz said.

While China has said officials will crack down on illegal activity, it is still rated the No. 1 country in the world for illegal fishing, according to a report from the Global Initiative Against Transnational Organized Crime, a nonprofit organization.

There is a "persistent demand" for more collaboration between the U.S. Coast Guard and Navy, such as adaptive force packaging, to counter China, Schultz noted. Adaptive force packaging incorporates transferable crew and equipment modules for more distributed forces.

"Who better than maybe the United States Coast Guard — who's a recognized enforcer of modern maritime free and open ocean — to go over there and say, 'Not so fast,'" Schultz said.

While the Navy has a lot on its plate, the service is taking the national security issue seriously, he said.

"We will match some Coast Guard capacity to their availability, the availability they make of naval platforms," he said. "We can do a lot of good things together."

U.S. Pacific Islands face some of the worst pressure from illegal fishing, according to a Congressional Research Service report titled, "The Pacific Islands." An estimated $616 million is lost every year to IUU.

"China, which accounts for more than a third of global fish consumption, is a major contributor to IUU fishing in the region," according to the report.

Navy Secretary Carlos Del Toro noted global warming is driving increased illegal fishing activity in the Arctic region. Melting ice is opening new routes for economic activity and presents new security threats, he said.

"It also increases resource competition and, of course, shifts the geopolitical and the security environment and has ecological impacts around the globe," he said.

Monica Medina, assistant secretary for oceans and international environmental and scientific affairs at the State Department, noted the importance of collaboration with industry and nongovernmental organizations.

"The tools are out there. It's a question of us really all sitting in the room together," she said.

To solve the problem and mitigate the damage of illegal fishing requires more equipment and platforms that can streamline data collection.

Duncan Copeland, executive director of Trygg Mat Tracking, is working with other surveillance organizations to help educate governments about their options for fishery tracking tools. As the problem of illegal fishing has grown, more technologies have come into play, and officials must determine the right products to use, he said.

But there is no perfect choice, he

Coast Guard photos

noted.

"The best picture is one in which multiple tools and systems are integrated in such a way that best reflects what an individual country or region's needs are," he said.

Trygg Mat Tracking, Global Fishing Watch, and the International Monitoring Control and Surveillance Network partnered last year to launch the Joint Analytical Cell, or JAC.

Data collection can be a powerful tool for preventing illegal activity, said Paul Wood, chief innovation officer at Global Fishing Watch. The organization's goal is to track every vessel larger than 15 meters in length using a combination of radar, optical satellites and radio frequency, he said.

"We think we're within a few years of getting there and doing that in a highly scalable way," he said.

The most important capability needed is the ability to share information, Wood said. If U.S. forces attempt to push a foreign fleet out of U.S. waters, the targeted ships can often effectively evade repercussions by switching to neighboring jurisdictions.

But if ship location and risk data is transparent, it is more likely authorities can curb illegal activity.

"Having an open free tool allows you to do that, and ultimately that gets the data in the hands of the key person that needs it," he said. "When you have open source, open free data, there's no classification issues, nobody has to ask permission to take a piece of data out of our system and share it with anybody else."

New satellite technology is driving innovation.

Satellites are getting smaller and more capable, said Dee Pack, a researcher at the Aerospace Corp. As they become less expensive and risky to send into orbit, commercial and nongovernmental organizations can afford to be part of the data collection process.

"You see small companies and NGOs putting up methane monitoring satellites to try to assess our understanding of global warming," he said. "It's possible that you could have the same thing happening with some of these technologies as applied to IUU fishing and monitoring," he said in January during the Space Policy Show hosted by the Aerospace Corp.'s Center for Space Policy and Strategy.

Additionally, the proliferation of satellites could help expand coverage to remote areas like Alaska and the Arctic region, said Will Cromarty, account executive at data analytics company Spire Global Inc.

"I've seen the more we launched the satellites, the more really deep insight we've had in a lot of the regions where IUU fishing can be the worst," he said.

Cloud computing and data aggregation technologies have also improved, enabling larger datasets for more accurate models, Pack noted.

"When you pull in advances in artificial intelligence and machine learning, the possibilities are really limitless," he said.

One of the most challenging problems for cracking down on IUU fishing is ships that turn off or spoof their automatic transmitter signals, Cromarty said.

The U.S. Coast Guard helps a Chinese Fisheries Law Enforcement Command officer seize a vessel suspected of illegal activity.

To track evasive ships that have "gone dark," determining how to merge sensors will be key.

"It's really that fusion of capabilities that from a technological perspective is going to resolve the dark vessel issue," he said.

The Pentagon's search for solutions has made some progress. Jared Dunnmon, technical director for AI and machine learning at the Defense Innovation Unit, pointed to a prize competition run by the Coast Guard and international partners in 2020 called the XV3.

The competition challenged participants to use data from synthetic aperture radar — radar that can be used to create 2D and 3D reconstructions of images — to locate and characterize maritime vessels anywhere in the world, he said. The goal was for users to be able to determine information such as the speed and size of the vessels.

Now DIU is in the process of evaluating how well the models created by competitors worked, he said. Then, the models will be available online so that U.S. allies don't have to wait for data to be shared.

"Allies and partners can literally go and take that model off the internet and run it themselves if it's useful," he said.

While there are commercial options for data curation, Dunnmon said they are not easily accessible for sharing. As long as the synthetic aperture radar data is available, the tracking capabilities for illegal fishing vessels should expand in the next couple of years, he added.

"We should be able to at least get the obvious stuff and make sure that we're spending either our enforcement efforts in places where we don't have that coverage, or we're spending our enforcement efforts on places where we detect that there are ships that we don't expect to be there," he said.

Meanwhile, he noted that data transparency can cause problems if fishing vessels can use the information to monitor law enforcement. For example, illegal fishing operators might use satellite imagery to watch out for officers about to perform enforcement action. However, time delays for certain information can be instituted to prevent criminal fishermen from disappearing before authorities can investigate, he said.

Because countries have to collaborate to create an effective anti-illegal fishing network, it can be challenging to overcome economic obstacles for less developed nations, Pack noted. However, cheaper and smaller satellites on the market could help overcome expensive barriers, he said.

Some critics have concerns that collecting data requires too many resources, said Beth Lowell, deputy vice president for U.S. campaigns at Oceana, an ocean conservation nonprofit. But it actually can help agencies work more efficiently if correctly utilized, she said.

"Sometimes we hear from the federal government side that data … can be a resource constraint," she said. "Collecting data is a challenge, but I want to come at this from a different angle — that data is actually an extremely powerful tool that actually can help the federal agencies work better, more effectively and efficiently if they actually know how to use it." **ND**

Marine Corps Sees Initial Successes With Restructure Despite Critics


Berger

BY MEREDITH ROATEN

The Marine Corps is making strides toward achieving Commandant Gen. David Berger's controversial vision for transforming the force, as it prepares for great power competition and expeditionary warfare operations.

In 2020, Berger unveiled his Force Design 2030 blueprint as a way to ready the service to deter China and prepare for potential conflict in the Indo-Pacific region. The strategy laid out an ambitious plan to cut end strength, divest from legacy systems and procure new platforms needed for extra operational flexibility.

"We're two years into it, largely successful so far in the leadership here in Congress allowing us to keep those [freed up] resources and plow them back into the Marine Corps of the future," Berger said at an event sponsored by the Center for a New American Security.

Carrying out the objectives of the plan by 2030 will be difficult, but it is necessary so the service can be an asset in a future fight, he said.

Looking forward, Berger's top priorities for the upcoming fiscal year 2023 budget include the light amphibious warship, also known as LAW, he said. The new class of warships would enable greater flexibility for maritime operations.

"If you're a maritime naval force, and you don't have the mobility on the water to go places on sovereign ships that you need, then you're in trouble," Berger said.

While the vessel is a top priority, the planned fleet of 30 to 50 warships has faced criticism. Some observers say the ships as designed may not be survivable enough for Marine Corps operations, which could add costs to production down the road.

The Navy is targeting a per unit procurement cost of $100 million to $150 million, according to the Congressional Research Service.

"The trade-off is that, because of the LAW's small size, they will not be able to support the customary level of global forward deployments, which may decline as a result," according to a Center for Strategic and International Studies report titled "U.S. Military Forces in FY 2022," which was released in November.

Another critical Force Design 2030 technology that has made progress over the past year is the Navy Marine Expeditionary Ship Interdiction System, also known as NMESIS. The Marine Corps successfully demonstrated the system in early 2021.

The platform — which features a missile launcher attached to a ground vehicle — will target and kill ships, adding to the service's existing fleet of long-range precision fires that can threaten adversaries' ground or maritime systems.

"Now you've got a whole set of kill chains that you can use to complicate Chinese targeting, or to threaten Chinese freedom of action," Berger said.

But the Marine Corps is still facing acquisition challenges, even though Congress has granted the military special authorities such as other transaction authorities for rapid acquisition and testing, he said.

"Congress has given us some [authorities, but] we haven't used all of it," he said. "I'm convinced we haven't squeezed all we can out of it in terms of rapid acquisition, rapid testing."

Berger said the current bureaucracy rewards inertia such as continuing existing programs of record. By the time the technology is developed it is already obsolete.

But he noted some resistance can be helpful to ensure the Marine Corps is not chasing after "a shiny object" but pursuing game-changing innovation.

"Some degree of that is actually a good thing but too much will definitely bring you to your knees," he said.

Meanwhile, integration between the Marine Corps and the Navy — a key component of Force Design 2030 — is progressing on the operational level. However, while the sea services are practicing how to implement Force Design 2030 together, the current resource allocation system does not support collaboration, Berger said.

"Our system is built for a model that resources everybody the same, so we have to build in a whole lot more flexibility than we're accustomed to," he said.

The Navy and Marine Corps have learned from working together, but the Defense Department needs to figure out how to best distribute resources for joint warfighting, he said.

Two years after its release, not everyone is onboard with Berger's vision for Force Design 2030. Many retired Marines see the service as "the Swiss army knives of the military" and able


A Landing Craft Air Cushion delivers a Navy Marine Expeditionary Ship Interdiction System launcher.

to adapt to any crisis, said Bryan Clark, director of the Hudson Institute's Center for Defense Concepts and Technology.

"The new model that they're talking about is going to mean that the Marine Corps is not like a one-size-fits-all unit," he said.

The passing of the 2022 National Defense Authorization Act reflects how well Berger has worked to make the case for changes to the Marine Corps, Clark said. However, "as these cuts get deeper on the divest side, and the changes become more significant on the invest side, it will get harder and harder to continue to make that case," he said.

The effort is "controversial" and "a work in progress," according to the CSIS report. A major challenge to the Marine Corps' progress is critics who worry about conflicts outside the Indo-Pacific region.

"The focus on China downplays the possibility of conflicts elsewhere," according to the CSIS report. "Since World War II, the United States has fought many regional conflicts but never a great power conflict."

However, what some critics don't understand is that every generation of warfighters in the last century has had to adapt to the conflict of the times, said retired Marine Dakota Wood, a senior research fellow for defense programs at the Heritage Foundation.

"The Indo-Pacific is much different than the deserts of Iraq, and China is a much more capable competitor than the Iraqi military under Saddam Hussein," Wood said.

Meanwhile, the Marine Corps' divestments of legacy systems still run the risk of going to pay the bills for the Pentagon instead of being funneled into new technology, Clark said.

While the service has found ways to save money for its new strategy, it is getting harder to hold onto those investments because of inflation and growing operational costs, he said.

"Further divestments are going to be unattractive to [Defense] Department leaders, meaning they've started this transition and are now halfway through and unable to complete," he said.

This could be a big problem for the Marines Corps' restructure if sufficient resources aren't available, he said.

"It will be a mixture between the three paths: changing the strategy and then changing the budget and then changing the divestment approach," he said.

One area for divestment is the Marine Corps' rotary-wing inventory. Force Design 2030 already calls for a reduction across the fleet, but Clark said cuts may have to deepen on legacy platforms like the MV-22 Osprey or AH-1 Cobra if more resources are not found.

Berger said in his fiscal year 2022 posture statement that programs of record could be modified to "ensure affordability and viability."

Vertical lift technology will be key in achieving the flexibility that is the goal

Marine Corps photos

of Force Design 2030. Officials will look at specifications for range, speed, electronic signature and signature management, Berger said.

"Think of every flying helicopter in the Marine Corps being like a 5G tower that's on the move, like it's constantly moving information and data," he said.

One of the restructuring's first significant investments was unmanned aerial vehicle procurement in 2021. The service plans to acquire a fleet of six MQ-9 Reapers — accounted for in the fiscal year 2022 budget — but it still has ground to cover.

"Despite having led the way on UAVs in the 1980s, the Marine Corps now lags far behind the Army and Air Force," according to the CSIS report.

The Marine Corps is still learning how to best incorporate unmanned platforms, including as part of vertical lift, Berger said.

Meanwhile, Navy Secretary Carlos Del Toro has thrown his support behind the Force Design 2030 effort. He released a strategic document in October that builds on both the Corps' blueprint and the Navy's Navigation Plan 2021.

Berger has supplemented Force Design 2030 with additional strategies to counter China. For example, he released "A Concept for Stand-in Forces" in December, which outlines how the Marines will conduct reconnaissance and counter-reconnaissance operations in the Pacific to prevent escalation.

Stand-in forces are "small but lethal" units that can be easily maintained in order to operate within a contested environment, according to the document.

"Their effort is to make sort of a bubble, a shield [and] push it way, way out," Berger said. "We have to be in there. We have to be close up [and] forward."

Upgrades to training and personnel management have to work in tandem with technology, Berger noted.

"Otherwise all the concepts and capabilities in the world aren't going to work with the current systems that we have," he said.

A Marine of the future will have to be able to juggle multiple skill sets and have the same flexibility as the force itself, he said.

The recruitment strategy for the 2030 plan aims to achieve "a better balance" of high school graduates and more mature recruits. The Marines will have to become more inventive with incentives for individuals to stay in the force, Berger said.

Bringing in more mature talent will enable Force Design 2030's smaller units and flexible warfare, Wood said.

Force Design 2030 foresees that the service will have to operate in smaller groups far away from each other, which means unit leaders must be able to make their own decisions, Wood said. Having leaders with experience that can make smart decisions will be critical, he said.

"They are going to shift the model from turning over three quarters of the Marine Corps every year to something that's less volatile," he said.

However, some ideas for attaining more experienced talent have generated pushback. For example, lateral entry, or bringing in a civilian to serve in an officer position commensurate with their civilian experience, was introduced in the service's Talent Management 2030 strategy document in November.

It is controversial to some Marines who feel everyone should have to go through the same training, Wood said.

It raises questions such as "is that a threat to the culture of the Corps … and the respect that would come along with somebody who has taken 15 years to become a staff sergeant or a gunnery sergeant?" Wood said.

Service leaders should "feel their way forward" with initiatives like this to assess how the culture is adapting, he said.

Meanwhile, whether Force Design 2030 comes to fruition or not could be determined in the near future, Berger suggested.

The Marine Corps tests an MQ-9B Reaper.

Marine Corps photo

"I have taken a hard look at both those plans and, overall, I'm quite satisfied with them," Del Toro told reporters after a recent speech at the U.S. Naval Academy.

Because so many of the concepts that are the backbone of the restructure are unproven, wargaming and experimentation will continue to shape its structure into the future. Planning for adjustments will help hedge the force against the unknown, Berger said

"It's an ongoing process," he said. "We knew we didn't have perfect visibility of what 10 years out might look like, but we had a pretty good aim point."

"This year and next year I think are really key," he told reporters in December at the Reagan National Defense Forum. "We've divested of things in order to move quickly. This year and next year are the keys. If the Department of Defense and the Congress sees this as the right approach, we'll know. If they see it as the wrong approach, I don't think anybody else is going to go down this path, because I wouldn't either. If you got rid of half of your stuff in your house and somebody took all your money and you didn't get it [back to buy other things], … that's not cool." **ND**

www.rheinmetall-defence.com/arv

TECHNOLOGY DRIVEN

AMERICAN RHEINMETALL VEHICLES

HX COMMON TACTICAL TRUCK

- **TECHNOLOGY FOR THE FUTURE:** The HX Common Tactical Truck features an advanced, interchangeable protected cab design, Advanced Driver Assistance Systems (ADAS), and drive by wire operation. The new open systems electrical architecture allows rapid integration of leader follower and autonomous capabilities that focus on protecting our most valuable combat asset – the Soldier.
- **COMMONALITY IN THE FAMILY:** The HX Common Tactical Truck is the new, next-gen variant of the globally successful HX family of military-off-the-shelf tactical trucks. It possesses an extremely high level of commonality and modularity across variants: cargo, load handling systems, tankers, and line haul tractors. With an HX family that can scale from 4x4 to 10x10, Rheinmetall can meet any military need.
- **COMMERCIALITY IN ITS DNA:** The HX Common Tactical Truck leverages best in class advances in commercial truck technology, safety, fuel efficiency, and emissions reduction. Ruggedized for the stresses of military service, the HX family provides an "off the shelf" capability. This commercial back-bone reduces obsolescence risk/cost, expands parts availability, and reduces sustainment demands.
- **A FAMILY OF ALLIED USERS:** The HX family of trucks are in use with an Allied user group of 20 nations creating common global supply chains, training opportunities and integrated operations among key allies operating around the world.

TOMORROW'S TRUCK. TODAY.

PASSION FOR **TECHNOLOGY.**

RHEINMETALL

Marine Corps Evolving Live, Synthetic Training Environments

BY MIKAYLA EASLEY

ORLANDO, Fla. — As the Marine Corps evolves to meet new challenges posed by great power competitors, the service's leaders are pressing for upgrades to its training systems.

The Corps is syncing its live and synthetic training environments to match operational changes outlined by Marine Corps Commandant Gen. David Berger in his "Force Design 2030" strategy. The document tasked the service to move away from tactics used in the previous two decades of warfare in Iraq and Afghanistan and prepare for future battlefields against sophisticated adversaries such as China and Russia.

"We have, I think unintentionally, put training third or fourth in sequence of our priorities," Berger said at the National Training and Simulation Association's annual Interservice/Industry Training, Simulation and Education Conference in Orlando, Florida. "We go after a capability, we figure out how we're going to structure the force, we buy platforms, and then we turn to the training guy and say: 'We need a way to train.' That's not going to work going forward."

In order for the Marine Corps to face evolving threats in less familiar operational conditions, service leaders agreed that training systems must keep up with the times.

"We're going to have to be able to train like we fight," said Brig. Gen. Matthew Mowery, assistant deputy commandant for aviation. That means matching training exercises to new strategies like expeditionary advanced base operations, he added.

EABO is a form of expeditionary warfare that "involves the employment of mobile, low-signature, operationally relevant, and relatively easy to maintain and sustain naval expeditionary forces from a series of austere, temporary locations ashore or inshore within a contested or potentially contested maritime area in order to conduct sea denial, support sea control or enable fleet sustainment," according to the service.

Accurately replicating the operational environment a Marine could face in training will be key to achieving Berger's vision as laid out in Force Design 2030, said service leaders during a panel at the conference.

Upon taking the helm of Marine Corps Training Command last year, Maj. Gen. Julian Alford said he first tackled how to revamp the training of the service's infantry. The Corps has fielded three new infantry immersion trainers — two on the East Coast and another on the West Coast — that has troops complete tasks under stress, he said.

"The first time that a Marine goes into combat should not really be the first time they go to combat," Alford said. He pointed out that when pilots attend flight school, they complete multiple flight and combat simulations before training in a live aircraft.

"We owe that to our young frontline infantrymen to do the same thing — particularly if we're going to do EABO … with small teams, squads, platoons, companies that are spread out," he said. "That's a different Marine Corps than we have today."

To make training more realistic and immersive, Marine Corps Systems Command is working to close a number of gaps, said Jim Fraley, the command's branch head for range and training area management. For example, the service is implementing next-generation, interactive targets that move and exhibit human behaviors.

It is also tailoring its training systems to replicate scenarios Marines may

Marine Corps photo by Lance Cpl. Jacquilyn Davis

experience in the Indo-Pacific region, said Maj. Gen. Austin Renforth, commanding general of Marine Air-Ground Task Force Training Command and the Marine Corps Air-Ground Combat Center in Twentynine Palms, California.

Twentynine Palms has developed a force-on-force exercise called the MAGTF Warfighting Exercise, or MWX, which first began in 2019. Designed to expand training focuses and address gaps, the live exercise invites international partners and Marines from different regiments to "adapt to a thinking enemy in a challenging environment where the adversary force is equipped with capabilities more consistent with a pacing threat," Renforth said.

Although Renforth called live exercises like MWX the "gold standard," he acknowledged that not all scenarios can be effectively replicated in a live training environment.

LEFT: U.S. Marines set up security during MAGTF Warfighting Exercise (MWX) in 2021.

BELOW: A Marine tests a virtual reality system at Camp Lejeune, North Carolina.

Marine Corps photo by Lance Cpl. Michaela R. Gregory

"We'll certainly rely on virtual constructive systems to supplement," he said.

Platforms that leverage synthetic capabilities like the live, virtual, constructive training environment, or LVC-TE, have been one of the command's foremost modernization priorities. LVC uses a combination of virtual reality and computer-generated entities to replicate live training. Systems Command was given authority to begin planning stages in July to develop what it wants the platform to look like.

Col. Luis Lara, program manager for training systems at the command, said the service was preparing for a milestone decision review to enter the execution phase of LVC-TE in December. An early version of the software is set to begin fielding at Twentynine Palms so long as the next phase is approved and funding is allocated, according to the command.

Renforth emphasized that the Corps can improve how it replicates real world threats.

"We're trying to create a pacing threat on a shoestring," he said. "We know what the pacing threat looks like. We know what effects they can put on our command-and-control systems."

At the same time, Force Design 2030 has prompted the Corps to shift focus away from the platforms themselves and onto the capability they represent, Mowery said.

For example, he said the service used to focus on making sure the F/A-18 Hornet combat jet was equipped to keep up with the technology of pacing threats. Now, the Marine Corps is paying more attention to the capabilities the platform brings to the table and evaluating it based on whether it meets the service's requirements.

"Once a program or a platform no longer meets the requirement or need, then we're moving on to something else," he said.

Mowery said that while the service was training pilots well before Berger released his Force Design 2030 planning guidance, he also realized "we were doing some things wrong." For example, better interoperability — particularly on the ground side of missions — is going to be a greater focus area for the service.

The training systems needed for EABO must also be easily deployable, shock-resistant and be small and portable enough so training exercises can be done year round rather than only during large annual events, he said.

Renforth's focus for force-on-force exercises is teaching future commanders how to make informed and competent decisions, he said. But some leaders struggle with the modern systems Force Design 2030 requires, causing them to make decisions based on previous training.

"We've got to get our commanders comfortable with these systems to where they have confidence in the systems to utilize all the information that comes from [them]," he said.

Equipping the vast training ranges at Twentynine Palms with better high-tech networks like 5G would be "a game changer," Renforth said, as it would give leaders a more comprehensive picture of larger exercises in real time. The ability to record and replay exercises for later review with training commanders would also help, he said.

Fraley said the Marine Corps is working with the Naval Surface Warfare Center Dahlgren Division in Virginia and industry partners to develop a device that would be able to replay and provide feedback to unit or fire team commanders.

"The ability to do that instead of having a green book in your hand and [another Marine] run around slapping tags on people and saying, 'You're dead,' would be extremely important," Fraley said, referring to how live infantry training is traditionally executed.

Brig. Gen. Arthur Pasagian, commander of Marine Corps Systems Command, said the service is searching for new ways to employ training systems that are both organic to the latest platforms they procure and sustainable for the future.

"That's at the peak of our attention as we develop these new weapons systems today, but also in a way that they harmonize with the gear that's ready for tonight's force and readiness," he said.

The aviation component of the Marine Corps is laser focused on technology that has an open architecture so the service won't need to procure entire new platforms as technology and adversaries evolve, Mowery said.

"We've got to be able to take a platform or system and be able to update that on the fly as needed," he said.

Renforth agreed the service needs to be more agile in how it procures new platforms to keep up with rapidly advancing technology. The lengthy time between buying a system and it being fielded creates training gaps, he noted.

"We'll procure something and we'll say, 'OK, this is a good program. In 2025, we're going to have it.' Well, what do we do in the interim?" he asked. "By the time 2025 comes around and we get this thing, it's outdated."

A persistent challenge for the Marine Corps has been figuring out how to balance being prepared for today's challenges and future fights.

"One of the things we say about Force Design 2030 — that's not an end state. You've got to get 2030 out of your head," Renforth said. "Really, it's a concept and we're in it now." ND

Tactical Vehicles

RECOMPETE FOR JLTV OFFERS COVETED PRIZE FOR VEHICLE MAKERS

BY YASMIN TADJDEH

More than six years after Oshkosh Defense was awarded a mega contract to build the Joint Light Tactical Vehicle for the Army and Marine Corps, and with few new military vehicle programs on the horizon, the Defense Department is poised to reignite a fierce industry competition for the next version of the JLTV.

When Oshkosh won the hotly contested and lucrative contract — which was initially worth some $6.7 billion — for the first iteration of the platform in 2015, it sent shockwaves across the military vehicle market. Oshkosh at the time was not the military vehicle juggernaut it is now, and the outcome had major ramifications for Humvee manufacturer AM General.

The JLTV — which is replacing portions of the Army and Marine Corps' Humvee fleet — was designed to balance mobility and protection, as well as achieve the "iron triangle" of payload, protection and performance.

It is expected that Oshkosh Defense, Navistar Defense, AM General and GM Defense will vie for the next phase of the program.

The JLTV joint program office — which is procuring platforms for both the Army and Marine Corps — was slated to release a request for proposals for a follow-up version of the vehicle by the end of January, said Michael Sprang, program manager for the JPO. A contract award is expected in September.

The RFP will be a culmination of years of work, Sprang told *National Defense*.

"When we first looked at the competitive market for JLTV, what we didn't want to do was just to [use] … lowest-price, technically acceptable" as the metric, he said. "We engaged with industry early and we've engaged with them often."

In August 2019, the JPO asked industry for information as it conducted market research and eight companies responded, he noted. Based on those responses, the office crafted an acquisition strategy for the follow-on vehicle and allowed industry to lease Joint Light Tactical Vehicles from Oshkosh.

"When you think about the JLTV, there's obviously an incumbent but we wanted the opportunity for other companies to be able to understand the JLTV," he said. Three companies leased vehicles.

According to George Mansfield, vice president and general manager of joint programs at Oshkosh Defense, those companies included GM Defense, Navistar and AM General.

The JPO has since released multiple draft requests for proposals and has hosted five industry days, Sprang said. The follow-on JLTV is known as the A2 version.

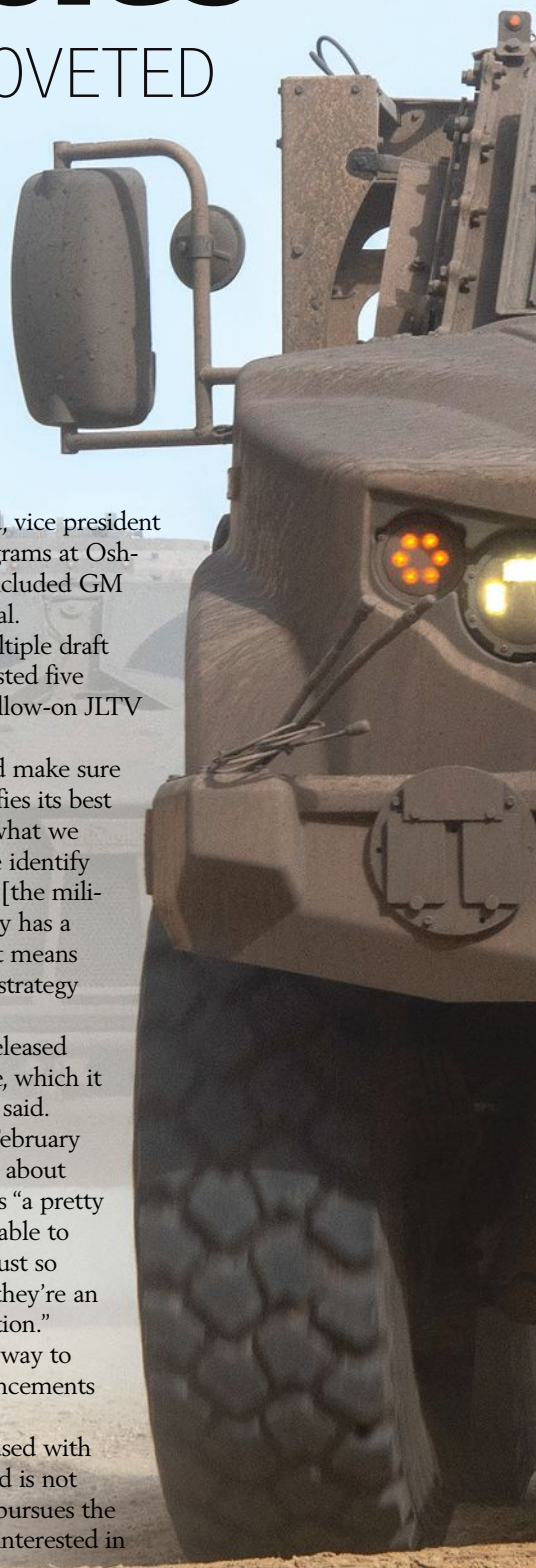
"We've really tried to shape and make sure that when the government identifies its best value, that industry understands what we mean by that," he said. "When we identify the requirements of the contract, [the military wants to ensure] that industry has a good comprehension of what that means so that they can create their best strategy for how to win the contract."

The joint program office also released the JLTV's technical data package, which it had purchased from Oshkosh, he said.

Since the first industry day in February 2020, industry has asked the JPO about 400 questions, Sprang said. That is "a pretty good amount so that we've been able to go back and forth with industry, just so that they have an awareness and they're an active participant in this competition."

Robust competition is the best way to control costs and bring new enhancements into the program, he said.

The joint program office is pleased with the JLTV's current capabilities and is not looking for massive changes as it pursues the A2, Sprang noted. However, it is interested in



Oshkosh photo


OSHKOSH

some key enhancements.

For example, the office plans to upgrade the platform's engine, he said. The current system is a Banks Power-modified GM Duramax engine, and the JPO is seeking the next-generation system from the same supplier.

"It's not a huge transition from the current engine," Sprang said.

The office is also incorporating changes the user community has requested. For example, soldiers and Marines have asked for more space be made available in the back of the platform.

"We've shrunk the space that's committed on every vehicle," he said. "It still has the ability to grow and expand if there is a lot of communication equipment that they need on specific JLTVs, but the vast majority will have space back so that they can put their own … rucksacks or additional payloads that they want in there."

The office has also identified some technologies that can help reduce the JLTV's signature profile. "The alternator, some gearing [and] insulation are key areas to reduce how loud it is both external to the vehicle and internal to the vehicle," Sprang said. "That was one of the concerns that we had from soldiers and Marines."

The government has also asked industry to look at technologies that are not part of the system's current configuration, and the joint program office would then give them an evaluated credit during source selection, he said. These include increased corrosion protection and fuel efficiency.

The office is pursuing two technologies relative to the latter, the first being for on-the-move operations, Sprang said. "There are different ways of doing this and we're leaving that up to industry to identify if they want to propose that or … how they would implement it."

The other is anti-idle technology using lithium-ion batteries.

"You have the ability to idle with just the batteries and so you can run your communication equipment, you can run your HVAC system," Sprang said. "The system will be smart enough to identify when the battery level is at a certain point [and] it will turn on the engine and it will charge the batteries back up. And if you're still idling, it will turn off the engine."

The office is also looking for new commercial driver enhancements that industry can offer such as lane departure warnings, backup alarms and 360-degree situational awareness.

"When you get into your vehicle today, … there are cameras all over the vehicle and you can see around the vehicle," Sprang said of commercial cars and trucks. "When you look at JLTV, there's transparent armor and there is opaque armor that you can't see through and that creates some blind spots. And so, a 360-degree situational awareness [system] gives more flexibility to see around the vehicle, and then also to project out when you're making turns."

After the contract is awarded, the winner will have 18 months to deliver the first vehicles and those platforms will go through about a year of testing, he said. According to slides from a November industry day, the projected value of the contract could be worth up to $6.5 billion.

The first fielded platforms will be ready around 2025, Sprang said. Oshkosh's current contract will continue to be leveraged until fiscal years 2023 and 2024 and then will be ramped down as the A2 comes into the fleet.

"That allows both the Army and the Marine Corps to have vehicles to field while we're ramping up under this new contract," Sprang said. "It creates this nice transition point."

The JPO is looking to procure about 15,400 vehicles and 7,600 associated trailers, though those numbers could still fluctuate based upon budgets, he said.

The office expects to see strong interest from industry for the program.

"Do I think it's going to be an effective competition or competitive? I absolutely do," he said. "I don't necessarily judge it by the number of companies [participating] but by the value of the companies and where they're going to put the proposals."

He continued: "Based upon the questions that we've gotten, based upon the discussions that have happened, we understand where industry may be, and it might not be the same number of interested companies today as it was maybe in 2019. But I think those that are still interested are going to be very competitive."

Mark Cancian, a senior advisor at the Center for Strategic and International Studies, anticipates that the program will be very competitive.

"This is the kind of vehicle that a lot of companies can make, and when you talk about an Abrams tank, there's really very few that can make a tank like that," he said. However, a "heavy truck is something that a lot of companies could make and as a result I think there will be a lot of interest."

As the incumbent, Oshkosh Defense is in a good position, he noted. AM General also has relevant experience given its history manufacturing the ubiquitous Humvee.

Oshkosh believes it is well positioned to win the follow-on contract, Mansfield said. "When we won back in 2015, … we always knew that we were going to have to recompete after eight years," he said.

To prepare, the company has been working with its supply base and making its assembly process as efficient as possible, Mansfield said.

"We believe we're in the best position," he said. "We designed the vehicle. We built over 14,600 vehicles to date. … We've got a talented workforce putting the vehicle together, and our supply base is second to none."

Meanwhile, GM Defense is continuing to evaluate how to best support the JLTV program.

"We are still actively engaged in a dialogue with the Army on this topic," a company spokesperson said in a statement. "Given our ability to leverage GM's com-

Defense Dept. photo

mercial technology combined with our core capability in integrated vehicles, we think there is an opportunity for us to provide real value to this program and a great opportunity to enhance warfighter capability. We continue to assess what kind of a role we can play and will discuss that in more detail when the time is appropriate."

Representatives from Navistar Defense and AM General did not respond to requests for interviews.

Meanwhile, as the military shifts its focus to great power competition, both officials and experts say the JLTV program, which has been used in counter-insurgency operations in the wars in Iraq and Afghanistan, will still be relevant.

The platform has utility for a variety of operational environments, Sprang said.

"It has growth capabilities. It has the flexibility to expand both in power, in weight and space," he said. "It has that ability for the multi-domain operations that we [will] have in the future."

Cancian also sees a future for the vehicle. Historically, the military has employed unarmored vehicles in conflicts such as World War II, the Korean War and the Vietnam War, he noted.

"Armored vehicles were an exception, rather than the rule," he said. But more recently, due to the scourge of roadside bombs in Iraq and Afghanistan, the military quickly pivoted to armoring its platforms and developing systems such as mine-resistant, ambush-protected vehicles.

The carnage of improvised explosive devices and the military's response to rapidly develop new armored vehicles has "been burned into everybody's experience," he said. There is a "sensitivity to casualties and vehicles during conflicts."

Those concerns will secure the JLTV's role in future engagements, Cancian said. Additionally, there will still be a need for the platforms in great power competition even though the threat will come more from artillery and long-range munitions as opposed to IEDs, he added.

Joint light tactical vehicles "could give you some protection from Russian artillery. And the Russians are very heavily invested in artillery, they always have been," he said.

As for the Pacific, the vehicles could also be useful in an engagement with North Korea which possesses a robust artillery capability, he added. **ND**

GM Defense photo

U.S. Military Wants Its Vehicles to Go Electric — With Detroit's Help

BY JON HARPER

GM Defense's all-electric military concept vehicle

To combat climate change, boost U.S. industry and achieve operational advantages, the Defense Department has ambitious plans to transform its fleet of ground vehicles through the introduction of electric and hybrid-electric drive technologies. Automakers see major opportunities to help the military and win business.

Addressing what it calls the climate crisis is a top policy priority of the Biden administration.

"The department is committed to meeting the challenge by making significant changes in our use of energy and increasing our investments in clean energy technology," Deputy Secretary of Defense Kathleen Hicks said in November during remarks at Wayne State University in Detroit, Michigan.

The Pentagon is developing a "sustainability plan," part of which will be focused on developing a zero emissions non-tactical vehicle fleet.

"Currently the Department of Defense has about 170,000 non-tactical vehicles — the cars and trucks we use on our bases," Hicks noted. "That's the largest fleet in the federal government, next to the U.S. Postal Service. Our success in transitioning this massive fleet to zero emissions, most of which will be electric, will depend on America's auto industry and autoworkers right here in Detroit."

General Motors has committed to investing $35 billion in advanced vehicle technologies, to include power and propulsion systems for electric vehicles, noted Steve DuMont, president of GM Defense. The parent company plans to have 30-plus EVs in its product offerings by 2035.

"All of that has relevance to what our defense customers are looking at," he told *National Defense*. "If you look at the non-tactical vehicles that are used in a [military] base or installation environment, to me that's just low hanging fruit."

DuMont has been talking with the brass across the services to discuss the

way ahead.

"When I met with [Deputy] Secretary Hicks, she made it really clear. I mean, her vision is let's start with the things that are easiest to do. And I put [electrifying the non-tactical fleet] in that category," he said. "There are opportunities to work with the DoD in that first area."

There will be some challenges involved, he acknowledged.

"There is infrastructure that needs to be put on the bases, there's a whole rollover of acquisition of these vehicles. But it truly is what we're doing today on the commercial side" of the automotive business, DuMont said.

GM is looking at creating microgrids to facilitate the transformation.

Army Lt. Gen. Duane Gamble, deputy chief of staff, G-4, said electrification of non-tactical vehicles and their deployment on installations will help inform how the Defense Department leverages EV tech for other elements of the future force.

"Building trust in our soldiers, our civilians and our leaders in our non-tactical wheeled vehicle fleet and the infrastructure that goes along with that … will help us transition and fully understand not only the technology, but the challenges associated with incorporating it into our combat vehicles," he told members of the House Armed Services subcommittee on readiness during a December hearing on operational energy.

The bipartisan infrastructure deal that Congress passed last year includes large investments in electric vehicles, batteries and the creation of a national network of charging stations, Hicks noted.

"On the non-tactical [vehicle] side, it's going to be all about the money and whether or not the money is really there," said Sharon Burke, a fellow in the New America think tank's Future of War project, and former assistant secretary of defense for operational energy.

"It's looking like … the administration and Congress together are setting up a situation where that's going to be possible, where the investment is going to be there," she said.

The Pentagon also wants to electrify its tactical vehicles — not just to combat climate change, but to achieve operational benefits as well, Hicks noted.

Gamble said the Army is at an "inflection point" for the tactical wheeled vehicle and combat vehicle fleets, largely because of technologies that have emerged from the commercial industry.

The initial push will be for hybrid-electric drive, or HED, because "full electrification for our complex weapon systems at the forward edge of the battlefield is a goal that we don't believe that currently our technology will support," Gamble said.

The main roadblock to full electrification is recharging in austere environments.

"How are you actually going to power these vehicles if you're talking about a deployment far from home?" Burke asked. "You can't run them off a grid if you're on a battlefield, so … until you have an answer to that question, you're not ready yet."

Hybrid-electric architectures for tactical systems are expected to yield major operational benefits, officials and analysts say.

HED could reduce fuel consumption by as much as 35 percent, Gamble noted. Other advantages include: extended range and persistence; increased onboard power for capabilities such as directed-energy weapons, jammers and electrified armor; reduced maintenance costs and associated logistics footprint; silent watch and silent mobility; and reduced thermal and acoustic signature.

Marine Lt. Gen. Edward Banta, deputy commandant for installations and logistics, told lawmakers that the Marine Corps is also eyeing hybrid technologies for new platforms and as a possible retrofit on legacy fleets.

"There's no reason not to look at that step right now," Burke said of moving toward hybrid-electric platforms. It doesn't add much additional cost compared with buying systems with internal combustion engines, and it provides performance gains, she added. "It's a good thing."

Jim Miller, BAE Systems' director of business development for combat mission systems, said: "The time is now for hybrid-electric drive and … it's one of those things we need to move fast on."

BAE has been tapped by the Army Rapid Capabilities and Critical Technologies Office to integrate its HED tech into Bradley Fighting Vehicles for demonstrations.

The company has a long history of working on this type of technology, including for commercial buses, he noted.

"They've created this baseline of maturity that we've taken advantage of on the combat vehicle side and led us to this," Miller said, adding that he's "reasonably sure this is going to work out well."

The contractor is wrapping up the integration work, and the first two vehicles are slated to be delivered to the military by June for testing, which will help inform the way ahead for the combat vehicle fleet.

In fiscal year 2022, the Army will also test hybrid-electric versions of Humvees and Joint Light Tactical Vehicles, according to Gamble.

BAE Systems' hybrid-electric Bradley Fighting Vehicle

BAE Systems photo

Miller said the HED for the Bradley was designed to be a scalable system that could be installed in all the vehicles that are part of armored brigade combat teams except for the M1 tank and the M88 recovery vehicle. "We're trying to make it as plug and play as we can."

Retrofitting a variety of legacy platforms could soon be "in the realm of the possible," he added, noting that the company recently held talks with the rapid capabilities office about potentially putting the system in the Armored Multi-Purpose Vehicle.

The contractor also plans to include HED in its offerings for new platforms including robotic combat vehicles and the Army's Optionally Manned Fighting Vehicle.

"We think that's the wave of the future and where it's going, and we're building that way," Miller said.

BAE has developed a robotic technology demonstrator with its own money that it has been showing off to military brass.

"We had all kinds of very positive feedback about moving in the right direction with hybrid-electric drive," Miller said.

Gamble said the "hybridization" of tactical wheeled vehicle and combat vehicle fleets is achievable between now and the end of the decade.

The Army aims to acquire "full electric" complex weapon systems in the light and medium categories in the 2030-2035 timeframe. Service officials believe the technology required will be mature enough by then, Gamble told lawmakers. Heavy platforms would likely come later.

But DuMont believes all-electric tactical vehicles could be ready for warfighters much sooner than some are predicting.

"I see the hybrid as maybe a transitional stage that likely will be very short lived, in my opinion, because I think we're going to be able to demonstrate the viability, the efficacy as well as the enhanced reliability … of having a single fuel source, a single power plant," he said.

Solving the recharging challenge for battlefield systems with fuel cells or other technologies is "the last piece of the puzzle" and a major focus of GM Defense, he said.

When that happens, "I think the adoption of these vehicles is going to come very quickly, just because the operator is going to be so impressed with the performance of them," he added.

GM has already proven it can create highly capable, fully electric tactical wheeled platforms, DuMont said.

The company built an all-electric military concept vehicle similar to the conventionally powered Infantry Squad Vehicle. Both systems are based on the Chevy Colorado ZR2, and the concept vehicle utilizes the same power plant as the Chevy Bolt.

"I've taken it out and demonstrated it with the Army. I've shown it to the Marine Corps. I've had Special Operations Command drive it," DuMont said. There's nothing the conventionally powered ISV can do that the concept vehicle can't do, according to DuMont.

Additionally, GM's Ultium technology, which is the foundation of the Silverado commercial EV truck that was announced in January, will be leveraged for GM Defense's offering for the Army's electric Light Reconnaissance Vehicle, which the service plans to pursue as its first fully electric tactical vehicle built from the ground up, he noted. Prototyping is slated for 2022.

Gamble said the Army is "thinking big but starting small" when it comes to these types of systems.

However, DuMont said the eLRV project could have outsized implications for industry teams that are eyeing future opportunities to electrify the military's fleets.

"It's tough to recover from a negative first impression," he said. "If we were to deliver an eLRV … and it didn't meet the expectations of the operator, that would be pretty tough and we would have to do a lot of work to overcome it. So, I am putting additional focus on making sure we get eLRV right."

To achieve its vision for electric and hybrid-electric platforms, the Pentagon needs to ensure that energy performance and electrification have "real value" attached to them when it develops strategy, concepts, doctrine and requirements, Burke said.

"Until the actual process by which the department decides what the future threat is and what they're going to build for it, until that includes a value for energy as a capability and a performance gain, then this won't be real," she said. "It has to get into the business of how the department builds for the future in order for this to actually happen."

She continued: "You need to see it incorporated in a program of record in an authentic way, not just a sort of boutique or showcase energy project." ND

AIMPOINT®
FIRE CONTROL SYSTEMS

FCS13RE™

SELECTED BY THE U.S. MILITARY

A direct view optic for crew-served weapons that greatly increases first round hit probability on both static & moving targets.

- Day / night use optic
- Onboard ballistic computer
- Integrated laser range finder
- Ballistically compensated 2 MOA red dot
- Programmed for use on: M3E1 MAAWS, M2 .50 BMG, MK 19 & MK 47 Grenade Launchers, H&K GMG, AT4, M240D/H, & M134 Minigun
- Communicates with programming units for 40mm HV airburst munitions
- Available accessories: 3XL Magnifier & TH60 clip-on thermal imager

THANK YOU TO THOSE WHO SERVE.
Discount for First Responders and U.S. Military at **www.aimpoint.us**

WWW.AIMPOINT.US/FIRECONTROL

M03552

Aimpoint®

Viewpoint BY MATTHEW BREEN AND EUNICE SOHN

Questions for the Army's Open Architecture Approach

■ The momentum surrounding CMOSS technology adoption continues to build.

CMOSS, which stands for Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance (C5ISR)/Electronic Warfare Modular Open Suite of Standards, is one component of the Army's effort to modernize its communication and network architecture and increase its ability to introduce new technical capabilities to the force quickly.

By embedding networked capabilities such as radio and communication waveforms, mission planning and command applications, assured positioning, navigation and timing information, and electronic warfare tools onto cards that are inserted into a common chassis within a tactical or combat vehicle, the Army is moving closer towards a scenario where plug-and-play mission equipment exists.

The excitement surrounding CMOSS is understandable. When appropriately matured, open architecture technology has the potential to support a step-change in Army warfighting capability. As conceptually envisioned, CMOSS equipment should more easily enable multi-mission equipment sets, shorten technology development cycles, allow for continuous introduction of new capability, and significantly reduce sustainment costs and equipment downtime.

Reports from the Army's Network Modernization Experimentation event, also known as NetModX, suggest that small-scale, controlled experiments to test card prototypes showed promising results. The Army is capitalizing on the success of initial card tests and moving rapidly to field a common chassis prototype.

While momentum and early success is good, the Army must be careful not to let the euphoria of the technology's potential and confidence from successful demonstrations overshadow the very real challenges that still must be addressed. For the idea to succeed, the Army will need to collaborate closely with industry to incrementally move the technology forward. Moreover, for industry to continue to invest in CMOSS and CMOSS chassis development the way the Army requires, greater clarity is needed on the end-state and organizational dynamics of how such a chassis will be managed now and in the future.

Specifically, there are several critical organizational, technological and industrial base questions that must be addressed before a full CMOSS capability set can be fielded as part of the Army's Network Capability Set 25. Without greater clarity on how these efforts will be funded, what stakeholder or group of stakeholders will arbitrate technical decisions, how responsibility for configuration and chassis management will be defined, and what procedures will be used for managing future technological developments, industry cannot invest in advancing CMOSS tech with confidence.

Industry has been provided little guidance regarding what the technical plan for the CMOSS chassis will be when it is rolled out to the force as part of the capability sets.

To clearly weigh the merits of upgrading to a CMOSS-based equipment standard, the Army must first understand and communicate what, if any, existing vehicle communication systems are being replaced. The chassis, in its initial configuration, is expected to incorporate a radio card, single board computer, and an assured positioning, navigation and timing card.

What does this initial capability set imply about existing vehicle technology, and how should industry plan to manage technical integration? Should industry assume that correspond-

Army photo

ing mission computers and tactical radios will be removed from the vehicle to accommodate the new chassis as this legacy technology is now redundant? If legacy sensors and line-replaceable units are not removed, how will existing vehicle communication and electrical architectures be required to change to adjust to the new infrastructure needs of a CMOSS-based system?

Moreover, for this endeavor to succeed, the Army will need industry to continue to push the technical maturation of CMOSS technology forward. However, industry can neither adequately plan for what capabilities may be required, nor invest with high confidence in capability development without a more precise understanding of what the technical end-state for a CMOSS chassis is envisioned to be and what boxes and capabilities it is likely to displace.

Meanwhile, there is funding uncertainty surrounding the effort.

The release of the president's budget request for fiscal year 2022 confirmed that the Army is entering a period of increasingly intense budgetary pressure. In the request, the Army saw a topline reduction of 0.9 percent in funding, driven by cuts to research, development, testing and evaluation, 7.6 percent, and procurement, 9.7 percent.

CMOSS chassis and card adoption will require significant investment to be deployed at scale. While important, it is unclear where such investment ranks within the hierarchy of the Army's many modernization priorities. While the current prototyping efforts are affordable, a large-scale technology insertion program will require major investment in an increasingly tight budgetary environment. Initial analysis indicates moving to an open architecture chassis will come at a considerable short-term cost premium to legacy technology solutions.

In the 2022 budget request, the program lacks a discrete funding line. Without long-term clarity on funding prioritization, target quantities, or price sensitivity, it is hard for industry to close the internal R&D business case necessary to accelerate the technical advancement the Army requires.

As such, there are several questions officials might consider with respect to funding and developing a CMOSS chassis.

Firstly, from where will resources come to fund this program and what other Army priorities might have to be sacrificed to make the chassis a reality? What does the deployment schedule for it look like and what production quantity can industry reliably plan around? Which program offices might be responsible for paying for the chassis? These questions will need thoughtful examination and the answers will need to be communicated to industry in a timely manner if this initiative is to succeed.

Army photo

Meanwhile, there is no clear leader for the program.

The implementation of CMOSS seeks to offer operational benefits, enabling plug-and-play capabilities using components from multiple sources across programs of record. However, the benefit of such a modular open architecture system raises questions regarding the allocation of certain program management, acquisition and sustainment responsibilities.

Without a clear delineation of roles and acceptance from all relevant communities, the complex stakeholder landscape involving various program offices, science and technology community, and industry vendors creates challenges, especially when it comes to managing technical development and future upgrades.

Successful execution of CMOSS will require an unprecedented level of coordination among the CMOSS board of directors including, but not limited to, at least three program executive offices and the network cross-functional team that currently oversee joint strategy development, as well as the various industry vendors.

As the CMOSS chassis progresses through its lifecycle, the Army will need to consider and address an ongoing list of questions for its success. At the highest level, it will be important to determine who will own and manage the final integrated chassis solution.

Whether it be the Army, an industry vendor, or a consortium consisting of both the government and industry representatives, the program needs a central authority to oversee testing, qualify cards, manage configurations, and resolve system-level issues stemming from disparate components. For instance, when the precision navigation and timing program manager introduces a new CMOSS-compliant card, it is unclear who will be the defined chassis manager overseeing the card integration and compliance.

From a logistical perspective, each vehicle solution is bound to face technical and integration challenges. For example, what works on the Stryker may not work on the Joint Light Tactical Vehicle, and vice versa. Furthermore, the chassis with CMOSS-compliant cards may not work properly in general, pass electromagnetic interference certification testing, or survive maximum system-level operating temperatures.

What makes CMOSS attractive is the ability to rapidly insert technologies. However, the process that enables rapid technology insertion and resolves ensuing technical challenges has not been communicated nor clearly outlined.

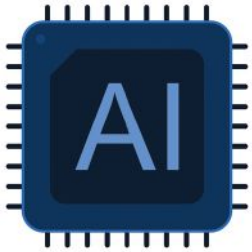
Uncertainty remains around how the government seeks to address these considerations, and more importantly, who will be responsible for managing these system-level challenges. The questions thus far not only highlight the need for the program offices at the implementation level to negotiate roles, but also industry vendors.

How will the government ensure industrial base collaboration in instances where an industry vendor may be responsible for testing, qualifying and integrating competitor products? On the other hand, does the Army seek to fill this chassis manager role itself, and if so, how will the Army avoid similar challenges it has faced when serving as its own integrator in the past?

To make its open architecture vision a reality, the Army may wish to comprehensively study its approach and clearly define a process that outlines respective responsibilities, identifies the intended chassis manager, and encourages collaboration among the various government and industry stakeholders for the long-term success of the chassis and broader CMOSS implementation. **ND**

Matthew Breen is a senior director and Eunice Sohn is a manager at the consulting firm Avascent, where they advise clients in the aerospace and defense industry and provide research and analytical support for aerospace and defense industry clients.

Army Sees Progress With Leader-Follower Vehicle Technology



BY YASMIN TADJDEH

The Army is attempting to leverage robotics and other capabilities to enable its "leader-follower" concept for vehicle convoys. After years of work, the Army has made strides in developing the technology.

At the height of the wars in Iraq and Afghanistan, roadside bombs planted by insurgents maimed and killed servicemembers and civilians alike, targeting vehicle convoys ferrying troops and supplies to bases.

To deal with the threat more immediately, the military invested billions of dollars into uparmored, mine-resistant vehicles that could withstand blasts better. At the same time, it kicked off an ongoing, long-term effort to build autonomous "leader-follow" tech that could cut down on the number of soldiers in harm's way in future fights as well as free up troops for other tasks.

The service is demonstrating progress. It has tested its leader-follower autonomy software at events such as Project Convergence 2021, where the Army tried out technology that can support its offering for the Pentagon's joint all-domain command and control concept. Additional work is being conducted at bases such as Fort Polk, Louisiana, and Fort Sill, Oklahoma.

The Army has primarily been using what it calls palletized load systems, or PLS, unmanned follower vehicles, during its experiments, said Maj. Benjamin Hormann, expedient leader-follower project officer at Combat Capabilities Development Command's Ground Vehicle Systems Center. Soldiers from the 41ST Transportation Company currently own 60 M1075 PLS trucks that are equipped with an autonomy system.

"The unit received new equipment training over two years ago and has implemented a 'train-the-trainer' strategy in order to maintain proficiency throughout the year," he said in an email. "This unit provides real-time feedback to software developers and engineers that get them the capability they want/need very quickly."

The vehicles are currently using a software version known as LF 1.3.

The Ground Vehicle Systems Center is employing what it calls an "engineering in the dirt concept" where soldier feedback is run through an agile software sprint to develop and update the system every 90 days, Hormann said. Meanwhile, the unit also provides information so requirements and doctrine can be updated.

The Army showed off its expedient leader-follower technology at the service's Project Convergence exercise at Yuma Proving Ground, Arizona, this past fall, he said. The annual experiment has been called a "campaign of learning" by officials and is meant to contribute to the Pentagon's JADC2 effort, which aims to better link sensors and platforms into an operating network.

At Project Convergence, officials employed two versions of its autonomy software and completed more than 3,000 miles of robotics testing, Hormann said. The autonomy system was tested on palletized load system trucks, the cold weather all-terrain vehicle and the logistics vehicle system replacement platform.

The Army plans to test leader-follower technology at Project Convergence 2022 with an autonomous missile launcher demonstrator as part of an effort with Army Futures Command's long-range precision fires cross-functional team and DEVCOM's Aviation and Missile Center, Hormann said.

Meanwhile, the service recently completed the final increment of capability improvements for its expedient leader-follower program, he said.

For example, the service merged existing autonomy software with a government-owned Robotic Technology Kernel, he said. RTK is the Army's library of modular software packages that can be used for common ground autonomy software. The software is based on what is known as the Robotic Open System Architecture-Military.

The most recent increment also developed a feature known as "assembly and disassembly" where autonomous PLS trucks could form into a column formation based on orders from a user, as well as "park" the platforms into a line, whether it be from front-to-back or side-to-side, he added.

Another new capability is a "retrotraverse" feature with trailers, which allows the PLS vehicle to reverse and employs what Hormann called a "pin-and-pin-out function."

This capability allows "the warfighter to back up an autonomous convoy with a trailer without having to get out and put the trailer traversing table locking pin in," he explained.

Coming up next for the leader-follower program is Army Test and Evaluation Command safety testing for maturation of its software version 2.0 system.

Over the next two years, the 41st Transportation Company is set to participate in three Collective Training Center exercises with leader-follower technology, Hormann added.

The GVSC and product management office for robotic autonomous systems also plan to further mature the technology's software and hardware, he noted. This includes increased reliability and further hardening of the system.

The Army is currently using a "buy, try, decide" procurement model and a mid-tier acquisition rapid fielding approach when it comes to acquiring the systems, he said.

"There will be a later decision point to increase capability and mass produce the optionally manned leader-follower system for the PLS program of record," Hormann noted.

The Army has been working on autonomous military vehicles since 1999, he said. Some of the platforms the technology has been tested on includes Humvees, HX60 tactical trucks, RG-31 mine-resistant ambush-protected vehicles, medium tactical vehicle replacement systems, M915 tractor trucks, medium tactical vehicles, LMTV light utility trucks and heavy equipment transporters.

More recently, the autonomy hardware and software systems developed through the Ground Vehicle Systems Center include the palletized load system, the cold weather all-terrain vehicle, the high mobility artillery rocket system as well as the Marine Corps' logistics

iStock illustration

vehicle system replacement platform and the Corps' Joint Light Tactical Vehicle Rouge Fires variant, Hormann said.

One company that has been working with the Army on leader-follower technology is Clarksburg, Maryland-based Robotic Research.

In 2018, the Army awarded the firm a three-year, $49.7 million contract to provide autonomy kits for large convoy resupply vehicles as part of the expedient leader-follower program. Robotic Research has had its participation extended with various National Advanced Mobility Consortium contract vehicles, said Jim Frelk, the company's senior vice president. It is currently offering the service technical support on the expedient leader-follower effort.

The organization has been working alongside vehicle manufacturers such as Oshkosh Defense to outfit platforms with its leader-follower autonomy software in places such as Fort Polk, Fort Sill and Camp Grayling, Michigan, for testing. The company provides the autonomy software and Oshkosh provides the drive-by-wire kit for the vehicles, he said.

The company has been working on capabilities such as "safe harbor" features, he noted. Safe harbor functions tell platforms what they should do if there is an attack or breakdown in the systems' sensors.

Leader-follower technology has matured substantially over the years and is at a point where it can now be deployed, Frelk said. "The basic software … that has been demonstrated, in our opinion, doesn't have a lot left to do before you begin to deploy it."

However, there are still some challenges and room for improvement. These include the hardening of sensors and better integration between the vehicles and the onboard equipment, he said.

There are typically seven or eight vehicles in an autonomous convoy, Frelk said. They are all equipped with an autonomy kit and any of the vehicles can take over as the "leader" platform.

"There's no requirement today that there will be a specific vehicle designated" as the lead platform, he noted.

Robotic Research is also working with the Army, the German Federal Ministry of Defence and Rheinmetall to support leader-follower technology with partner nations.

The U.S. Army wants "to expand this capability and make it interoperable with other vehicles … for convoy operations with allied forces," he said.

While the Pentagon has shifted its focus from counterinsurgency operations to great power competition with adversaries Russia and China, Frelk said there is still a need for leader-follower technology.

"There is still going to be vulnerabilities to convoy operations and [a desire to] to reduce the number of deaths and improve … the functionality of moving things rapidly," he said. "Leader-follower is going to be useful."

Additionally, the autonomy packages that are being tested with the leader-follower program are not just relevant for convoy operations, Frelk said. The program has an impact on other vehicles including combat systems.

The same "autonomy kit that's proved out on leader-follower is being deployed on other systems that are weaponized systems," he said. "Think of it as a springboard to combat vehicles and other vehicles being able to operate in GPS-denied environments autonomously."

The basic software stack is portable and can be used with a variety of systems, but different platforms may require separate sensors, he noted. For example, the autonomy needed for off-road operations will be different compared to on-road ops.

"It's a tweaking of the system, not a whole new system," he explained.

Besides working with the Army, Robotic Research also has contracts with other Defense Department components such as the Defense Logistics Agency, Frelk said. Last year, DLA awarded the company a contract to develop an unmanned autonomous guided vehicle to tow loaded carts inside and outside warehouses.

DLA has 20 storage sites and more than 570 warehouses, according to a Robotic Research press release. The development of the AGV could lead to follow-on contracts for as many as 100 vehicles.

The company is also working with the Defense Threat Reduction Agency on counter-weapons of mass destruction efforts, Frelk said.

Meanwhile, in late 2021 Robotic Research completed a $228 million Series A funding round to expand its commercial offerings. That will bear fruit for the military, Frelk said.

"The government gets to benefit from the number of miles that are being driven with similar autonomy capability and the lessons learned there," he said. **ND**

A convoy of semi-autonomous palletized load system vehicles

Defense Dept. photo

BY HEBERTO LIMAS-VILLERS

Improving the Shipbuilding Industrial Base

■ In the 2022 National Defense Authorization Act, Congress authorized $4.9 billion in funding for Arleigh Burke-class destroyers and an additional $4.7 billion for shipbuilding to include two destroyers, two expeditionary transports and a fleet oiler.

The increased attention to U.S. naval capabilities comes after increasing competition with China, as well as discussions around changes to the current force structure. Currently, the Navy is required by law to have at least 355 ships, though plans are in place for expanding the fleet to between 398 and 512 vessels, which includes both manned and unmanned platforms.

This objective is largely aspirational as the number of both private and public shipyards has significantly declined with gaps in experienced personnel, rising costs and a boom-bust cycle in naval acquisitions.

The United States became a global power through its power-projection capabilities, including its naval prowess. To maintain its edge, it must build those capabilities once again.

Since 1993, the number of public shipyards the Navy used fell from eight to four — two on the West Coast and two on the East Coast — due to the "peace dividend" of the 1990s. However, these four shipyards have limited functional dry docks, old equipment, and regularly delay maintenance for the submarine and aircraft carrier fleets.

The U.S. shipbuilding industry is bolstered by 22 private shipyards. Three shipbuilders have left the industry and only one shipyard has opened since the 1960s. Both Huntington Ingalls Industries and General Dynamics, the two largest U.S. shipbuilders, reported a record new construction backlog for 2020 competing for dry-dock space with essential ship maintenance.

What is left is a diminished industrial base incapable of even maintaining the Navy's current presence. Worse, U.S. shipbuilding is significantly behind China, which has dozens of shipyards capable of building and maintaining a fleet that can project naval power beyond the First Island Chain. Because of the nation's investments, the Chinese navy grew to approximately 350 ships by 2020, and Beijing now has the largest navy in the world by ship numbers albeit not by tonnage.

Efforts are being made by the U.S. Navy to renovate its public shipyards through a 20-year, $21 billion Shipyard Infrastructure Optimization Plan. However, more attention needs to be given to the private shipyards that already construct and maintain most of the fleet from fleet oilers to destroyers.

Private shipyards remained largely profitable during the COVID-19 pandemic, though their margins have been negatively impacted. The main issues that limit private shipbuilders in the long term lies in personnel, rising costs of materials, and inconsistent acquisition priorities that threaten to consolidate the industry further if not properly addressed.

Having enough skilled technicians to construct and maintain these ships is a considerable problem for industry. Since the 1990s, the workforce has aged, leaving shipyards with an increasingly fragile workforce with a dearth of skilled younger workers in the pipeline. While shipbuilders like Huntington Ingalls have some form of an apprenticeship program, demand for a skilled workforce during COVID remains considerable. This lack of skilled technicians causes delays in construction and maintenance, compromising the Navy in a possible future engagement.

Fortunately, there is a growing recognition of this employment gap by the Defense Department. In June 2020, it announced a pilot program to train new welders and other specialized roles for public shipyards. While it is starting small, programs like these will help eventually bridge the gap with proper funding and training provided.

Another issue shipbuilders face is the rising costs of materials. This is a problem throughout the entire economy, though the Congressional Budget Office found that the Navy shipbuilding cost index was 1.2 percent higher than overall inflation between 1986 to 2009. This is partly due to specialized construction needs in contrast to the general economy, low competition among shipyards and low-volume orders.

In the long term, encouraging more contractors to provide shipbuilding capabilities will lower the cost index, though this will require an increased budget for the Navy.

Lastly, the main issue inhibiting private shipbuilding is the inconsistency in demand from the Navy. Currently, there is a bipartisan consensus on increasing the service's size, though this follows decades of boom-and-bust cycles in procurements reducing the industrial base as seen with the closure of Huntington Ingalls' Avondale Shipyard in 2014.

The Navy's shipbuilding plan has also been unhelpful, given a vacillating post-Cold War period with halting efforts to modernize and properly adapt to the era, as seen with the Littoral Combat Ship program and Zumwalt-class destroyers. Shipyards are harmed as each program requires significant investment to properly construct and maintain new ships, only for it to be squandered when the Navy cancels orders and moves to develop other systems.

Further, this encourages consolidation that limits the competition needed for a robust naval acquisition strategy. To ensure that the shipbuilding industrial base doesn't deteriorate further, it is important that there is a consistent procurement of ships and a clear commitment toward new systems as needed.

In the long term, more shipyard capacity must be built — both by the government and private sector — to meet the demands of a larger U.S. Navy. However, significant changes to training and acquisitions need to take place to ensure sustainability for the longer term. ND

Heberto Limas-Villers is a junior fellow at NDIA.

Huntington Ingalls photo

BY SUSAN CASSIDY, ASHDEN FEIN AND ROBERT HUFFMAN

Pentagon Releases Updated CMMC Documentation

The Defense Department has been increasingly focused in recent years on protecting controlled unclassified information, or CUI, within its supply chain. Until recently, contractors were working to implement requirements set forth under CMMC Version 1.0 in anticipation of the rollout.

However, the Pentagon announced CMMC Version 2.0 in November and released key documentation with implications for contractors.

CMMC 2.0 simplifies certain aspects of CMMC 1.0 and requires compliance with fewer technical controls. A key difference between the versions is the reduction in the levels from five to three in CMMC 2.0 — Foundational (Level 1), Advanced (Level 2) and Expert (Level 3) — as well as the elimination of all maturity processes.

Under the new version, a Level 1 self-assessment is required where federal contract information, or FCI, is involved. A Level 2 self-assessment/attestation or third-party certification is required where CUI is involved, and a Level 3 assessment is required when the Defense Department determines that a contractor must implement additional practices to reduce the risk associated with advanced persistent threats.

The Pentagon has stated that CMMC 2.0 will not be a contractual requirement until the department completes the rulemaking needed to implement the program. However, it released key documentation over the final weeks of 2021 that provides insight into forthcoming program requirements, including: a model overview document; self-assessment scopes for Level 1 and 2 assessments/certifications; assessment guides for Level 1 and 2 attestations/certifications; and the artifact hashing tool user guide.

Although that rulemaking process is estimated at nine to 24 months, these documents are highly relevant to any contractors selling to the department.

The newly released overview document outlines the general requirements that contractors must implement to achieve each level. It affirms that Level 1 of CMMC 2.0 is equivalent to all of the safeguarding requirements from Federal Acquisition Regulation clause 52.204-21 and Level 2 is equivalent to all of the technical controls in NIST SP 800-171 Rev. 2. It also indicates that Level 3 certification requirements will be a subset of the requirements in NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171," but it does not specify which requirements will apply.

In each case, the levels build on one another, i.e., a contractor must implement all of the technical controls at Levels 1 and 2 plus additional Level 3 requirements to achieve a Level 3 certification.

The CMMC self-assessment scope for Level 1 and Level 2 is used to define those assets within the contractor's environment that will be in scope of the assessment and self-attestation/third-party certification. Specifically, this document relates to the description of the environment that will store, process, and/or transmit FCI (Level 1) or CUI (Level 2), which are considered to be "in-scope assets."

Each of these documents makes clear that there are no documentation requirements for out-of-scope assets and that such assets should not be part of the assessment. Notably, each document addresses "specialized assets," which include: government property; internet of things or industrial internet of things; operational technology; restricted information systems; and test equipment.

Specialized assets are not part of the assessment scope under Level 1 and are therefore not assessed against CMMC practices.

Specialized assets are part of the assessment scope under Level 2, however, and contractors are required to document these assets in the system security plan and detail how they are managed using the contractor's risk-based information security policy, procedures and practices.

The Level 1 and Level 2 assessment guides are intended to provide certified assessors, contractors, and IT and cybersecurity professionals with guidance to help prepare for an assessment, including self-assessments. The two guides are similarly organized, and each provides: an overview of the assessment and certification process; information about assessment criteria and methodology; clarification of the intent and scope of various terms of the CMMC; and assessment requirements and specifics for each practice.

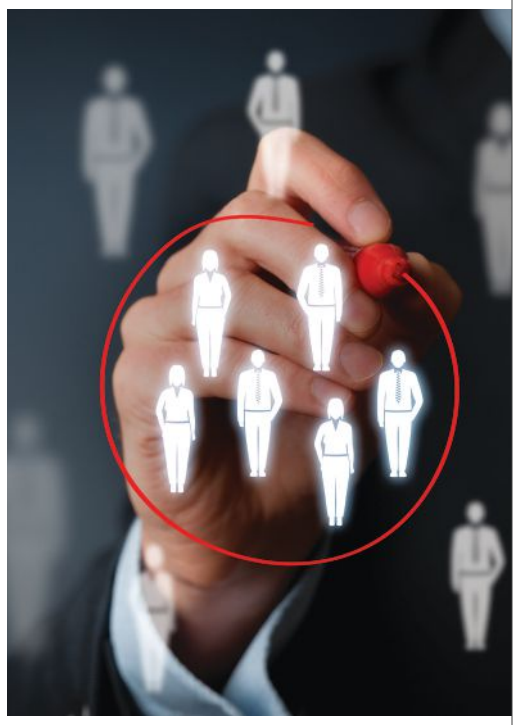
Specific information in the guides includes the type of documentation to be assessed, documentation of assessment findings, and examples of implemented technical practices, among other things. The Level 2 assessment guide also indicates that it leverages information included in NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information."

The artificial hashing tool user guide provides an overview of the CMMC's artifact hashing tool, which is used to create a unique digital fingerprint (i.e. SHA-256 hash) for each document, file, or other artifact used as proof of compliance. The document explains that assessors do not take copies of artifacts of evidence with them after an assessment because these articles are proprietary to the contractor. Instead, the assessor generates unique fingerprints of each file using the tool and follows the instructions set forth in the guide so that the assessor can document the exact artifacts, and the contractor could produce those artifacts in the future, if needed. ND

Susan Cassidy and Ashden Fein are partners and Robert Huffman is senior of counsel at Covington & Burling LLP. Ryan Burnette, an associate at the firm, also contributed to this article.

iStock illustration

Association Launches Career Center



The National Defense Industrial Association unveiled its new NDIA Career Center at the start of 2022. The center is a member benefit that brings together employers with the most qualified job seekers in a variety of in-demand defense and national security fields.

NDIA members with vacancies can connect with highly qualified candidates through 30-day and 60-day postings, emailed alerts and more. Members looking for jobs have several features to pursue openings, including a quick-search capability and advanced search tools to look for specific companies, experience levels, qualifications and other qualities.

"NDIA perceived a need for an avenue to bring exceptional candidates and employers together," said Christine Klein, the association's senior vice president for meetings, divisions and partnerships. "We are pleased with this offering and excited about the NDIA Career Center. I am sure our members will find this an immeasurable benefit."

NDIA corporate members can receive a discount package for posts that include company logos on the career center homepage, sending job alerts directly to candidates, and other benefits. The center can be accessed at jobs.ndia.org. ND

Nominations Open for William J. Perry Award

NDIA is calling for nominations for the 2021 William J. Perry Award. Nominees must have made significant contributions that have led to the strengthening of U.S. national security by the direct application of precision strike capabilities to Defense Department systems and/or to the enhancement of the industrial technology base for application to precision strike technology.

The award will be presented at the Integrated Precision Warfare Review taking place May 4-5 in Arlington, Virginia. Nominations are due March 18.

Please contact George Webster at gwebster@NDIA.org for more information. ND

Call for I/ITSEC 2022 Papers

The National Training and Simulation Association's Interservice/Industry Training, Simulation and Education Conference Committee invites interested individuals to submit previously unpublished work and encourages original papers for its 2022 conference.

I/ITSEC 2022 will take place Nov. 28 through Dec. 2 in Orlando, Florida. This year's theme is "Accelerate Change by Transforming Training (ACTT): It's Time to ACTT!"

iStock illustrations, NDIA photo

The theme "establishes a challenge to our community based on the pandemic and global environments to enhance, adapt and accelerate our solutions to meeting training requirements through advanced technology and approaches," organizers said.

"Being faced with declining resources, increased competition and the ability to rapidly implement new technology across the community, we must be able to achieve this transformation before the solutions and approaches themselves become obsolete," they added.

Prospective authors are encouraged to read through I/ITSEC subcommittee descriptions found at https://bit.ly/3tc8n0u and submit abstracts for papers that discuss the core research the industry will put forth to improve the next generation of learning.

Proposals are due by Feb. 21. ND

NDIA Calendar

■ The National Defense Industrial Association continues to follow all developments regarding COVID-19 and is diligently examining each event to determine the best course of action as we look forward to gathering leaders in government, industry, and academia again to solve the most challenging issues in national security in person.

NDIA will be implementing the following policies for all of our meetings, conferences and events: *(Local and State regulations permitting.)*

■ **PROOF OF VACCINATION:** All attendees will be required to upload proof of vaccination or proof of negative PCR COVID-19 test performed by a medical professional within 72 hours of arrival on-site for badge pick-up. Details for securely uploading documentation will be provided on the event website.

■ **MASKS:** Fully vaccinated attendees are encouraged to wear face masks but, in accordance with CDC guidance, may make that choice for themselves. If you are not fully vaccinated, you are required to wear a face mask in public places.

■ **WAIVER:** All registrants are required to sign the COVID-19 waiver during the online registration process. Attendees may disclose their vaccination status at the time of signing.

The health and safety of all our registrants are our highest priority, and we will continue to follow local, state and CDC guidelines to keep everyone safe.

Visit NDIA.org/events for more information.

Christine M. Klein
Senior Vice President, Meetings, Divisions & Partnerships

FEBRUARY

8-10 2022 Virtual Expeditionary Warfare Conference
Virtual
www.NDIA.org

23 NTSA February Webinar
Virtual
NTSA.org

28-March 2 2022 Tactical Wheeled Vehicles Conference
Norfolk, VA
www.NDIA.org/TWV22

MARCH

7-10 2022 Pacific Operational Science & Technology (POST) Conference
Honolulu, HI
NDIA.org/POST

15 36th Annual National Logistics Forum
Salt Lake City, UT
NDIA.org/Logistics36

28-30 Undersea Warfare Spring Conference
San Diego, CA
NDIA.org/USWSpring22

30 NTSA March Webinar
Virtual
NTSA.org

APRIL

6-7 2022 DLA Land & Maritime Supplier Conference & Exhibition
Columbus, OH
www.NDIA.org

6-7 Munition Executive Summit
Parsippany, NJ
www.NDIA.org

25-27 2022 Joint NDIA/AIA Spring Industrial Security Conference
Clearwater Beach, FL
NDIA.org/ISCSpring

27 NTSA April Webinar
Virtual
NTSA.org

26-28 22nd Annual Science & Engineering Technology Conference
Miami, FL
NDIA.org/SET22

NDIA | CAREER CENTER

Connecting Talent with Great Opportunities – NDIA Career Center

The National Defense Industrial Association offers qualified defense and national security professionals and employers an intuitive platform to identify the next best opportunity or candidate.

Looking for the Right Candidate?
Interested in a better way to engage with and recruit qualified defense and national security professionals? NDIA's new online career center will make searching for candidates easier.

Looking for the Right Job?
Looking for your next career opportunity? The NDIA Career Center is your solution.

Complete your profile today at Jobs.NDIA.org

Next Month

Navy Sustainment
■ Sustainment of ships is a perennial challenge for the U.S. Navy. Navy leaders and experts provide an update on what the sea service is doing to tackle the problem.

Navy and AI
■ As the Navy continues to invest in new tech, *National Defense* will look at how the service is bringing digital infrastructure and artificial intelligence to the fleet.

Navy Autonomy
■ The Navy is investing heavily in autonomous systems and has stood up new testing and integration centers to support the technology. Officials hope the tech can give sailors greater situational awareness, free up time for different tasks and keep them out of harm's way.

China's Missiles
■ The Chinese military is advancing its missile capabilities. How should the United States respond to this growing threat?

Army Long Range Strike
■ The Army will deliver 24 capabilities to warfighters by 2023, including several long-range strike systems. The service is prioritizing the weapons, which officials have said could be instrumental in great power competition.

Bridging the Aerial Refueling Gap
■ The Air Force is facing a 13 percent gap in aerial refueling capacity through the mid-2020s as it retires aged KC-135 and KC-10 tankers faster than they can be replaced by the troubled KC-46A. The options to fill the gap include the controversial bridge tanker and advanced tanker.

Space Force
■ Now in its third year of existence, Space Force leadership has bold plans as they continue to build out the service. In our next issue, *National Defense* examines what lies ahead for Guardians.

FEBRUARY 2022 Index of Advertisers

Interact with the companies whose products and services are advertised in *National Defense*.

Are you prepared for CMMC 2.0?

A resilient defense supply chain enables the mission and national security.

Our nation's supply chain is constantly under attack. The Defense Industrial Base (DIB) that enables the DoD's mission is critical to military superiority and national security. CMMC certification is designed to improve the DIB's resiliency and will be required for all organizations supporting the DoD.

CMMC requirements are exacting. As a CMMC-AB Registered Provider Organization and C3PAO Candidate, Coalfire Federal can help you effectively prepare with our CMMC Advisory services.

Contact us today to discuss your CMMC strategy and explore how Coalfire Federal is helping the Defense Industrial Base prepare for CMMC certification.

COALFIRE FEDERAL

Protect the mission.

CoalfireFederal.com | cmmc@coalfirefederal.com

Get Ready for CMMC 2.0 with C3 Integrated Solutions

The C3 CMMC Readiness Program

C3 Integrated Solutions specializes in securing our nation's Defense Industrial Base using the Microsoft Government Cloud.

Our C3 CMMC Readiness Program leverages Microsoft 365 GCC High, Azure Government, and industry leading partners to meet Cybersecurity Maturity Model Certification (CMMC) requirements in a methodical, incremental approach.

To get the most out of GCC High and understand your road to compliance, turn to C3 Integrated Solutions.

Get started today

To learn more about the C3 CMMC Readiness Program, visit c3isit.com/CMMC.

Microsoft Partner
Microsoft
Gold Cloud Productivity
Gold Windows and Devices
Silver Enterprise Mobility Management
Silver Collaboration and Content
Silver Security

Inc.5000 N° 34 2021 IT MANAGEMENT

CMMC-AB REGISTERED RPO

2021 BEST PLACES TO WORK Arlington

C3 INTEGRATED SOLUTIONS
connect, communicate, collaborate

(571) 384-7950 | info@c3isit.com
3033 Wilson Blvd | Suite 700 | Arlington, VA 22201