

National DEFENSE

NATIONALDEFENSEMAGAZINE.ORG

SPECIAL REPORT:
Contested Logistics
PAGE 34

ChatGPT:
Friend or Foe?
PAGE 30

RISE OF THE DRONE SWARMS

Pentagon Pushes to Field Thousands
Of Small, Smart, Cheap Robots

PAGE 18

JANUARY 2024

\$6.99US \$7.99CAN



NDIA NDIA'S BUSINESS &
TECHNOLOGY MAGAZINE

AI project blowing up?



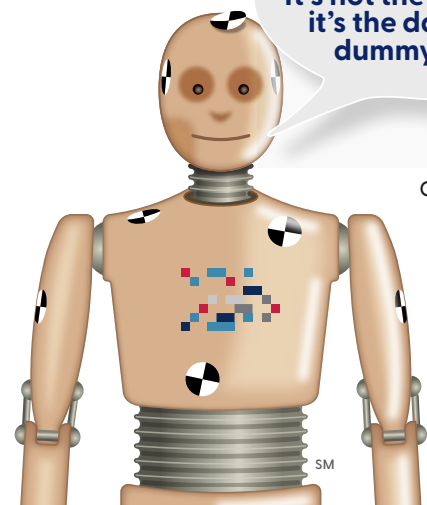
You're not alone. The vast majority of companies that implement an advanced technology application are initially disappointed with its mediocre performance. This typically isn't a fault of the application; **it's caused by the data** and a lack of alignment with business goals.

It's not the tool,
it's the data
dummy.

Our DataInFormationSM suite of solutions can get your data into the proper formation through data validation, cleansing, labeling, analysis and more.

- We operate 100% in the USA, so your data stays in the US
- Our workforce is 80%+ veterans and military families

Our human-enhanced data solutions will get your project back on track and your AI/BI/ML tool performing at its best. And that's no accident.



DataInFormationSM

Liberty Source PBC ■ Fort Monroe, Hampton, VA ■ 757-214-9643
sales@liberty-source.com ■ liberty-source.com

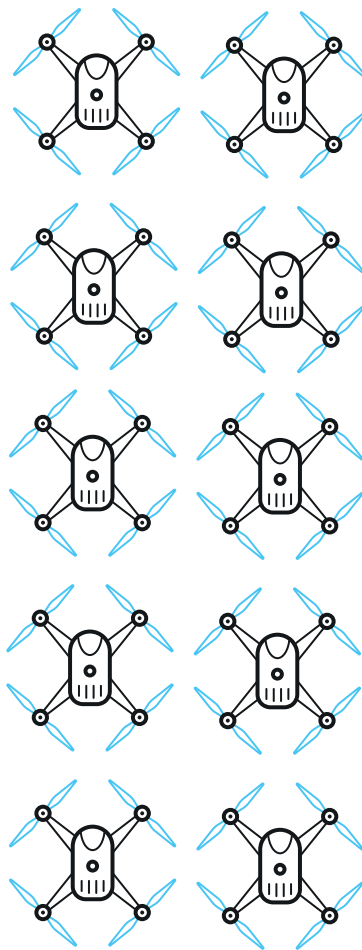
CAGE Code: 7EWU6 UEI: JE8WCRU4TGM7

CONTENTS

January 2024 | Volume CVIII, Number 842 | NationalDefenseMagazine.org

NDIA'S
BUSINESS &
TECHNOLOGY
MAGAZINE
NDIA

**National
DEFENSE**



REPLICATOR 18

• Deputy Secretary of Defense Kathleen Hicks laid out an ambitious goal when she announced the Replicator initiative in August to field thousands of all-domain, attritable, autonomous swarming robots within two years. But its true measure of success may lie in its ability to revolutionize the acquisition process.

CONTESTED LOGISTICS 34

• The Defense Department is on the hunt for new tactics, techniques, procedures and technologies that can ensure supply lines are open in the event of a major conflict.

GENERATIVE AI 30

• Experts suggest increasingly intelligent large language models are not something to be feared, but rather tools to make human lives easier. They just need to be used effectively.

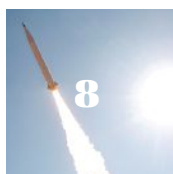


CORRECTION: On page 13 of the November 2023 issue, the story “Turkish Companies Developing Kamikaze Robotic Sub” misidentified the boat builder on the project as Kraken Yachts. The company said it is not involved in the project.



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. Copyright 2024, NDIA

CONTENTS



4 NDIA PERSPECTIVE

Views from the association's leadership

6 EDITOR'S NOTES

From the desk of the editor in chief

BY STEW MAGNUSON

7 EMERGING TECHNOLOGY HORIZONS

Looking toward the tech of the future

8 DISPATCHES

News from the U.S. and around the world

COMPILED BY STEW MAGNUSON

14 ALGORITHMIC WARFARE

What's coming in artificial intelligence, big data and cybersecurity BY JOSH LUCKENBAUGH

15 BUDGET MATTERS

Who's funding what in Washington

BY SEAN CARBERRY

16 INDUSTRY PERSPECTIVE

Cloud Service Providers as the Technical Arsenal of Democracy

BY JASON ATWELL

18 COVER STORY

Replicator Initiative Looks to Swarm Through 'Valley of Death'

BY JOSH LUCKENBAUGH

22 Indo-Pacific Focus Provides Hint Into Replicator Shopping List

24 COMMENTARY

Opening the Replicator Program's Pandora's Box

BY DR. JAMES GIORDANO

26 ROBOTICS

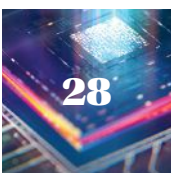
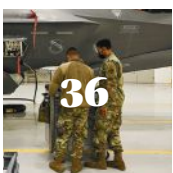
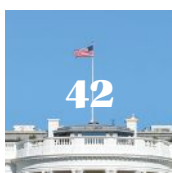
'Disaggregation' Called the Future of Naval Warfare

BY SEAN CARBERRY

28 SPACE

Quantum Science Finding Its Way Into Satellite Technology

BY LAURA HECKMANN



30 TRAINING AND SIMULATION

Large Language Models Have Pitfalls for National Security

BY LAURA HECKMANN

32 Air Force Overhauling Training To Take On Near-Peer Foes

33 Army to Replace 'Laser Tag' System for Soldier Training

34 ARMY LOGISTICS

Army to Live Off the Land in Contested Environments

BY ALLYSON PARK

36 GOVERNMENT PERSPECTIVE

The Role of Logistics, Sustainment In Integrated Deterrence

BY CHRISTOPHER LOWMAN

38 NAVY FUEL LINES

Navy Going Digital to Increase Energy Efficiency

BY JOSH LUCKENBAUGH

40 NDIA POLICY POINTS

Views from the association's policy division

41 NDIA BOARD OF DIRECTORS

42 GOVERNMENT CONTRACTING INSIGHTS

Analysis of the newest rules and regulations

CONTRIBUTED BY COVINGTON & BURLING

43 NDIA NEWS

Happenings at the association

44 NDIA CALENDAR

A complete guide to NDIA events

48 NEXT MONTH

Preview of our next issue

48 INDEX OF ADVERTISERS

Connect with our sponsors

STAFF

EDITOR IN CHIEF

Stew Magnuson

(703) 247-2545

SMagnuson@NDIA.org

CREATIVE DIRECTOR

Brian Taylor

(703) 247-2546

BTaylor@NDIA.org

MANAGING EDITOR

Sean Carberry

(703) 247-2542

SCarberry@NDIA.org

SENIOR EDITOR

Josh Luckenbaugh

(703) 247-2585

JLuckenbaugh@NDIA.org

STAFF WRITER

Laura Heckmann

(703) 247-2543

LHeckmann@NDIA.org

EDITORIAL ASSISTANT

Allyson Park

(703) 247-9469

APark@NDIA.org

ADVERTISING

SVP, MEETINGS, DIVISIONS & PARTNERSHIPS

Christine M. Klein

(703) 247-2593

CKlein@NDIA.org

SALES DIRECTOR

Kathleen Kenney

(703) 247-2576

KKenney@NDIA.org

ACCOUNT EXECUTIVE

Jacob Wright

(703) 247-2568

JWright@NDIA.org

National Defense

2101 Wilson Blvd.

Suite 700

Arlington, VA 22201

NDIA

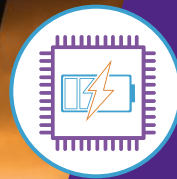
NDIA MEMBERSHIP: The National Defense Industrial Association (NDIA) is the premier association representing all facets of the defense and technology industrial base and serving all military services. For more information please call our membership department at 703-522-1820 or visit us on the web at NDIA.org/Membership

Solutions for Automating Mission-Critical Development



Multi-Domain

From sea to space



Low SWaP

Low size, weight and power



The Broadest IP Portfolio

From standard cells to AI acceleration



AI-Driven EDA

Faster development with improved results



DMEA Accredited Services

US DoD trusted silicon design services



Targeted Solutions for Aerospace, Defense, and Government

Security, Space, 3DHI, Photonics, and Digital Twins

New Industrial Strategy Echoes Association Goals

The horrific Oct. 7 terrorist attack on Israel has been difficult to comprehend. As we pray for peace, we need to understand this attack has immediate implications for the U.S. military and its defense industrial base.

The attack was conducted with a combination of new military technology and old civilian equipment such as bulldozers, rubber boats and paragliders. The attack reinforced the need to prepare for the changing character of war, with an emphasis on new uses of technology and new operating concepts.

But that is only part of the story. To deter this from devolving into a wider regional conflict, the United States sent significant force elements, including a second carrier strike group and Air Force jets armed with advanced munitions, into the region. It was an important, visceral reminder of the lesson history teaches us: wars often start with the tactical surprise of new technologies, but they are almost always won through the enduring strength of robust industrial bases.

For the past year — using its annual “Vital Signs” report on the health of the U.S. defense industrial base and more — the National Defense Industrial Association has been conducting an educational campaign to highlight the necessity of transforming a brittle industrial base, which was shaped and resourced for low-intensity conflict, into a threat-informed, resilient defense ecosystem that can both deter near-peer competitors and be responsive at scale to multiple contingencies and crises.

This transformation will require time, money, strategic discipline and patience.

To this end, Secretary of Defense Lloyd Austin released the department’s inaugural “National Defense Industrial Strategy,” which notes today’s industrial base is not postured to respond to the dynamic requirements of near-peer modern conflict.

Furthermore, the department notes the current state of U.S. supply chains and workforce, technological change, spending constraints and geopolitical threats need action if we are to sustain our competitive advantage. The



strategy has notable strengths, including highlighting the dangerous gaps between the robust and resilient industrial base called for in the 2022 National Defense Strategy and the current industrial capability and capacity. It also recognizes that to be a true mobilization partner with industry, the department needs to prioritize and optimize defense needs beyond traditional cost, speed and scale.

The strategy identifies clear goals, two of which especially resonate with industry: the need to rebuild resilient supply chains and the need for dynamic production and workforce readiness.

As the Defense Department moves into the implementation phase, NDIA will encourage it to engage with industry to ensure government and industry are aligned on goals, actions and metrics.

There are three areas that merit ongoing attention: the cause and



effect of the current posture of the defense industrial base, the funding gaps and the performance metrics.

First, the Defense Department must internalize that the current defense industrial base has been shaped by bipartisan policy and resourcing decisions it and Congress made over the last 30 years. Some of those decisions have been obviated by the subsequent relationships between the financial markets and institutions and the publicly traded companies, including those companies in the defense industrial base.

Today’s public boards are highly attuned to institutional investors who deploy massive amounts of capital in multiple sectors on a global scale and expect healthy returns on their investments. Those markets and companies respond to contracts, not press releases. As it implements its strategy, the department must pay more attention to its intended and unintended market signaling and infuse more rigorous discipline into a predictable requirements process.

Second, the strategy acknowledges many of the current known risks in the defense industrial base are due to past budget decisions. Therefore, the department will need to address the requirement for additional resources to support the proposed actions in the strategy.

Finally, all stakeholders — inside and outside of government — need to be clear on why we must make the defense industrial base resilient.

To reiterate, the industrial base needs to be a threat-informed, resilient ecosystem that can deter near-peer competitors, respond to multiple contingencies and crises and, if needed, be able to surge to respond to conflict. This requires that investors understand the exact nature of the threat and what is at stake for them and the concomitant need for an industrial base that is resilient through conflict by design, not just designed to be resilient through competition.

If the strategy is to be an actionable and effective roadmap for the necessary seismic shift our defense industrial base needs, we need your intellectual rigor, expertise and experience with us in this effort. Throughout 2024, NDIA is doubling down on its commitment to providing strategic forums to connect you and your company across every echelon of the Defense Department. Our goal is straightforward: we are determined to improve the readiness of the defense industrial base so warfighters never enter a fair fight.

Therefore, I invite you to join us as we kick off our 2024 strategic conference season. Please start by attending the 38th Annual National Logistics Forum Feb. 6-7 in Oklahoma City, Oklahoma. The theme of this year’s forum is “Integrated Deterrence: Driven by Logistics.”

For nearly four decades, this national event has brought together senior defense officials, industry and acquisition leaders, logisticians, financial experts and coalition partners to exchange ideas and share insights into the best ways to support our nation’s warfighters. We look forward to seeing you there! **ND**

Michael Bayer is NDIA board chair and president and CEO of Dumbarton Strategies.

**NDIA
MEMBERSHIP
INCLUDES A
NATIONAL
DEFENSE
SUBSCRIPTION**



NDIA

STRENGTHENING THE INDUSTRIAL BASE FOR THE NEXT 100 YEARS

**National Defense Industrial Association
Affiliated Organizations**



JOIN US



Holidays with the CRINKs, Not a Lot of Fun

HALIFAX, Nova Scotia — When first hearing the word CRINKs, I thought they were talking about some wacky family in a movie. Wasn't that a hit comedy? "Meet the CRINKs," or "Holiday with the CRINKs?"

In fact, CRINKs isn't a family name. It's an acronym for China, Russia, Iran, North Korea.

And there's nothing funny nowadays about them.

The term "CRINKs" was first heard at the 15th annual 2023 Halifax International Security Forum, and the term is the brainchild of its founder and president Peter Van Praagh. The forum invites about 300 attendees from 75 democratic countries each year — diplomats, academics, military officers, politicians, activists and journalists — to engage in discussions about the state of democracy around the world and to get what he calls "an annual dose of moral clarity."

The violent new era of global conflict is the direct result of Vladimir Putin's invasion of Ukraine, he asserted.



who ironically called all the attendees "war criminals."

They served as an immediate reminder that since the 2022 Halifax conference, the situation in the world seems to have only grown worse after Hamas' terrorist attack on Israel in October — as well as an example that not everyone in the world enjoys what they had: the right to free speech.

A key assertion over the weekend was that the CRINKs are increasingly coming together in an unholy technological alliance.

While there were some participants who referenced the days of yore when China and Russia were at odds, the evidence that this alliance is real is becoming more obvious, even for those of us who have no access to intelligence reports.

Iranian-made drones are used to attack Ukraine. North Korea and Iran share rocket technology. Putin met with Kim Jong Un in Russia's Far East to discuss military matters, and so on.

Back at the IDEX defense trade show in Abu Dhabi in 2009, *National Defense* reported on a Chinese company's catalog distributed to potential customers that had pages of "Big Brother" technology for sale.

Now, 15 years later in Tehran, "Chinese cameras are everywhere to identify unveiled women," Iranian activist and president of the World Liberty Congress Masih Alinejad said during a panel discussion.

Look for China to sell its AI-enabled surveillance systems to any dictator who has the cash in the coming years.

And it's not just "hard power" technologies, the other countries are picking up on Russia's disinformation tactics, techniques and procedures to divide and conquer the populations in unfriendly nations.

China ahead of the Taiwan elections was actively spreading disinformation to influence voters, said Vincent Chao, spokesperson and director of the Democratic Progressive Party of Taiwan.

In one recent case, the People's Republic of China successfully managed to place a front-page story in a Taiwanese newspaper that claimed the United States was pressuring Taiwan to build bioweapons.

"The tell-tale signs that this

was misinformation were still there, but they weren't as obvious as in the past," Chao said.

Once, North Korea had little capability to conduct cyberattacks, theft and espionage. Having almost no one in the population with access to the internet — that seemed logical.

But it learned. It first paid for "hackers for hire" to do its dirty work, but those contracts must have included some training because today North Korean operators are reportedly adept at raiding cryptocurrency accounts and are using the funds to build rockets.

Look for this "hackers for hire" model to be repeated. Any country with the inclination and enough cash will be able to use social media to meddle in their neighbors' elections.

Dictators are creating a network for how to censor, do surveillance, spread fake news and use social media, Alinejad said. They are helping each other suppress their own people and those outside their border, she added.

Steve Tsang, director of the China Institute at the School of Oriental and African Studies at the University of London, wrote in a paper distributed at the forum that Putin's ultimate defeat in Ukraine would put China at the center of the CRINKs' orbit.

"CRINKs is a partnership of convenience rather than an alliance sharing a common goal. Its members know that the existing world order is not conducive to their ultimate ambitions," he said.

The good news during a time of decidedly bad news around the world is that the CRINKs might be a partnership of convenience, but the rest of the free world has tech alliances that are more than just expediency.

The Quad — the United States, Australia, Japan and India — have a nascent tech alliance to counter China, and the AUKUS agreement between Australia, the United States and the United Kingdom is looking stronger every day.

There are the Five Eyes, NATO and too many bilateral technology sharing agreements between freedom-loving nations to list here.

And as Van Praagh said, as long as their resolve can't be shaken, the CRINKs don't stand a chance. **ND**



"Our goal this weekend is to show China, Russia, Iran and North Korea — what we call the CRINKs — that our resolve cannot be shaken. When the democracies of the world work together, there is no challenge that cannot be met," he said at a press conference.

After Putin fails in Ukraine, then the world will return to some sort of normalcy, he asserted.

Outside the hotel where the forum took place on day one was a crowd of two dozen pro-Palestinian protestors — one with a bullhorn,

Enabling Logistics in Contested Environments

The Defense Department has enjoyed decades of military supremacy. Because adversaries lacked the capability to target U.S. and allied forces and supplies in transit to a theater of operation, the military has conducted unobstructed deployment and resupply activities. Today, China has been identified as the “pacing threat,” ending the era of uncontested logistics.

The Joint Chiefs of Staff recognized the need for the department and each military service to modernize to meet this new challenge, leading to the creation of the Joint Warfighting Concept — a threat-informed operational document detailing how the Joint Force will operate and fight cohesively across all domains.

Contested logistics — a key tenet of the concept — describes a problem set, including increased threats to supply chains, reduced mobility and the need to operate in a resource-constrained environment.

To contribute to the conversation, the National Defense Industrial Association’s Emerging Technologies Institute recently released “Enabling the Joint Warfight.” The report is based on several panel discussions hosted by ETI that focused on the capabilities and technologies necessary to address the operational challenges that the concept describes. The panels focused on building flexibility in logistics, plans and operations to ensure that the warfighter remains sufficiently supported during a future conflict.

To increase resiliency, the Defense Department must address key technical challenges. Tangible benefits will arise by improved data management, shortening the decision cycle time and building resiliency into command and control.

To plan for and adapt to logistics failures, data will need to be collectively visible to the Joint Force. Service stovepipes inhibit data management, which affects how the services coordinate delivering supplies such as replacement parts. There are several initiatives by the Joint Staff Logistics Functional Capabilities Board to understand how the services are gathering their data.



While there is some improvement in coordinating needs such as fuel, transparency and data-sharing between the services remains an uncomfortable but necessary step for supply chain visibility, interoperability and the development of artificial intelligence solutions for data management.

Better data management will also enhance the department’s ability to embrace digital engineering. Models, structured data and infrastructure are key to revolutionizing how the services approach the acquisition materiel life-cycle. In fact, ETI is working with the Air Force and Army on adopting digital materiel management capabilities to help facilitate collaboration between industry and government. For logistics, these processes will enable automated, data-driven decision-making, which will help proactively address issues, including diminishing manufacturing sources and materiel shortages.

The Defense Department’s ability to automate — or otherwise speed up — decision-making will be a key enabler of resilient logistics. This would allow commanders to make faster threat assessments and ensure logisticians can provide multiple materiel options in real-time. Machine learning tools can help support decisionmakers with analysis, namely network modeling, decision optimization and advanced pattern recognition — all of which will help the military respond more dynamically to a fast-paced battlespace.

The cyber and space domains play an integral role in the department’s ability to command and control, where increasing resiliency will be accomplished vis-à-vis distributed control.

The Joint Requirements Oversight Council is working to identify capabilities through experiments like live exercises, wargames and tabletop exercises. Operating successfully in a contested environment entails using different nodes, routes and distribution platforms.

However, combat is becoming so complex that it has begun to render live exercises insufficient for making informed decisions. Among the greatest needs is to invest in modeling and simulation experimentation tools to support the development, integration and transition of next-generation contested logistics solutions such as autonomous systems and additive manufacturing.

Lastly, the Defense Department will need to continue to enhance intra-agency, commercial and international relationships to create new ways of delivering fuel and supplies to the front lines. Access is key in a future conflict in the Indo-Pacific. By partnering with commercial industry, it can leverage shipping lanes and ports to build resiliency in its logistics operations.

At NDIA’s Emerging Technologies Conference in August, Defense Logistics Agency representatives noted their inventory managers are working with industry to support surge capacity and increase supply chain resiliency. The Defense Department is also seeking to establish agreements with international allies and partners in the region for needs such as airfields or distribution networks on the ground.

The department has identified last mile delivery as a current shortfall. Ultimately, harnessing commercial and international partner logistics capabilities will be crucial to solving infrastructure, force posture and delivery gaps.

While the Joint Warfighting Concept was created to prepare for a potential conflict in the Indo-Pacific, the modernization changes it calls for will lead to benefits that are applicable to every combatant command. Capabilities such as faster decision-making loops and route optimization will give the Defense Department the agility to succeed in any 21st century fight. With these kinds of sustained investments, it can ensure it will operate effectively in contested environments by using its personnel and equipment as efficiently as possible. **ND**

Alan R. Shaffer served as deputy undersecretary of defense for acquisition and sustainment. Wilson Miles is an associate research fellow at NDIA’s Emerging Technologies Institute.

DISPATCHES

NEWS FROM THE U.S. AND AROUND THE WORLD COMPILED BY STEW MAGNUSON



Precision Strike
Missile Increment 1

Army Looks to New Missile to Attack Enemy Ships from Shores

BY STEW MAGNUSON

HALIFAX, Nova Scotia — The Army's top officer in the Indo-Pacific theater welcomed the recent news that the service's new Precision Strike Missile has successfully completed a crucial test.

"The Precision Strike Missile — and the work that is going on with our Program Executive Office for Missiles and Space — is an absolutely crucial capability out in the Pacific," Gen. Charles Flynn, commanding general of U.S. Army Pacific, told reporters at the Halifax International Security Forum.

A few days prior to the forum, the Army and contractor Lockheed Martin

at the White Sands Missile Range in New Mexico successfully completed a test of the new missile at a range shorter than 85 kilometers, although the service would not disclose the exact distance it traveled.

Three weeks after the conference, the Army confirmed in a Dec. 8 statement that it had received the Precision Strike Missile Increment 1 Early Operational Capability missiles.

The Army's stated goal is to have the Precision Strike Missile travel as far as 500 kilometers but has only achieved 400 kilometers. The short-range test conducted Nov. 13 was operationally more difficult to execute than a long-range test, a Lockheed Martin statement said.

"The short-range flight represents the most stressful, dynamic environment for the missile as it maneuvered at hypersonic speeds to align to the target," the statement said. Hypersonic speeds are generally defined as Mach 5 or above.

The test verified the missile's accuracy, maneuverability and structural integrity, the statement said.

The new missile is fired from the legacy High Mobility Artillery Rocket System, or HIMARS, which is also manufactured by Lockheed Martin.

Flynn said the new missile combined with the launcher will be a powerful tool for multi-domain operations where the Army and the Marine Corps may be called upon to fire at ships from positions ashore.

"What the HIMARS capability represents is the ability to not be fixed. It allows you to have mobile, reloadable, distributed — both lethal and nonlethal — capabilities because it's tied to the joint targeting network," he said.

The possibility of having the Army, Marines and U.S. allies in the Indo-Pacific that also operate the HIMARS system — and could therefore deploy

the new Precision Strike Missile as well — will be a powerful capability in the region, Flynn said.

"I'm aware of the recent success, and in my view, it can't come fast enough. And I'm communicating that back to my Army leaders," Flynn said.

The fact that it has not yet demonstrated the requirement to fly 500 kilometers didn't bother Flynn. He would accept an incremental so-called "80 percent solution" to have the capability in Indo-Pacific Command, he said.

Testing incrementally at different ranges is important because the Army will need a "range of variants" to achieve different capabilities, Flynn said.

Lockheed Martin — which has received three production contracts for the missiles so far — indicated there were still more tests to come.

"The demonstration is the first of several production qualification tests moving the [Precision Strike Missile] closer to fielding and delivery of early operational capability missiles this year," Jay Price, Lockheed Martin vice president of precision fires at the company's missiles and fire control division, said in a statement. It "is a critical capability and the top long-range fires modernization priority for the U.S. Army."

Another missile system Flynn is looking forward to deploying in 2024 is the Strategic Mid-Range Fires System, also known as the Typhon missile system. It leverages existing Navy Raytheon-produced SM-6 missiles and Raytheon-produced Tomahawk cruise missiles that are modified for ground launches, with Lockheed Martin serving as the integrator. Like the Precision Strike Missile, it is intended to target ships at sea.

The Army's Rapid Capabilities and Critical Technologies Office within two and a half years of conceiving of the system successfully demonstrated an SM-6 missile launch — and later a Tomahawk missile launch — from the prototype system, "confirming the full operational capability of the system," an Army release said, with Flynn adding that a "battery or two" is ready to deploy.

"We intend to deploy that system in the region. I'm not going to state where and when," he said, steadfastly declining to say if they would be on U.S. or foreign soil.

Plans so far call for four batteries, which include four launchers, an operations center and a number of support vehicles and trailers. **ND**



'Made in Russia' No Selling Point

• The largest arms broker in the Indo-Pacific and across Asia for the last 50 years has been Russia, noted the U.S. Army's commander in the region **Gen. Charles Flynn**.

But that's going to change because of the Russian invasion of Ukraine, he predicted on the sidelines of the Halifax International Security Forum.

When potential customers now "look at what's happened in Europe, they see that that Russian equipment is not reliable, and it's not working. Moreover, the supply chain associated with that, the training associated with that — parts, ammunition, follow-on modifications — that is all at risk," he said.

"It may come fast, and it may come cheap, but it's not very reliable when you're in a fight. So, ours might come a little bit slower. It may be a little more expensive, but it works," he added. **ND**

AUKUS for Pre-K

• The AUKUS partnership between Australia, the United Kingdom and the United States is intended to last for decades to come, but to make that happen, the three nations must prepare the next generation to play their part in the alliance, said **Bonnie Jenkins**, the U.S. State Department's lead on AUKUS implementation.

For AUKUS to be successful, "we have to invest in our workforce here in the United States, but also in Australia as well as the United Kingdom," Jenkins said at the Atlantic Council recently. This will involve Australians coming to study in U.S. and U.K. schools, and vice versa.

Additionally, the partners recognize "the next generation of young people who are in pre-K are also going to be working on AUKUS," and developing that future workforce from an early age is vital, she said. Talented workers will be needed not just in shipyards, but across several emerging technology areas, she added.

"I think we may have found another compelling way to explain the broader context of AUKUS ... it starts in kindergarten," said **Markus Garlauskas**, the director of the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security. "I think that's great." **ND**

Impatience Is a Virtue

• U.S. Special Operations Command is called on to conduct high-priority missions around the world. That's one of the reasons its commander, Army **Gen. Bryan Fenton**, described SOCOM as "a very impatient command," when it comes to innovation and trans-



FENTON

formation. "And we're supposed to be that way. Based on the type of missions we get, the teammates that join our organization, they drive us each and every day to go faster, to think deeper and certainly to get to a solution and to an effect very quickly," he said at the Aspen Security Forum in Washington, D.C.

"Each and every day, we don't think we're going fast enough. We always want to go faster," Fenton continued.

"And as we put it against the prism of what's coming in the next 10 years, we've got to go even faster," he said. "And I think there's a lot of ways to do that."

One way is to learn and adopt from partners and allies, some of which are ahead on tech innovation, he said. Some are ahead on human capital and business practices, which can be more important than technology, he said.

Ultimately, he said, there are four pillars to transformation in SOCOM: people, technology, organizations and tactics, techniques and procedures.

"First and foremost, [when] we talk about transformation, it's really better people. 'Human is more important than hardware' is a longtime, first-off truth and motto for Special Operations Command," he said. **ND**



Navy Agrees: People Are the Priority

• To prepare for potential conflict in the Indo-Pacific, the Navy's top three priorities are its people, ensuring readiness and implementing digitalization, said **Rear Adm. Douglas Small**, commander of the Naval Information Warfare Systems Command.

Recruiting and retaining personnel is the "number one priority," he said during a keynote speech at the Eastern Defense Summit in Charleston, South Carolina.

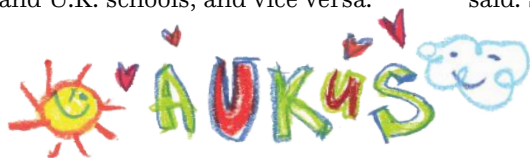
"We're in a competition for talent," he said. "We need to make sure that we are the employer of choice."

The Navy's second priority is readiness, from information warfare readiness to utilizing live, virtual and constructive training to prepare warfighters.

"We're trying to lay out what the continuum of readiness looks like, from the installation system all the way up to being able to execute as a striker," Small said. "How do we get to a continuum of readiness between coming out of a maintenance availability and then getting ready for high-end training and getting ready to deploy?"

The third priority is digitalization. For the Navy, that encompasses everything from development, security and operations, how to deliver software in a more modern way, "data-driven everything," and model-based engineering, he said.

To strengthen strategic deterrence, the Navy needs "actionable solutions. To me, that means things that are ready to go today, not ideas to build upon," Small said. **ND**



Innovation Nation

Container System Replaces Hazardous Burn Pits

BY SCOTT R. GOURLEY

FORT DEVENS, Massachusetts — Against a background that has led the Department of Veterans Affairs to identify “23 presumptive conditions for burn pit exposure,” the Army is entering production on a safer alternative to open air burning or backhauling of solid waste.

The Expeditionary Solid Waste Disposal System will provide a new incineration module to support the Army’s 150-person Force Provider Expeditionary Base Camp.

The module will reduce the use of burn pits by providing a cleaner solution for onsite disposal of 1,000 pounds of solid waste per 24-hour period for an approximate 92 percent volume reduction, Lt. Col. Dan-

iel O’Neill, product manager for force sustainment systems in the Program Executive Office for Combat Support and Combat Service Support, said at the Army’s Future Capabilities Integration Laboratory at Fort Devens, Massachusetts.

“The system also reduces soldier, civilian and local population exposure to pollutants from open air burn pits and reduces the amount of trash that must be backhauled, reducing soldiers’ exposure and attacks during convoy operations,” he explained. “Reducing waste held onsite also deters potential vermin that could spread disease and disrupt operations.”

The system comprises three Tricon shipping containers, each weigh-

ing approximately 9,500 pounds, that are attached to create a single 8 by 8 by 20-foot module. The system is designed to be set up and operated by soldiers using the Army’s all-terrain 10K forklift.

O’Neill said the system is simple to operate, requires minimal training and requires no contractor support.

In operation, soldiers will load the primary incineration chamber through a large front door, which is then sealed and electronically locked. The operator uses push-button controls to start the system, which does not require attendance or further operator input. A full batch burn cycle consists of a five-hour burn time fol-

lowed by a five-hour cool-down, with stack pollution controlled by automatically maintaining a secondary burn chamber at an average of 1,600 degrees Fahrenheit.

The system allows two burn cycles per day to incinerate up to 1,000 pounds of solid waste.

The system completed development and testing requirements in July 2020, with a July 2021 production contract awarded to Enercon Waste Systems, doing business as Eco Waste Solutions USA, he said.

Funding has recently been received for production of 10 units, and the contract “is open for ordering through July 2026 should additional funding become available,” he added. **ND**



The Expeditionary Solid Waste Disposal System

F-16 Electronic Warfare Suite Achieves Key Milestone

BY LAURA HECKMANN

DUBAI, United Arab Emirates — The next-generation F-16 fighter is receiving a tailored, all-digital electronic warfare suite, and after a successful Drop 2 test in November, it’s one step closer to taking flight.

The Viper Shield all-digital electronic warfare suite, developed by L3Harris, is custom designed to be the baseline on Lockheed Martin’s advanced F-16 Block 70/72 aircraft, but prior blocks can be easily upgraded with the new suite as well, Anna Gragossian, director of business development for electronic warfare at L3Harris, said recently on the sidelines of the Dubai Airshow.

The system, which is an upgrade of previous L3Harris electronic warfare systems, provides a virtual electronic shield around the aircraft, designed to detect modern radar systems. The upgrade

addresses new threats and creates interoperability with the F-16’s APG-83 fire control radar, she said.

L3Harris announced the system’s successful Drop 2 integration test on Nov. 8, demonstrating full radio frequency compatibility with the F-16’s onboard APG-83 radar.

The test included continuous exposure with APG-83 energy for more than 12 hours to determine whether the radar pulses would interfere with electronic warfare functionality. The test “proved Viper Shield’s ability to filter out signal processing streams from the APG-83 radar pulses without any performance compromise,” according to a company press release.

Viper Shield’s analog predecessor could only detect one threat at a time, Gragossian said. The new system’s upgraded architecture will “allow us to see

all of the threats simultaneously and defeat them simultaneously,” improving situational awareness through electronic countermeasures, she added.

The all-digital architecture will also use commercial-off-the-shelf technology to make it smaller, lighter and easier to upgrade.

Viper Shield’s Drop 3 increment delivery, which as of the time of publication was scheduled for December, will be production representative, Gragossian said — “so, that’s a big milestone.”

The Drop 3 hardware will be used at Lockheed Martin’s System Integration Lab for multifunctional testing, followed by flight testing scheduled for early 2024.

Viper Shield has five drops planned, with the fourth and fifth scheduled for the first and third quarters of 2024, she said. “And then what happens after Drop 5 is finalizing the remaining testing integration, and then be ready for production in ... [the fourth quarter] of 2025.” **ND**



Scott Gourley photo, L3Harris illustration

Lockheed Martin Simulator Prototype Gets Rid of Projectors

BY STEW MAGNUSON

DISPATCHES

ORLANDO — Lockheed Martin is working on a radically new approach to immersive training systems that have previously relied on a series of projectors to create high-fidelity images.

AMAZE — the Amorphic Appearance Zero-Projector — is a visual display system that relies on today’s commercial LED panels and does away with the traditional dome-shaped simulators that have dominated the training market for decades.

“Projector-based dome systems have capably served the training environment for a long time,” said Erik Etz, director of business development at Lockheed Martin Training and Logistics Solutions. But new commercial LED panels are brighter with better contrast and becoming less expensive, he said while unveiling the prototype to a handful of reporters at the company’s Orlando facility.

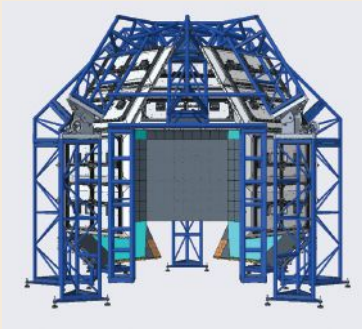
Beaming images from projectors onto domed screens takes up space, uses a lot of energy and is high main-

tenance. Swapping out a bulb can take hours, he noted. “There are unique sustainment challenges associated with those projector-based dome systems that typically involve significant hardware structure outside the dome.”

LED panels, however, are not round but come in squares. The prototype shown to reporters was a series of rectangles and triangles patched together, but when standing in the correct position, the system provided a seamless view of a jet fighter swooping through a valley.

The screen has two layers: a fiber-optic light relay that projects the image onto the LED layer, said John Magda, visual display system engineer.

“We’re not asking any of our vendors to create specific shapes for the solution. And that’s how you can really keep the initial procurement costs



down,” Magda said.

The image on the screen is two times brighter than traditional projected images and has three times better contrast, Etz said. But the biggest selling point is the reduced footprint of the simulator and lower sustainment

costs, which the company projects as being 35 percent less than domed systems over a period of 10 years.

“And the price points for LEDs are continuing to plummet,” Etz added.

Lockheed Martin has developed the prototype with its internal research and development funding. It revealed the system to customers during the Interservice/Industry Training Simulation and Education Conference in November in Orlando, with an eye to marketing it for aviation simulators first, although it could potentially be used for any type of platform, he noted. **ND**

BY THE NUMBERS

U.S. Federal Agencies’ Top 10 Fields of Research by Industry Grants, 2017-2023

Field of Research	Total Grants to Industry	Percentage of Total Industry Grants
Artificial Intelligence and Image Processing	4,547	23%
Materials Engineering	3,221	16%
Other Physical Sciences	1,688	8%
Information Systems	1,677	8%
Electrical and Electronic Engineering	1,341	7%
Communications Technologies	948	5%
Physical Chemistry (incl. Structural)	946	5%
Public Health and Health Services	915	5%
Interdisciplinary Engineering	807	4%
Clinical Sciences	789	4%

Source: Center for Security and Emerging Technology

Lockheed Martin illustration

Coast Guard Goes All-In on Zero Trust Architecture

BY ALLYSON PARK

CHARLESTON, South Carolina — In order to strengthen cybersecurity and implement zero trust architecture, the Coast Guard must invest in understanding data, a service official said.

Zero trust architecture refers to evolving cybersecurity paradigms that prioritize protecting data by repeatedly authenticating, authorizing and validating system, application and data access.

Implementing zero trust architecture presents a change to how the Coast Guard approaches security, especially when the Defense Department and the individual services have differing requirements.

“We need to focus on better identity management, focusing on the data side of that,” Capt. Andrew Campen, engineering services division lead at

the Command, Control, Communication, Computer, Cyber and Intelligence Service Center at the Coast Guard, said at a panel at the Eastern Defense Summit in December. “[We must] realize that data is the piece that’s important, not the system itself. Identity management is key for us. Understanding data is key for us.”

Successfully implementing a zero trust architecture is incredibly dif-



ficult in the digital age, especially with the vast amount of mobile devices and defense and security technology.

“I think we’re also challenged here as we get into today’s world, all the new mobile devices, all these new toys that we’re bringing to the table,” Rear

Adm. Chad Jacoby, assistant commandant for acquisition and chief acquisition officer of the Coast Guard, said. “We want to introduce them to our IT environment. How do we do that from a zero trust architecture perspective? It’s going to be very difficult.”

Though achieving zero trust architecture is critical to safely conduct multi-domain operations, protecting other data is also crucial.

“A lot of departments out there with commercial environment needs, we need to protect our data, whether it’s our health records, our financial data,” Campen said. “We want to secure our personnel data in the Coast Guard and our operational data to make better decisions as well.”

Zero trust architecture is complex, and the Coast Guard must focus on understanding data and understanding the different roles it can play, Jacoby said.

“There’s the server workstation zero trust architecture to solve, but there’s also the operational technology zero trust architecture to solve, and it allows me to bring that from the center and say that our embedded systems on our ships, aircraft and shore stations need to meet the same mandate,” he said. **ND**

Hello, Goodbye

• Special Operations Command named **Melissa Johnson**, member of the Senior Executive Service, as its new acquisition executive. Johnson is responsible for more than 1,000 personnel providing acquisition, technology and logistics support to Special Operations Forces. Johnson served 24 years on active duty, with her final assignment as the program executive officer for SOCOM’s Fixed Wing Programs.

Israel’s Rafael Advanced Defense Systems appointed **Yoav Turgeman** as its chief executive officer. The appointment is pending approval from the appointments committee,



JOHNSON

the minister of defense and the regional cooperation minister responsible for government companies. Turgeman served in various command and staff roles in the Israeli Navy for 25 years, retiring as a colonel. Since 2018, he served as the chief executive officer of Elta Systems. He will succeed retired **Maj. Gen. Yoav Har-Even**.

The Center for Strategic and International Studies announced **Clayton Swope** as deputy director of the Aerospace Security Project and senior fellow with the International Security Program. Swope brings more than 20 years of experience on national security, space and technology. He will play a role in



TURGEMAN

expanding CSIS’s work and impact on national security, aerospace and space policy development and strategy. Before joining CSIS, Swope led national security and cybersecurity public policy for Amazon’s Project Kuiper, an initiative to increase global broadband access through a constellation of satellites in low Earth orbit.

Austal USA announced **Jim Blastos** as the company’s vice president of supply chain management. His responsibilities will include procurement, strategic sourcing, warehousing, logistics, material management and production control activities for the company. He has more than 25 years of experience in developing strategic organizational transformation, collaborative solutions and operational processing as well as leadership positions in supply chain and operations in

the Navy and industry.

Todd Harrison has joined the American Enterprise Institute as a senior fellow, where he will focus on the defense budget, defense industrial base and space policy. He joined the think tank from Metrea, where he was senior vice president and head of research.

Hudson Institute’s Center for Defense Concepts and Technology announced **Jordan Schneider** as its Andrew W. Marshall Scholar for the 2023-2024 academic term. Schneider is a noted China expert, blogger and podcaster. In addition to traditional research, Schneider’s scholarship will include long-form discussions with experts across disciplines to explore how technology, operational concepts and organizations drive and respond to changes in the character of war. **ND**

New AUKUS Investor Group to Accelerate Emerging Tech Development

BY JOSH LUCKENBAUGH

Innovation company BMNT Inc. on Dec. 5 announced the creation of the AUKUS Defense Investor Network, which is dedicated to accelerating the development of advanced military capabilities for the trilateral partnership between Australia, the United Kingdom and the United States.

The U.S. Defense Investor Network was founded in 2019 by BMNT entrepreneur-in-residence Heather Jo Richman, who described the network as “a thing that’s not a thing.”

The network does not have or take funding such as dues, is not incorporated or a non-profit, Richman, who now chairs the U.S. network, explained in an interview.

“It really is just a network ... where investors who are either very well-versed in national security investing, or not at all versed in national security investing, can come and share thoughts and hear from senior leaders, from program managers, from people that are really trying to get these things done inside of our Department of Defense and intelligence community.”

Defense investor networks also exist in the United Kingdom and Australia, and “we thought it made a lot of sense that ... as our countries are figuring out how to work together, our private capital communities also need to figure out how to work together and figure out what that means,” Richman said.

“We talk about mission acceleration and innovation at the speed of trust,

and the more that we can really build the bridges between the various investment [and] private capital communities in those three countries, it’s going to be a benefit to everybody,” she added.

Co-chaired by the leaders of each country’s network, the AUKUS Defense Investor Network consists of leading private capital investors from more than 300 institutional venture capital firms, corporate venture capital groups and family offices from the three partner countries, representing more than \$265 billion, a BMNT press release stated.

“Access to private capital is vital to help scale the innovative dual-use companies who are important suppliers to defense and the wider national security community,” John Ridge, chair of the AUKUS Innovation Working Group, said in the release. “I am excited to see the creation of an AUKUS Defense Investor Network, which I hope will increase awareness and understanding of our shared security challenges across the venture capital community and help our cutting-edge companies bring their creativity to bear against some of our toughest national security challenges.”

The network will focus on Pillar 2 of AUKUS, the goal of which is to develop interoperable, advanced military capabilities in emerging technology areas such as cyber, artificial intelligence, quantum sciences, undersea capabilities, hypersonics and counter-hypersonics, electronic warfare and

information sharing — “areas where private sector investment can accelerate government investment in developing solutions to critical security challenges,” the release said.

In a Dec. 1 joint statement, U.S. Secretary of Defense Lloyd Austin, Australian Deputy Prime Minister and Minister for Defence Richard Marles and U.K. Secretary of State for Defence Grant Shapps said they welcomed the creation of the AUKUS Defense Investor Network, which will “facilitate targeted industry connectivity.”

The three leaders announced several initiatives to increase industry participation in AUKUS, such as convening the first AUKUS Advanced Capabilities Industry Forum in the first half of 2024, and launching a series of innovation challenges in which companies from across the three countries will be able to compete for prizes on a common innovation challenge topic. The first innovation challenge in early 2024 will focus on electronic warfare.

Richman said the AUKUS Defense Investor Network will be “piggy-backing” on other AUKUS events, as well as holding network-only meetings.

“Meeting people in person is always ... amazing. It’s a different level of getting to know someone and trusting someone,” she said. “So the more that we can take advantage of those opportunities, especially when there are large events where we’ve got people traveling internation-

ally already ... it is really important to get together and to build that trust.”

The more investors can talk and understand each other’s approach, as well as gain insight into each military’s capability needs, the more effective the network will be, she said.

From venture funds to private equity firms to family offices to high-net-worth individuals, everyone “has a different investment thesis,” she said. “I’m just finding that the more that all of these different groups learn about true threats, real threats, how they can help, what capabilities are needed, how that’s going to work ... the more they know, the more they know. And the more they know, the more they understand, and so they’re willing to do things a little bit differently.”

Along with managing different time zones, the network will also need to have “constructive conversations, making sure that we’re being realistic about the value” of different investments or technologies “to each of the countries,” she said.

Potential reforms to export laws such as the U.S.’ International Traffic in Arms Regulations are “top of mind for a lot of folks,” so “it will be interesting to see what happens and what sorts of challenges we are able to tackle [or] aren’t able to tackle,” she added. **ND**

— Posted Dec. 8 at NationalDefenseMagazine.Org.



Industry, Government Must Share Responsible AI Burden



A common question to Defense Department officials is how to ensure artificial intelligence is “responsible” enough to deploy on the battlefield. Companies developing AI systems for the military need to ask themselves this question as well.

The private sector is developing important, innovative technologies at such a rate that “industry and government are now — if not co-equal — near-peer partners in national security,” said Klon Kitchen, a senior fellow at the American Enterprise Institute. The government is realizing and reconciling itself to the fact that it is no longer the only national security stakeholder.

“Industry is ... now a center of gravity for foreign policy and national security,” he said.

While companies may not want to have to worry about the national security implications of their products, “I’m sorry ... you’ve worked very hard to build and gain this level of influence, now you have to deal and reconcile yourself with the responsibilities that come with that influence,” Kitchen said during a recent panel discussion hosted by the National Security Law Journal and National Security Institute at George Mason University.

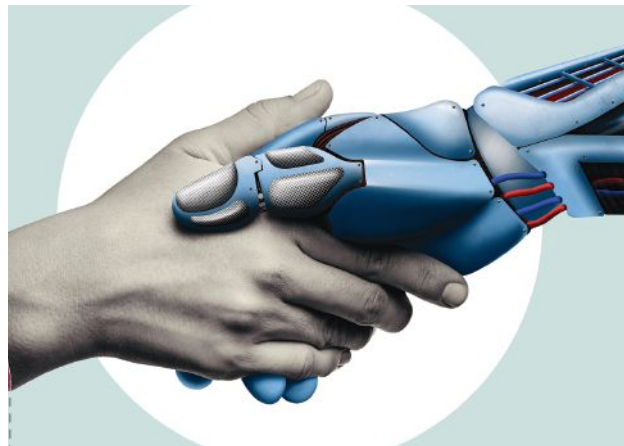
“And so what’s happening right now is the renegotiation of a social contract between government and industry and what is now a shared burden in a way that has previously never been shared before,” with AI the “quintessential example” of that shift, he said.

On Oct. 30, President Joe Biden signed an executive order on safe, secure and trustworthy AI. Kiersten Todt, former chief of staff at the Cybersecurity and Infrastructure Security Agency, said a key element of the executive order “is looking at bias and how do we mitigate the bias for artificial intelligence? How do we ensure that the technology that we’re building, when it exponentially takes something that we’re looking to be able to grow and differentiate, is not doing

that in a negative way? How are we ensuring that the data makes sense?”

Data provenance is critical to AI, “and it’s very hard to reverse engineer data provenance,” Todt said during the panel. “So, what can we do now with technology to ensure that there are data standards ... so that you understand what’s going into it, but importantly, it’s building that security into it.”

Earlier in October, the FBI hosted a summit with leaders of the Five Eyes intelligence alliance, along with business leaders, entrepreneurs, government officials and academics “to discuss threats to innovation, coming trends in the use and potential exploitation of emerging tech and means to work together to advance both economic security and public safety,” a FBI release stated. The Five



Eyes group comprises the United States, Canada, the United Kingdom, Australia and New Zealand.

The event was “unprecedented,” Todt said. “You had the Five Eyes coming together to talk to CEOs of technology companies in Silicon Valley ... to say, ‘Your technology, what you’re building, you may think this is just a revenue generator ... but you are now part of our national security infrastructure. So, you have a responsibility and an obligation to look at what the impact of your technology is. How are your choices being made, so that when we’re building out our infrastructure from a United States perspective, we’re doing it with security, critical infrastructure, resiliency all in mind?’”

With private industry, rather than the Defense Department, now leading research and development of critical technologies like AI, “we should just accept the fact that the department is always going to be behind ... so it’s really always going to be how quickly we can adopt what we’re behind in,” said Whitney McNamara, vice president of Beacon Global Strategies.

“We simply don’t have the national budget to spend trillions of dollars to be the leader in R&D in every area, so we should be thinking about what makes sense for us to spend money” on for internal government research, “and what makes sense to be procuring from the commercial sector,” McNamara said during the panel.

Building the ecosystem to properly adopt technology like AI is something the government struggles with, she said. Whereas the Defense Department might just say, “I want to put AI on my drone and go do something,” it must also ask questions like, “Where’s the data coming from? What’s the process? Who secures the data? Do

we need to manage data? Is it open-source data? How does my algorithm interact with my data? How do I test and evaluate it, especially if I’m expecting my AI to act in slightly unpredictable ways ... it’s like this really kind of nebulous process,” she said.

“I think there’s a lack of an appreciation sometimes” for what it will take to adopt AI, she said. “When we say AI, we’re really just talking about processing power and data and test and evaluation architecture, which isn’t always the sexiest topic.”

Getting the right AI systems and architectures in place will take a team effort between government and industry, Todt said.

“This is a great opportunity where the U.S. government has really the power of the purse when it comes to procurement, to incentivize behaviors that it may not be able to regulate,” she said. “We talk a lot about the incentives for industry to do this security and safety, and where regulation will come we’ll have to see, but if the U.S. government starts to say, ‘We’re going to see that safety and security in our research as a differentiator, and that will allow us to work with you more easily,’ then we start to see a market and a culture evolve where that’s prioritized.” **ND**

Why Ukraine Assistance Is U.S. Assistance

On Dec. 14, Congress gave the Defense Department a Christmas present — a 2024 defense bill. However, batteries were not included, as Congress had yet to pass a 2024 budget or the \$106 billion supplemental funding package the White House put on its Christmas list months ago.

The emergency funding would provide some \$60 billion for Ukraine, \$14 billion for Israel and \$14 billion to counter the surge in illegal border crossings into the United States. The border security provisions were holding up passage, with many Republicans calling for additional immigration reforms before they would agree to the supplemental. Prospects for passage looked dim at the time of writing.

In the meantime, previously appropriated military support for Ukraine is running low — along with enthusiasm from some lawmakers for new appropriations for the nation as the war ground to a stalemate heading into winter.

During a Dec. 7 fireside chat at the Aspen Security Forum, U.K. Foreign Secretary David Cameron made an aggressive pitch — to a roomful of the converted — for continued U.S. support to Ukraine.

“The biggest beneficiary of Pax Americana was America, and it’s worth making that argument over and over again,” he said.

“The value for the money of what you’ve put in is astounding,” he continued. “What is it? Like maybe 10 percent of your defense budget used by the Ukrainians has destroyed half of Russia’s prewar military assets. Now, if that isn’t a good investment, I don’t know what is.”

Later in the discussion, the moderator referred to a recent American Enterprise Institute analysis in *The Washington Post* that found 90 percent of the \$68 billion in military aid provided so far to Ukraine had been spent in the United States, benefitting U.S. manufacturers and workers.

According to the AEI analysis and article authored by Marc Thiessen, 117 production lines in at least 31 states are manufacturing weapons provided to Ukraine. That does not include smaller items like spare parts or small arms ammo.

“In other words, as happens with foreign military aid, our aid to Ukraine is not only creating American jobs but also reinvigorating our dangerously atrophied defense industrial base,” Thiessen wrote.

Cameron jumped on that point.

“Ultimately, lots of our constituents and members of the public live in places — whether in the United Kingdom or in the states — where there’s a big industrial base, and there’s jobs, and there’s investment that will go in as a result,” he said.

“I think we’re at a point where we’ve got to stop thinking about how we’re running down our existing stocks to supply Ukraine,” he continued. “We need to think much more about how we build up our stocks. And I think in the more dangerous and insecure world that I was talking about, supply chains, stocks, defense commitments, these things have become more important, and they’re also more important for allies.”

Mark Cancian, senior advisor with the Center for Strategic and International Studies’ International Security Program, has also researched the domestic benefit of Ukraine aid.

“Aid to Ukraine is something of a misnomer,” he said in an interview. “It’s really ‘funds as a result of the war in Ukraine’ because a lot of it goes to U.S. agencies,” including the Defense Department, he said.

There are multiple ripple effects of military assistance to Ukraine that benefit the U.S. military and industrial base, he said.

“We sent things that are in our inventory,” Cancian said. “We were sending top-of-the-line equipment, but when we replace it, we replace it with whatever the most current version is.”

For example, the United States is sending M113s and will replace them with new Armored Multi-Purpose Vehicles, he said.

“And on things like munitions, they have a shelf life,” Cancian said. “The shelf life on a Javelin is 20 years, and we send them Javelins with 18 years on them — they were only going to be around another two years and we would have to get rid of them. Now, we buy a new Javelin, so we restart that clock. So, that helps our inven-



tories also,” he continued.

Thiessen made a similar point, noting Stinger missile production had shut down in 2005 until last year when the Pentagon signed a \$625 million contract to restart production to support Ukraine.

“Without our Ukraine resupply effort, the Stinger production line likely would have remained dormant — perhaps until bombs started dropping in a conflict over Taiwan,” he wrote.

Furthermore, NATO allies are donating weapons to Ukraine and buying new weapons from U.S. manufacturers.



“In all, our analysis found that there are at least 13 production lines in 10 states and 11 U.S. cities producing new American-made weapons for NATO allies to replace the equipment they have sent to Ukraine,” Thiessen wrote.

Not to mention the supplemental package includes \$3.4 billion for the U.S. submarine industrial base and other funding to build capacity in the defense industrial base that officials say is crucial to deter and defend against Chinese aggression in the Indo-Pacific, Cancian noted.

One would think members of Congress would be crowing about the benefits to U.S. workers and congressional districts of continued military support for Ukraine, but participants at the forum like Paula Dobriansky, vice chair of the Atlantic Council’s Scowcroft Center, expressed dismay that the message isn’t getting out.

“I think that word needs to get out more. ... It’s a very significant one,” she said. “[It] matters not only for our security but for that of Ukraine, because you can’t have limitless munitions. You have to have manufacturing. You have to have a strong industrial base. So, it’s in our interest. It’s in Ukraine’s interest. It’s in Europe’s interest. It’s in the global community’s interest.” **ND**

INDUSTRY PERSPECTIVE

Cloud Service Providers as The Technological Arsenal Of Democracy

BY JASON ATWELL



The United States has always led with the private sector when it comes to national power, both in preserving our own and protecting that of our partners and allies.

Many of the greatest accomplishments in U.S. history have been made possible by a close, purposeful relationship between the public and private sectors.

The U.S. government and our largest, most dynamic corporations have achieved great things together: Liberty ships, the Apollo program and the internet all met a government need using creative commercial wherewithal. The “tech industry” has been a key player in many of these types of initiatives.

We are now in an environment where tech companies are perhaps the crucial arbiters of how we project power, ensure global stability and collaborate with our allies. This has the potential to bring into ever closer alignment the bulk of the United States’ and likeminded allies’ defining attributes through the same platforms that host popular culture, foster democratic values and help us collaborate and communicate with friends and colleagues the world over.

It would be nearly impossible to maintain our position and relevancy without the internet’s connectivity and the efficiency of its attendant infrastructure.

The relationship between tech and government is not new, and it may be obvious to most, however we are in the early stages of a renewal of the dynamics involved as well as the global competitive landscape, one that will see the large-scale adoption of cloud computing as a defining and enabling characteristic.

It is no accident that the recently published “National Defense Science and Technology Strategy” specifically highlights “cloud computing and data sharing” as the new “norm” and a critical component of

modernizing and upgrading digital infrastructure.

The role of public-private partnership in pursuing national security goals has become a central component of our strategic frameworks and the international order, and cloud service providers will play a vital role in national security and international stability.

Governing documents, such as the White House’s May 2021 “Executive Order on Improving the Nation’s Cybersecurity,” have placed the providers at the center of forward-looking planning and initiatives. They provide the infrastructure and services that enable governments to collect, store and analyze data, as well as communicate and collaborate with one other.

The synergies created by this shared platform usage can be used to track and monitor threats, develop new technologies, or even plan and execute military or homeland security operations. This creates an unprecedented opportunity for interoperability. Instead of merely selling allies vehicles and guns, we can now marry them up with our command-and-control networks, intelligence analytical frameworks and data streams.

In the past, large industrial entities such as railroads, oil companies and steel mills played a similar role in national security. Cloud service providers are different in that they are not tied to any particular country or region, nor are they inherently tied to the industrial capacity for war-making, as they can also enable soft power. This makes them both methods of deterrence in terms of military resilience, but also ties them to peaceful alternatives to rogue regimes and adversarial nations. They are both guarantors of deterrent stability and enablers of civil society, giving them a uniquely advantageous position in an age of renewed great power competition.

It is a very deliberate and historically appropriate parallel when President Joe Biden recently praised the defense

industry in terms of “the arsenal of democracy” and invoked World War II. The war in Ukraine has clearly demonstrated that the United States is still an indispensable partner for the defense of democracy, and that it cannot fulfill that role without its technologically enabled economic might.

It is widely acknowledged that Ukrainian organizational and infrastructure resilience was only possible through cloud technology. This model will only become more essential to national security and international stability in the future.

The United States is currently engaged in competition with China for global dominance. Both countries are investing heavily in cloud computing and artificial intelligence. The United States has a distinct advantage in having several leading cloud providers, including Amazon, Microsoft and Google. These companies have the resources and expertise to protect the nation and its allies as discussed above.

China is also investing heavily in cloud computing, but it does not have the same level of capabilities or global market share as the United States, which, along with Europe, has also taken steps to limit Chinese access to this technology to preserve information dominance, thus securing America’s role as the provider of secure platforms and technology in conjunction with trusted service providers.

The role of cloud service providers in national security will continue to evolve. As new technologies emerge,





cloud providers will need to adapt to meet the changing needs of governments and other customers.

However, the basic role of cloud providers will remain the same: to provide the infrastructure and services that enable governments to project national power and achieve

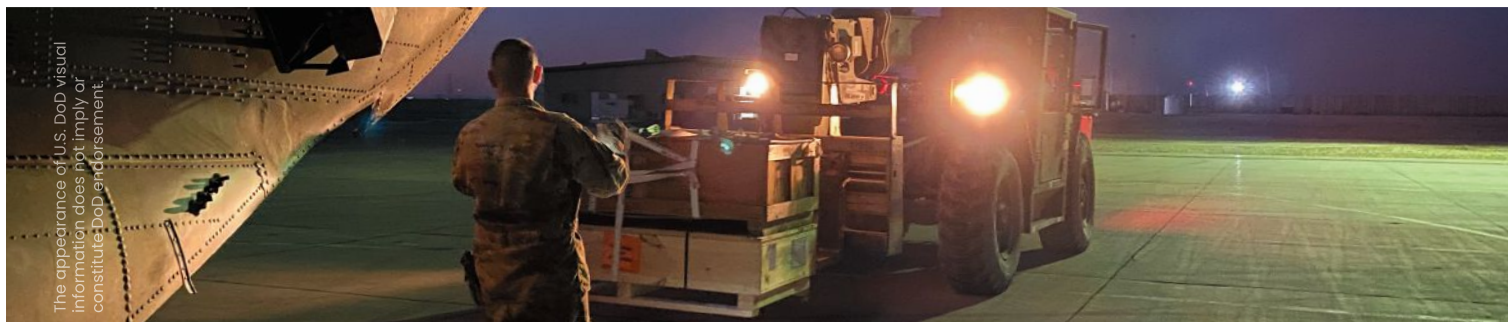
their objectives. The first version of the arsenal of democracy played to America's strengths on the factory floor; we couldn't win the war without General Motors, but we also needed Ford and Chrysler and many others to scale our advantage.

Likewise, cloud service provid-

ers can provide this new technological arsenal, but we can only do it together and in close partnership with the government. **ND**

Jason Atwell is a program manager at Google Public Sector and Mandiant Intelligence.

Need a **Contract Vehicle?** Partner with Us.



Our pre-competed DLA contracts allow us to rapidly deliver your products and services to your Federal customers.

Darley Partner Advantage

-  100+ years of experience supporting military customers
-  Expedite your sales cycle
-  Expand your customer reach
-  Avoid federal contracting hurdles



Audrey Darley | 4th Generation Darley
VP Supply Chain, Defense
audreydarley@darley.com
Scan to inquire about a partnership.

You Serve Others. We Serve You.™

**National
DEFENSE**



NUMBERS GAME

Replicator Initiative Looks to Swarm Through ‘Valley of Death’

BY JOSH LUCKENBAUGH

Deputy Secretary of Defense Kathleen Hicks laid out an ambitious goal when she announced the Replicator initiative in August: within two years, the Defense Department will field thousands of all-domain, attritable, autonomous swarming robots to counter China’s military mass.

While that objective in and of itself is quite eye-catching, Replicator’s other goal — to revolutionize how the Defense Department does business by building a bridge across the so-called “Valley of Death,” where innovative defense technologies fail to make it to the field — could be the real success story of the initiative.

There are several programs across the services focused on autonomous systems: the Army recently announced plans to deploy human-machine integrated formations, the Navy’s first and only uncrewed, high-altitude drone reached initial operational capability in 2023 and the Air Force is developing unmanned, collaborative combat aircraft to fly alongside its Next Generation Air Dominance fighter jets.

While these examples may not reflect exactly what Replicator is after — Hicks has described the initiative’s shopping list as “small, smart, cheap and many” systems that could potentially “move the needle” in the Indo-Pacific — the initiative is “not a new program of record” and will leverage “exist-

ing funding, existing programming lines and existing authorities to accelerate production and delivery at scale,” she said at the Defense News Conference in September.

Congress made clear during the 2023 budget cycle that it wants the Defense Department to “use its full authorities” for acquisition, Hicks said during a Defense Writers Group event in November. “We don’t think you’re pushing hard enough, do what you can with what you have’ is the gist of what we read.

“And I’m a big believer [that] we need to be problem-solvers in DoD,” she continued. “The answer to every question is not, ‘I need more money and more people.’ So, Replicator is a great example of how we are taking that feedback from Congress, look-

tematic, senior-level focus ... on how do we remove barriers beyond just the resourcing piece ... to make sure things make it across the Valley of Death.”

Jaret Riddick, a senior fellow at Georgetown University’s Center for Security and Emerging Technology, said the fact it was a senior leader such as Hicks who announced the Replicator initiative sent a “clear demand signal” to industry.

The initiative is a “clear declaration” for the United States to “create an offset against one of China’s greatest strategic advantages, and that’s mass — having more ships, more planes, more missiles, more people,” Riddick said during a recent discussion hosted by the Center for Security and Emerging Technology.

Additionally, the announcement coming from the deputy secretary of defense gives Replicator “sort of the gravitas, the serious focus on this, in a

ter’s director of analysis, said the Deputy’s Innovation Steering Group is the “critical piece” to make Replicator’s ambitious goal a reality.

“Having a group like this with all the relevant people in the room ... really focuses the department and the decision-making processes on this issue and what needs to happen,” Mikolic-Torreira said. “The key players that have influence on the process who have authority, who have powers to make this happen, are all in the room with the vice chairman and the deputy secretary, [who are] in some polite fashion breathing fire on them, and the system responds very effectively to this.”

That doesn’t mean the group won’t run into challenges, such as how to acquire systems on as great a scale as Hicks has stated, he said. That is where the Defense Innovation Unit will play a key role, Riddick said.

DIU is “oriented to really engage”

across the “network of industry partners,” particularly nontraditional defense companies — “the folks who have been sort of maturing these technologies in the commercial space,” Riddick said.

DIU Director Doug Beck said expanding the aperture “of players that are providing capability into this space” — and thus expanding the industrial base “on which you can rely ... makes an enormous difference.

“A lot of those players — including some of those more emerging commercial tech players who are playing in this space — are working very, very hard on solving” potential issues for Replicator, such as scalability and supply chain challenges, he said during

ing a media roundtable in November.

Aditi Kumar, DIU’s deputy director of strategy, policy and national security partnerships, said for Replicator the organization is not only “looking at the programs already in the department’s pipeline that fit the mission need,” but also identifying capability gaps, such as domain area or enabling infrastructure, “and this is where we’re looking at leveraging our solicitations process to bring in new entrants,” exploring if industry can fill those gaps.

DIU is planning to host a Replicator technology summit in early 2024, “where we’re bringing in our partners here to think through what



Army officials operate a swarm of drones during an exercise at the National Training Center in Fort Irwin, California.

ing to problem solve for ourselves and working with what we have at hand.”

The Defense Department has a number of “alternative acquisition strategies,” such as middle-tier acquisition to field systems within two to five years and the software acquisition pathway, to facilitate rapid, iterative delivery of software capabilities, but “we are very acclimated to — for perfectly logical reasons — a particular acquisition strategy: a program of record that we can track through the budget that has specific line items, it moves through different colors of money, etc.,” Hicks said. Changing the acquisition system will require “a more sys-

condensed time period to really learn how we can accelerate and how we can get these sort of processes in place that help us to be able to do things quickly in the environment that we’re in.”

In response to Replicator, “we’ve seen mobilization” both inside and outside of the government, he added. To lead the initiative, the Defense Department has established the Deputy’s Innovation Steering Group — co-chaired by Hicks and the vice chairman of the Joint Chiefs of Staff — along with the supporting Defense Innovation Working Group, led by the Defense Innovation Unit.

Igor Mikolic-Torreira, the cen-

capabilities are critical to this, and how we build some of the common architecture pieces and other enabling pieces to deliver a capability that, over the long term, the department can benefit from,” Kumar added.

DIU is not only oriented to form unique connections with the private sector but can also build relationships with the “operational community — so, the combatant commands to the actual warfighters,” Riddick said. “Those types of connections will certainly be necessary to understand” the needs of the warfighter, and what systems will fit those needs.

Defense Department officials have shown reluctance to publicly discuss details about what systems will be bought as part of Replicator. In November, Hicks said the department will select the initial batch of candidates “in the next about three weeks,” but as of press time, no announcement had been made.

“We’re being very careful ... about the way in which we talk about Replicator” so as not to reveal too much information to China and other strategic competitors, Hicks said — similar to how the Pentagon has remained cagey with details about the B-21 Raider



strategic bomber and the Next Generation Air Dominance fighter programs.

The department will be “clear and transparent” with Congress about Replicator, “but how we choose to speak about it” publicly, “in terms of the particular programs or projects that we’ll be accelerating through Replicator, is to be determined.”

What is known is that the systems will be bought in “tranches,” or as Kumar put it, “successive batches.”

“The reason we’re approaching it in successive batches is because there are some ... systems that are ready to go from a scaling perspective,” that have been “tested and validated” and “we have high confidence that they will meet the mission need,” Kumar said. “There might be other systems where some, or all, pieces of that work still need to be done,” such as analysis, testing or evaluating scalability. “As we answer those questions, those systems will start getting wrapped into

the successive batches.” New entrants can deliver systems in later tranches that fill gaps in the current portfolio.

Buying systems in tranches also gives the Defense Department flexibility if a robot isn’t performing correctly, “buying down risk” that would otherwise be passed to the warfighter, she added.

“How do we buy down risk so that we can move forward [and] give ourselves the optionality to iterate on those decisions?” she said. “Because at the end of the day, taking that risk now is taking that risk away from the warfighter later. ... We want to proceed in steps so that we are learning at each point and then making the next decision based on those learnings, as opposed to making big decisions up front and then locking ourselves into something.”

Michael O’Connor, a major in the Space Force and a Department of the Air Force fellow at the Center for Security and Emerging Technology, said buying systems in tranches solves a common problem, “where you have huge waves of demand ... out of the military for capabilities, for either commodities or new systems, every time the world gets extra interesting. And



YOUR MISSION: First.

OUR SOLUTIONS: Fast.

Booz Allen®

We deliver technology with velocity to accelerate insights, secure joint connectivity, and speed innovation. Explore AI-powered solutions sculpted from the mission up.

We innovate. You accelerate.

BoozAllen.com/Defense

then you have these peace dividends where industry has been scaled back because the DoD is scaling back.

“If you can have this constant demand signal, it’s much easier to plan for, it’s much more efficient, and I think it also helps keep a more healthy industrial base. And ultimately, that will also be useful” as a process that can be repeated going forward, O’Connor said.

The goal is to replicate this process for other defense technologies, Beck said. “It’s about delivering concrete results in 18 to 24 months while driving the process to accelerate technology at scale in a way that is replicable. We’re focusing first on ... unmanned, autonomous, attritable systems, with multiple thousands across multiple domains, and there will be other Replicators” in the future.

The end product of Replicator will be “simultaneously the impact of fielded systems that [help] to deter major conflict — or win if forced to fight — in the Indo-Pacific, and the learning that we have from having done that, that allows us to do it again and again and again,” he said. “And in order to do that, we’re going to have to hit snags, learn from them and break down systemic barriers along the way. If, in fact, those barriers were already all broken down and it was simple, we wouldn’t have to do this. So, we’re doing that on purpose, and that’s part of what this is all about.”

Lauren Kahn, a senior research analyst at the Center for Security and Emerging Technology, said while fielding thousands of autonomous drones within the next two years would technically be a success, what would actually make Replicator a notable achieve-

ment is if the Pentagon can indeed “replicate this system again elsewhere” and prove it can “regularly overcome this kind of Valley of Death ... to make sure that the DoD can actually access all the resources that are available to it.”

Mikolic-Torreira concurred. “Are we going to be successful if after two years we have a few thousand drones of various kinds in the force? Yes, in some sense, but I think that’s the disappointing success,” he said. “The really useful success is if we get this institutionalized where you’re continuously buying fairly large tranches of drones” and sustaining this “clear demand signal for products.

“Replicator is a real success if it spawns its continuation,” he said. If consistently buying and upgrading systems “gets instantiated as part of that process ... now you’ve got the demand signal that the industrial base will respond to. ... So to me, that’s the biggest long-term measure of success is if it changes the department in that way.”

While driving change in the Defense Department’s acquisition processes is important, for Hicks, the warfighter is Replicator’s top priority.

“What to look for on Replicator is, does the United States Department of Defense field within 18 to 24 months thousands of attritable, autonomous systems? If the answer to that question is ‘yes,’ and we’re able to talk about the way we burned down risk to make that happen and deliver capability, that builds trust on the commercial sector side that we can move within that two-year cycle and increase investment opportunities for companies that are trying to be in that space,” she said.

“And most importantly for us, it delivers capability to the warfighter faster. That’s what Replicator is about.” **ND**



QX-58A Valkyrie
unmanned aerial vehicle

Indo-Pacific Focus Provides Hint Into Replicator Shopping List

The Defense Department’s Replicator initiative is aiming to acquire thousands of attritable, autonomous systems within the next two years to counter China’s military mass. The Pentagon has revealed few details about what types of systems it wants for the initiative, but the department’s focus on the Indo-Pacific could be a clue into what robots do or do not fit the bill.

Since September, the newly-established Deputy’s Innovation Steering Group — co-chaired by Deputy Secretary of Defense Kathleen Hicks and the vice chairman of the Joint Chiefs of Staff — as well as the supporting Defense Innovation Working Group, have been focused on three distinct steps concerning Replicator, according to a Defense Innovation Unit release: working with Indo-Pacific Command to understand warfighter needs and pinpoint mission areas for all-domain attritable autonomy to address; surveying existing all-domain attritable autonomy capabilities that are already underway across the services and nominating systems that can best support the previously-identified mission sets; and evaluating those systems against a set of criteria to identify which ones Replicator will accelerate first.

Aditi Kumar, the Defense Innovation Unit’s deputy director for strategy, policy and national security partnerships, said during a recent media roundtable the criteria for Replicator includes autonomy, attritability — which she defined as “the cost of the system relative to alternatives that would help us meet that same mission need” — scalability and resiliency “to achieve their mission in a denied environment.” These criteria “will not change across the tranches,” she said.

These criteria echo Hicks’ similarly broad but more succinct description of the desired systems when she announced the Replicator initiative at the National Defense Industrial Association’s Emerging Technologies for Defense conference in August: “small, smart, cheap and many.”

The Defense Department is looking at systems “in all domains,” Hicks said at a recent Defense Writers Group event. The initial Replicator tranche will be focused on capabilities that “can move the needle for particularly” Indo-Pacific Command in the next two years, she added.

Space Force Maj. Michael O’Connor, a Department of the Air Force fellow at Georgetown University’s

Center for Security and Emerging Technology, said while the initiative is keeping its options open to robots in any domain, certain systems will be more effective than others in the Indo-Pacific, adding that his views were his own and did not represent those of the government.

The Defense Department must consider the robots as platforms themselves — “they need to be able to get close enough to a potential fight to make a difference” — as well as the payloads they will carry — “a drone in and of itself can only do so much,” O’Connor said during a recent discussion on Replicator hosted by CSET.

For any mission, such as intelligence, surveillance and reconnaissance or electronic warfare, a robot must have enough payload capacity “to get the job done” — and “the more power each of those payloads consumes, the shorter the legs, the shorter the range” one will have, he said. And having the necessary range is particularly challenging in the Indo-Pacific given its vast ocean expanses.

In the Indo-Pacific, operators face a tough task maintaining a “minimum distance — the nearest piece of land or a ship you watch” a robot from, O’Connor said. Whereas in Ukraine, “the fight is maybe 10 kilometers away [and] you’re going to have a line of sight to your drone, you may need to be able to do things more autonomously in the Indo-Pacific because the fight may be so far away, or the electronic environment may be so contested, that you just cannot control your drone with a direct line of sight — you can’t do [a first-person view] drone.”

And if you have thousands — or even hundreds — of robots, “it’s hard to find 100 pilots and put them all in one place,” he said, adding that groups such as the Air Force’s Task Force 99 and the Navy’s Task Force 59 are conducting research and development on operating many unmanned systems all at once and doing the command and control to use them effectively, which is an important factor.

“So, can you do the command and control? Do you have the payloads to accomplish what you want in your mission, and then can you get into the fight when you need to?” he continued. “Those are a bunch of the knobs you can turn ... most of them are technically solvable, it’s just you have to figure out where on that cost/size performance curve you want to be.”

The Defense Department could buy thousands of small quadcopters, for example, “but they’re not likely to be able to cross the distances involved in the Indo-Pacific,” he said. “You can buy ... larger platforms” like the 30-foot-long XQ-58 Valkyrie, “but then you’re going to be challenged on cost.”

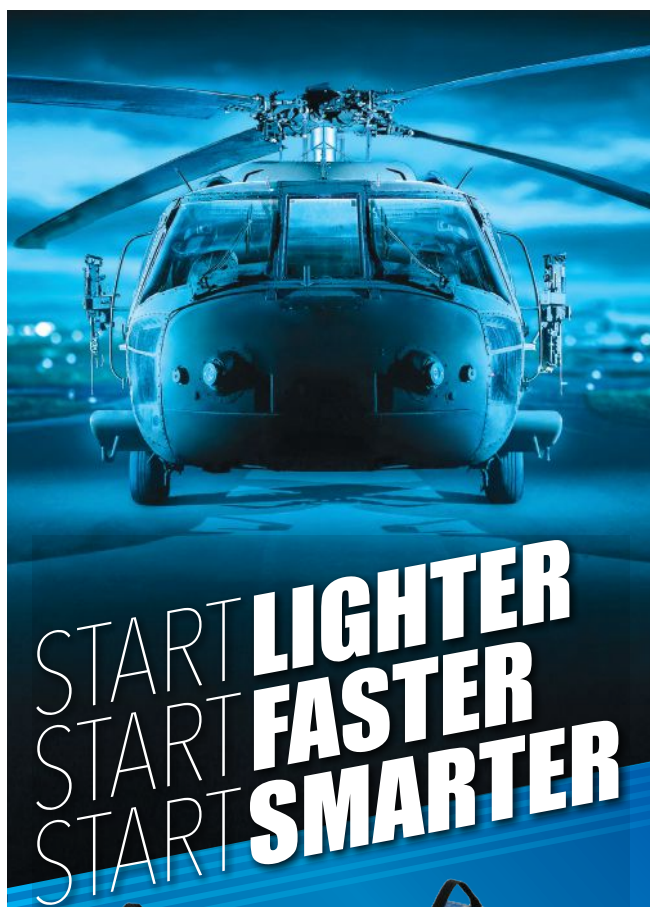
“So, in between there’s likely a sweet spot that you can buy mid-range drones if we’re talking aerial vehicles — likely things with wings — and then you have a similar situation with maritime [robots],” he said. “You’ve got small, you’ve got big — the answer is probably somewhere in the middle.”

The use cases for ground-based robots in the Indo-Pacific are limited, he added. While they could assist with aerial logistics, even those missions “are going to be challenging given the water involved and the distances in the Indo-Pacific.”

“I could be wrong here, but it’ll really depend on what the mission requirements are and what the creativity of industry can deliver,” he said. “And because ... we want to do this in 18 to 24 months, it has to be what is ready now, or very, very, very, very soon.” **ND**

— Josh Luckenbaugh

Air Force photo



Certified **Lithium-ion** Aircraft Batteries

Cut aircraft battery weight and increase your useful load. Like you, True Blue Power® batteries are always mission ready. They fully recharge within 30 minutes and deliver superior performance in the most rugged environments. Even better, you’ll eliminate expensive battery maintenance and the need for ground power units. **Start LIGHTER, start FASTER and start SMARTER every time.**

TRUE BLUE POWER®
A division of Mid-Continent Instrument Co., Inc.



truebluepowerusa.com/GETSTARTED

COMMENTARY

Opening the Replicator Program's Pandora's Box

BY DR. JAMES GIORDANO

China's ongoing dedication to developing unmanned vehicles for military applications has prompted the United States' unveiling of the Replicator program — an initiative described by Deputy Defense Secretary Kathleen Hicks to “master the technology of tomorrow” by creating and employing “attributable, autonomous systems in all domains.”

While Hicks was quick to assure that these technologies will be “in line with our responsible approach to AI and autonomous systems,” the use of such systems can be seen as a Pandora's box, from which emerge initial perceptions that the use of these technologies may decrease human costs of engagement but will also prompt questions of whether, and to what extent, such systems may affect thresholds and tolerances for their engagement in “drone warfare.”

The use of drones of any sort — non-autonomous, semi-autonomous or autonomous — may reduce national governments' and societies' tolerance for conflict and war for several reasons. These include tactical and/or strategic considerations of the battlefield effectiveness and efficiency of such systems in warfare, risks of human casualties incurred by their use and net incentives through which a society's tolerance for conflict can be seen as a relative calculus of perceived necessity, expected value of the gains from success, losses from failure and the impacts of material and human costs from potential outcomes.

Axiomatically, Hicks identifying these systems as being “attributable” means that these technologies are designed to be replaceable, and thus costs of their production in relation to possible losses is constituent to their overall value proposition.

Similarly, if there is some sense that the use of these technologies could reduce risk of harm to combatants or populations involved, the lower relative human costs might promote conflict, at least initially.

However, if machine or structural

target destruction is not sufficiently deterrent, machine-to-machine engagement will become disadvantageous, and it is likely that more tangible or advantageous human assets, including populated command, control and domiciliary centers will be targeted. Indeed, the use of machine systems' technologies may enable more effective and human-cost efficient targeting of enemy assets, for example, for the group doing the targeting.

If such technological weapon systems are relatively common knowledge, there may be an iteratively decreasing tolerance for human battlefield engagements, and the availability, viability and/or cost of these technologies would be largely irrelevant to public reaction to loss, as these sentiments tend to be emotional rather than technical or financial — at least initially.

In this light, the potential for technological loss — versus human loss — would tend to reduce a population's tolerance for human harm, and either implicitly or explicitly increase tolerance for machine vs. machine engagements. Machines targeting other machines — and not humans — if adopted by all parties possessing these technologies, could lower thresholds for conflict given perceived reduction in human costs. But as previously noted, sustaining machine-to-machine, or structural, targeting is a tenuous, if unrealistic, notion.

As true of most advanced weapons systems, costs of hardware and programming required to develop and maintain such autonomous technological systems are significant. And although such expense tends to diminish over time, this is nascent technology, and thus it is difficult to predict how long costs will remain

high. Therefore, the high initial costs could decrease tolerance and raise thresholds for engaging in conflict.

For example, the high cost of these technologies could affect how military commanders use such resources in certain circumstances and in this way, may alter tactical and strategic decisions, contributing, in part, to new determinations of acceptable losses.

In this way, the introduction of unmanned, autonomous military technology may change tolerance for engagement like the Cold War threat of using nuclear weapons, so that one state may be able to deter actions of another through sheer possession of such armament, given that deterrence is aimed at modifying or preventing behavior by leveraging high costs of an action against its relative gains.

To be sure, the effects of develop-



ment and planned use of such technology may alter international relations by empowering those states that possess it to deter competitors' and adversaries' hostile intent and foster non-belligere approaches of settling differences — particularly when such technology is limited, not widely available and/or exists in greater quantity or effective iterations, thereby producing asymmetrical capability.

As well, it may be that the use of autonomous systems with increasing levels of decisional capacity will enable more specific mission targeting, and in doing so, reduce large-scale conflict. But this rests upon a presumption that the current model of military engagement such as counterterror-

ist/insurgency operations employed by Western nations, especially the United States, will remain the norm. This is unlikely, as the shifting architectonics of science and technology, socioeconomics and changes in geopolitics are evoking very differently scaled conflicts, as evidenced by current wars in Ukraine and Gaza.

Hence, it is highly probable that the use of advanced, autonomous, unmanned technologies in military operations will change tolerances and thresholds for engagement, as based upon the relative costs that nations — and populations — ascribe to technological and human resources. For example, certain nation states — or non-state actors — might place a relatively higher value upon technological resources than human assets — due in part to factors such as a large national population and/or

nology through ongoing research and evaluation of current and future tools and processes in/for ethico-legal, social and economic guidance.

Priorities must focus upon: realistic appraisal of the science and technology and its capabilities and limitations; surveillance of which — state and/or non-state — actors possess such science and technology, and how cultural and political factors tend to influence these actors' decisions and behaviors; acknowledgement that autonomous, unmanned technologies can affect the conduct of, and amenability to, conflict; recognition of potential trajectories and valences of such effects; and developing valid models that can be used to forecast end-state scenarios that could be deductively used to inform and plan current and future policy governing research, development and uses in practice.

Such technology forecasting and mapping could use exploratory and normative methods to identify and assess capabilities and gaps in technology, information and socioeconomic and political structures relevant to military technology applications. Crucial to these efforts would be to address and acknowledge — including proposed responses to — the changing nature of warfare and thresholds and tolerances for war. Methods for technology futures' prediction include group idea building and program planning, informed forecasting and multi-

criteria decision-making. Each has value when used singularly, yet, when employed alone, is somewhat limited in scope and application.

Instead, the “advanced integrative scientific convergence approach” enables a combinatory utility. This entails three overlapping practices. The first is foresight: identification and realistic definition of possible developments and uses of science and technology — in this case, autonomous, unmanned technologies.

Second is the assessment of the possible and most probable effects of the technology upon particular domains and dimensions — in this case military operations and tolerances and thresholds for conflict.

The third is “prediction,” which describes the features, performance and manifestations of projected trajectories of the technology at defined points in the future.

The advanced integrative scientific convergence approach could be used to pulse current and emerging international developments and trends in autonomous, unmanned technology and relate these to both other domains of science and technology and present and projected sociopolitical factors to model near- and intermediate-range future uses and effects in specific settings on local, regional and international scales.

At a minimum, this may enable more detailed descriptions of both the current state of the swarming technology and the socioeconomic and geopolitical variables that exert pushing and/or pulling forces upon its use.

Still, it is important to recognize that the advanced integrative scientific convergence approach — like the advanced autonomous technologies upon which analyses focus — remains incipient and, therefore, should be regarded as a work in progress requiring ongoing assessment and revision to remain apace of global progress in technology and the shifting geopolitical and military postures contributory to its employment.

But the proverbial “cat is out of the bag,” or Pandora’s box is open, and these technologies are now a current reality and clear and present issue. Hence, the time is now to consider — and foster discourse and guidance focusing upon — how the development and proposed use of such advanced technologies will change political, socioeconomic and public postures toward, and engagement of, warfare. **ND**

Dr. James Giordano is Pellegrino Center professor at Georgetown University; Stockdale distinguished fellow of science, technology and ethics at the U.S. Naval Academy; and is currently serving as a non-resident senior fellow of the Simon Center for the Professional Military Ethic at West Point.

The views and opinions expressed in this essay are those of the author and do not necessarily reflect those of the Defense Department and/or those institutions and organizations supporting his work.



certain ideological constructs — and in such circumstances, the threshold for warfare in which there is greater potential for technological versus human loss would be elevated, and tolerance for such loss would be low.

More difficult to forecast is how a conflict pitting humans directly against decisionally capable autonomous machines would affect thresholds and tolerances for warfare, given that differing values would influence perspectives and actions relative to the probabilities of human and technological losses that would be incurred.

Predictions of this sort require analysis of, and preparation for, multi-domain and multidimensional effects of emerging science and tech-



Adaptation Battles

'Disaggregation' Called the Future of Naval Warfare

BY SEAN CARBERRY

SYDNEY — It's Dec. 7, 2031, and a pair of Australian Air Force battle management operators are casually chatting as they monitor the control center screens. Suddenly, 1,000 incoming targets appear. The operators sound the alarms, and the fleet in the harbor engages air defenses.

However, it's no match for the incoming missiles, aircraft and electronic deception that overwhelm the defenses and sink the ships in the harbor. Reports come in from around the country indicating similar attacks.

While fictional, that scenario was informed by Russia's 2014 invasion of Crimea that decimated the Ukrainian navy, said Rob Sutton, managing director of Mirragin RAS Consulting, during a November presentation at the 2023 Indo-Pacific Sea Power Conference in Sydney.

Ukraine learned from its 2014 losses, adapted in preparation for Russia's 2022 invasion and achieved more effective sea denial, he said.

"This time they achieved it using uncrewed surface vessels, or USV, cobbled together from readily available equipment and ordnance," he said. "The Ukrainian USV would navigate to their target using the Starlink internet service. ... The use of USV enabled Ukraine to expand the area of sea denial because Russian warships found it increasingly risky to venture from the heavily

guarded harbor at Sevastopol. Without a navy, innovation and adaptation had given Ukraine an edge."

The concept of "adaptation battle" has been at play throughout the war, he continued. "Ukraine innovates; Russia responds. Russia acts; Ukraine adapts."

The key adaptation Australia needs to make is to incorporate autonomous and robotic systems into its military and develop sovereign production capability, he said.

"The ongoing war in Ukraine has accelerated the use of autonomous technology in warfighting, and Australia must ensure that it is not on the wrong side of the asymmetric advantage in any future conflict," he said.

Australia is hardly the only country drawing such conclusions from the war in Ukraine. The conflict highlights macro trends driving toward a future where naval operations will rely less on large ships and more on masses of uncrewed vessels, said Bryan Clark, senior fellow at the Hudson Institute, during a panel at the exposition in Sydney.

"The growing threats posed to naval forces are playing out in two different ways when you look at the littoral operations versus open ocean operations," he said. "In the littoral environment, what we're seeing is an increasingly contested environment to the point where manned naval forces in a combat situation will have dif-

ficulty surviving at any scale, even with improvements to self-defenses.

"Even with more resilient ships, you get to the point where naval forces in the littoral areas are going to have difficulty operating and surviving," he continued. "So increasingly, we're seeing that be a role turned over to unmanned systems."

That is driving requirements for "command and control [and] orchestration of unmanned systems in very chaotic, nearshore environments — especially when conducting kinetic operations against enemies and trying to do that in an effective way," he said.

In the open ocean, different trends are playing out.

"The ability of long-range weapons to be able to hold at risk naval forces at thousands of miles away from an enemy's coast — for example. China is driving towards distribution to try and create more targets to dilute those attacks over a wider number of potential contacts," he said. "But that distribution is limited because we can only buy so many manned platforms. And so, you get to a certain point where distribution is unable to be expanded."

That again means turning to unmanned systems, he said.

"The other macro trend we're seeing is with regard to manpower and cost constraints, or financial constraints on navies," he said. Whether it is the U.S., Australian or Japanese navy, there are human capital limitations.

“When we try to expand the number of contacts or targets that need to be asked to engage, or we want to distribute the force more ... those are going to have to be unmanned systems to a large degree — or potentially optionally unmanned systems where you have a manned platform that can be unmanned — in a high threat environment,” he said. “That’s the way that we’re going to be able to distribute the force over a large number of platforms.”

That means thinking about “functionally decomposing our traditional multi-mission platforms into a larger number of less multifunctional platforms,” he said. “And that puts demands on orchestration and command-and-control, networking and also automation, because those individual unmanned or optionally unmanned platforms will have to be able to operate with very little human interaction [for] potentially very long periods of time.”

“So, automation is not just a matter of making the system smart enough to do guidance and control,” he said. “It also means making it able to address mechanical failures and address unforeseen situations and navigate in a GPS-denied environment.”

Those are challenges industry is trying to solve, said James Cowles, senior business development manager for L3Harris Autonomous Surface Vessels, during a demonstration of the company’s technology in Sydney Harbor.

If the objective is to have a swarm of UAVs moving in formation, “we can go do that tomorrow,” he said, adding that so far, the company has only operated about five vessels together in an autonomous formation.

“I don’t think there are any insurmountable challenges,” he said. “I can go and put hundreds of USVs out, and I put them in formation and it will be fine — I don’t need more or new software to do that. It will be really labor-intensive and quite hard. But it’s really doable.”

However, having hundreds of USVs conducting complex, independent missions and operating with self-healing network capabilities, that’s a different matter, and the technology isn’t there yet, he said.

“It’s developing the system so that one, there’s a coordination in it, but also the coordination is not node specific,” he said. So, if a node vessel is sunk, it doesn’t render the other vessels helpless.

Then there is the question of the desired behaviors of the robotic vessels, he said.

“OK, you see a potential hostile asset, and you go and swarm around it. Is that what we’re trying to do? Are you trying to form a barrier? Are we trying to swarm around our vessel to protect them? What’s the goal?” he said.

The goal is complexity for the adversary, Clark said.

“You’ve got a littoral combat ship and a bunch of unmanned surface vessels, one way to use them would simply be to use the unmanned surface vessels to extend the reach and the range and persistence of that manned platform, which hasn’t really changed from the enemy’s perspective how you’re going to fight and just means a few more targets to shoot at,” he said.

“But if instead, you free those unmanned systems to go off and conduct independent operations that you may have loose control over to create more challenging, more complex operations for the enemy to target, or to give you sensor capabilities for longer-range engagements, or for you to be able to conduct [anti-submarine warfare] over a larger area, those are different ways of fighting that you decompose or disconnect or decouple the manned platform from most of the elements of the kill chain,” he continued.

“So, we go from having all the pieces of the kill chain inside of your manned platform, inside the skin of your ship ... to instead, I’ve got to rely on basically the entire kill chain being off of my ship, and the only thing that I’m doing is maybe the command or control and then launching a weapon — everything else is being done by something else,” he said. “That’s a very different model.”

It’s a model the Defense Department is exploring through initiatives like Replicator, which seeks to accelerate the development, procurement and fielding of thousands of attritable, autonomous systems in all domains in 18 to 24 months.

Deputy Secretary of Defense Kathleen Hicks told reporters in November U.S. Central Command’s Task Force 59 is where much of the Navy’s autonomous surface and sub-surface experimentation is taking place, and that experimentation is

both about technology and tactics.

“The Ukrainians are showing a lot of how that rapid iteration is happening, and how much you have to adjust [tactics, techniques and procedures] as you go,” she said. “It’s not all about the technology and the initiatives that we’ll push through.”

The systems and platforms will have to “ride alongside” concepts of operations and tactics, techniques and procedures growth, she said. “And that’s where things like Task Force 59 — not the only place we’re doing it — where we can bring all that together and move quickly through experimentation and exercise to fielding is so important to how we’re going to get there in that 24-month timeframe.”

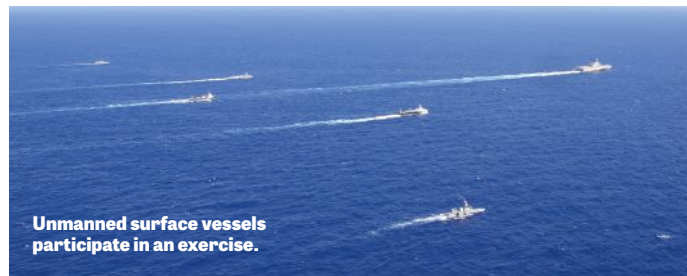
The required sea change in tactics and doctrine might be more difficult than developing the technology, Clark said.

“We’re kind of at the point now where the new technologies have gone beyond just making the existing way of fighting better, but they force you to think about fighting entirely differently,” he said.

“It’s going to come when we’ve got leaders that are willing to embrace a new approach to delivering military capability where you think about decomposing or disaggregating the functions of our traditional platforms into a broader collection of manned and unmanned assets,” he said.

That is ultimately a culture change, he added.

“Culture is a huge part of that,



because you have to have a military that’s willing to change how it fights and be able to embrace those [changes] and then instill those lessons throughout the entire force,” he said. “That’s difficult in the U.S. military because the services and communities within each service have their own norms and doctrines that are difficult to change when new technology comes along.” **ND**

Space Oddities

Quantum Science Finding its Way Into Satellite Technology **BY LAURA HECKMANN**

DUBAI, United Arab Emirates — Quantum technology might evoke science fiction tropes like shrinking humans and time travel, but experts think it has real-world applications to secure and improve space systems.

“Unfortunately, quantum is still, for some people, part of sci-fi, but actually we are using quantum technology in space already,” Sana Amairi-Pyka, lead scientist for quantum communications at the Technology Innovation Institute in Abu Dhabi, said during a panel discussion at the Dubai Airshow’s Space Pavilion in November.

The quantum technology of everyday use, such as in smartphones and personal computers, is what Markus Krutzik, head of joint lab integrated quantum sensors at Ferdinand-Braun-Institut, Leibniz-Institut für Höchstfrequenztechnik in Berlin, called first-generation quantum technology.

At the beginning of the 20th century, quantum mechanics and laws of quantum physics were being formulated, he said. Now, they’re being transferred into technology.

Quantum mechanics in simple terms is the field of physics that explains how extremely small objects have the characteristics of both tiny pieces of matter, called particles, and a disturbance that transfers energy, called waves.

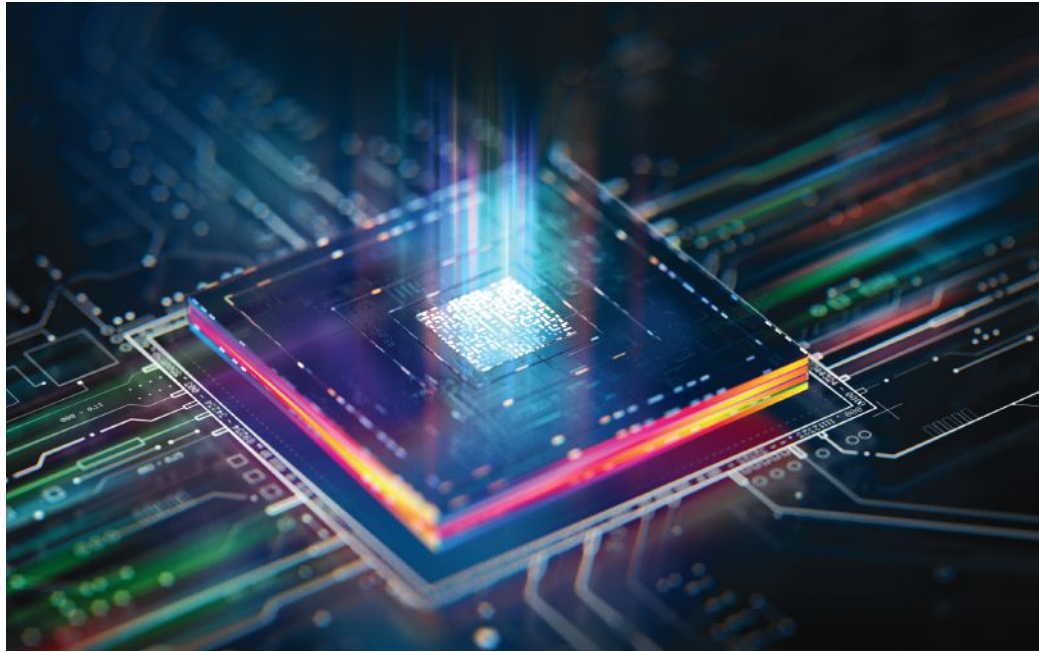
The study and application of their interactions, down to the atomic and subatomic level, is aimed at more efficient and powerful processing, such as quantum computing. Quantum computing uses a basic unit of information called qubits instead of a digital computing’s binary codes to perform faster and more effectively.

Krutzik develops optical clocks and quantum sensors, “especially for ... operation in space,” he said. Clocks are one example of what quantum technology could bring to space: enhanced navigation.

Quantum sensors utilize quantum mechanics to improve accuracy by sensing changes in motion and

electric and magnetic fields. The technology eliminates GPS vulnerabilities such as drifting perimeters and atmospheric disruptions.

“When you open up your phone and you find the next restaurant, you see ... your little blue point, which is giving you a position on the map. And that’s actually based on optical clocks, which are orbiting around our planet,” he explained. “And with quantum technologies, maybe we have the solution to help to increase the posi-



tion on such navigational devices.”

James Grieve, director of quantum communications at the Technology Innovation Institute, said using sensing technology and clocks for enhanced navigation is “really interesting,” and “we should probably be doing these things right now.”

Currently, a machine in Singapore can detect local gravity with a perimeter based on quantum physics. Called gravity mapping, the process uses quantum sensing to detect anomalies in gravity fields.

Alexander Ling, associate professor of physics at the National University of Singapore, said the machine has already been deployed in Singapore

to help the Energy Market Authority use gravity mapping to find geothermal energy sources underground.

While classical search perimeters can be used to conduct these searches, they tend to drift, causing inaccurate data, he said. A quantum perimeter can serve as a calibration station, “so your classical perimeters that are deployed will come back regularly to be calibrated before being deployed again. And that allows you to build up a really highly accurate map of a particular region.”

Ling said he believes this technology could be used in space — if there is enough risk appetite to “[put] one of these things directly on a satellite.”

In addition to more accurate navigation, quantum technology could also strengthen security in space — an area the U.S. Space Force has called a “significant challenge.”

A quantum random number generator is a piece of technology “we already use a lot in cybersecurity,” Ling said, but can now be made “very small, very compact, running on physical principles based on quantum mechanics.”

Grieve displayed a random number generator developed at the Technology Innovation Institute, small enough to fit on a keychain.

“So, this is the kind of size and scale of maturity we can make some of these devices, and this is based on quantum photonic principles,” he said. The generator is not yet space qualified, he said, “but I think if there’s interest, we could easily do this.”

The generator is one of four

quantum-backed security projects Grieve is working on within the quantum communications lab at the institute, including quantum key distribution and a ground station that will connect to global quantum networks by receiving signals from orbiting quantum satellites.

Quantum key distribution is a secure communication method for exchanging encryption keys between two parties, and is more secure “because the laws of quantum mechanics make it random” and provide “very strong durability guarantees,” he said. “We don’t think it’s possible for any technology developed by humans in the future to retroactively attack the system. So, it’s the best way we know to secure communications.”

The reason quantum encryption is more secure than regular encryption is because it relies on the laws of physics rather than mathematics.

Robert Bedington, co-founder and chief technology officer of Singapore-based company SpeQtral, said they are already demonstrating secure quantum technology that can work in space.

Among SpeQtral’s technology is a commercial quantum key distribution satellite, with laser communications and entanglement-based quantum key distribution, meaning it can enable secure communication in trusted, node-free networks over long distances.

“And we’re moving now from that physics experiment into developing systems that can distribute keys securely around the world to protect global communications against this threat of quantum computers,” Bedington said.

Krutzik said quantum sensing technology is also being used on some rockets and on the International Space Station as part of the Cold Atom Lab. Germany has activity dating back 20 to 25 years focused on paving the way for quantum technologies in space, he added.

Until now, many efforts have been focused on Earth observation, but Krutzik said “there are many articles already written up and assessed where you can see that the sensitivity of such missions using quantum sensors will be improved dramatically and also in specific frequency ranges” as the technology transitions into space.

That transition is what is taking the first generation into the next, Grieve said — “figuring out other things we can do with these technologies.”

And the more compact, inexpensive and robust the technology, “the wider the ecosystem of possible applications,” he added.

While Ling said an appetite for risk is a prerequisite for accomplishing that, another is standardization.

“It’s not just in cybersecurity we need standardization, but I can also tell you that a lot of the technology demonstrators that we have managed to achieve in Singapore ... would not have been possible if the satellites were not standardized,” Ling said.

Using a standardized form factor of cube satellites to demonstrate quantum technology means “your insights are sort of well understood, how you interconnect them,” Ling said. “And so this allows small university teams to actually take on very challenging technology experiments because you’re working towards a standard, working in a space where there are no constraints.”

The standards also allow cheap access to space launches, he said. In 2013, Ling’s team attempted to launch its first experiment in space, working with a Danish satellite group to put an instrument into a cube satellite.

“Unfortunately, the rocket blew up, so we didn’t get into space,” he said. “But 12 months later, we managed to launch another instrument on another cube satellite. Now, can you imagine in a traditional space mission ... a turnaround time in 12 months to build a new instrument? And this is only possible because we have standards in cube satellites. These standards [are] going to be important as we try to combine very exciting technologies from both quantum and new space together.”

And it’s going to be a collaborative effort, Krutzik said.

“I think we share similar issues, which are challenging factors which you can solve with engineering,” he said. “There are key components which we all need in these applications.”

Lasers, for example — at specific wavelengths with specific performance criteria, “which space hardens,” he said. “So we need lasers, we need electronics, we need vacuum systems. That’s pretty much classical technology, but it needs to be integrated and hardened in a way that it reliably works in space.”

That means getting it outside of a laboratory, he said.

“You can show that all this technol-

ogy and the systems work in ... the laboratory, but if you want to bring this up to space, you need to push technology developments,” he said.

Government has a role to play in making that happen, but just what that looks like is still being defined.

Grieve said there is “plenty of government support” for development work such as satellites and clocks, and while quantum technology is expen-



SpeQtral and Toshiba's multiplexed quantum key distribution terminal

sive from a developmental perspective, for the end user, “devices don’t necessarily have to be expensive.”

What would be nice, he said, is to have a transition plan that moves these technologies out into the private sector after development. “So, governments will of course fund development, but moving past that, if you want to have some kind of sustainable industry based on these devices, we have to identify use cases. And we have to bring in users and see how these technologies can benefit real activities that actually matter to society.”

Connecting the right people to accomplish this is one of “many challenges,” he said — “trying to bring people who ... have potential use cases, where we think they might have a use case, or ... trying to do exploratory work and have these conversations to see where some of these technologies make sense.”

Whether or not this problem falls on the government to solve, “I’m not 100 percent sure,” he said. “But as a sort of manager of the community, it would be nice to have government assistance in trying to make these connections.”

With so many variables at play, quantum technology’s success in space will come down to the “level of appetite,” Grieve said. “A lot of people here are very excited about space. ... It’s refreshing. It’s encouraging, and it’s the kind of environment in which we hopefully will see lots of very excited young engineers coming into the field and trying to ask what they could do.” **ND**

Trust But Verify

Large Language Models Have Pitfalls For National Security **BY LAURA HECKMANN**

ORLANDO — Generative artificial intelligence: eerie or exciting? Experts suggest the increasingly intelligent large language models are not something to be feared, but rather tools to make human lives easier, revolutionizing how we learn and train. We just need to learn how to use them effectively.

Critic or proponent, one fact is undeniable: generative AI is here, and it's getting smarter. Industry and academic experts suggest this leaves one option: get comfortable with it.

Generative AI is an architecture, Svitlana Volkova, chief AI scientist at Aptima Inc., said during a panel discussion at the National Training and Simulation Association's Interservice/Industry Training, Simulation and Education Conference in November.

"It's a neural architecture generating pre-trained transformers," she said. "And there are different versions — models that can learn efficiently from really large data and can be easily adapted to do many tasks."

Large language models use algorithms and artificial intelligence to mimic human intelligence and generate large sets of data. But it's only as good as its input, or the learner, which means humans are in the driver's seat — or can be, if they learn to apply it creatively and responsibly, the panel suggested.

The evolution of the learner has moved through machine learning, supervised learning and deep or representation learning, Volkova said. Today, it has arrived at what she called in-context learning, "where there is a very large model that has been trained on a lot of data," she said.

In-context learning is a method of prompt engineering — crafting prompts to feed the model to improve the effectiveness and accuracy of its task. For example, a simple prompt such as "drink water" could be refined to include a plastic cup or filtered water.

Andy Van Schaack, associate profes-

sor of the practice of engineering at Vanderbilt University, called prompt engineering "very interesting. It's just remarkable how changing a few words can make a big difference."

New users exploring large language models should not get hung up on the particulars of prompt engineering, he said. "Just launch ChatGPT and start chatting with it. In fact, the first great prompt is, 'I'm brand new to this, how should I begin?' And then begin having a conversation with it as though you're talking to another person."

Users can take the concept a step further with super prompts — supplying the model with more detailed signals to teach it to respond more effectively.

Keith Brawner, program manager at the Institute for Creative Technologies — a Defense Department-sponsored University Affiliated Research Center working in collaboration with the Army — gave an example of a super prompt: "Hi, my name is Keith. I can read diverse opinions and value them, but those opinions don't necessarily change my mind. I can talk about the following subjects with expertise. I value complete answers more than I value incomplete answers."

A super prompt could be pages long, but it can also be "easily automated," he said. In a way, it already is — by copying and pasting the super prompts before every new chat, he said.

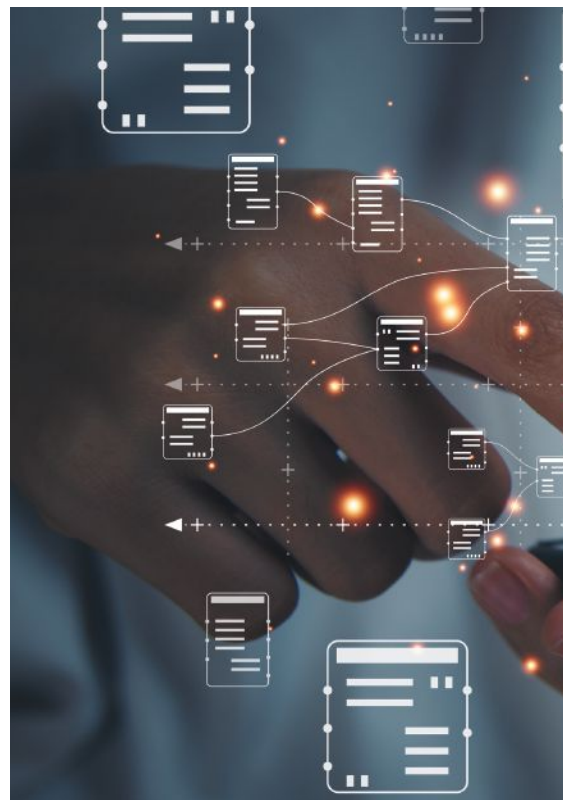
If prompts and super prompts sound overwhelming, Van Schaack said not to worry — they will likely disappear. He speculated the average human will eventually become comfortable enough interacting with AI — and the systems will become sophisticated enough — that prompt engineering will fade into the background.

"I think right now, we do want to have experts who really know how to squeeze out of these systems the very best possible, but the people on the backend ... are creating sort of intermediary agents who are translating our ill attempts at prompting into more sophisticated prompts for the system itself," he said.

At its core, mastering generative AI systems is rooted not in the field of computer science, but human performance, he said.

"There are decades of research on how to get two people to work together productively," he said. "And so we take those evidence-based approaches for collaborative work and bring it into this world. I think we're going to see the same positive results."

But it's not all positive. Those who fear the rise of the machines are not unwarranted in their concerns, the panel acknowledged. With great power comes great responsibility, and artificial intelligence comes with data poisoning, privacy concerns and security risks.



Van Schaack said there are two main issues with generative AI: privacy and security concerns about the training data and how humans interact with it, and how that data is being used to train models in the future.

He noted the training component for ChatGPT can be turned off, but he simply would not use any commercial systems for confidential or classified work. Concerns over what commercial providers are doing with collected data and who can access it "are absolutely valid," he said.

From a military training and simulation perspective, when data often is confidential or classified, evaluating

trust and privacy depends on what you're trying to do, Brawner said.

"You see policy coming down ... saying, 'Hey, if large language models help you do your job, please use one of the offline versions. Please don't let everybody know exactly which reports you are summarizing, but if they help, knock yourself out.'"

Tasks such as providing specific terrain level targeting data, however, are a different story — "Let's back up a second to this trust and safety and privacy question," he said. Policy is emerging from the National Institute of Standards and Technology, including certifications of various terrain types for different applications and classified enclaves with classified

Data poisoning is an adversarial attack that tries to manipulate a model's training dataset to control its predictive behavior, and it's a "big issue," she said. There is no impenetrable guard against it, but Van Schaack said there are measures to mitigate it.

"There are a lot of ways of improving these generative AI systems," he said. "Faster microprocessors, more memory, write better algorithms, better training datasets, and so the race right now is how do we get these systems that can score better on ... these various benchmarks?" Better quality data could be a start, he said.

Companies are being more thoughtful and deliberate about the data they feed their systems, he said. "So

TRAINING & SIMULATION

tems, especially with ... models that are huge, that it's practically impossible to validate," she said. "So, there will be a lot of research in this area, too."

Throw into the mix of caution and excitement a sense of urgency: a global race to develop the smartest systems is in full swing, Van Schaack said.

"You look at the number of papers that come out, you look at the number of patents that are being produced, there's as much work being done in the field of AI in China [as] ... the United States and certainly other nations," he said.

The good news is also the bad news: 15 people in an office anywhere can produce "phenomenal models, good or bad," he said. "And so, it would be naive to think that adversaries ... are not capable of beating us in many ways."

As nations race to develop the smartest systems, another concern could be artificial superintelligence, he said.

"It's going to develop the next generation of itself that's going to be even better, and then it just kind of takes off from there," he said. "And so there is a race to produce that, because intelligence is power."

Van Schaack predicted five years down the road, computers will be "as capable as we are at any cognitive task," possibly more, with artificial superintelligence. There will be pockets where a system can't handle certain types of problems, "but that's just a PhD thesis away from being solved."

Humans are already utilizing generative AI to send emails, summarize reports and gather training data. As it continues to rapidly evolve, the focus needs to remain on how humans think about it, Van Schaack said. The human brain will not change.

"Computers are evolving very quickly ... the human brain isn't going to evolve, and so we still need to think about cognitive psychology," he said. "We still need to think about ... psychological principles that help human beings to acquire and retain knowledge and skills, those things won't change."

"And so, we'll want to continue to focus on those as we think about training," he continued. "But how do we use AI to develop those instructional systems? How [will] those systems ... adapt based upon the interaction of the learner?" **ND**



large language models, he said.

At "the highest levels, when lives are really on the line, all of those questions start to come into play," he said. The military does have ways to test and verify large language models, such as secure enclaves that ensure large language models are not uploaded, he said.

The size of language models has made security trickier as well, Volkova said. Models used to be much smaller — today, "we're talking about billions of parameters ... sometimes even trillions," she said. "So, how can we make sure that the terabytes of data [weren't] poisoned?"

instead of grabbing everything you can on the internet and just dropping every subreddit you can throw on there, they're being much more careful about it, and they're also producing guardrails, metaphorically, about how you can respond."

Volkova said a framework is needed for verifying data and developing proper safeguards and defense mechanisms "to make sure that we are testing these models really carefully." She said NIST is already working on one, and "policy is moving."

"We need new technologies to make sure that we're developing safe, secure and trustworthy generative AI sys-

Air Force Overhauling Training To Take On Near-Peer Foes

ORLANDO — The Air Force is undergoing a top-to-bottom reorganization to transition from counterterrorism operations to competition with more powerful rivals, and its training and simulation systems will be a part of the overhaul.

Secretary of the Air Force Frank Kendall kicked off a campaign last year to address “capability gaps” when it comes to fighting near-peer competitors, Lea Kirkwood, program executive officer for Agile Combat Support, said recently at the Interservice/Industry Training, Simulation and Education Conference in Orlando.

There is a lot of change going on across the Air Force, “and that is no different within the simulators portfolio,” she said.

The service — to start these reforms — is working its way through a series of “cross-cutting operational enablers.” The first of these so-called COEs were electronic warfare, munitions and mobility. Next up is testing and training, which falls under her purview, Kirkwood said.

“When we think about that high-end fight, and we think about how agile our airmen can be, how capable they can be, how can we instill next-gen training is what the secretary is going for,” she said.

Col. Charles Ryan, senior materiel leader for the simulators division at PEO Agile Combat Support, said the Air Force’s main line of effort to overhaul its training and simulation technology is the Simulator Common Architecture Require-

ments Standards, better known as SCARS.

Most fourth-generation simulators were built as standalone, stove-piped systems, he noted. That was OK when they were developed. “But it’s not how we fight today,” he said.

SCARS will enable the Air Force’s vision of a day when all simulators are interconnected so, for example, a pilot training in a jet fighter simulator can simultaneously connect to pilots training on tanker or bomber simulators, or both.

There are three guiding, main lines of effort to reach the service’s grand vision, he said.

One is developing, fielding and sustaining a common synthetic environment, called the Joint Simulation Environment.

The F-35 Joint Strike Fighter’s simulators, which incorporate the Navy, Air Force and Marine Corps models, inspired the Air Force to duplicate and expand the capability, he said.

The Air Force wants to simultaneously simulate missions with F-35s as well as other advanced aircraft such as the F-22 and those in development such as the

Next Generation Air Dominance family of systems.

The Joint Simulation Environment concept was rolled out in 2022, but Ryan noted it has been slow to get started.

“It frankly hasn’t made as much progress as I would have liked it [to] at this point,” he said. It took a lot of time to stand up the development team, but now that it is in place, “we’re picking up speed,” he said.

The second line of effort is to increase the capability and interoperability of the distributed training networks that will connect them all together.

And the third will be to ensure sufficient concurrency, fidelity, connectivity and recapitalization of training systems.

“That is what I call the blocking and tackling. That is maintaining currency for our training systems that are in the field today,” he said. There are 14 legacy simulator programs that will have to be maintained, he noted.

Implementing SCARS is the training program’s top priority, Ryan said.

There are two big advantages to creating the interoperable system, he said.

One is “concurrency.” In other words, making sure the latest tactics, techniques and procedures pilots are experiencing in the real world are being quickly and efficiently integrated into simulations.

“This is a gateway to increasing that, which is something we struggle with immensely right now — maintaining concurrency between the jet and the training device,” he said.

The second sea change will be interoperability.

“Most of our training devices from the fourth-gen fleet were built in stovepipes, and they had no intention of having those things work together,” he said.

Another big piece of the new system will be cybersecurity, which also wasn’t built into the legacy systems. Tightening up security by sending out updates and patches to all the simulators through the network will mean less downtime, he added.

Ryan noted there has been some confusion about the differences between SCARS and the Joint Simulation Environment. SCARS will enable the latter, he said. “They’re not in conflict in any way,” he added.

By SCARS version four, the program will be adopting the Government Simulation Interface standards, he said.

But first, SCARS should provide a common hardware that will be applicable to the joint environment.

As for software, a first step will be creating a common geospatial database that can replicate the Earth’s terrain.

While not mentioning the Army’s One World Terrain program by name, Ryan acknowledged that there are similar government databases already in existence, but they may not be a perfect fit.

A foot soldier may “care about a leaf on a tree,” but a pilot flying at 40,000 feet — maybe not so much, he said.

“I’ll just explicitly say the [Joint Simulation Environment] is going to become the cradle to grave common thread for understanding mission effectiveness for the Air Force. And I think the Navy’s on the same track and potentially Space Force in the future as well,” he said. **ND**

— Stew Magnuson



Air Force photo



Army to Replace ‘Laser Tag’ System for Soldier Training

ORLANDO — For more than four decades, the Army, other militaries and law enforcement agencies around the world have used a laser-based system to train personnel using small arms in force-on-force exercises.

With lasers attached to guns, a trainee fires at an opponent — or perhaps a vehicle — outfitted with a series of sensors. If he or she scores a hit, the victim is alerted and could be declared injured or dead.

It is a high-end, more sophisticated version of laser tag.

But now, the Army is looking to replace the Multiple Integrated Laser Engagement System, better known as MILES.

The laser-based technology has been a part of soldier training since the early 1980s, although the system the Army uses has undergone several upgrades since then. The latest was in 2012.

It is looking more like the Army will have to come up with a new acronym for the system as the “L” in MILES is likely to go away, said one senior Army official.

“We can arguably go out and buy a new laser-based system that will be a new version of the old technology. But our senior leaders have told us not to do that: don’t go out to buy new versions of old technology,” said

Brig. Gen. William Glaser, director of the Army Synthetic Training Environment Cross-Functional Team, during a panel discussion at the Interservice/Industry Training, Simulation and Education Conference in Orlando, sponsored by the National Training and Simulation Association.

Optical and GPS-paired devices are among the new concepts that could replace lasers in simulated engagement training, he said.

Ray Chandler, Lockheed Martin synthetic training environment campaign manager and former sergeant major of the Army, told reporters at one of the company’s Orlando facilities that the current version of MILES only supports about 45 percent of a brigade combat team that cycles through a combat training center.

“So, 55 percent of the combat power and brigade does not have the ability to play in the battlespace for the training part. That’s huge. If you can go from 55 to 100 percent of all those enablers and allow everyone to be a part of the game, it’s an exciting thing,” he said.

Other flaws in laser systems include the inability to simulate indirect fires, he said. A leaf or a raindrop also can cause the laser beam to go awry, and if someone hides behind something as thin as a cardboard box, the laser can’t penetrate it even

though a real bullet could, he noted.

Lockheed Martin is going the GPS route as it gears up to compete for the MILES replacement contract.

Since 2019, it has been investing its own dollars in the new system and later received Army Other Transaction Authority agreements to fund prototypes for a geo-paired system it calls SIMRES.

It allows a lightweight universal weapon orientation module about the size of a pack of gum to be placed on any type of barrel. The operator can then input into the software its ballistics, which MILES cannot do. It also takes into account environmental conditions.

The module affixed to the barrel is paired with a sensor mounted on a soldier’s helmet, which can provide a wealth of data to instructors that they previously couldn’t collect, he said.

“If you’re firing your laser, you’re not necessarily getting any real-time feedback other than a hit,” Chandler said.

The new system can record where the soldier was looking, track his movements on the battlefield, time how long it takes to acquire a target and fire, and also tell instructors when he pointed his weapon at a friendly.

The company is currently working on three OTAs to create prototypes for M4 rifles, M320 grenade launchers and ground combat vehicles.

A spokesman for Glaser said the Army is looking to field a MILES replacement in about 2027. **ND**

— Stew Magnuson



Out of Their Element

Army to Live Off the Land in Contested Environments **BY ALLYSON PARK**

After two decades of counterterrorism and counterinsurgency operations in permissive theaters, the Army is pivoting to the Indo-Pacific, where a near-peer adversary and an expansive maritime theater present immense challenges for logistics and sustainment in a conflict.

That's why the Army and the defense industry are investing in environmental research and technology to help the service and the Joint Force conduct and sustain operations in contested and distributed environments.

While a potential conflict in the Indo-Pacific would be fought largely in the air and sea, the Army would still play a critical role providing long-

range fires and other effects for the Joint Force. Preparing for that is a key focus for the Army of 2030, Maj. Gen. Kimberly Colloton, deputy commanding general for military and international operations for the Army Corps of Engineers, said at the Association of the United States Army's annual meeting and exposition.

"To maintain a military advantage over our adversaries, we must [better] leverage and exploit faster new technologies across all domains," she said. "We know that forward-positioned ground forces, those able to converge effects from land, air, sea, space and cyberspace, can complicate our adversaries' decision-making, disrupt their actions and assure

our allies and partners."

Supplying and sustaining those forward-deployed forces will require new technologies, tactics and thinking, which is why the Army in March created the Contested Logistics Cross-Functional Team based in Huntsville, Alabama, in partnership with Army Materiel Command, as announced by Gen. James Rainey, commander of Army Futures Command.

Given the distances involved in the Indo-Pacific theater, the Army is looking to reduce what it needs to carry and increase what it can extract or rely on from the environment, which is why the Defense Department and Army are investing in research and development for alternative energy sources, water purification and geo-spatial data gathering.

While the service already has capabilities to identify water sources in complex environments and to purify that water to sustain warfighters, this process can be streamlined further, said Dr. Martin Page, materials engineer at the Cold Regions Research and Engineering Laboratory.

"Water supply is one of the top demand signatures on the battlefield for resupply," he said. "And as we think about moving forward toward contested logistics environments, with an increased focus on mobility and dispersion at large unit scales, we need to think about how we can reduce that [logis-

tics] tail further and give our commanders options for technologies that can increase freedom of action, operational reach and endurance."

Reducing demand and increasing production at the point of need are two key pillars of achieving a more sustainable water supply process, meaning that the Army is focusing on using each drop of water "as efficiently as possible" and on being able to produce water on the move, untethered from a water source.

"We found that water recycling or water reuse, specifically of graywater, can have a big impact in those types of environments, reducing demands by up to 50 percent in some cases," Page said. "When we think about mobile

operations, we're thinking about looking at less showering and less laundry support in those environments in our planning. And so, we need to increase our focus on being able to produce water at the point of need."

The Army, the Cold Regions Research and Engineering Laboratory and the Army Combat Capabilities Development Command Ground Vehicle Systems Center are developing the Advanced Low Logistics H₂O, or ALL-H₂O, system, a wheeled system that is focused on hygiene support, demand reduction and increasing production at the point of need through the lens of hygiene support.

"It's basically a system that can provide shower and laundry support, but it also has an onboard water recycling capability that can recover 75 percent of the water as clean water that can go back into the shower and laundry systems," he said.

The All-H₂O system was featured at Project Convergence in November 2022, and it underwent additional testing at Fort Leonard Wood in Missouri this summer, working toward reaching technology readiness level six milestones.

"We are working on the system; we're continuing to do research on increasing that water recovery beyond 75 percent. But what we're finding is that for various reasons, we're not going to ever get to 100 percent recovery," Page said. "There's always going to be some need for either resupply or point in the production, no matter how hard we try on that."

Another critical challenge in contested environments is providing power, and the Army Corps of Engineers — in collaboration with the Department of Energy, Army labs and other services and agencies — is researching fuel cells and hydrogen for alternative energy generation and storage.

Hydrogen can be used as an alternative energy storage medium, both in stationary and mobile applications. The Army has invested in a research project called H₂Rescue, a hydrogen fuel cell and battery hybrid emergency vehicle that can immediately begin exporting 25 kilowatts worth of power in an emergency.

"It replaces having to pull in additional generators," Nicholas Josefik, engineer at the Army Engineer Research and Development Center's Construction Engineering Research Laboratory, said. "This vehicle can drive about 1,500 miles on a

single tank of fuel and can immediately begin powering, just plugging in whatever items you have."

H₂Rescue can be integrated into many different vehicle platforms, and the fuel cell can even produce some usable water, he added.

The Army, in partnership with the DEVCOM Ground Vehicle Systems Center Laboratory in Michigan, is developing this fuel cell-powered system that is for both tracked and wheeled vehicles, capable of exporting power and delivering hydrogen in the field.

"It's another way to dispense hydrogen, to create power in the field and just give us different opportunities for types of energy generation," he said.

Along with H₂Rescue, the Army Corps of Engineers is also looking to generate hydrogen fuels in the field via a distributed low-energy wastewater treatment system that can harvest two different types of usable fuels, Josefik said.

"We're able to harvest methane and hydrogen, along with treating the water and having usable water," he said. "Our researchers are leading the way and looking at, instead of spending all that energy and time just to treat our wastewater, [harvesting] that into usable fuels and increasing our energy security, our resiliency and reducing our logistical burdens of bringing fuel in the field."

In addition to water and power solutions, the Army is exploring technology to improve overall management of logistics in contested environments. The Army, along with the Army Geospatial Center, is investing in a project called the Geocentric Environment for Analysis and Reasoning, or GEAR, to help warfighters operate more efficiently.

GEAR is a tool that provides location-based information and data, and depending on that data, it determines how certain tasks should be prioritized, said Heather Speight, physical scientist at the Army Geospatial Center.

"If you have something that's important to you, maybe three objectives that really matter, [we] put them on a map together and then see if there's an area that seems to be the area

that we want to focus on," she said.

The Army Geospatial Center is currently working with U.S. European Command to develop GEAR, she said. The service mainly utilizes GEAR to gather data on airports, seaports and large cities, as well as the larger transit network.

GEAR can also factor in climate variables, Speight said.

"When we come to climate change considerations, a climate-informed assessment may need to include flooding, it may need to include climate migration, it may [need] to include sea level rise," she said.

GEAR's ability to collect and interpret relevant climate data and its effect on future Army operations, as well as its varying effects on different domains, is absolutely crucial, Speight said.



"Environmental issues and water issues fall into Army challenges," she said. "One of our jobs here is to come up with ways that we are going to help [the Army] wrap its arms around those requirements and really help them understand those environmental challenges in a manageable and meaningful way."

GEAR will allow the Army to integrate new information into existing workflows, which is key especially as climate change continues to alter existing environments, she said.

"The thing with GEAR is we're allowing you to take the work you already do and conduct an analysis and then add a few more variables and see if the analysis changes," she said. "In that way, we're helping to really see whether or not climate is going to change things, or if really climate didn't make that big of a difference, and we just continue with operations as normal." **ND**

GOVERNMENT PERSPECTIVE

The Role of Logistics, Sustainment in Integrated Deterrence

BY CHRISTOPHER LOWMAN

In my first year as the assistant secretary of defense for sustainment, I have observed the contested, dynamic and distributed nature of the new strategic environment.

Peer competitors increasingly hold our defense ecosystem at risk. The future of war will be fast, mobile and lethal and requires the Defense Department to think about sustainment through the lens of integrated deterrence, which is a holistic and coordinated approach that integrates all elements of national power to address and respond to a wide range of threats and challenges.

Realizing the benefits of integrated deterrence from a sustainment perspective hinges on our ability to: prevail in a contested logistics environment; modernize the industrial base across the network of organic, domestic and international partners; establish data-informed sustainment; and find and fix operations and support cost drivers.

In recent decades, U.S. forces have operated without much strategic risk to logistics. We operated from secure bases and became comfortable with uncontested and unchallenged movement throughout the theater of operations. During that time, the capabilities we have fielded — like the F-35 Joint Strike Fighter and other enduring platforms — have utilized sustainment strategies that assume a more permissive strategic environment.

Today, the strategic environment is defined by challenges to logistics agility, flexibility and survivability through kinetic and non-kinetic disruptions. To navigate and prevail through a contested logistics environment means ensuring that logistics, supply chain operations and transportation capabilities are resilient and can operate effectively in hostile environments.

Therefore, I've launched a campaign of tabletop exercises to stress the life cycle sustainment strategies for existing capabilities, given the realities of a contested logistics envi-

ronment, to better inform current sustainment gap mitigation efforts and future sustainment strategy design. To secure enduring military advantage, the Defense Department must ensure that the combatant commands are postured with sufficient resources such as munitions, fuel and spare parts. They must also have the capabilities to perform maintenance, manufacturing at echelon, storage and transportation and withstand and recover quickly from disruptions.

The future calls for resilient sustainment strategies that are more distributed, flexible and responsive to changing operational and strategic conditions.

One example of reducing risk within a contested environment is the need to mitigate demand for ocean lift capabilities by employing strategies that satisfy demand closer to the point of need.

Advanced manufacturing, which includes 3D printing, provides an opportunity for manufacturing parts on demand, which can be useful in situations where supply chains are disrupted or contested. By integrating advanced manufacturing at different levels, the joint force can produce crucial parts in contested environments in a distributed manner, increasing an adversary's dilemma and ultimately U.S. integrated deterrence posture.

To enable full implementation, the office of the assistant secretary of defense for sustainment is working to ensure secure transmission of intellectual property and accurate accounting of its use to ensure appropriate compensation to the IP owner, as well as assessing our department's approach to modernizing intellectual property licensing rights or fee strategies, which requires close collaboration with our industry partners to identify the appropriate changes in policy and process.

The office of the assistant secretary of defense for sustainment is charged with providing advice and assistance to the undersecretary of defense for acquisition and sustainment, deputy



secretary of defense and secretary of defense on sustainment functions including logistics, material readiness and product support. In addition, the office is responsible for budgetary, policy and management oversight for sustainment functions in the Pentagon.

At the enterprise-level strategy, the department is looking 15 years down the road at sustainment capabilities within the organic base and development pathways to better share our future vision throughout the defense industrial base and its commercial partners. My goal is to create a more collaborative, transparent environment that ensures capital investments, whether government or commercial, result in more integrated support for the industry of the future.

We've developed goals to ensure strategic alignment across the service modernization efforts and are applying a results-oriented management framework to define an optimum investment approach. This will not only ensure the industrial base is able to keep pace with the rapidly evolving technological landscape but will facilitate smoother integration of these advanced systems into the defense infrastructure.

Today, the services are working to modernize depot maintenance organizations, operations and technologies. They are improving processes, deploying interoperable maintenance repair, overhauling information technology systems and retaining world-class capabilities properly sized to workload requirements. The objective is to meet materiel readiness goals with modernized, efficient and resilient infrastructure at the service and enterprise levels.

Instrumental to the success of the sustainment modernization effort is striking a balance between the organic industrial base and the commercial industrial base.

We must maintain the right balance of capabilities between it and industry, both domestic and international, to ensure resiliency, economic viability and the overall health of all partners. The goal is to create a more complementary defense industrial base that minimizes the duplication of capacity and capability, balancing organic and commercial industry repair capabilities and capacity. The Defense Department is committed to being as transparent as possible when outlining government investments in the organic industrial base, focusing on how it

plans to have capabilities complement rather than compete with industry.

To achieve this balance, we are adopting increasingly transparent approaches to foster a more collaborative relationship between the industrial base partners, ultimately driving efficiency and effectiveness in our modernization efforts.

One initiative that should be the subject of future sustainment strategies is being resilient and flexible with commercial partners that emphasize a regional sustainment concept, which would utilize existing allied and partner maintenance, repair and overhaul capabilities and U.S. industrial base capital investments to provide sustainment support service using allied and partner national and/or commercial capabilities partnered with U.S. industry within the various theaters of operation.

Building upon and working collaboratively with industry and allied nations would minimize disruptions, optimize supply chains, maximize availability in theater, minimize reliance on long over-ocean transportation routes and further distribute the maintenance, repair and overhaul capabilities regionally to increase resilience and survivability. Building a regional sustainment concept would foster new and innovative supply chain resiliency, improve our ability to identify and respond to future challenges and aid in integrated deterrence.

Given the rapid pace of technological advancements, the department must harness new capabilities and workforce competencies to effectively sustain the force both now and in the future.

For instance, we have only just started tapping into the potential of machine learning and artificial intelligence to address sustainment challenges. As part of this effort, we are developing new capabilities that utilize data and analytics to enhance sustainment-related decision-making at all echelons both within the operational and strategic levels and throughout the weapon system life cycle.

The distributed nature of the battlefield necessitates greater precision in our inventory requirements, increased visibility of our joint transportation needs and capabilities and a better understanding of failure probabilities to efficiently deploy our maintenance resources.

I've challenged the services to operationalize conditions-based maintenance-plus at echelon to shift

maintenance from an unscheduled, reactive approach to a deliberate, predictive approach. It facilitates performing maintenance based on evidence of need, when it optimally supports operations, as opposed to providing maintenance at failure, which can negatively impact unit readiness.

Taking advantage of the sensor platforms the department has invested in over the last 20 years by implementing conditions-based maintenance-plus decision support tools at echelon helps provide a better understanding of system performance, including associated cost drivers and support options, while also enabling more precise inventory management of critical items.

Consequently, we are concentrating on the creation of business intelligence tools that enable decision-making at each echelon to ensure the battlefield logisticians have the information they need to make actionable decisions that maximize availability and readiness. By pursuing programs in supply, transportation and maintenance functional areas, we strive to leverage data and analytics to further improve sustainment-related decisions across all levels of the department.

As we face the emerging challenges of today's strategic landscape, we are adopting transformative solutions to drive down operating and support costs while enhancing operational availability across the services. The goal is to incentivize the services and defense agencies to collaborate, align efforts both horizontally and cross-functionally and to ensure we are delivering the highest materiel readiness return on investment.

Key to this endeavor are efforts like the Rapid Sustainment Improvement Program, which is a cornerstone of our strategy designed to address cross-service cost drivers that do not rise above the individual service prioritization levels but collectively account for significant sustainment cost across the department. Through this program, the department can prioritize and resource commercially available sustainment technologies that demonstrate positive returns on investment and can be scaled quickly to improve availability and lower operations and sustainment costs.

Implemented beginning in fiscal year 2024, the department has identified and funded a full range of projects and identified proposed projects for 2025, which include key enablers such as conditions-based maintenance-plus

business intelligence tools at echelon, and has started on the effort to solicit industry input for 2026 projects.

This decentralized decision-making process fosters a more agile and responsive structure, ultimately securing our ability to deliver combat power at the point of need. Through this approach, the department can better allocate resources, prioritize efforts, field existing solutions more rapidly and adapt quickly to evolving challenges, ensuring that our military remains prepared and effective in an ever-changing landscape.

The dynamic and contested nature of the strategic environment demands



a new approach to logistics and sustainment. Integrated deterrence, as an element of the current National Defense Strategy, offers a comprehensive framework to address emerging challenges and ensure military advantage. Key areas of focus include prevailing in a contested logistics environment, modernizing the industrial base, leveraging data and analytics for sustainment decision-making and finding and fixing operations and sustainment cost drivers.

The current era offers a unique opportunity for collaboration and knowledge exchange between the Defense Department, international partners and industry stakeholders, setting the stage for development of effective regional sustainment strategies that meet the demands of modern warfare.

By adapting to the changing strategic environment and embracing an approach that uses integrated deterrence to combine our strengths to maximum effect, the department can ensure the United States and its allies maintain a decisive edge in an increasingly competitive and challenging world. **ND**

Christopher Lowman is the assistant secretary of defense for sustainment.

Fueling the Fleet

Navy Going Digital to Increase Energy Efficiency

BY JOSH LUCKENBAUGH



Refueling Navy ships while at sea — particularly larger vessels like destroyers — takes a lot of time and effort, requiring a supply ship to come fill up the tank.

While this may not be such a daunting task in peacetime, in a potential Indo-Pacific conflict an underway replenishment could become an easy target for an adversary. The Navy is going to need to make the most of every tank and spend as little time as possible at the pump, experts have said.

The service's Global Energy Information System, or GENISYS, could play a key role in improving decision-making and fuel efficiency across the fleet. Its goal is "to accurately and consistently track surface ship energy usage to improve operational readiness," a Navy spokesperson said in an email.

GENISYS consists of three applications: two ship-based applications called eLogBook and the Shipboard Energy Assessment System and an ashore, cloud-based component called the Fleet Energy Conservation Dashboard, the spokesperson said. The system achieved initial operational capability in 2023 "after GENISYS validated its ability to automatically

transfer data from the ship-based applications on an Arleigh Burke-class destroyer to the Fuel Energy Conservation Dashboard application live on the government cloud," the spokesperson said. As of the end of fiscal year 2023, GENISYS has been installed on 12 destroyers.

The Navy leveraged Small Business Innovation Research funding to create GENISYS, with Beacon Interactive Systems and Frontier Technology Inc. serving as the developers and ManTech International Corp. as the software integrator, the spokesperson said.

Beacon CEO ML Mackey said through the SBIR program, the company has been able to take its experience in the commercial sector "to bring to bear on DoD problems and deliver capabilities into the hands of the warfighter."

The company's first SBIR program was focused on "the question of how do you decrease the cost of keeping our ships mission-ready by addressing the big cost driver, which was the people doing the work?" Mackey said in an interview. "And the proposers on our topic proposed a lot of the mainstream kind of stuff that was being suggested across the DoD. We were outside the DoD, [and] we said, 'Well, you'd figure out how to make it easier for them to

An Arleigh Burke-class guided-missile destroyer and a supply ship conduct an underway replenishment during a training exercise.

get their work done,' which is what we had done for" private companies such as Olympus, MetLife and IBM.

A major time-consuming task for sailors is logging activity on a ship — and in the Navy, "every single thing that happens on a ship gets logged," Mackey said.

Beacon president and chief technology officer Mike MacEwen said the logs include everything from orders given on the bridge, to when equipment is turned on and off or valves are changed out in the engine room, to personnel, sea state and environmental data — "they do one where it's trying to figure out how much fuel and water are in [the] tanks, and they do it manually" — to combat system orders, to "what happens when you enter a harbor. So, it's all this very minutiae data about everything happening on a ship."

Before GENISYS — which is still the case for the majority of the fleet that has not received the system — all the ship logs were, or are, done on paper, Mackey said. Beyond taking a lot of time to do, the handwritten logs are messy and hard to read, causing problems such as information getting missed, she and MacEwen said.

In contrast, eLogBook digitizes the ship's records for engineering, deck and daily fuel and water, reducing the burden on sailors to record the information and the time required to access the logs, the Navy spokesperson said.

"It's much more accurate to click a button than to handwrite scrawl — and if you've ever seen a written log book ... I mean, you can't read them. It's insane," MacEwen said.

And now that "all this digital information on the ship" is in one place using eLogBook, that data can be fed into algorithms that tell the sailors whether they are operating efficiently with the energy that they have, Mackey said — and that's where the Shipboard Energy Assessment System, or SEAS, comes into play.

SEAS consolidates information into decision aids to inform the ship's operators on energy utilization, helping ship operators conduct missions as efficiently as possible, the Navy spokesperson said.

Having a system like SEAS continuously running operational energy calculations to determine whether the ship is "operating at peak energy efficiency — and if you're not, what should we do about it?" — will help the Navy increase a ship's time "on station," meaning increasing the time between refuelings, as well as allowing the service to make "informed decisions at the edge," Mackey said.

This could prove useful if and when a ship must conduct contested logistics — a scenario where "I have to figure out how to get something from here to there in a difficult situation," MacEwen said. "Since I have a limited resource — fuel — [and] I don't have a lot of gas stations, [and] I need to go do something, if I can figure out my operating parameters around that and have it with confidence," knowing exactly "what I have and what I can perform and what I can do" rather than a rough estimate, that can save the ship from having to refuel unnecessarily.

Underway replenishment is a risky mission in contested waters as the supply ship has to come up next to the vessel receiving fuel. "So, I spend an hour in my [destroyer] next to 10 million gallons of fuel driving in a straight line," MacEwen said. "If you're talking contested logistics, that's a really dangerous moment. So for the Navy, it can help them either extend the duration of that ship before they need to do a replenishment, or I can change my route. I can go pick up some gas and

then go, or from a battle group perspective, I can send a different ship to do a thing because they have more gas. So from a planning perspective, operations, safety, it kind of hits all those."

The system can also do "what-if analysis" and send out alerts, he said. For example, if "the captain says, 'All ahead full,'" — meaning to operate the engines at full speed — "but if engineering doesn't make a change on an engine to go all ahead full, you want to know that. You want to know that pretty quickly." And "because it's digital instead of paper," the system can send out an alert that notifies the sailors, "Hey, something happened here."

On shore, the Fleet Energy Conservation Dashboard "consolidates energy information across ships to inform naval planners and engineers on how energy is used across multiple ships," giving the Navy "better data analytics to optimize the energy efficiency of ship modernization and new ship designs," the service spokesperson said.

In its entirety, the GENISYS suite will help the Navy conduct and plan for distributed maritime operations — the service's new warfighting concept in which the fleet is dispersed in small detachments across a large area — the spokesperson said.

"Distributed maritime operations stress fuel logistics and supply lines," the Navy spokesperson said. "Information from GENISYS enables reduced energy demand of forward-deployed assets and provides logistics planners with higher fidelity energy data sets tied to specific mission profiles to more accurately forecast near-term energy needs."

Following the successful deployment of GENISYS on the Arleigh Burke-class ships, the Navy plans to install the system on its San Antonio-class amphibious transport docks in 2024, a service release stated. The Navy spokesperson said that while the Arleigh Burke-class and San Antonio-class ships are the only planned deployments of the system, expansion onto other platforms is possible in the future.

"GENISYS can be deployed on any platform with the proper tailoring to that platform's unique require-

ments," the spokesperson said.

In its fiscal year 2024 budget request, the Navy asked for \$9.6 million for energy management or measurement software and systems, which includes funding for GENISYS.

The investment would help fund the system's fielding and sustainment to support the Navy's digital transformation, enable distributed maritime operations and fulfill the Navy's operational energy management system requirement, according to Defense Department budget documents. The funding would also support GENISYS' transition out of the research-and-development phase, which includes shipboard installations, user training events, critical or routine maintenance requirements such as cybersecurity, and periodic updates.

So far, sailor feedback regarding GENISYS has been "generally positive, although more time and training is needed to fully understand and utilize



USS Arleigh Burke guided-missile destroyer

the capability," the Navy spokesperson said. Mackey and MacEwen said Beacon is actively participating in the installation of GENISYS in the fleet, as well as providing training.

"The whole goal of this is there's all this data on a ship. Let's use it, let's make it really, really valuable," MacEwen said. "Put it together, run a calculation, give you some knowledge. ... It's helping that [commanding officer] know what to do, when."

Mackey lauded the Navy's "Herculean effort" to get the SBIR-funded GENISYS "accredited and part of a program of record that is right now doing energy calculations and could be a basis for additional operational algorithms.

"It was non-trivial this path getting here, for them as well as for us," she said. **ND**

Partnering to Balance AI Innovation, Responsible Use

The year 2023 was notable for artificial intelligence. Scientists and engineers have been making progress on AI since the 1950s, but as ChatGPT celebrated its first birthday and “generative AI” became a mainstream term, 2023 left the world realizing how far we have come and how rapidly AI is reshaping the global landscape.

Over the past year, the AI whirlwind also highlighted the need for government and industry to work together domestically and internationally as the technology advances.

AI is a powerful tool that offers tremendous benefits to society and national security, and it is no longer just a topic of speculative discussion around the office water cooler. C-suite executives across all major industries are utilizing AI to improve their product and service offerings to consumers.

Within the defense industrial base, innovators are partnering with the government to equip warfighters with AI-enabled systems to improve the speed, quality and accuracy of decisions in the field, which can provide the decisive advantage needed to deter or win a fight.

However, there is also a growing awareness of AI’s potential risks and the negative impacts of its misuse. Along with its rapid advancement, these concerns are increasing the demand for policymakers to shift their attention to this innovative tool. Policymakers responded throughout the past year with several initiatives focused on AI development, deployment and policies across the federal government.

On Oct. 30, the Biden administration released Executive Order 14110 on “Safe, Secure and Trustworthy Development and Use of Artificial Intelligence,” which includes more than 100 specific actions across more than 50 government entities focused on the development and deployment of AI through federal agency actions, regulation of industry and engagement with international partners. Many of these regulatory actions will occur over the next two years, including at least 11 directly involving the Defense Department.

Quickly following the release of EO 14110, the Office of Management and

Budget announced a new draft policy to govern the use of AI by federal agencies. This guidance builds on previous work by the National Institute of Standards and Technology, which released a voluntary “AI Risk Management Framework” in January 2023 as a guide for industry.

That guidance also builds on work by the White House Office of Science and Technology Policy, which released the “Blueprint for an AI Bill of Rights” in late 2022, focusing on protecting individuals and communities from the potential risks of AI.

The Pentagon underscored AI’s critical role in national security with its Nov. 2 release of the “2023 Data, Analytics and Artificial Intelligence Adoption Strategy,” which builds upon and supersedes the 2018 AI Strategy and the 2020 Data Strategy. This 2023 strategy prioritizes speed of delivery, continuous learning and responsible development to leverage AI’s potential for safeguarding our national security interests globally.

Congress is also investing time



and energy in exploring AI issues. In June, Senate Majority Leader Chuck Schumer, D-N.Y., announced the “SAFE Innovation Framework,” which aims to ensure AI is developed and deployed in a responsible and transparent manner while promoting innovation and supporting the potential societal benefits of the technology. In addition to several congressional hearings and numerous legislative proposals introduced in both chambers, Schumer has hosted a series of large public forums with experts to discuss various AI topics, including intel-



lectual property, national security, workforce and privacy.

Undoubtedly, the United States is home to some of the best and brightest innovators in the world, and private industry is committed to managing the potential risks of AI as it further advances the technology. As the federal government continues to pursue proposals to both promote and regulate AI, it is essential that the administration and Congress partner with industry to ensure the proper balance of innovation and responsible use. This is especially true in the face of competitive adversaries like China, whose AI advancements underscore the imperative for the nation to sustain its technological edge.

Similar to the importance of working internationally to address many of today’s pressing national security imperatives, it is encouraging to see the United States collaborating with international allies and partners to advance a globally coordinated approach to AI.

In May 2023, AI governance and interoperability were an essential focus of the annual G7 Summit discussions, which led to the creation of the “Hiroshima AI Process Comprehensive Policy Framework.” Following the U.K. AI Safety Summit in early November, the United Kingdom and United States also unveiled the jointly developed “Guidelines for Secure AI System Development,” which 23 domestic and international cybersecurity organizations co-sealed.

It may be too soon to label 2023 as the “Year of AI,” as we will continue to see progress in 2024 and beyond.

However, in addition to the development of domestic and international regulatory frameworks, investments in AI research and development, talent cultivation and infrastructure will provide further opportunities for government and industry to partner together to advance AI technologies and help ensure the United States maintains its technological leadership to benefit our society and safeguard national security. **ND**

Michael Seeds is the National Defense Industrial Association’s senior director for strategy and policy.

NDIA BOARD OF DIRECTORS As of 12/15/23

Hon. Michael J. Bayer - Board Chair
Hon. Lisa S. Disbrow - Board Vice Chair
Maj. Gen. Arnold L. Punaro, USMC
(Ret) - Immediate Past Board Chair

Hon. David L. Norquist, President & CEO
Angela M. Ambrose

*Paul Arcangeli

Col. John Armellino, USMC (Ret)
Jeffrey W. Bohling
John A. Bonsell

*Vice Adm. Sean Buck, USN (Ret)

Rodney D. Bullard
Maj. Gen. Timothy Byers, USAF (Ret)
Dr. David Caswell
Lt. Gen. John B. Cooper, USAF (Ret)
Col. Kenny Cushing, USAFR
Paul DellaNeve

*Joe DeVooght

Dr. Tomás Díaz de la Rubia
Michael P. Dietz

*Tara Murphy Dougherty

Jaymie A. Durnan
Paula Edwards
Alan Faver
Lt. Gen. Richard P. Formica, USA (Ret)

*Ken Garber

Robert A. Geckle, Jr.

*Pete Giambastiani

Bruce Gjovig

*Will Goodman

Lt. Gen. David D. Halverson, USA (Ret)
Deirdre Hanford

*Tania Hanna

David Hathaway
Hon. Stephen C. Hedger

Lt. Gen. Thomas A. Horlander, USA (Ret)
Raanan I. Horowitz
Vice Adm. Richard W. Hunt, USN (Ret)
Gretchen Larsen Idsinga

Tamara Jack

Logan Jones

John M. Kelly

Dr. Richard "Doc" H. Klodnicki

Matthew J. Kuta

Brett B. Lambert

*Louis Lauter

Col. Anthony "Lazer" Lazarski, USAF (Ret)

Daniel A. Lerner

Maj. Gen. Lee K. Levy II, USAF (Ret)

Meagan S. Linn

Col. Armando "Mandy" Lopez, Jr.,
USA (Ret)

ML Mackey

Leigh Madden

Dr. Theresa Juneer

Laura McAleer

*Elaine McCusker

Kris McGuire

Andrew McKenna

Megan Milam

*Jamie Jones Miller

Kevin "Morty" Mortensen

Amy Motko (NTSA Nominee)

Jana Weir Murphy

Michael Niggel

Fola Ojumu

Gen. Terrence "Shags" O'Shaughnessy,
USAF (Ret)

*Michele Pearce

Brian E. Perry

Hon. Stephen W. Preston

*Marisa Rhode

Col. Reginald O. Robinson, USAF (Ret)

Betsy Schmid

*Dan Sennott

Raj Shah

Edward J. Sheehan, Jr.

Lt. Gen. Jay B. Silveria, USAF (Ret)

Robert Simmons

Kraig M. Siracuse

Mary N. Springer

Dr. J. Mitch Stevison

*Robert Stewart

Dr. Robert H. Sues

Col. Pete Trainer, USAF (Ret)

Tricia Ward (WID Nominee)

*John Wason

Maj. Gen. Martin Whelan, USAF (Ret)

Brent Wildasin

Dr. Joseph Bravman - Emeritus

Dale W. Church - Emeritus

Edward M. Fortunato - Emeritus

John D. Illgen - Emeritus

Joanna T. Lau - Emeritus

James McAleese, Jr. - Emeritus

Terrance J. McKearney - Emeritus

Hon. Michael Wynne - Emeritus

Col. William Glenn Yarborough, Jr., USA
(Ret) - Emeritus

Harold L. Yoh III - Emeritus

***Welcome new members!**

Look for National Defense On Your Newsstand

Available nationally
at Barnes & Noble,
Walmart, Army &
Air Force Exchange
Service (AAFES) and
Books-A-Million



SHARE
PHOTOS
WHERE YOU FIND
THE MAGAZINE
AND TAG US ON
SOCIAL MEDIA
#NATIONALDEFENSEMAG

Facebook Twitter Instagram @NATIONALDEFENSE @NATIONALDEFENSEMAGAZINE

White House Reveals ‘Better Contracting Initiative’

Echoing the Obama administration’s Better Buying Initiative, and as a next phase in the federal government’s enterprise approach to procurement, the Biden administration announced the Better Contracting Initiative — a four-pronged initiative designed to ensure the federal government gets better, and more consistent, terms and prices when purchasing commercial goods and services, while enhancing support for small and disadvantaged businesses.

The fact sheet noted that the enterprise approach to purchasing common goods and services under the Obama administration resulted in better deals that has avoided \$90 billion in costs for taxpayers since fiscal year 2016.

The first prong addresses how the Office of Management and Budget will leverage data across federal agencies to get lower prices and better terms. Under the initiative, OMB will launch a new, centralized data man-

agement strategy and tools to allow for greater sharing of price data and information on vendors and contracts across agencies within the federal government. This sharing of information will not only result in better value solutions but will also advance equity by allowing federal procurement officials to focus their searches on information that could support decisions to use a small business set-aside, according to the fact sheet accompanying the announcement.

approach adopted under the General Services Administration Multiple Award Schedules program. The administration presumably hopes that it will drive greater savings and more pricing consistency, consonant with the type of benefits that GSA reported after implementing transactional data reporting.

The second prong addresses how GSA will negotiate common enterprise-wide software licenses. “Prices routinely vary up to 20 percent for the same software across agencies,” the fact sheet said.

Under the initiative, GSA will negotiate government-wide information technology software license agreements with a large — but unnamed — software provider. The fact sheet stated that these government-wide IT software licenses will reduce the price variance in software procurement, secure more favorable terms and conditions and save time across the federal government by obviating the need for each agency to plan, research and procure the same software solutions.

Beyond software, federal agencies will retain the ability to leverage best-in-class enterprise contracts for common goods and services, consistent with efforts that grow small business participation and supply chain diversity.

The third prong addresses how federal agencies will save money and avoid waste by getting contract requirements right the first time. Noting that each year federal agencies buy more than \$110 billion in professional services, the administration announced that OMB will issue guidance directing federal agencies to use a proven methodology to pinpoint requirements for high-priority professional services acquisitions.

“Contracts often don’t clearly reflect the agencies’ needs, resulting in expensive modifications,” the fact sheet noted. To mitigate those costs, GSA will sponsor a series of facilitated requirements development and acquisition planning workshops for service contracts with acquisition teams across the federal government. GSA will also help train government procurement personnel to facilitate similar workshops at their own agencies.

The fourth and final prong addresses how federal agencies can receive better value from sole-source and other high-risk contracts. Select civilian agencies that have significant sole-source contracting or priority programs with underperforming contracts will engage with specialized teams of cost and engineering experts to participate in interagency peer reviews to bring down what OMB describes as inflated prices.

Agencies will also be able to leverage “hybrid” contracts for appropriate acquisitions. “Hybrid” contracts allow for multiple types of payment — cost-reimbursement, labor-hour, fixed-price — to better align with levels of risk during different parts of the lifecycle of a large acquisition for development and production.

The fact sheet cited efforts by the Defense Department to institute “peer reviews where independent procurement teams review terms to deliver a second opinion and leveraging special teams of cost and engineering experts like the Navy ‘Price Fighters’ to reduce the risk of inflated prices” as examples of strategies that have reduced costs.

Expert pricing advice offered during peer reviews helped the Defense Department realize cost avoidance of nearly \$300 million with an investment of just less than \$2 million in fiscal years 2020 through 2023, the fact sheet stated.

As a result of the Better Contracting Initiative, the Biden administration estimates that the federal government will generate more than \$10 billion in annual savings and cost avoidance while improving the performance of federal procurement contracts. The fact sheet noted that last year, the federal government purchased \$700 billion of goods and services.

As with many such initiatives, whether those expectations are realistic will depend upon the accuracy of the administration’s assumptions, details of the initiative’s implementation and the marketplace’s responses. **ND**

Chanda Brown is an associate, Susan Cassidy is a partner and Robert Huffman is a senior of counsel in the Washington, D.C., office of Covington & Burling LLP.



NTSA Honors Adm. Robb, Modeling, Simulation Awardees

The late retired Rear Adm. James Robb received the Lifetime of Service Award at the Interservice/Industry Training, Simulation and Education Conference in Orlando.

Robb's "exceptional expertise impacted the direction of [the] National Training and Simulation Association, including increased emphasis on gaming, cybersecurity, artificial intelligence, advanced integrated live/virtual and constructive architectures and big data," the association said.

Robb passed away in November.

A keystone achievement during his presidency was the continued expansion of the NTSA scholarship program. At I/ITSEC 2023, the association awarded \$180,000 to six Bachelor's degree, nine Master's degree and 10 Ph.D. scholars.

NTSA is an affiliate of the National Defense Industrial Association.

Robb lived a lifetime of service and commitment in the Navy and in the private sector. He was a proven champion of I/ITSEC and even more so of the modeling, simulation, training and education community.

Each year, the association presents at I/ITSEC awards for out-

standing achievement in the development or application of modeling and simulations. Award nominees may come from government, industry or academia.

This year's awardees include: Dr. Susan Numrich of the Institute for Defense Analyses, recipient of the Lifetime Achievement in Modeling & Simulation Award; General Santander Police Cadet School in Colombia received the Simulation and Training International Award; Training Operations at Help Me See Inc. received the Simulation and Training Award; the Gladiator Delivery Team at the U.K. Royal Air Force Capability Delivery received the Training Systems Acquisition Award; and the Dynamic Altitude Breathing Threats Research and Development Team at the Naval Air Warfare Center Training Systems Division and Naval Survival Training Institute received the Education and Human Performance Award.



Receiving the Lifetime of Service award on behalf of Adm. James Robb are Rear Adm. (Ret.) Fred Lewis, Courtney Chapman (daughter), Judy Robb (wife), Kendall Valenzuela (daughter), Debbie Langelier, Allison Lewis and Justin Robb (son).

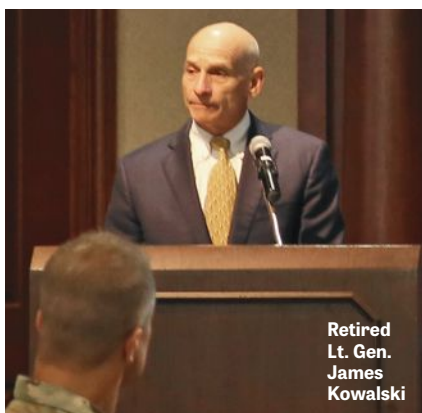
NTSA at the conference also announced its inaugural Top 10 Under 40 awardees for this year. These awardees are being recognized for significant impact to the modeling, simulation and training community via their leadership, professionalism and volunteerism.

The 10 awardees are: David Ellsworth and Matthew Hackett, both of the Army Combat Capabilities Development Command; Jeremy Joseph, Bluedrop USA Inc.; Thomas Kehr, CESI; Anastacia MacAllister, General Atomics Aeronautical Systems Inc.; Jennifer McArdle, CAE USA; Douglas Orellana, ManTech International; Evan Oster, Aptima Inc.; Navy Lt. Tiffany Peterson, Special Operations Command and Arorae Corp.; and Summer Rebensky, Aptima Inc. **ND**

Red River Chapter Inaugurates Award

N DIA's Red River Regional Chapter honored James Kowalski with the first Lt. Gen. Edgar S. Harris, Jr. Award.

This is the inaugural Harris Award, which will be presented annually to local community leaders in the defense industry and academia that have significantly contrib-



uted to the development and sustainability of Barksdale Air Force Base and the defense industry in Northwest Louisiana.

Kowalski retired from the Air Force in 2015 after serving as the commander of Air Force Global Strike Command and deputy commander of U.S. Strategic Command. He later worked at Northrop Grumman, where he

was vice president and corporate lead executive for strategic programs.

Kowalski in his acceptance speech highlighted the importance of the command and the base in the current geopolitical climate, saying that Northwest Louisiana is "at the nexus between the rise of aggressive nuclear-armed adversaries and the Air Force major command responsible for two-thirds of the nuclear force needed to deter them." **ND**

NDIA **NDIA MEMBERSHIP:** The National Defense Industrial Association (NDIA) is the premier association representing all facets of the defense and technology

industrial base and serving all military services. For more information please call our membership department at 703-522-1820 or visit us on the web at NDIA.org/Membership

NDIA CALENDAR

February

6-7 38th Annual National Logistics Forum

Oklahoma City, OK

NDIA.org/Logistics38

12 Congressional M&S Leadership Summit 2024

Norfolk, VA

NTSA.org

26-28 2024 Tactical Wheeled Vehicles Conference

Charlotte, NC

NDIA.org/TWV24



FOR THE LATEST
NDIA CALENDAR:
NDIA.ORG/EVENTS

March

4-7 Pacific Operational Science & Technology (POST) Conference

Honolulu, HI

NDIA.org/POST

13-14 2024 IPMD Meeting and Program Management Tools & Services Forum

Tucson, AZ

NDIA.org/IPMDSpring24

18-20 Undersea Warfare Spring Conference

San Diego, CA

NDIA.org/USWSpring24

19-21 2024 Munitions Executive Summit

Parsippany, NJ

NDIA.org/MES

21-22 2024 Human Systems Conference

Arlington, VA

NDIA.org/HS24

April

3 Dwight D. Eisenhower Award Dinner

Arlington, VA

NDIA.org

9-11 IT²EC 2024

ExCeL, London

itec.co.uk

16-17 Ronald Reagan Missile Defense Conference

Washington, DC

NDIA.org/RRMDC

HOSTED BY:



2024 Department of the Air Force Modeling and Simulation Summit

TRAINING IN A DIGITAL WORLD

This year's theme, *Training in a Digital World*, highlights the Department of the Air Force's drive to upskill personnel through digital training. The goal of the M&S Summit is to gather Air Force and Space Force M&S experts to learn about new M&S initiatives and techniques, network across military services and with industry experts, and to hear our technological leaders' perspectives on how M&S can transition more training from the real world to digital.

The 2024 DAF M&S Summit will provide a forum for shared information, ideas, and connection of M&S professionals across the DoD, industry, academia, and international partners. The three-day summit agenda includes: Eminent Keynote Speakers from Military, Government, and Industry Leaders | Distinguished Panel Discussions and Q&A sessions | Track Session Presentation Focus Areas | VIP Tour for Distinguished Visitors | M&S Industry Exhibition Hall | Classified M&S Briefing Sessions | M&S Tool Overview.

Save the Date!

7 – 9 May 2024 | San Antonio, TX | DAFMSS.org

ORGANIZED BY: **NTSA**



2024 Pacific Operational Science & Technology (POST) Conference

Posturing for Tomorrow - Partnered / Positioned / Prepared

Join NDIA and the U.S. Indo-Pacific Command as we examine the theme *Posturing for Tomorrow - Partnered / Positioned / Prepared*. This groundbreaking event promises to deliver an unparalleled platform for collaboration, innovation, and exploration of Department of Defense (DoD) opportunities for joint research, development, and experimentation. Experience workshops that will push the boundaries of knowledge and foster new ideas, network with renowned industry names, and visit more than 50 industry companies showcasing their cutting-edge technologies and services in the exhibit hall. POST 2024 is not to be missed! This is your chance to be at the forefront of operational science and technology, to collaborate with the industry's finest, and to shape the future of this dynamic field!

Registration Now Open!

March 4 – 7, 2024 | Honolulu, HI | [NDIA.org/POST](https://ndia.org/POST)

38TH ANNUAL NATIONAL **LOGISTICS** FORUM

NDIA

Register Today!

Prepare yourself and your organization for the challenging future of contested logistics and network with leaders and innovators at the 38th Annual National Logistics Forum! For more than three decades, this national event has brought together senior leaders, defense officials, industry acquisition, coalition partners, and logistics and financial leaders to exchange ideas and share insights into the supportability of our nation's warfighters. Attendees will tackle issues and challenges facing the logistics community and learn about the innovations and initiatives designed to address them. Don't miss this opportunity to engage with other logistics professionals and senior leaders!

February 6 – 7, 2024 | Oklahoma City, OK | [NDIA.org/Logistics38](https://ndia.org/Logistics38)

2024 **TACTICAL** **WHEELED VEHICLES** CONFERENCE

NDIA

Register Today!

Contested Logistics: Sustaining the Formation

This extraordinary conference is recognized industry wide as the premier event focused on the tactical wheeled vehicle industry and its support to the Department of Defense and our nation's warfighters. This event brings together leaders from the DoD, the military services, industry, prime contractors, subcontractors, suppliers, and academia to address present and future tactical wheeled vehicle requirements. The conference provides a unique atmosphere for open discussion between participants on the needs of the military users.

February 26 – 28, 2024 | Charlotte, NC | [NDIA.org/TWV24](https://ndia.org/TWV24)

2024 HUMAN SYSTEMS CONFERENCE

NDIA

Register Today!

This year's Human Systems conference will feature conversations related to implementation of Human Systems Integration (HSI) within existing defense platforms, as well as an activity designed to help designers and acquisition managers keep pace with the evolving role of the human in order to meet user needs and minimize lifecycle costs. In addition to this discourse, we will hear from industry, government, and academic partners about ongoing HSI work and how the evolving role of the human leads to new dynamics between warfighters and the systems they use.

March 21 – 22, 2024 | Arlington, VA | [NDIA.org/HS24](https://ndia.org/HS24)



DLA SUPPLY CHAIN ALLIANCE CONFERENCE & EXHIBITION

NDIA

Save the Date!

Next year's conference promises to be one of the best, with government and industry leaders focusing on future logistics support strategies, challenges, and streamlining efforts to better support the warfighter. Join us as we host dynamic speakers from industry and defense with backgrounds in logistics and acquisition, aviation, and land and maritime. No matter if you are a small business looking to begin a working relationship with DLA or an established large business that wants to strengthen the relationship you have already developed, we look forward to your participation at this event!

April 23 – 24, 2024 | Columbus, OH | [NDIA.org/DLA24](https://ndia.org/DLA24)



CO-HOSTED BY
DLA Land and Maritime

NEXT MONTH

Electric Vehicles

Despite significant technological challenges, both the Marine Corps and the Army are pursuing ways to make hybrid/electric tactical vehicles a battlefield reality with support from the Defense Innovation Unit. In this new electric vehicle “space race,” which service will be the first to field an electric tactical vehicle?

Army Truck

The Army this year will begin evaluation of prototypes for its Common Tactical Truck program. *National Defense* catches up with service officials and the industry competitors to learn more about how this new family of vehicles will support the Army’s shift to multi-domain operations.

Artillery

Combat operations in Ukraine have served to spotlight the significant contributions of modern field artillery systems. A number of recent Army programs have focused



on enhancing those contributions and capabilities in the future.

Navy’s MQ-25 Stingray

Entry into service of the Navy’s MQ-25 Stingray — the “pathfinder” capability for future hybrid manned-unmanned carrier air wings — has slipped from 2024 to late 2026. Pentagon reports cite inadequate testing and evaluation prior to production decisions, questions about its unit cost

and analysts’ assertions that further investments are needed now for it to be effective in contested environments.

Navy Acquisition Priorities

The Navy is focusing on its digital transformation and modernizing current infrastructure and information readiness. China poses a technology pacing threat, and strategic deterrence is still the priority.

Air Force KC-135 Recap

The Air Force plans to announce an acquisition strategy this fall for its KC-135 recapitalization program, either making additional purchases of Boeing’s KC-46 or a version of Airbus’ A330 MRTT. Practical and political considerations will impact which tanker is chosen, but the program’s biggest challenge is accurately identifying how many aircraft to purchase.

CJADC2

The Pentagon’s vision for linking sensors and shooters through a cloud and using AI to speed up decision-making — known as Combined Joint All-Domain Command and Control — faces a lot of pitfalls before a capability can be fielded. Service leaders sound off on a few of them.

Stock illustration

INDEX OF ADVERTISERS Interact with the companies whose products and services are advertised in National Defense

ADVERTISER	INTERACT	PAGE NO.
Booz Allen	BoozAllen/Defense	21
Coalfire Federal	CoalFireFederal.com	Back cover
Darley Defense	darley.com	17
Liberty Source PBC	liberty-source.com	Inside front cover
RAVE Computer	rave.com	Inside back cover
Synopsys	Synopsys.com/A&G	3
True Blue Power	truebluepowerusa.com/GETSTARTED	23

National DEFENSE

NDIA'S BUSINESS & TECHNOLOGY MAGAZINE

NDIA

For information on advertising in National Defense or one of NDIA's electronic offerings contact:

ADVERTISING

SVP, MEETINGS, DIVISIONS & PARTNERSHIPS
Christine M. Klein
(703) 247-2593
CKlein@NDIA.org

SALES DIRECTOR
Kathleen Kenney
(703) 247-2576
KKenney@NDIA.org

ACCOUNT EXECUTIVE
Jacob Wright
(703) 247-2568
JWright@NDIA.org

NDIA MEMBERSHIP: The National Defense Industrial Association (NDIA) is the premier association representing all facets of the defense and technology industrial base and serving all military services. For more information please call our membership department at 703-522-1820 or visit us on the web at NDIA.org/Membership

WE'VE GOT THE COMPUTE POWER

RAVE Computer provides purpose-built, optimized compute that delivers unparalleled performance to power your most demanding training and simulation equipment and environments.



INTRODUCING the Enterprise Power Bundle, featuring the Varjo XR-4 headset and the RenderBEAST™, RAVE's whisper-quiet compact workstation optimized and Varjo-certified for reliable, immersive excellence.

RAVE's Enterprise Power Bundle includes options for Varjo's Enterprise licensing, and NVIDIA's RTX™ 6000 Ada GPU with NVIDIA Omniverse™ Platform Enterprise license. Additional bundled peripherals include USB monitor and keyboard all packaged into a single-person-lift wheeled Pelican case with handle for your immersive training needs.

RAVE has a significant stock of XR-4s ready to ship and offers corporate XR-4 demonstrations in our RenderBEAST Demo Zone. Schedule a visit today at sales@rave.com



VALUE-ADDED RESELLER OF THE YEAR 2022
NORTH AMERICA



RAVE Computer

"RAVE's RenderBEAST line of computers unleashes the full potential of NVIDIA RTX GPUs, harnessing their power for unparalleled performance excellence."

- Kevin Berce, NVIDIA Senior Director Public Sector Software

"When launching the XR-3 and XR-4, Varjo chose RAVE's RenderBEAST for the best possible experience. An investment in better hardware can make up for a multitude of software sins."

- John Burwell, Varjo Global Head of Simulation and Training



Coalfire Federal CMMC Services

GET CERTIFICATION READY



Experienced. Accurate.

As an authorized C3PAO and a Department of Defense contractor also subject to CMMC requirements, Coalfire Federal is uniquely qualified, and armed with first-hand experience, to help you ensure CMMC certification success on the first attempt.

Protect the mission.



CMMC Advisory Services

INCLUDING:

CUI Boundary Analysis
CMMC Gap Analysis
Remediation Support

[LEARN MORE](#)

coalfirefederal.com/cmmc/advisory



CoalfireFederal.com
info@coalfirefederal.com

COALFIRE
FEDERAL