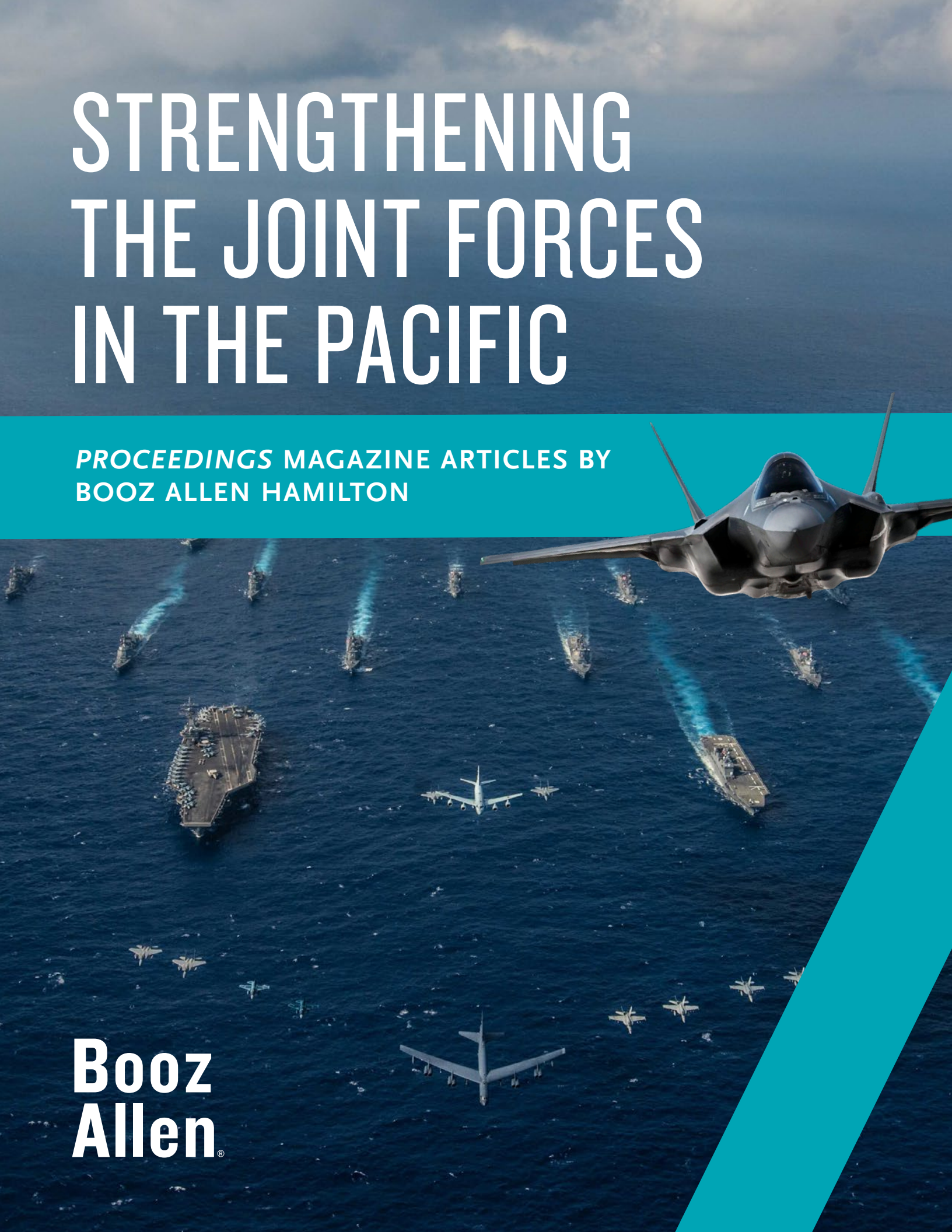


# STRENGTHENING THE JOINT FORCES IN THE PACIFIC

*PROCEEDINGS* MAGAZINE ARTICLES BY  
BOOZ ALLEN HAMILTON

**Booz  
Allen®**





**ON THE COVER:** The aircraft carrier USS Ronald Reagan (CVN 76), left, and the Japan Maritime Self-Defense Force helicopter destroyer JS Hyuga (DDH 181), right, sail in formation with 16 other ships from the U.S. Navy and the Japan Maritime Self-Defense Force as aircraft from the U.S. Air Force and Japan Air Self-Defense Force fly overhead in formation during Keen Sword 2019. Keen Sword 2019 is a joint, bilateral field-training exercise involving U.S. military and JMSDF personnel, designed to increase combat readiness and interoperability of the Japan-U.S. alliance. (U.S. Navy photo by Mass Communication Specialist 2nd Class Kaila V. Peters)

The appearance of U.S. Department of Defense (DOD) visual information does not imply or constitute DOD endorsement.



# INTRODUCTION

We are pleased to present this collection of articles, by Booz Allen authors, that were originally published in the U.S. Naval Institute's *Proceedings* magazine. In these articles, former Navy leaders and advanced technology experts at Booz Allen offer new approaches to some of the most difficult challenges facing the joint forces in the Pacific.

We are grateful for the opportunity to share our insights and expertise in critical priorities such as contested logistics, AI, allies and partners, space, unmanned autonomy, and accelerated readiness.

In addition, we offer our thanks to retired Adm. James Stavridis, who has generously reviewed these articles and offered his perspective.

Respectfully,

Jennie Brooks  
*Executive Vice President*  
*Booz Allen Hamilton*  
*brooks\_jennie@bah.com*

Rex Jordan  
*Senior Vice President*  
*Booz Allen Hamilton*  
*jordan\_rex@bah.com*







# CONTENTS

## NEW SOLUTIONS FOR SPACE & ACCELERATED READINESS

- How Satellite Swarms Can Take Down Hypersonics ..... 6
- Using Large Language Models to Protect Satellites from Attack ..... 8
- How Well is an Officer Handling the Pressure of Battle? Wearables May Be Able to Tell..... 10
- Training for Shipboard Emergencies as a Pier Service ..... 12

## AI FOR THE PACING THREAT

- Enhancing Counter-C5ISR Operations with AI ..... 16
- Quantum Sensing for PNT in GPS-Denied Environments ..... 18
- How AI Can Help the Joint Forces with Persistent Targeting..... 20
- Making Sense of Conflicting Sensor Data with AI Fusion ..... 22

## STAYING IN THE FIGHT WITH CONTESTED LOGISTICS

- Overcoming Shattered Supply Chains with AI..... 26
- The Power of AI-Enabled Predictive Maintenance..... 28
- AI-Enabled Predictive Maintenance in Contested Environments..... 30
- Protecting Navy Port Supply Operations from Cyber Attacks ..... 32


## BUILDING A UNIFIED FORCE IN THE PACIFIC

- Strengthening JADC2 in the Pacific with Line-of-Sight Communications ..... 36
- Integrating Allies and Partners with Digital OPLANs ..... 38
- How “AI Agents” Can Integrate Allies and Partners..... 40
- Protecting Missions from Cyber Attack with Real-Time Risk Maps ..... 42

## KEYS TO UNMANNED AUTONOMY IN THE PACIFIC

- Why We Need “Brain-Inspired AI” for True Unmanned Autonomy..... 46
- Protecting Classified Algorithms in Unmanned Systems in the Pacific ..... 48
- Making Digital Engineering for Unmanned Systems More Open ..... 50
- Keeping Unmanned Agile with AR/VR Training ..... 52

- AFTERWORD..... 55

The background is a deep blue space filled with numerous small, multi-colored stars. A large, solid teal shape, resembling a stylized '7' or a large arrow pointing towards the bottom right, is positioned on the right side of the image. The text is in a bold, white, sans-serif font, stacked in four lines.

# **NEW SOLUTIONS FOR SPACE & ACCELERATED READINESS**





# HOW SATELLITE SWARMS CAN TAKE DOWN HYPERSONICS

By Lt. Gen. Trey Obering, U.S. Air Force (Ret.) and Vito Partipilo

An adversary launches hypersonic missiles at a carrier group in the Pacific. Booster rockets carry the warheads—hypersonic glide vehicles—to the edge of space. But before the boosters can release their payloads, they are suddenly attacked by a swarm of small satellites. The satellites smash into the boosters, destroying them.

The technology needed for such a defense against hypersonic missiles is now available, and it is cost-effective. By leveraging dramatic cost reductions in space launch, as well as a range of technologies currently used in commercial endeavors—from Starlink to Uber—the joint forces have new opportunities to reduce the hypersonic threat. And satellite swarms can also be a powerful defense against conventional ballistic missiles.

## HITTING HYPERSONICS AT THE EDGE OF SPACE

The Defense Department is improving its ability to intercept hypersonics in the glide phase, using both conventional and hypersonic missiles. But that remains an extremely complex task, given the glide vehicles' speed—more than a mile a second—as well as their formidable maneuverability and low flight paths.

The idea behind swarms of small satellites is to destroy hypersonic missiles when they're most vulnerable—when they're in the boost phase, on a predictable trajectory like a conventional



missile, and are easier to detect and track. Although it's difficult for land- and sea-based defensive weapons to get to the booster rockets before they release their warheads, swarms of small satellites are in a much better position to intercept them. The satellites can track the hypersonic missiles from the time they're launched, and can be there when the boosters reach the edge of space. The same approach can be used to intercept an adversary's conventional ballistic missiles throughout most of their trajectories.

## HOW THE SWARMS WORK

A swarm might have thousands of small satellites in low-earth orbit, at the edge of space, something that SpaceX's Starlink constellation has shown to be both technologically and economically feasible. There are now about 5,000 small Starlink satellites in low-earth orbit, and SpaceX has received government approval to increase that number to 12,000.

The satellites in the DoD swarm would connect with each other through an "internet in space," a network backbone created by another set of satellites. With this approach, all of the satellites in the swarm have the same information, so that if one satellite spots a missile launch, they all see it. It's similar to the way Uber works. Each Uber driver serves as a node in a network, providing information to help create a common operating picture.

Another advantage of the swarm's network is that it is largely protected against jamming. While an adversary might be able to jam a handful of the small satellites, that would have no effect on the overall network. This is another way that the swarm is similar to Uber's peer-to-peer network: if an Uber driver accepts a rider and then drops out, the system automatically looks for another driver. In this sense, the swarm's network is self-healing.



## ADVANCED AUTONOMY

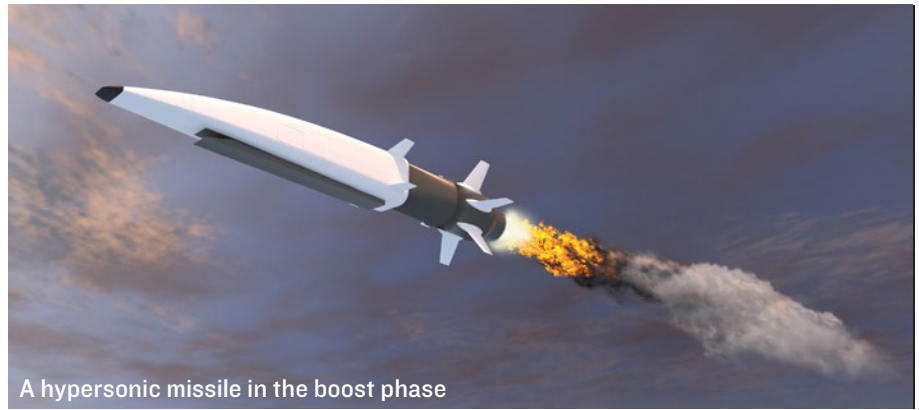
With the DoD swarm, the network backbone would allow the small satellites to coordinate their efforts autonomously, with the help of AI. For example, if the swarm spots 20 booster rockets, the satellites would decide among themselves which satellites will try to intercept which boosters. They might take a shotgun approach, with five or ten satellites, for example, trying to hit each booster. Once one of the satellites succeeds, the others rejoin the swarm, ready to go after other boosters.

The satellites can also aid land- and sea-based defensive systems. While much of the swarm might be intercepting boosters, other satellites might use lasers to illuminate glide vehicles that make it through.

The artificial intelligence that can provide the small satellites with these and other advanced autonomous capabilities is currently available. And in fact, those capabilities are akin to the ones that will help unmanned surface, undersea and aerial vehicles achieve their own autonomous missions.

## COST-EFFECTIVE DETERRENCE

One challenge facing swarms is that, in the booster phase, hypersonic missiles look the same as conventional ballistic missiles. So, the satellites would have to go after every missile—they can't wait to see which ones are carrying hypersonic glide vehicles. This means that if an adversary launches hundreds of missiles—both



A hypersonic missile in the boost phase

ISTOCK

conventional and hypersonic—the swarm may be unlikely to get them all. However, the adversary would not know which of its missiles will get through and which ones will be destroyed, potentially leaving open a huge response capability. In this way, satellite swarms can act as a deterrent.

As SpaceX has demonstrated with its Starlink constellation, putting thousands of small satellites into orbit is cost-effective. One reason is that multiple small satellites can be part of a launch, which accounts for a major portion of the cost a satellite. The swarm's small satellites are also less costly to build, operate and maintain.

Hypersonic missiles pose a new kind of threat, requiring new kinds of defenses. One such defense is a satellite swarm that targets the hypersonics where they are most vulnerable—at the edge of space.

### LT. GEN. TREY OBERING

obering\_trey@bah.com,  
is a Senior Executive Advisor at Booz Allen, specializing in space and missile defense. He is the former Director of the Missile Defense Agency.

### VITO PARTIPILO

partipilo\_vito@bah.com,  
is a senior lead technologist at Booz Allen specializing in space missile defense architecture modeling and simulation. He is a chief engineer supporting the Space Sensing Command at Los Angeles Air Force Base.



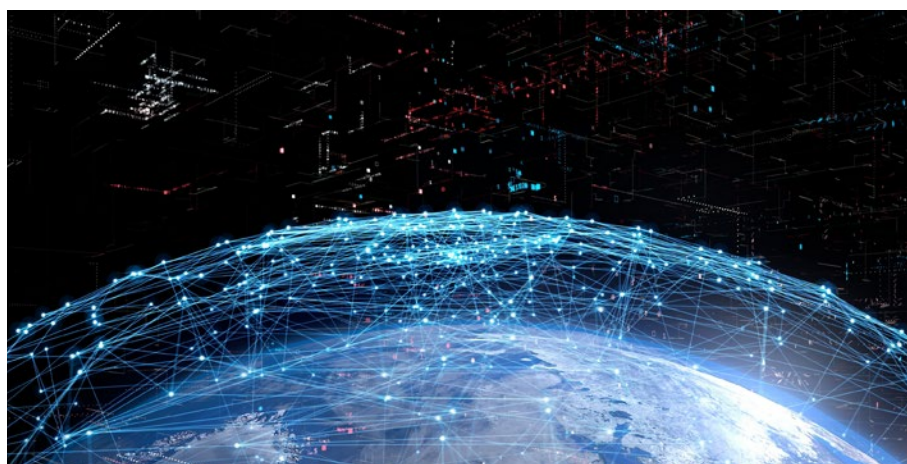
# USING LARGE LANGUAGE MODELS TO PROTECT SATELLITES FROM ATTACK

By Lt. Gen. Trey Obering, U.S. Air Force (Ret.) and Collin Paran

War has broken out in the Pacific, and our adversaries are using everything in their arsenal to disrupt our satellite communications and surveillance—to strike us blind. They’re trying to jam the signals between our satellites and ground stations. They’re trying to hijack the satellites, by sending commands that seem to be coming from our ground stations, but are actually coming from their own. They’re aiming missiles and lasers at the satellites, and even using their own satellites to take ours out of commission.

Ideally, our satellites would be able to think for themselves, so they could detect and defend against such attacks almost instantly, without waiting for operators at ground stations to analyze the threats and then determine possible courses of action. Having such a “brain” on board each satellite would be particularly valuable in the coming years, when there may be mesh networks of thousands of small DoD satellites—far too many for ground stations to fully monitor.

Defense organizations may soon have the ability to equip their satellites with this level of intelligence. Large language models, a form of generative AI, can develop a contextual understanding of a situation and—mimicking the human brain—make sophisticated inferences and suggest a complex set of actions.



ISTOCK

## ONBOARD INTELLIGENCE

For example, based on an awareness that war has broken out, or may be about to, a large language model might infer that certain seemingly innocent radio signals actually indicate a probable attack. The model might then execute the defensive measures it has determined have the highest probability of success, taking into consideration not just the adversary’s capabilities, but also how other satellites in the network are currently faring against similar attacks.

And it would do all this without needing to rely on ground stations to detect and analyze the signals, recognize the threat, and then work out how best to respond. It is important to note that any actions suggested by large language models would be constrained by humans through guardrails, based on mission context.

Attacks on satellites—whether by cyber, missile, laser or an enemy satellite—can happen so quickly that instructions from ground stations may not arrive in time. A satellite with a large language model doesn’t have to wait for instructions from a cybersecurity expert on the ground, for example. The large language model on the satellite *is* the cybersecurity expert.

In a sense, a large language model would be like having a team of human operators on each satellite, performing a number of specialized actions at once—such as analyzing data on an attack, formulating a response, and communicating with other satellites in the network.

And a large language model’s response to an attack can be highly sophisticated. For example, if an adversary fires a ground-based missile at a satellite, the model on the satellite might quickly figure out how to outmaneuver it.



Or, a model might recognize that an enemy satellite is moving into a position that suggests it is about to attack. The model could then determine the best defensive measures—even anticipating how the enemy satellite might respond to those actions, and plotting out moves to outwit it, like a chess game.

## SOPHISTICATED COLLABORATION

With mesh networks, satellites connect with each other through an “internet in space,” and can communicate even if signals from the ground are disrupted. It’s similar to the way Uber works. Each Uber driver serves as a node in a network, providing information to help create a common operating picture. And what one satellite sees, they all see.

If a satellite in the network were attacked, its large language model could not only determine the best defense, it could pass that information along to all of the other satellites. For example, say an adversary jams the ground signals going to a group of satellites. Large language models on those satellites might detect the attack and quickly switch communications to different frequencies, with each model choosing the frequency it predicts will work best.

If a satellite finds a successful frequency, it can communicate that to the others in the immediate group under attack—as well as to the thousands of other satellites in the network. If one of the other satellites picks a bad frequency, and is cut off from the ground, it can communicate that to the group as well. The large language models in a mesh network combine what they’ve learned to figure out what works and what doesn’t, as teams of human operators would. With each attack, the network of large language models get smarter about defense.

Just as important, the large language models in the mesh network would work together for the greater good—that is, taking defensive actions not just to protect themselves, but to make sure the satellite constellation as a whole is doing what it needs to do.

BOOZALLEN.COM/DEFENSE



This might even mean that some satellites would sacrifice themselves—moving into the path of incoming missiles, for example—to protect the larger network.

## AWARENESS OF CONTEXT

One of the strengths of large language models, compared to conventional AI, is that they have a much greater ability to understand context. Say, for example, a model learns that the network is under attack from an adversary, and then gets commands from the ground that don’t reflect the conflict, such as an order to observe a region far from the war zone. The model might then take steps to determine whether it is being hacked—it could, for example, query other satellites about whether they are getting the same commands. It might also alert operators at the ground station of the possibility of an insider threat.

Having hundreds or thousands of large language models in a network would help make sure any single model stays accurate and on task. If a model went rogue, so to speak, or was compromised by an adversary, the other models in the network would likely recognize that it was deviating from the group—and possibly quarantine it. They might designate another satellite to take over its role, and perhaps recommend that ground control shut it down.

It would be no more difficult or expensive to equip satellites with large language models than with conventional forms of AI. Large language models are offering new opportunities for defense organizations in a variety of applications—including in protecting satellite communications and surveillance from crippling attacks.

### LT. GEN TREY OBERING

obering\_trey@bah.com

is a Senior Executive Advisor at Booz Allen, specializing in space and missile defense. He is the former Director of the Missile Defense Agency.

### COLLIN PARAN

paran\_philip@bah.com

is an AI architect at Booz Allen who builds large language models for a variety of applications for the Space Force, Navy, Army and Air Force.

*Booz Allen subject-matter experts Evan Montgomery-Recht, Timothy Snipes and Karis Courey contributed to this article.*



# HOW WELL IS AN OFFICER HANDLING THE PRESSURE OF BATTLE? WEARABLES MAY BE ABLE TO TELL

By Irik Johnson and Commander Alan Kolackovsky, U.S. Navy (Retired)

What if, during a battle at sea, the commanding officer on a ship could tell whether a key officer, such as the TAO, is crumbling under stress—and may start making bad decisions—based on that officer’s heart rate, blood pressure, galvanic skin response and other stress measures?

While wearable devices are commonly used to improve performance in sports, the joint forces may soon have the opportunity to use wearables—along with AI—to determine whether officers and others are both mentally and physically sharp in critical situations.

Because this information can be presented to the commanding officer on a laptop, he or she could, from anywhere on a ship, tell whether the CIC watch officer, for example, was in danger of making a serious mental error in battle, and perhaps would need to be quickly replaced.

Wearable data and AI can aid in peacetime as well, helping to make sure officers can stay focused on preventing potential disasters, such as collisions, fires, flooding, and man overboard—and can quickly make the right decisions if such a situation occurs.

## HOW WEARABLES MEASURE STRESS

The latest wearable devices—including watches, chest straps, rings, headbands and earpieces—can generate a host of metrics to show a person’s stress levels. For example, some devices measure a person’s heart rate variability—the time between each heartbeat—which fluctuates during the day. Heart rate



U.S. NAVY (CHRISTOPHER SYPERT)

variability can show whether a person’s nervous system is in fight-or-flight mode, which indicates stress, or is leaning more toward recovery and healing.

Other devices estimate stress levels by measuring galvanic skin response, which can indicate when sweat glands are triggered by emotions—even in small ways we may not be aware of. These and other metrics, such as resting heart rate and blood pressure, are combined to create a full picture of how well a person is coping with stress.

## THE ROLE OF TRAINING

The key question, of course, is not whether a person is stressed—which could be the case with anyone in battle—but whether the stress is interfering with his or her ability to perform mission tasks, and could lead to poor decisions. There are several steps to determining this.

It begins during training. Outfitted with wearables, officers and others go through various drills that mimic battle conditions. As trainers add stressors—such as unpredictable complications and increased tempo—they can monitor how well individuals perform as their stress levels increase.

Data from the wearables might indicate, for example, that individuals experiencing heightened stress have slower reaction times, or less working memory, or perhaps mental tunnel vision, in which they’re focusing on a single threat or goal without seeing the larger picture. All these can lead to poor decisions.

This approach has another benefit, helping to pinpoint whether a person is making mistakes because of stress, or because he or she needs more training. This might be revealed, for example, when an individual is making mistakes during training, but is showing no signs of increased stress.

## BRINGING IN AI

By correlating stress levels and decision-making during intense training, defense organizations can begin to predict how well an individual will perform in real-world conditions. But training alone can't tell the whole story—it is unlikely to show whether a person can perform every possible mission task at every possible stress level. This is where AI comes in.

Machine learning, a form of AI, has the ability to find patterns in large datasets. The first step is to use machine learning to find patterns in how well an individual performed different tasks at various stress levels during training. Next, defense organizations can bring together the data from large numbers of people who were monitored for stress during training—and look for those individuals who showed the same patterns. With enough such individuals, most if not all possible combinations of stress levels and mission tasks will likely be covered. This provides a greater ability to predict how well an individual will perform a particular task at a particular stress level—even if he or she was not in that exact situation during training.

## WEARABLES IN BATTLE

Here's how this might apply in an actual battle: An officer of the deck, for example, is outfitted with wearables. Data from the wearables show that the officer's stress levels are skyrocketing. Based on the training data from the officer as well as the relevant individuals in the larger group, a machine learning model might predict that the officer can still handle some critical mission tasks, but is at risk of making serious mistakes with one or two others.

At the same time, the machine learning model can track how an officer's ability to perform a task is rapidly changing as his stress is increasing. For example, the data might show that a few minutes ago, the officer was doing fine, but now his decision-making ability is suddenly deteriorating.

Such information—on key officers throughout the ship—can be conveyed instantly to the commanding officer



ADOBE STOCK

and the executive officer through dashboards on their laptops or tablets, enabling them to take timely action.

The information can also be sent to the officers themselves, so that they can try to bring down their stress levels through techniques they learned during training. An officer might do some quick deep-breathing exercises, for example, or he might recall a time when he performed well in a high-stress training situation—giving him confidence he can do it now.

While the technology for such an approach is currently available, several obstacles would need to be overcome to make it feasible. For example, policies would need to be changed to allow TAOs and other officers to use wearables in secure spaces. Infrastructure changes would be needed as well, such as sensors that would enable data to be transmitted across decks and compartments. Ships would also need edge computing with AI to collect and analyze the data.

With this approach, data from wearables is kept private and secure—it is deidentified until it reaches the commanding officer or other authorized person. That way, if the data is intercepted, it can't be connected with a specific individual.

In addition to its use in wartime, data from wearables can also be valuable in peacetime situations where there is little stress. Data can show, for example, whether officers or others aren't getting enough regular sleep, or aren't drinking enough water, or for other reasons may not be mentally sharp and might make mistakes that could endanger the ship or its crew.

### IRIK JOHNSON

johnson\_irik@bah.com, integrates wearable technologies, data science and virtual reality to improve training and performance for Booz Allen's DoD clients. As an expert on sports science, he has optimized athletic programs for the NFL, NBA and MLB.

### COMMANDER ALAN KOLACKOVSKY

kolackovsky\_alan@bah.com, is a retired Naval Limited Duty Officer, whose assignments included Executive Officer NIWC PAC. He leads Booz Allen's 5G/CBRS infrastructure deployment, delivering emerging technical solutions including unmanned systems capabilities.

*Booz Allen subject matter experts Commander Jarrod (JRod) Groves, U.S. Navy (Retired) and Maggie Corry contributed to this article.*



# TRAINING FOR SHIPBOARD EMERGENCIES AS A PIER SERVICE

By Commander Eric Billies, U.S. Navy (Ret.), Maj. Nick Zimmer, U.S. Army (Ret.), and Fire Control Technician Chief Petty Officer Joe Reck, U.S. Navy (Ret.)

## FIRE

*A near-aboard torpedo explosion starts fires and flooding in a Virginia-class submarine operating at periscope depth. In the auxiliary machinery room, the CO<sub>2</sub> scrubber is in flames, spewing thick black smoke. Nearby sailors hit the cutoff switch and then quickly strap oxygen tanks on their backs and spray fire extinguishers, putting out the electrical fire. But the blaze has spread to the lagging, and it's moving quickly.*

The sailors unreel a hose, pull back the bail on the nozzle to test the water flow, and then advance on the fire. They feel the hot wind from the flames, and smell the acrid smoke. The sound of the fire, echoing in the small room, is deafening. The sailors struggle to control their emotions, and do the job they were trained to do.

All this is taking place inside a 40-foot shipping container on a pier next to the sailors' actual submarine. The sailors are wearing headsets that are creating a virtual-reality machinery room on fire. The cutoff switch, oxygen tanks, fire extinguishers, hose and nozzle are all physical props that the sailors can manipulate. The hot wind they feel is created with heat lamps and fans, and the smell of smoke is artificial. The roaring sound of the fire is in their headsets.

Only the sailors' emotions are real.

This is a type of "mixed reality," combining VR images and physical



ILLUSTRATION GENERATED BY AI

props that users can "see" in their headsets and actually touch. Because it is a multi-user environment, sailors can physically work together, and learn from each other, as they train.

Recent advances in immersive technologies—which create simulated environments that users can participate in—are helping to make this kind of training both feasible and cost-effective for the joint forces.

Mixed reality does not replace school-house training. Rather, it gives sailors and others the opportunity to increase their training "reps and sets" in a realistic environment that can essentially be a portable pier service. The shipping containers can be placed on a pier next to a submarine or a ship, with the props inside the container configured to the individual vessel—and any number of training scenarios.

## FLOOD

*The torpedo explosion has damaged the submarine's seawater flanges, and the water pressure from an intake valve has cracked a 10-inch pipe in the forward lower level of the engine room. Water is spewing from the pipe, quickly flooding the room. Sailors activate the flood-control switch, but that system has been damaged as well.*

The sailors grab a flooding repair patch kit and gloves. With water spraying in their faces, they press the patch to the pipe, just off the rupture, and hold it down with a chain and chain wrench. Fighting the intense water pressure, they roll the patch over the rupture, and then quickly apply the strapping and ratchet it down with a bandit kit.

All this is taking place in another part of the shipping container. Once again,

the sailors are wearing headsets, maneuvering in a simulated, VR-created environment with props. The gloves and tools in the patch kit are real, and the cracked pipe is made of real metal—though the water rushing from it is created by VR. Intense air pressure in the pipe simulates the water pressure, making it difficult for the sailors to apply the patch. Small nozzles spraying mist and compressed air give the sailors the feel of water on their faces. Thanks to an advanced immersive technology known as “pass-through,” the sailors can actually see their gloved hands, the pipe, patch and tools, in the simulated scene.

Also once again, the intense sensory environment—and the physical struggle to get the patch on the pipe quickly—is triggering the sailors’ emotions. For some, the stress is making them less efficient, and more prone to the kinds of mistakes that can slow things down.

One of the advantages of mixed reality training is that sailors can go through the drill again and again, learning how to control their emotions and remain calm as they work quickly. In addition, sailors can be equipped with wearable devices, such as watches or chest straps, that measure stress. Data from the wearables might indicate, for example, that sailors who are experiencing heightened stress have slower reaction times, or less working memory, or perhaps mental tunnel vision, in which they’re focusing on a single threat or goal without seeing the larger picture. When sailors are wearing oxygen tanks, devices can tell whether the sailors are so stressed they’re using up their oxygen too fast, taking them out of the fight.

The information can be sent to trainers, and also to the sailors themselves—in real time—so they can try to bring down their stress levels through various techniques, improving their efficiency and conserving their oxygen. For example, sailors might do some quick deep-breathing exercises, or might recall times when they performed well in other high-stress training situations—giving them confidence they can do it now.

BOOZALLEN.COM/DEFENSE



ILLUSTRATION GENERATED BY AI

## SUBMARINE ESCAPE

*Despite the efforts of the sailors, fire and flooding are spreading throughout the submarine.* The captain gives the order to abandon ship. Sailors move quickly to the logistics escape trunk and don their submarine escape immersion equipment (SEIE). The first three sailors climb in the escape trunk and the hatch is sealed. It’s pitch black, so they crack open chem lights.

In the half-darkness, they turn the valves that let seawater in up to their waists, and then—amid the deafening sound of rushing water, and water splashing in their faces making it hard to see—they turn other valves that equalize the pressure inside the chamber and outside the submarine so the escape hatch can be opened. The high stress and sensory deprivation are almost overwhelming. But the sailors must work fast, and they can’t make even a minor mistake in lining up the valves—otherwise, they may disable the escape trunk not only for themselves, but for the 125 other sailors on the sub waiting for their chance to survive.

This scene is taking place in still another part of the shipping container on the pier. The escape trunk is a mock-up of a real one, with the valves as props, and the sailors’ headsets providing VR images of the rising water, the darkness, and the increasingly obscured vision.

Then the training exercise is over, and another set of sailors enter the shipping container. The next day, the submarine heads back out to sea, and the shipping container is moved to another pier, where the props—and the VR scene—are reconfigured for another submarine, and another crew.

## COMMANDER ERIC BILLIES

(billies\_eric@bah.com), is a retired surface warfare officer who leads Booz Allen’s business in the Pacific Northwest helping DoD clients chart innovative approaches to immersive (VR/AR/XR) training.

## MAJ. NICK ZIMMER

(zimmer\_nicholas@bah.com) is a retired Army infantry officer and Green Beret NCO who has led Booz Allen’s Seattle Immersive Studio, developing immersive training solutions for DoD clients.

## FIRE CONTROL TECHNICIAN CHIEF PETTY OFFICER JOE RECK

(reck\_joseph@bah.com), is a retired Navy chief who spent 24 years on submarines and was a master training specialist. As a senior lead engineer at Booz Allen, he helps develop innovative immersive training solutions for Navy clients.





# AI FOR THE PACING THREAT





# ENHANCING COUNTER-C5ISR OPERATIONS WITH AI

By Commander R. Scott Oliver, U.S. Navy (Retired), Commander Alan Kolackovsky, U.S. Navy (Retired), and Carl Jacquet

One of the challenges of counter-C5ISR operations is the difficulty in getting a full picture of the electro-magnetic environment. Individual sensors provide only slivers of that environment, and the data is often hard to integrate. At the same time, analysts looking at that data often focus only on the radar, radio and other signals that they already know about. Much of how potential adversaries are using the electromagnetic environment—to track our forces, for example, or to execute their command-and-control—often remains unknown.

However, advances in data integration, AI, predictive analytics and other areas of data science are now giving the joint forces the opportunity to gain a much more comprehensive view of our potential adversaries' C5ISR. By bringing together and analyzing all the available electromagnetic data—rather than just looking at portions of it in pockets—we can begin to see larger patterns, and more possible attack surfaces, in our adversaries' C5ISR. There are fewer unknown unknowns, and more paths to counter-C5ISR activities.

## INTEGRATING A WEALTH OF C5ISR DATA

Although the joint forces are already collecting much of the data they need to get that more complete picture, it is difficult to bring that data together for analysis. Data is often stored in stove-piped databases, or in formats that other organizations can't easily



access. In addition, organizations may be reluctant to share their data out of security concerns.

With new approaches to machine learning—a form of AI—as well as other analytics, the joint forces can get a far more comprehensive understanding of the electromagnetic environment. But analytics, no matter how advanced, don't reach their full power in limited datasets. They need large amounts of data to find overarching patterns and identify critical anomalies. If you're looking for a needle in a haystack, you need a haystack.

Fortunately, it is now possible for the joint forces to bring together and analyze the full range of data they are now collecting—and to do it securely. This can be done through a hybrid approach to data integration, using both an enterprise-wide data lake, and localized AI on ships, submarines and ground stations. With the data lake, the joint forces can store an almost unlimited amount of data on a network of computers and in the cloud. The data lake can seamlessly

accept data from any source, and in any format, and make it available for analysis by AI and other analytics.

One of the strengths of the data lake is that it is far more secure than conventional methods of storage. As each piece of data is ingested into the data lake, it is tagged with its “visibility,” governing who has access to the data and under what circumstances. This means that individuals and organizations can only see the portion of the data in the data lake that they're authorized to view. While the insights generated by AI and other analytics may be used by decision-makers across organizations, the underlying data remains protected.

The second part of the hybrid approach calls for localized AI, for example machine-learning models on ships and submarines. The data lake's insights into adversaries' C5ISR are downloaded onto the machine-learning models. If vessels are at EMCON or otherwise cut off from accessing the data lake through the cloud, they can use the machine-learning models to

process data coming in from sensors, taking advantage of the data lake's knowledge base.

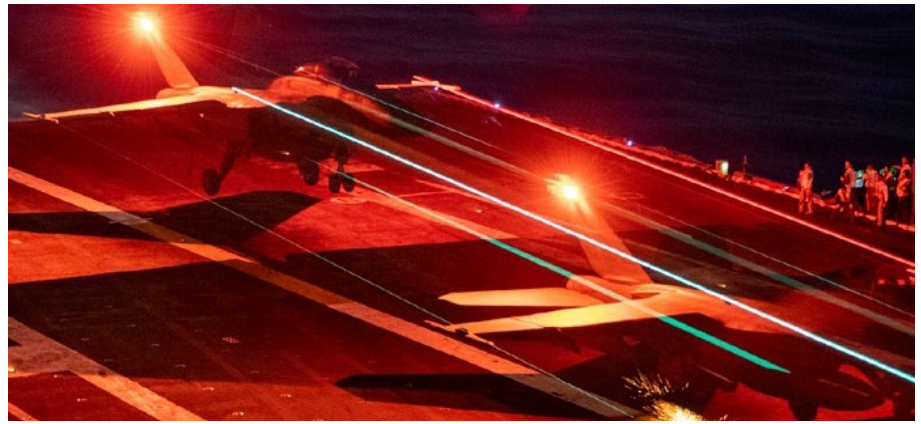
Once the ships and submarines are connected back to the data lake, they can upload the new insights they've gained. Those insights become part of the data lake, and are then shared back to the localized machine-learning models across the fleet. The hybrid approach—the data lake combined with on-board machine-learning models—makes it possible for the joint forces to maintain a rich, continuously updated picture of adversaries' C5ISR activities, even in communications-denied environments.

### **FINDING PATTERNS AND ANOMALIES**

Once all the data is brought together in the data lake, the AI starts doing its work. It begins by finding “patterns of life” in the electromagnetic environment—the normal radio, radar and other signals that are consistently seen day-to-day by sensors. In looking for patterns, the AI can also factor in data from numerous other sources, ranging from known military training routes (both friend and foe), to commercial communications to local weather conditions (which can affect signal behavior).

In the next step, the AI looks for anomalies in the data—signals or other electromagnetic activity that don't fit into the normal patterns, things that, in a sense, shouldn't be there. These anomalies can hold crucial clues to the unknown unknowns in adversaries' C5ISR.

For example, if a group of Navy ships is moving through an area, onboard sensors may detect sudden and unexpected electromagnetic activity from what was thought to be a nearby fishing trawler, transmitted on frequencies that analysts never thought to look at. At the same time, other sensors might detect equally sudden and unexpected signals coming from an island several hundred miles away, perhaps followed by signals from other locations. Even without knowing the content of the signals, the AI can begin to map out



an adversary's C5ISR network nodes—for example by identifying the primary and subordinate organizations, along with command-and-control paths. Anomalies may also provide early indications of an adversary's tactical and strategic moves.

### **LEARNING HOW ADVERSARIES REACT TO COUNTER C5ISR**

Because the AI is looking at the entire electromagnetic environment, it can also see how adversaries respond to our counter-C5ISR efforts, for example as they switch frequencies or modes of communication. Predictive analytics can take this a step further, by anticipating which of those actions an adversary is most likely to take in a given situation, based on how the adversary has responded in the past. This knowledge gives the joint forces a greater ability to monitor an adversary's communications across frequencies and modes, as the adversary seeks to evade our counter C5ISR.

A more comprehensive picture of the electromagnetic environment also provides a better understanding of how our forces appear to adversaries' C5ISR, by showing how we may be emitting signals we're not aware of.

An AI-enabled data lake, along with localized machine learning models and other data science approaches, give the joint forces the opportunity to leverage the vast amounts of electromagnetic data they are currently collecting. When brought together, these technologies can significantly strengthen our ability to conduct counter-C5ISR operations, including in contested environments.

### **COMMANDER R. SCOTT “SHERM” OLIVER**

oliver\_robert@bah.com  
a retired EA-18G Growler Naval Flight Officer whose assignments included the Joint Staff J8 and the SecDef's Electromagnetic Spectrum Operations Cross-Functional Team, leads numerous Booz Allen projects focusing on EM spectrum superiority.

### **COMMANDER ALAN KOLACKOVSKY**

kolackovsky\_alan@bah.com  
a retired Naval Limited Duty Officer, whose assignments included Executive Officer NIWC PAC, leads Booz Allen's 5G/CBRS infrastructure deployment, delivering emerging technical solutions including unmanned systems capabilities.

### **CARL JACQUET**

jacquet\_carl@bah.com  
a Senior Intelligence Planner with Booz Allen, served 26 years in the Army, supporting 7 JTFs as a planner and a simulation expert. He provides intelligence planning and analysis on major contingency plans in support of U.S. Army Pacific.



# QUANTUM SENSING FOR PNT IN GPS-DENIED ENVIRONMENTS

By Jake Farinholt

In the event of a conflict or confrontation, the joint and allied force could lose access to satellite capabilities, most notably GPS. Ships, submarines, and aircraft would need to rely almost entirely on other technologies for positioning, navigation and timing (PNT), particularly inertial systems.

Unfortunately, because inertial navigation devices such as gyroscopes and accelerometers lose accuracy over time—and wouldn't be able to be recalibrated in a GPS-denied environment—inertial navigation would be reliable for only a limited period.

But an emerging technology, quantum sensing, offers the possibility of increasing the accuracy of inertial navigation by orders of magnitude, greatly extending operational availability in GPS-denied environments.

The idea behind quantum sensing is fairly straightforward. Essentially, quantum refers to the realm that exists at the atomic and sub-atomic level. That realm is extremely sensitive to minute changes in the environment—changes that cannot be detected in the everyday world. Quantum sensing harnesses that sensitivity, allowing measurements that are far more precise than what is possible through conventional approaches.

Although using quantum for inertial navigation is a technology of the future, that future may not be far away. Quantum sensing is already used in atomic clocks—including in



ISTOCK

military satellites—and in devices such as MRI machines. Government and private researchers are making rapid advances in quantum sensing for inertial navigation, and some devices may be ready for deployment by the military in as little as five years, according to the NATO Review.

For that to happen, however, defense organizations need to take steps now to make sure that the quantum gyroscopes and other devices being developed are practical for current and future ships, submarines, and airplanes. Quantum sensing devices typically require a great deal of size, weight, and power, and researchers are now focusing on ways to make them work for the Navy and other services.

It's important that defense organizations develop deep expertise in quantum sensing, and take the lead in driving the requirements, so that the quantum devices can be deployed as

soon as possible. China is now aggressively pursuing quantum sensing for inertial navigation, and could leave the U.S. behind.

## HOW QUANTUM SENSING WORKS

The behavior of atoms, particles of light, and other denizens of the quantum realm can reveal a great deal about what is happening in the larger physical world. For example, when a cloud of atoms inside a vacuum is in an excited state, the atoms become highly sensitive to the gravitational field around them. By looking at the patterns the atoms form, quantum devices can create a picture of the gravitational field around a ship or submarine. With repeated readings as the ship moves, that picture becomes increasingly detailed. Onboard computers can then overlay the picture with maps of Earth's gravitational field to determine the ship's precise location.

An entirely different type of quantum sensing can measure the surrounding magnetic field, also helping to plot a ship's location. With a quantum magnetometer, a tiny wire made of special materials is made so cold that it has virtually no electrical resistance. This eliminates “noise” on the wire, so that when an electrical charge is sent through it, the wire becomes highly sensitive to the magnetic field at the atomic level. The device takes a series of measurements to determine the surrounding magnetic field, which can then be compared to magnetic field maps of the world.

Additional types of quantum sensing can aid other aspects of inertial navigation. A quantum gyroscope, for example, uses the wave nature of atoms to measure angular rotation. An atomic clock sets its watch by the predictable rate that excited atoms decay. A quantum accelerometer measures the movement of supercooled atoms.

What all these quantum devices have in common is that they are self-contained and completely independent of GPS or other outside communications. In addition, because measurements in the quantum realm are far more accurate than with conventional approaches, quantum inertial navigation can be relied upon for much longer periods.

## MOVING FROM THE LAB TO THE REAL WORLD

While quantum sensing devices have been proven to work, with the exception of atomic clocks they are generally too large to be of practical use for inertial navigation. For example, the refrigerators needed to supercool the wires in quantum magnetometers can take up a great deal of space—and what works in a laboratory may not fit on a submarine. In the lab, some optics-based quantum sensors feature a collection of mirrors, glass plates, lasers, and various electronics that sit on a platform the size of a dining room table.

Much of the research now being done on quantum sensing, including in



DoD laboratories such as the U.S. Naval Research Laboratory, is focused on how to make the devices small enough to fit on ships, submarines, and airplanes without a significant drop-off in accuracy and precision.

A key challenge is that it's often difficult to determine how well a smaller and lighter device, with reduced power requirements, will perform until it has been built. In addition, each type of quantum sensing device has its own complex set of trade spaces. Manufacturers may have to experiment with a number of prototypes to get the right balance of size and performance. This process might in some cases be too costly to be feasible—and too time-consuming for the DoD to keep pace with adversaries in the race for quantum sensing.

One solution is for defense organizations to use modeling and simulation to test how particular quantum devices would work in the real world. This can be done by building models based on research data. Many research papers have been published describing different approaches to quantum sensing devices, and this information—along with data from various prototypes that have been built so far—can be used to build the models.

By continuing to play a major role in the ongoing research—including with modeling and simulation—the joint force can gain the information and expertise needed to drive the requirements for quantum sensing, rather than relying entirely on industry. Such an approach can significantly speed the adoption of quantum sensing for inertial navigation, helping to extend operational availability in GPS-denied environments.

## DR. JAKE FARINHOLT

(farinholt\_jacob@bah.com)

is a senior lead scientist at Booz Allen, where he leads the firm's overall quantum sensing business in the national security sector, as well as the firmwide quantum sensing business. For more than a decade, he has provided expertise in quantum technologies to the intelligence community, as well as to the Navy and other defense organizations.



# HOW AI CAN HELP THE JOINT FORCES WITH PERSISTENT TARGETING

By Lt. Gen. Chris Bogdan, U.S. Air Force (Ret.) and Patrick Biltgen, Ph.D.

One of the thorniest challenges in the Indo-Pacific is persistent targeting—how can the joint forces keep track of a constantly changing array of often fast-moving targets, over vast open spaces, against adversaries adept at hiding what they’re doing? How can you make sure you’re always matching up the right sensors with the right targets, and at exactly the right times, so you can maintain custody on critical targets with the needed handoff from one sensor to the next?

These are complicated problems that require rapidly bringing together and analyzing, in real time, a growing ocean of information on both targets and sensors—something that is becoming increasingly difficult using conventional manual approaches. However, those are just the kinds of problems that artificial intelligence solutions are well suited to handle. With advances in machine learning and other forms of AI, the joint force now has the tools and opportunity to make an exponential leap in persistent targeting in the Indo-Pacific and elsewhere.

## **GAINING SITUATIONAL AWARENESS**

Establishing and improving situational awareness through the use of AI starts with a robust capability to gather, store and process large amounts of data. Fortunately, today there are data platforms that can securely bring together the full range



of data that the joint force collects on targets and sensors. These platforms can seamlessly accept data from any source, and in any format, and make it fully available to AI and other data fusion and analytic applications.

The application of trained AI models on these large sets of data can then result in rapid target identification, factoring in current or last known locations, as well other target characteristics. These models can also correlate other sensor information about a target, such as patterns in the electromagnetic, acoustic and IR signatures.

## **PREDICTING TARGET PATHS**

Properly trained AI models also can predict where targets are likely to go, so operators can optimize potential sensor-to-sensor handoffs to maintain persistent targeting and help commanders maneuver their forces

in advance of adversary action. The AI models do this by analyzing historical data on the adversary targets and actions, looking for behaviors and patterns, such as where those targets have gone in the past in particular circumstances. For example, when there’s a certain combination of adversary aircraft flying in a “package”—such as two tankers, four bombers and six fighters—what kinds of missions did such a group execute in the past and what flight path did they tend to take? How have such patterns been changed in the past by our responses, and by other factors, such as the weather?

The power of AI comes from its ability to combine vast amounts of historical data with the current context from any number of sources, such as intelligence, political developments, and weather. This can then provide commanders with likely paths for targets of interest and

assign confidence and probability values to the different potential target movements.

### PREDICTING SENSOR ACCURACY

AI solutions can also identify which available sensors are best suited to maintain target custody, and can continuously perform sensor-target pairings, at machine speed, with automated handoffs—across large geographies with multiple targets and multiple sensors. For example, based on the historical data, which types of sensors have been most successful in tracking targets with certain characteristics? Which sensors are most accurate in a particular combination of environmental factors? AI models, for example, can account for water depth, sound-velocity profiles and arrival path in tracking a submarine, and also factor in the sensor's position relative to the target. Such AI solutions can then help optimize the sensor-target pairing, ensuring the right sensor is on the right target and the right time.

AI also can look many moves ahead, to identify the best sensors—not just for the upcoming handoff, but for the next handoff and the next ones after that. As the targets move, AI models can continually update “best-sensor-to-use” calculations, in the same way that a smartphone map application continually reconfigures for the fastest route. The ability to project a complex target-tracking scenario five, ten or twenty moves ahead at machine speed can provide commanders with a huge information edge in a rapidly unfolding scenario.

### PRIORITIZING AND ORCHESTRATING THE SENSORS

It's not uncommon that a particular sensor is needed for two different targets at the same time. How does the commander decide? Here again AI can help. It starts by evaluating the targets themselves and ingesting the commander's target prioritization

and the likelihood of the loss of target custody. For example, a commander may prioritize a highly accurate sensor for a high-priority target. But if the custody of that high-priority target can be assured with a different sensor for a short period of time, then the highly accurate sensor could potentially be re-tasked and then returned to the high priority target without any mission degradation. That would free up the more accurate sensor to provide information on a target that might otherwise be difficult to acquire.

The promise of AI is that it can sort out much of this complexity in real time to maintain persistent targeting and custody on multiple targets in an ever-changing environment. AI solutions can also deal with changing commander priorities, changing environmental factors, sensor degradation, and adversary counteractions all at machine speed—delivering the commander a synchronized battlespace-awareness plan optimized for both sensor and targets.

These AI solutions also learn over time. As they get “smarter,” they can better sort out which combinations of sensors are most effective at tracking which targets and under which conditions. As models incorporate more data and the results of human decision-making across many different scenarios, they will also improve anomaly detection, target path prediction, and synchronized sensor-target pairing.

### STAYING AHEAD OF ADVERSARIES

As the battlespace in the Indo-Pacific and other areas of interest becomes increasingly complex and crowded, and as adversaries get more skillful at hiding their intentions, persistent targeting will only get more difficult. Integrating AI solutions into today's operations can give the joint forces a strategic edge.



**LT. GEN. CHRIS BOGDAN**  
bogdan\_christopher@bah.com

is a Booz Allen senior vice president who leads the firm's aerospace business, delivering solutions to DoD, NASA, and commercial clients. As a 34-year U.S. Air Force officer and test pilot, he flew more than 30 different aircraft types and was the Program Executive Officer for the F-35 Joint Strike Fighter Program for the Air Force, U.S. Navy, U.S. Marine Corps, and 11 allied nations.

**PATRICK BILTGEN, PH.D.**  
biltgen\_patrick@bah.com  
is the director of AI mission engineering at Booz Allen, leading data analytics and AI development for space and intelligence programs. He is the author of *Activity-Based Intelligence: Principles and Applications*, and recipient of the 2018 Intelligence and National Security Alliance (INSA) Edwin Land Industry Award.



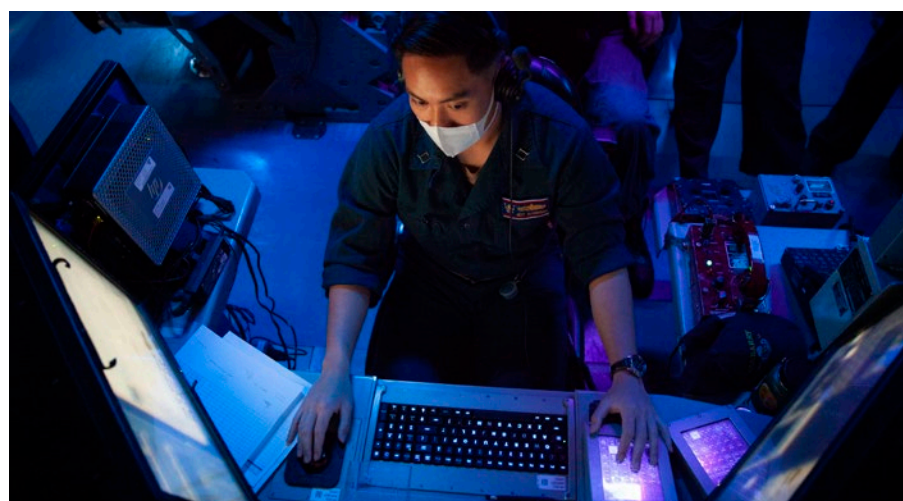
# MAKING SENSE OF CONFLICTING SENSOR DATA WITH AI FUSION

By Adam Weiner

In the coming years the Navy will gain access to a rapidly growing profusion of sensors, not just through new fleets of unmanned vehicles combined with existing systems, but through multi-service sensors as well, as part of a joint operating environment. If the Navy is to maintain dominance in the INDOPACOM AOR, it must be able to extract maximum insight from those sensor assets.

One of the key challenges in gaining that insight is resolving the inconsistencies that frequently arise when multiple sensors are looking at the same contact. Different sensors often have their own inherent strengths and weaknesses. One sonar sensor might have more precise bearing resolution on a contact, for example, allowing for a better targeting solution. But a different sonar sensor might have better narrowband frequency information, making contact classification more accurate. The greater the number of sensors, the more valuable data is available—but also the greater number of differences in the data, and the more noise that operators have to sort out to make the best identification.

Machine learning and other forms of artificial intelligence will aid this process, but they also contribute to the problem themselves. In many cases there will be multiple algorithms looking at the same stream of sensor data, each making its own prediction of classification, location track, and mission intent—all based on the



algorithm's particular strengths and weaknesses. It may not be easy to reconcile their differences.

One advantage of machine learning is its ability to present a confidence value, or score, that a commander can use in decision-making. For example, machine learning algorithms—based on data from multiple surface and undersea sensors—might say that there is a 99.99 percent chance the contact is a manmade object, a 95 percent chance the contact is a Chinese submarine, and an 85 percent chance the contact is a Han Class SSN. But how do you know if the conclusion is reliable if there is so much variability between the sensors, and between the algorithms themselves?

The Navy can address this challenge by using AI in another way. The AI fuses the algorithms that process the

sensor data (algorithm fusion), and then fuses that result with the results of other sensors using non-linear models such as deep neural networks (sensor-data fusion). The AI then refines that result with a third layer (context fusion), which brings together and analyzes additional Navy datasets for contact identification.

The result of this multi-layer, AI-enabled fusion is a far more accurate score for the commander—and one that can rapidly bring together a large number of sensors from manned and unmanned systems, significantly shortening the time to decision-making and action.

The three-step process works in a particular order—first algorithm fusion, then sensor fusion, then context fusion. Each step is critical to the final score.

## ALGORITHM FUSION

Machine learning algorithms identify objects by looking for patterns in historical and current data, and then finding those same patterns in real-world situations. As the Navy rolls out machine learning for sensor data, there will likely be multiple algorithms for each radar, sonar or other sensor stream. This gives the AI more ways to detect, classify and analyze a contact, but it also adds complexity—each algorithm will generate its own and possibly different confidence score for the contact information.

Algorithm fusion addresses this complexity through ensemble learning approaches that produce a single, overarching score. It doesn't do this by averaging the algorithms' scores. Rather, it uses a dynamic weighting scheme applied to each score, based partly on how well the algorithm has performed historically in similar situations. For example, there may be five algorithms looking at the same sonar data of a contact. One algorithm might have proved more accurate at identifying submarines based on the particular frequencies the contact is emitting. Another algorithm might be more accurate at the particular angle on the bow that the sensor has with the contact. A third algorithm might be more accurate in the particular combination of environmental factors such as water depth, sound-velocity profile, and arrival path.

The weighting is also based on mission and domain knowledge that has been programmed into the fusion process. In the example, this weighting takes into consideration the relative importance of all relevant factors in making an identification.

The fusion process doesn't throw out any of the algorithms, but instead identifies the strengths of each one in the current situation, and then brings those strengths together to produce the single confidence score. Fusion uses all the available algorithms to full advantage.

## SENSOR-DATA FUSION

Often, multiple sensors may be looking at the same contact—radars on different manned and unmanned surface vehicles in a group, for example, or different types of sensors, such as radar and SIGINT, on the same platform. In the next phase—sensor-data fusion—the AI brings together and evaluates all the relevant data streams, to produce a more comprehensive score for the commander.

Sensor-data fusion assigns weights to each of the data streams, largely based on the quality of its data. There are a number of reasons why sensor data quality can vary. For example, one sensor might generate a lower resolution than others, based on its location. Or, the sensor might be older, and have a lower sensitivity than newer versions. Some sensors—such as those on unmanned vehicles—may have smaller optics than large, complex sensors, and so might generate less robust results. Once the AI assigns weights to the different data streams—based on their strengths and weakness—it fuses the results, refining the overarching confidence score.

## CONTEXT FUSION

In the same way that Navy operators of radar, sonar and other sensors look at the larger context of a contact to help make an identification, the AI brings in disparate data sources to refine the score. Data sources can range from known military training routes (for both friend and foe), to previous operational data collected on missions, to the seasonal migration of dolphins and whales.

The AI can bring together and analyze large numbers of relevant datasets at once—far more than an individual operator could review. The results of the context fusion may lower or raise the final confidence score for the commanding officer.

Ultimately, AI-enabled fusion squeezes more insight from the Navy's existing and growing sensor assets—resolving conflicting data and creating a clearer understanding of the INDOPACOM AOR tactical environment.



### ADAM WEINER

weiner\_adam@bah.com,  
a Vice President at Booz  
Allen, leads the firm's Navy  
Sensor Fusion, Human  
Signatures, and Navy  
Warfare Center business.



# STAYING IN THE FIGHT WITH CONTESTED LOGISTICS





# OVERCOMING SHATTERED SUPPLY CHAINS WITH AI

By Col. Boyd Miller, U.S. Marine Corps (Ret.), Ki Lee and Scott McCain

If supply chains are disrupted during a conflict in the Pacific, commanders will have to figure out—on the fly and often separate from one another—how to get logistical support through other means. However, they may not have the information they need to get that support in the fastest and most secure ways possible. And, if they tap supplies from alternative sources, they may not know how that will impact the missions originally designated for those supplies.

Deep reinforcement learning—an emerging form of AI—may soon make it possible for the joint forces to create what might be thought of as a self-healing supply web. For missions in the Pacific, for example, this web would provide commanders with a constantly updated, near-real-time operational view of supply chains, platforms, and recommended routes.

If, for example, a port in the Pacific were lost, commanders would see a revised operational view showing new locations where the replenishment could come from, and the best ways to get it to the various points of need. The supply web would also map out the cascading implications of the lost port, showing how OPLANs and missions across the Pacific would likely be affected. Dashboards would allow commanders to work together to choose among the best alternatives, based on mission priorities, rapidly changing conditions, and other factors.



## TRANSFORMING FROM SUPPLY CHAIN TO SUPPLY WEB

The supply web would be created by securely bringing together a wide range of siloed supply-chain data from across the DoD, and consolidating it in a data mesh. Advanced analytics then use that data to map out the entire supply chains for various OPLANs, operations and exercises. The data includes all the relevant ports, airfields and other supply sources, as well as the current and expected stores of fuel, munitions and other supplies at those locations. Various other aspects of the supply chains are also integrated into the supply web, such as capacity, routes, and expected demand.

The next step in creating the supply web is to bring in deep reinforcement learning, a goal-based form of AI. Deep reinforcement learning uses numerous possible scenarios—created through modeling and simulation—to learn what works and what doesn't to achieve a particular goal.

A key feature of deep reinforcement learning is that it essentially adopts the point of view of a particular entity—whether a person, a country, or for example, the joint forces and allies and partners in the Pacific—and then tries to achieve that entity's goals. With the supply web, the reinforcement learning might look at hundreds of thousands of scenarios of how a conflict in the Pacific could unfold, learning not just what will help a particular mission, but what is needed by the allied forces as a whole.

Even before logistics become contested, the supply web would serve several important functions. The supply web's AI looks at the current supply chain operational view, and evaluates numerous scenarios—far more than human planners could—to identify for commanders optimal ways to support OPLANs and missions.

When there are changes to supply chains, such as shortages or delays in moving shipments, that information is

automatically fed into the data mesh. The supply web is constantly pulsing the mesh, staying fully updated.

At the same time, the AI uses intelligence and other information to predict where supply chains are most vulnerable to disruption by adversaries, including through kinetic warfare and cyberattack. Such vulnerabilities might be hidden, and revealed only by working through many thousands of possible scenarios. This gives commanders the chance to address those vulnerabilities before a conflict—for example, by moving supplies afloat or to locations that adversaries may be less likely to attack.

### A SELF-HEALING WEB

The supply web becomes particularly valuable if supply chains are disrupted. If a replenishment ship is lost, for example, the deep reinforcement learning reconfigures—in near-real time—how supplies can get to the points of need. In this sense, the supply web is self-healing. One reason this healing happens so quickly is that the AI doesn't start from scratch—it uses what it has already learned through the hundreds of thousands of course-of-action scenarios.

In a conflict, the supply web would continuously reconfigure logistics in any number of ways. For example, a multi-day battle in the Pacific might take a carrier strike group so far afield that many of the ships would run out of missiles before the expected replenishment could reach them in time. The AI would run new scenarios—leveraging its prior learning—to work out the how supply chains could be rearranged so that the group could get the replenishment.

Currently, it is difficult for planners to get a full understanding of how multiple supply chain disruptions in a conflict might cascade across an AOR. Supplies will have to be rerouted in numerous ways, all at the same time. If a carrier gets fuel from



U.S. NAVY (GREG JOHNSON)

a new location, what does that mean for the missions that were originally meant to get that fuel?

The supply web's deep reinforcement learning would work out these implications in near-real time as the disruptions occur. And instead of reconfiguring supply chains mission by mission, it would work toward the ultimate goal—winning the war.

The supply web would not take away decision-making from commanders. Rather, it would give them more hard data to work with, and help them make faster decisions. For example, the supply web might present one alternative that will get supplies to the point of need faster, and another that will be slower but more secure. Commanders still need to use their experience and judgment to decide on the best path.

Commanders across an AOR can work together on the alternatives through common, interactive dashboards. They are able to ask questions of the data to gain more insight for decisions. And, they can add in new information for the supply web to consider, such as changing conditions, mission priorities and OPLANs.

### COL. BOYD MILLER

miller\_boyd@bah.com, is a contested logistics subject-matter expert in Booz Allen's artificial intelligence division. He has more than 30 years of experience in defense, joint, and maritime logistics operations, including as J4 Director, United States Southern Command.

### KI LEE

lee\_ki@bah.com, is Booz Allen's Global Defense Technology Officer. He drives technology innovation, application, and adoption for Booz Allen's global defense business, with a focus on supporting mission needs and gaps.

### SCOTT McCAIN

mccain\_scott@bah.com, is a veteran logistics and sustainment expert at Booz Allen who designs, develops, and implements cognitive-enhancing software solutions that enable a wide range of DoD clients to address the complex challenges of contested logistics.

*Booz Allen AI subject-matter experts Curtis Wright, Jhordan Figueroa, and Mitch Pleus contributed to this article.*



# THE POWER OF AI-ENABLED PREDICTIVE MAINTENANCE

By Captain Jeff James, U.S. Navy (Retired), Doug Hamrick and Aaron Van Blarcom

A credible Pacific deterrence posture for the U.S. Navy requires that the fleet of ships, submarines, and aircraft be available to the combatant commander at a rate that outpaces potential adversaries, in order to maintain control of strategic geographic areas and vital supply chains. A new, AI-enabled approach to predictive maintenance can help achieve this goal, and increase operational availability across the INDOPACOM AOR and elsewhere.

With this approach, AI looks for patterns in vast amounts of maintenance sensor data to predict when parts or systems might fail—and can often find potential problems long before they show up on watchstanders’ consoles. At the same time, the AI helps supply-chain personnel deliver the necessary parts and repair crews with just-in-time logistics. These two components—diagnostic and supply chain—together make up what is known as AI-enabled predictive maintenance.

One way that AI-enabled predictive maintenance helps keep Naval forces forward deployed is by lowering the risk that a key propulsion, weapon or other system will fail during operations, potentially taking the vessel or aircraft out of action. It also reduces the need to bring ships and submarines into port for lengthy planned-maintenance work.

AI-enabled predictive maintenance is not so much a revolution as an



evolution, building on the Navy’s rapid progress in sensor technologies, advanced analytics, secure satellite communications, cloud computing and a host of other areas.

## PREDICTIVE DIAGNOSTIC ENGINEERING

A key aspect of the process is predictive diagnostic engineering. Currently, sensors on propulsion, auxiliary and combat systems feed data to watchstanders’ consoles, prompting alerts whenever readings, such as engine speeds or fuel-oil temperatures, exceed safe operating limits. Predictive diagnostic engineering—which can be conducted either onboard or through a common data network—brings together and analyzes such sensor data from across the Navy. It looks not just at a fuel pump on a single ship, for example,

but at all similar fuel pumps currently or formerly in use across a ship class or fleetwide. What emerges in the data is a predictable pattern of decay—essentially, the normal lifecycle of that type of pump.

The AI then compares the data from an individual ship with the overall patterns, looking for anomalies. It may find, for example, that the decay pattern of a particular fuel pump is moving much faster than might be expected—even though the sensor readings on the consoles aren’t yet changing. The AI might also look at what happened to other fuel pumps with similarly accelerated decays, to provide an estimate of when the fuel pump in question will ultimately fail.

In addition to the maintenance-sensor data, the AI brings in contextual data to provide a higher fidelity estimate. It might look at atmospheric conditions affecting the ship, such as temperature

and humidity, and evaluate how those conditions have historically sped up or slowed down decay patterns. The AI might also consider a ship's maintenance records—factoring in, for example, repairs previously made to the fuel-oil system, and the historical impact of those repairs on similar fuel-oil systems.

## **A SECURE COMMON DATA NETWORK**

To determine the larger data patterns of parts and systems, predictive diagnostic engineering brings together data from across the Navy through a common network. Maintenance and other data is transmitted from ships, submarines and aircraft via satellite to the network, and then integrated with historic data. Thanks to advances in cybersecurity, this data transmission can be done securely, using the same protocols now in place for communications, navigation, logistics, and other types of data.

The network is designed with open frameworks and other architectures, making it vendor-agnostic and able to accept data from any of the Navy's different types of propulsion, auxiliary and combat systems. This ability to bring data together is critical, because the more maintenance data that is collected across the Navy, the more accurate the AI becomes. Data transmitted from a ship not only helps diagnose specific problems on that ship, it also adds to the larger pool of data about those systems—which in turn helps the AI to better diagnose problems on other ships.

## **JUST-IN-TIME LOGISTICS**

When the AI predicts that parts or systems are heading toward failure, it identifies what maintenance and repairs will be needed, and when. For example, by looking at the pool of data on a particular type of engine—including problems and repair histories—the AI can determine which actions, taken at which times, have proven most effective in keeping the engine operational.

Once the AI has identified a potential failure, it can help get parts—and if necessary, specialized maintenance crews—to the ship or submarine in time for repairs. The AI can look across the entire supply chain, pinpointing where the parts and maintenance crews are, when they can become available, and how they can best get to the vessel.

The AI does this by analyzing a wide range of databases related to Navy supply chains and logistics. In some cases, the AI may recommend sending the parts and crews to a forward port that the ship or submarine is expected to visit, while in more urgent cases the AI may recommend delivering the parts and crews to a certain location at sea.

By running simulations, the AI works out the logistics of getting the resources where they need to be, and at the optimal time. The AI can also put in place alternative plans if conditions change, for example if it detects that the decay pattern of a part is suddenly accelerating, or if a forward port is no longer available.

## **STRENGTHENING PACIFIC DETERRENCE**

AI-enabled predictive maintenance is not a single, overarching system, but rather a system of systems that integrates many of the advanced technologies the Navy is currently developing.

These include machine learning and other forms of AI, as well as open architectures and other technologies that make it possible to analyze large amounts of disparate data. In addition, new sensor technologies, data links, and communications networks are enabling increasingly sophisticated diagnostic engineering, and the Navy's advances in cyber and electronic warfare are making the transmission and storage of maintenance data more secure.

The Navy now has an opportunity to bring these and other capabilities together to strengthen deterrence activities in the Pacific, by increasing the operational availability of forward deployed ships, submarines and aircraft.



### **CAPTAIN JEFF JAMES**

james\_jeffrey@bah.com, a retired Surface Warfare Officer whose commands included the USS PIONEER (MCM 9), USS HOPPER (DDG 70), and Joint Base Pearl Harbor-Hickam, leads Booz Allen's infrastructure, energy, and environmental business across the PACRIM, delivering technical solutions leveraging AI and ML to Navy, Marine Corps, Air Force, and Joint clients in the region.

### **DOUG HAMRICK**

hamrick\_douglas@bah.com, leads Booz Allen's development of AI-enabled predictive maintenance and supply-chain capabilities for clients throughout the DoD and other federal agencies.

### **AARON VAN BLARCOM**

vanblarcom\_aaron@bah.com, a solution architect on Booz Allen's PACRIM analytics team in Hawaii, develops a broad range of AI and machine learning solutions for Navy clients.



# AI-ENABLED PREDICTIVE MAINTENANCE IN CONTESTED ENVIRONMENTS

By Justin Neroda, Joe Rohner, and Commander Jarrod Groves, U.S. Navy (Retired)

AI-enabled predictive maintenance can help keep the joint forces operationally available across the Indo-Pacific and elsewhere. But how well does it work in contested environments—when it may be most needed?

One of the challenges of AI—whether for predictive maintenance or for other applications, such as C5ISR systems—is that to stay accurate, it may need to be retrained with the latest data as conditions change. Such retraining, essentially a recalibration of the AI, is particularly important in contested environments, where conditions often change rapidly and unexpectedly.

Machine learning models, which use AI, are typically retrained in cloud-based networks, with powerful computers and staffs of AI engineers. But access to the cloud is not always necessary. With thoughtful preparation, the joint forces can conduct the retraining locally—such as on shipboard computers, including laptops and platforms—and without the assistance of AI experts.

## THE CHALLENGE OF AI-ENABLED PREDICTIVE MAINTENANCE

Predictive maintenance for the Navy illustrates the challenge of keeping AI accurate in contested environments and how defense organizations can overcome the obstacles. With the help of AI, predictive maintenance begins by bringing together and analyzing sensor and non-sensor data on propulsion, auxiliary, and combat systems across the Navy. The machine



learning models look not just at say, a fuel pump on a single ship, but at all similar fuel pumps currently or formerly in use across a ship class or fleet-wide. What emerges in the data is a predictable pattern of decay—essentially, the normal lifecycle of that type of pump.

The machine learning models then compare the data from an individual ship with the overall patterns, looking for anomalies. The machine learning may find, for example, that the decay pattern of a particular fuel pump is moving much faster than might be expected. By looking at what happened to other fuel pumps with similarly accelerated decays, the machine learning can provide an estimate of when the fuel pump in question may stop working properly. The advantage of AI-enabled predictive maintenance is that this entire process can play out long before the sensor readings on watchstanders' consoles begin to show any problems.

Retraining is necessary when the new data coming in from sensors is significantly different from the data the model was initially trained on—so much so that the model may no longer be able to accurately predict when maintenance will be needed. This is known as model drift. To stay accurate, the model needs to be retrained with the new data to find new, more relevant patterns.

## DESIGNING MODELS IN A NEW WAY

Retraining can be difficult, however, if machine learning models do not have access to the powerful computers in cloud-based networks. Many of the basic tasks of AI, such as pattern recognition, can still be conducted on shipboard and other local computers, though they typically have less processing power. Retraining, however, is far more computationally intense. Machine learning algorithms might run through millions of calculations to identify new patterns

of decay, a process generally requiring cloud-based computers.

However, most of those calculations are usually not needed. By stepping in and selecting only the most necessary calculations, AI developers can design models that can be efficiently retrained on less-powerful computers.

There is both an art and a science to choosing the right calculations with predictive maintenance. Developers are not just identifying which calculations are most helpful in retraining, they're also making tradeoffs between speed and accuracy. The more critical a part or system is to ensuring mission success, the more accurate a model needs to be, and so the more calculations may be required.

To do this balancing, developers need a thorough understanding not just of aircraft, ship, and submarine maintenance, but of how the parts fit into larger systems, and how those systems fit into the mission. Balancing speed and accuracy—in the context of mission—is key to designing machine learning models that can be retrained in contested environments, whether for predictive maintenance or for other applications of AI.

### **BRINGING IN AUTOMATION AND AI-READINESS**

One of the advantages of cloud-based machine learning networks is that they are often staffed with AI experts who can decide whether the data has changed so much that a model needs to be retrained. Since it's impractical to have an AI engineer aboard every ship and submarine, this decision will need to be largely automated when the model is disconnected from the cloud. AI developers can build in this capability when they design the models, by establishing thresholds that will automatically trigger a recommendation for retraining.



The actual decision of whether to retrain is made by maintenance analysts and leaders—but here again preparation is needed. AI developers can create dashboards that clearly explain the reasons for the retraining recommendation. Maintenance analysts and leaders can then use their knowledge and experience to determine whether the retraining makes sense.

The more that maintenance personnel know about AI, the better they will be able to make these kinds of decisions. While they don't need to be able to develop the AI itself, it will be helpful if they understand how AI works, and how it applies to maintaining parts and systems. As AI becomes increasingly integral to predictive maintenance, C5ISR and other applications across the joint forces, this basic AI-readiness will gain in importance.

Keeping AI accurate in contested environments can be challenging. But by designing AI specifically for those environments, and making the AI accessible to shipboard personnel, the joint forces can meet that challenge.

#### **JUSTIN NERODA**

neroda\_justin@bah.com  
is a vice president in Booz Allen's AI practice who focuses on developing integrated end-to-end AIOPs pipelines to efficiently and effectively operationalize AI for DoD and intelligence community clients.

#### **JOE ROHNER**

rohner\_joseph@bah.com  
is a director of AI in Booz Allen's Chief Technology Office who leads the delivery of AI solutions for the U.S. government, with a focus on the Department of Defense.

#### **COMMANDER JARROD**

##### **"JROD" GROVES**

groves\_jarrold@bah.com  
is a retired Naval Aviator and a vanguard member of Naval Analytics Community who leads Booz Allen in delivering analytic solutions, leveraging AI and machine learning, to Navy and Marine Corps.



# PROTECTING NAVY PORT SUPPLY OPERATIONS FROM CYBER ATTACKS

By Jandria Alexander and Gregory Buck

As large-scale cyberattacks by China and Russia on American government agencies and corporations have demonstrated, it can be difficult to prevent nation-states from planting malware on sensitive networks—even those with strict access controls. It can also be difficult to know that it has happened. Suspected Russian hackers in the SolarWinds supply-chain attack remained undetected on networks for as long as nine months before they were discovered.

This kind of vulnerability has significant implications for Navy cybersecurity, including at ports in the Pacific where replenishment ships take on supplies. One of the risks is that an adversary could plant malware on port computer systems and then activate it at a critical moment, crippling resupply operations. This might unfold, for example, if a naval confrontation between the U.S. and an adversary in the INDOPACOM AOR seemed imminent, and the Navy wanted to top off fuel, munitions and other supplies on combatant ships for maximum mobility and flexibility.

It wouldn't be necessary for the malware to infect and disable every supply-related computer system in a port—a single attack anywhere along the line could disrupt the entire resupply operation. For example, malware could disable the pumps that transfer fuel to the replenishment ships, or the cranes that load palletized munitions and other supplies.



Malware could freeze the inventory-control systems that dictate which supplies go on which ships, or it could cut the power in critical places.

Ports around the world are being increasingly targeted by hackers. Cyberattacks on the maritime industry's operational technology (OT) systems have grown by at least 900 percent over the last three years, with some port operations being knocked out for days or even weeks, according to the maritime cybersecurity company Naval Dome.

Current cybersecurity measures at Navy-controlled and commercial ports tend to focus on identity and access management, dictating who has access to which systems. While that is critical, it is not enough. Nation-states like China and Russia are increasingly adept at bypassing identity and access controls in sensitive networks—such as with last year's SolarWinds attack, which came through a routine

software update to thousands of customers, including in parts of the Pentagon and other federal agencies. China is accused of an even more massive attack on American government and business organizations this year, in which hackers exploited vulnerabilities in a Microsoft email service to plant hidden malware.

While such attacks have proven hard to prevent, the Navy can take specific steps to strengthen cybersecurity at Navy-controlled and commercial ports in the Pacific and elsewhere. There is no silver bullet, however. Defending ports against sophisticated cyberattacks calls for a multifaceted approach—one that combines traditional methods, such as redundancy and manual backups, with advanced technologies such as AI-enabled threat detection. Such an approach focuses not just on protecting the IT and OT systems in ports from malware intrusion, but keeping them resilient in the face of a successful breach.

## COMPENSATING CONTROLS

Redundancy and manual backups may seem to be obvious solutions, but such compensating controls are actually among the most challenging aspects of port cybersecurity. Navy-controlled and commercial ports typically have dozens of complex IT and OT systems. No port has the resources to fully back up every part of every system, either through redundant systems or manual processes. Some areas will inevitably have less protection than others.

The key is to identify and back up the most critical systems, so that even if a cyberattack disables some port operations, the resupply operation can continue. This calls for determining how much disruption an attack on any IT or OT system might cause, and then prioritizing resources to protect the most important systems. For example, can a backup server reside in the same rack as the primary one, or does it need to be in a different building, or even in another part of the Pacific? Does the port need an entire backup power grid, or is it sufficient just to back up certain systems?

## STRONG CYBERSECURITY HYGIENE

Cybersecurity hygiene is also critical. Currently, this tends to vary from port to port, and often does not fully consider the kind of sophisticated cyberattack that might come from a nation-state like China. To protect against such attacks, there must be regular and comprehensive penetration testing of both IT and OT systems. Such testing should focus not just on known vulnerabilities, but on architectural and system-integration weaknesses.

Other hygiene measures include frequent software updates to reduce vulnerabilities. However, software updates can take critical systems offline for extended periods, and they can have unintended effects, causing parts of systems not to work properly. Updates also carry the risk of a malware attack. So, while frequent updates are necessary, they must be done strategically, balancing benefits and risk.

The same kind of balancing should be applied to identity and access controls. The fewer people who have access to the various networks in a port, the more cybersecurity protection—but at the same time, overly strict controls could slow resupply operations to a crawl.

## AI-ENABLED THREAT DETECTION

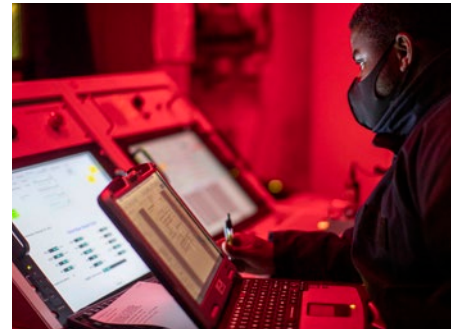
The next layer of defense is aimed at detecting malware that has been hidden on port systems, but not yet activated. Such malware is often very difficult to find—cybersecurity experts may not know where to look, or even what to look for. However, AI can hunt for second-order effects of an attack—subtle evidence that hackers are or have been active in a system.

The AI does this by finding unexpected patterns, or anomalies, in the massive data that courses through systems every day. In some cases, the AI recognizes these anomalies as known activities of cyberhackers, while in other cases, the patterns may be unfamiliar—but still suspicious. When either of these situations occur, cybersecurity experts can investigate the potential threat, and then take mitigating actions.

## STAYING RESILIENT

Despite these and other defensive measures, an adversary may still find a way to plant and activate malware on port systems. Ports need to be ready for this possibility with measures in place that will rapidly isolate and limit any damage, keeping essential resupply operations up and running. Such measures—many of them automated—range from incorporating targeted access controls and “zero-trust” architectures to taking systems offline and putting manual backup plans into action. Many of these same actions can be taken if cybersecurity experts discover significant vulnerabilities in systems that could open the door to adversaries.

Through a full awareness of the risks, and careful planning to mitigate them, the Navy can build cyber resilience into port supply operations in the Pacific and beyond.



### JANDRIA ALEXANDER

alexander\_jandria@bah.com, a nationally recognized cybersecurity expert and Booz Allen vice president, leads resilient platform systems and enterprise digital transformation strategy and solutions for Navy clients.

### GREGORY BUCK

buck\_gregory@bah.com, the coordinator of Booz Allen's Federal Threat Hunt team, is the former Deputy Chief of Staff of the Cyberspace Solarium Commission.





# **BUILDING A UNIFIED FORCE IN THE PACIFIC**







# STRENGTHENING JADC2 IN THE PACIFIC WITH LINE-OF-SIGHT COMMUNICATION

By Mike Morgan and Steven Tomita

Back in the 1990s, when the U.S. military still relied primarily on line-of-sight rather than satellites for C4ISR and other communications, the Office of Naval Research developed and tested a breakthrough approach—a self-organizing mesh network for Navy line-of-sight communications.

With this network, a ship, for example, can send radar data far beyond the horizon, using ships, planes and Navy stations in a series of line-of-sight relays. Algorithms chart the most efficient path from one line-of-sight platform to the next. Data might travel half a dozen or more “hops” before reaching its ultimate destination.

As innovative as the research was, the mesh network was never put into operation—satellite communications were quickly coming on their own in the Navy and the other services, and there was no longer a pressing demand for line-of-sight relays to go beyond the horizon.

There may be a need for such mesh network again. In the event of a conflict in the Pacific, satellite communications could be degraded or denied, undermining the effectiveness of Joint All-Domain Command and Control (JADC2). If that were to happen, the DoD would need to rely on line-of-sight networks for sensor, command-and-control, and other data. Unfortunately, current approaches to line-of-sight networks have significant limitations—such networks tend to be inefficient and unstable over long distances.



However, by bringing back the mesh relay network developed by the Navy in the 1990s—and updating it with AI and infrastructure improvements—the DoD can strengthen its ability to maintain JADC2 in a satellite-denied environment.

## CURRENT APPROACHES TO LINE OF SIGHT

One of the weaknesses of current line-of-sight networks is that they try to create a global topology, or map, that shows all the connections between various platforms, as well as the most efficient communications routes. Satellite networks can create such global topologies because every platform can “see” the satellites. However, it is much more difficult to line-of-sight networks to create fully comprehensive maps.

Line-of-sight communications must be conducted at relatively low power to avoid giving away the platforms’ locations to adversaries. But lower power means lower bandwidth, or capacity. And when line-of-sight

networks try to create a global topology, they often end up using most of the available bandwidth just maintaining the map. Each time there’s a change in connectivity—with a ship or plane moving into or out of line-of-sight—the routers and algorithms on the network’s platforms have to completely update the global topology. This intensive router-to-router traffic between platforms not only crowds out intelligence information, sometimes there’s not even enough bandwidth for the router traffic itself. This can be a particular issue for U.S. forces in the Pacific, where airborne and seaborn platforms are constantly moving in and out of sight of one another. A global topology is typically not sustainable in a frequently changing line-of-sight environment.

## ADVANTAGES OF THE MESH NETWORK

Instead of trying to create a global topology, the mesh network developed by the Navy in the 1990s uses an innovative relay system that moves data from one line-of-sight hop at a time.

Here's how it works: For example, say a UAV needs to send radar data to a number of ships, planes, and bases beyond the horizon in the Pacific. With the mesh network, the UAV and all of the platforms within its line of sight are using their routers and algorithms to communicate with one another. In essence, they're creating a highly localized network map.

It wouldn't be practical for the UAV to send its data to all of its line-of-sight neighbors—that would create too much network traffic. Instead, the UAV determines which neighbors have the most line-of-sight connections of their own and sends its data only to them. In the next step, the platforms that get the UAV's data relay it to their own line-of-sight neighbors that have the most connections. This process is repeated, from one group of line-of-sight platforms to the next, until the UAV's data reaches its ultimate destinations.

A major advantage of this approach is that data moves throughout the network with the minimum number of platform-to-platform relays. This makes the most efficient use of line-of-sight's limited bandwidth, freeing up capacity for intelligence data. And because the fewest possible platforms are relaying the data from one hop to the next, it lowers the risk of detection by adversaries. There's another benefit: Unlike line-of-sight networks that try to create global topologies, the mesh network is self-healing—it seamlessly incorporates constant changes in connectivity.

The latest advances in AI have the ability to make the mesh network far more powerful than Navy researchers envisioned in the 1990s. In particular, AI can help maximize routing and network efficiency, by determining which platforms, and which data transmissions, have the highest priority based on the operational mission and the commander's intent.

#### **BUILDING A MATURE LINE-OF-SIGHT INFRASTRUCTURE**

Mesh networks alone, however, are not enough. In order for them to operate

efficiently—even with AI—they need to be part of an infrastructure that is geared toward line-of-sight communications, not just satellites. For example, in recent years sensors have been increasingly designed to stream data through satellite communications. However, it is difficult for lower bandwidth, line-of-sight communications to manage and consume streamed data. Too much data from too many sensors will bog down a line-of-sight network.

This means that sensors will need to operate differently in a satellite degraded or denied environment—instead of streaming oceans of data, they will only be able to send the most relevant bits of information. Here again AI can help, by selecting the most relevant sensor data based on mission, evaluating network conditions, and determining how much data can be sent at a given time.

In addition, sensors will need to be specifically designed to accommodate line-of-sight communications. One example of the way this is being done now: With some small UAVs, the resolution on the cameras is intentionally lower, and the frame rates are intentionally slower, so that the video can be processed more easily through line-of-sight communications.

A line-of-sight infrastructure also calls for changes to the routers and algorithms that communicate with one another to form a mesh network. The DoD now largely relies on commercial, proprietary routers and algorithms that are specifically designed for global topologies. With open operating systems and other open approaches, the DoD can develop routers and algorithms tailored to line-of-sight communications.

U.S. forces in the Pacific may someday need to transition from satellite to line-of-sight communications in order to maintain JADC2. By leveraging the mesh relay network the Navy developed in the 1990s, updating it with the latest AI, and developing a mature line-of-sight communications infrastructure, the DoD can help meet that challenge.



#### **MIKE MORGAN**

morgan\_mike@bah.com  
is a principal at Booz Allen who leads the firm's NAVAIR line of business. He has over 20 years of experience supporting NAVAIR programs with a focus on systems development and cybersecurity for unmanned systems and C4ISR solutions.

#### **STEVE TOMITA**

tomita\_steven@bah.com  
is a principal and director of technology and digital engineering at Booz Allen, where he has been driving innovation and capability delivery to the Navy and DoD for 20 years.



# INTEGRATING ALLIES AND PARTNERS WITH DIGITAL OPLANs

By Maj. Gen. David Clary, U.S. Air Force (Retired), Kevin Contreras, and Doug Hamrick

Comprehensive operation plans (OPANs) can help integrate the U.S. and its allies and partners across the Indo-Pacific—but to stay ahead of fast-moving changes in the region, it is increasingly important that the plans be frequently and rapidly updated. The challenge is that OPLANs tend to be static documents that often must be updated manually, a process that can be cumbersome, time-consuming, and incomplete.

However, by bringing their OPLANs into an interactive digital planning environment, the joint forces can use what’s known as “rapid modeling and simulation,” aided by AI, to test and refine their OPLANs—often as fast as conditions change. And they can use that same modeling and simulation to help put the plans into action in a confrontation.

A digital planning environment can be particularly valuable in integrating the coalition in the Indo-Pacific as a combined force of forces. The digital environment brings together vast amounts of data from across the coalition, making it possible to run tens of thousands of simulations to help planners determine how the U.S. and its allies and partners can work together in optimal ways.

And because the digital environment is interactive, planners can experiment hands-on with scenarios of their own—moving red or blue force assets in a particular area of the South China Sea, for example, and then watching



as the AI-aided modeling and simulation predicts how a confrontation is likely to play out. Planners can collaborate at the same time from multiple locations across the Indo-Pacific, including from allied and partner nations.

Nothing about this approach takes away decision making from planners or commanders. Rather, it gives them more hard data to work with, often in near-real time. They still need to use their experience, knowledge, and judgment to evaluate the data and update the OPLANs as they see fit.

## **BUILDING THE DIGITAL OPAN ENVIRONMENT**

Advances in data science are now making it possible to bring together and integrate an almost unlimited amount of OPLAN data from any number of sources. This includes all of the relevant time-phased

force-deployment data now in spreadsheets, PowerPoint presentations, and other formats, which can be digitized through natural language processing and other techniques. Current OPLAN data can be combined with a wide range of unstructured data, from sources such as real-time intelligence reports, satellite imagery, acoustic signatures, and infrared thermography.

In addition, defense organizations can bring in large amounts of information about our potential adversaries, including detailed historical data—for example, how they have responded to certain activities by the joint forces in the past.

With this approach, all of the available data is ingested into a common, cloud-based repository, such as a data lake, and tagged with metadata. This breaks down stove-piped databases and makes it possible to analyze the entire repository of information—and all at once.

Although the data is consolidated, it is actually more secure than it would be in scattered, traditional databases. By tagging the data on a cellular level, defense organizations can tightly control who has access to each piece of data and under what circumstances.

### TESTING AND REFINING OPLANS WITH RAPID MODELING AND SIMULATION

Once defense organizations have created a digital planning environment, they can test and refine their OPLANS with modeling and simulation, taking advantage of the combined information in the data lake to factor in tens of thousands of variables. With the help of AI, new rapid modeling and simulation tools can play out OPLANS' courses of action, along with the branches and sequels, to determine the probability of coalition success every step of the way.

Planners might find, for example, that some bases would be at risk of running out of fuel or munitions during a conflict, or that certain U.S. aircraft would likely be more successful than others in particular missions. The AI might recommend courses of action, or specific branches and sequels, that planners may not have considered.

At the same time, advanced visualization tools, including interactive maps showing coalition and adversary forces, would allow planners to test out possible new scenarios. They might plug in different types of aircraft, for example, to see which are likely to be most effective, or pair manned and unmanned systems. Interactive visualization tools can also allow them to pose critical questions, such as whether a particular action would have a higher likelihood of success than others, but would cost more lives.

A digital environment also enables planners to take advantage of an emerging form of AI, known as reinforcement learning, to help predict adversaries' first moves and subsequent actions. By analyzing vast amounts of data about a country—including its military capabilities,

its doctrine, and its past actions—reinforcement learning can create an “AI agent” to represent that country in modeling and simulation. A unique feature of reinforcement learning is that allows the AI agent to pursue its own best interest, so that in modeling and simulation it would behave much like that country would.

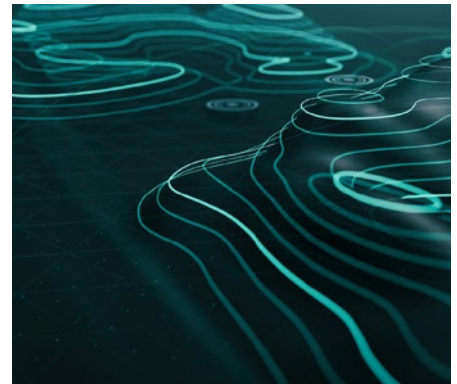
### RAPIDLY UPDATING OPLANS

Just as important, a digital environment makes it possible for planners to update OPLANS almost as fast as conditions change. New information—such as changes in coalition or adversary logistics and capabilities—is constantly fed into the digital environment. Ongoing AI-aided modeling and simulation quickly recalculates how current OPLANS are likely will play out and makes new recommendations.

Planners can see, often in near-real time, how they might need to modify their OPLANS. If they do decide to make changes, they can run their updated OPLANS through another round of modeling and simulation and see the new predicted outcomes. They can then continue to refine the plans as needed.

The same approach can help the joint forces make a seamless transition from operation plans to execution plans. As conditions rapidly cascade in a crisis or conflict, for example, decision-makers can quickly see the actions they might take that have the highest probability of success. Because the AI has already worked out tens of thousands of scenarios with the OPLANS, it can take advantage of what it has already learned to stitch together—in near-real time—new recommended courses of action.

The joint forces have a wealth of data available for operation planning. An interactive digital planning environment, along with AI-aided modeling and simulation, would allow them to take full advantage of that data to keep OPLANS updated and help integrate the allies and partners into a joint force of forces.



#### MAJ. GEN. DAVID E. CLARY

[clary\\_david@bah.com](mailto:clary_david@bah.com)

is principal at Booz Allen, where he leads the firm's support to coalition warfighters in the Republic of Korea.

#### KEVIN CONTRERAS

[contreras\\_kevin@bah.com](mailto:contreras_kevin@bah.com)

leads Booz Allen's delivery of digital solutions for the rapid modeling, simulation, and experimentation of multi-domain concepts for DoD and global defense clients.

#### DOUG HAMRICK

[hamrick\\_douglas@bah.com](mailto:hamrick_douglas@bah.com)

leads Booz Allen's development of AI-enabled predictive maintenance and supply-chain capabilities for clients throughout the DoD and other federal agencies.



# HOW “AI AGENTS” CAN INTEGRATE ALLIES AND PARTNERS

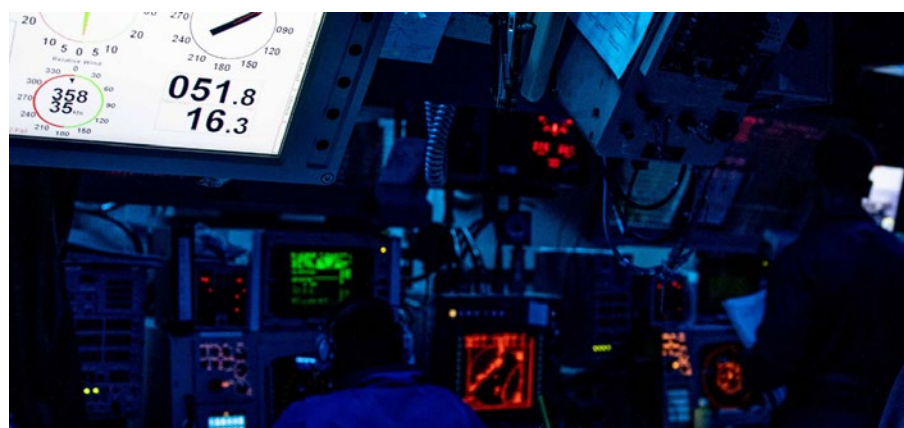
By Lt. Col. Michael Collat, U.S. Air Force (Retired) and Vincent Goldsmith

One of the challenges in integrating the U.S. and its allies and partners in the Indo-Pacific is that there is a great deal of complexity in how a potential adversary might engage each of the different countries in different ways leading up to a conflict—tactically, strategically, economically, and politically. And there is just as much complexity in how each country might respond in its own way.

It is difficult for wargaming and exercises to fully capture this complexity, with its clues to effective mission-partner integration. However, an emerging form of AI known as reinforcement learning can play an important role. Essentially, this technology makes it possible for each country in a virtual wargame—whether an adversary, the U.S., an ally, or a partner—to be represented by its own AI “agent.”

Each agent—a sophisticated algorithm—brings together and analyzes vast amounts of data about that country, including its military capabilities, its political and economic environment, and its posture toward the other nations. A unique feature of reinforcement learning is that allows the AI agent to pursue its own best interest, so that in a wargame representing a country, the AI behaves much like that country would.

This can provide valuable insight into the often-difficult challenges of mission-partner integration. For example, an AI agent representing a



critical partner in the Indo-Pacific might discover, over multiple scenarios, that certain security cooperation activities would likely elicit economic or diplomatic pressures from an adversary, and that the best course of action would be to disengage and remain neutral.

Or, the AI agent might find that if allies or partners have certain defensive weapons or other protections in place before a conflict, that would deter—or at least defer—adversary aggression. Such AI-informed scenarios can help map out the steps needed to make sure our allies and partners get the capabilities they to maximize deterrence.

Defense organizations are already beginning to use reinforcement learning in operational planning, by wargaming how opposing forces might engage tactically in battle. But reinforcement learning can go even further, by helping to integrate the

U.S. and its allies and partners in the Indo-Pacific through all phases of competition, crisis, and conflict, to help create a force of forces.

## HOW REINFORCEMENT LEARNING WORKS

With reinforcement learning, algorithms try to achieve specific goals, and get rewarded when they do. Using trial and error, the algorithms test out random possible actions. The closer those actions get the algorithms to their goals, the higher their score. If the actions move the algorithms way from their goals, the score drops.

In this way, the algorithms can rapidly work through thousands or even hundreds of thousands of scenarios, in a game-like setting, to determine the best course of action. With each iteration, they learn more about what works and what doesn't, and get closer and closer to the optimal solution.

Because the algorithms can perceive their environment in a virtual wargame, and participate autonomously, they are considered to be AI agents. And reinforcement learning is well suited for wargaming. An AI agent can take a side and play a role, trying to achieve its own specific goals and learning as it goes along. Just as important, multiple agents in a wargame—for example, representing various allies and partners in the Indo-Pacific—can learn how to best work together to achieve common goals in the face of an adversary.

Virtual wargaming is just one example of how reinforcement learning can assist defense organizations. It can also help optimize weapons pairing, the kill chain process, cybersecurity, and other challenges.

#### HOW REINFORCEMENT LEARNING IS TRAINED

The process of integrating allies and partners with reinforcement learning begins by bringing together a wide range of data about a particular country. In addition to information on the country's military and other resources, it can include its recent history—for example, how an ally's economy and politics were affected by outside pressures in the past, and how the country responded when faced with certain pressures from an adversary. All this information teaches the AI agent what kinds of actions it might see from agents representing other countries, and what kinds of actions it can take on its own.

At the same time, the AI agent is provided with that country's goals, based on the knowledge of experts on its culture, politics, economy, military, and other areas. The agent is then programmed to use the actions at its disposal to achieve those goals. While it may be impossible to capture the full picture of a country—or the complete international environment—even limited AI agents, interacting with one another, can provide important insights. And as new information about countries is added into the mix, AI agents continually learn.

#### REINFORCEMENT LEARNING IN ACTION

In a virtual wargame, AI agents for the adversary, the U.S., and various allies and partners enter a scenario and begin interacting with each other autonomously—each balancing its own strengths and weaknesses to achieve its goals the best way possible. In one scenario, for example, an adversary might try to use economic or diplomatic coercion against a number of different allies and partners at the same time, or launch sophisticated disinformation campaigns designed to pit countries against one another and break apart the coalition.

With each country pursuing its own best interest, the AI agents can reveal how they might work together against the adversary, or splinter from the others. A partner in the Pacific might decide to provide some assets to the coalition, but not others. An ally might be particularly susceptible to an adversary's disinformation campaign, and refuse to cooperate with other allies or partners. These kinds of scenarios can suggest actions the U.S. and its allies and partners might take, which they can then try out as the virtual wargame continues.

A wargame can play out with hundreds of thousands of iterations, giving the AI agents the chance to try out any number of possibilities, and find the best solutions. Throughout the process, domain experts continually verify the AI agent's goals and actions, making sure they accurately reflect the real world.

Reinforcement learning doesn't replace current approaches to wargaming, planning and other activities. Rather, it is a powerful tool to aid decision-making, as leaders seek to integrate the U.S. and its mission partners into a potent force of forces in the Indo-Pacific.



**LT. COL MICHAEL COLLAT**  
collat\_michael@bah.com  
is a Booz Allen principal leading the delivery of data analytics, counter-malign foreign influence, and digital training solutions across USINDOPACOM. A former Air Force intelligence and communications officer, he has also led projects delivering cyber fusion processes, information operations assessments, and regional maritime and aerospace strategies.

**VINCENT GOLDSMITH**  
goldsmith\_vincent@bah.com  
is a Booz Allen solutions architect providing transformational technical delivery across USINDOPACOM. He focuses on wargaming, modeling and simulation, immersive, cloud, and AI solutions, and he partners with warfighters in region to integrate the latest innovative technology into their base-lines, to advance the mission.



# PROTECTING MISSIONS FROM CYBER ATTACK WITH REAL-TIME RISK MAPS

By Dale Savoy and Capt. Alan MacQuoid, U.S. Navy (Ret.)

Perhaps the greatest challenge in protecting mission-critical systems from cyberattack is that there are so many possible ways an adversary could strike. A shipboard missile system in the Pacific, for example, might be disabled by an adversary that jams satellites or spoofs sensors, or disrupts command-and-control communications, or perhaps shuts off power to the cooling system of a building, a thousand miles away, that houses DoD computer servers. A single component of a mission-critical system might have dozens of such vulnerabilities, some well-known to cyber defenders—but potentially many others that are commonly overlooked.

The task of charting a system's complex web of cyber dependencies, when done manually, can take months, even years. And even then, defense organizations often can't capture the full range of downstream vulnerabilities that can endanger a mission.

However, new approaches, which take advantage of advances in machine learning and modeling and simulation, are now making it possible for the joint forces to create comprehensive maps of cyber risk to mission. With these maps, defense organizations can get a clear view of where their mission systems are most vulnerable to cyberattack, often in real time. Organizations can then prioritize their resources to best protect their most important missions.



U.S. NAVY (MC2 KALEB J. SARTEN)

## BUILDING A RISK MAP OF “PROBABLE” DEPENDENCIES

Defense organizations usually have good understanding of their information technology (IT)—their computer-connected systems—and so can protect those components with traditional cyber defenses. However, organizations don't always know all the ways their computer networks rely on operational technology (OT), which can range from HVAC systems on a base to radar sensors on a ship.

Organizations theoretically could connect much of their operational technology to their computer networks. However, they're reluctant to do so, because it would greatly expand the attack surface, providing many more ways a cyber attacker could gain access to the system. Unfortunately, that leaves defense organizations with limited visibility into their OT vulnerabilities. For example, an organization's

high-priority communications network might be using only one of 25 antennas at an airbase, but the organization doesn't know exactly which one it is. Tracking down the right antenna would take time, and it isn't feasible to manually go into that level of detail for every possible piece of OT. A single Navy base might have thousands of complex system dependencies.

However, defense organizations can take a different approach, by creating a map of probable dependencies with the help of machine learning. For example, an organization might not have the resources to fully protect all 25 antennas at the airbase, just to make sure the one being used by the high-priority network is covered. But if it could narrow down the number to four or so—based on the types of antennas commonly used with such networks—it might be feasible to put protections in place.

Machine learning can play a key role here. The first step is to provide machine learning models with the known IT and OT dependencies of various mission systems across the DoD, based on knowledge gathered manually over the years. The models would then look for patterns in the data, and predict a given system's most likely dependencies—for example, certain types of antennas used by a certain types of mission systems. To make sure the machine learning models are accurate, cyber analysts would do regular spot checks, and work with AI experts to tweak the models as necessary.

### **MODELING AND SIMULATION TO PLAY OUT RISK SCENARIOS**

Once organizations have created a map of probable mission dependencies, they can use modeling and simulation to gain a deeper understanding of the vulnerabilities. By playing out various scenarios, the modeling and simulation might show, for example, how damage to computer servers on the ground could disable a particular satellite array, which in turn could prevent GPS signals from updating a carrier group's inertial navigation. With such scenarios, defense organizations can gain insight into which vulnerabilities would have the most impact on a mission, and so know where to focus their efforts.

At the same time, defense organizations can use modeling and simulation to identify alternative paths if a mission dependency is compromised. For example, modeling and simulation might find that a high-priority mission system could quickly and successfully switch from one set of sensors to another—or perhaps could use the bulk of another system's IT and OT dependencies if necessary.

All this information can be presented to cyber analysts and decision-makers with user-friendly dashboards and other visualization tools that show, at a glance, where potential vulnerabilities lie. The dashboard might show, for example, a mission system's 100 or so

probable dependencies, identifying the ones that are not fully protected.

### **REAL-TIME MONITORING OF CYBER RISK TO MISSION**

Creating a map of mission dependencies is not a one-and-done job. On any given system, components are constantly being switched in and out as technology and requirements change. And as missions change as well, they might take on new vulnerabilities. Once the map of dependencies is created, however, it becomes easier to keep track of changes. Cyber analysts can log in new IT and OT components as they come online.

Because the modeling and simulation is run continuously, with each change it automatically looks for newly created vulnerabilities, and possible alternate paths if a mission dependency is compromised.

### **PROTECTING MISSIONS UNDER ACTIVE CYBER ATTACK**

Real-time monitoring of cyber risk to mission is critical if a system is under attack. Analysts can be alerted if a particular dependency is being attacked or has already been compromised. The alerts would show the likely impact to the mission—which could be minor or major—and present analysts with alternatives.

In some cases, the rerouting of dependencies might be automatic—for example, a missile system might move from one set of sensors to another. Other situations might require cyber analysts and decision-makers to step in to do the rerouting, using the dashboards and other visualization tools as guides.

With the help of machine learning, modeling and simulation, and other advanced approaches, defense organizations can build real-time cyber maps that show the often hidden ways missions could be degraded by adversaries. Organizations can use the maps to plug vulnerabilities as they arise, and move quickly to protect missions under active cyberattack.



#### **DALE SAVOY**

(savoy\_dale@bah.com)

leads Booz Allen's cyber warfare domain efforts in vulnerability and mission risk analysis. His focus is on defending DoD weapon systems and critical infrastructure from cyberattack, through mission-dependency mapping and vulnerability management.

#### **CAPT. ALAN MACQUOID**

(macquoid\_alan@bah.com)

is a leader in weapon systems and critical infrastructure cyber risk assessment and mitigation efforts. He has over 35 years of experience integrating kinetic and non-kinetic effects with emphasis on cyber across all domains of warfare.



# KEYS TO UNMANNED AUTONOMY IN THE PACIFIC





# WHY WE NEED “BRAIN-INSPIRED AI” FOR TRUE UNMANNED AUTONOMY

By Ayodeji Coker, Ph.D., and Jandria Alexander

A group of five unmanned surface vehicles in the South China Sea spots a contingent of enemy vessels, but can’t get that information back to operators—it’s a contested environment, and satellite communications in the area are jammed. The UVs, working together, determine that one of them needs to leave the area to send a message back.

They decide among themselves which of the five should go, based on which has the best information and the best chance of sending the message without being detected. The chosen UV leaves the area, and figures out for itself when conditions are right to send the message, and the safest, most efficient way of sending it.

The artificial intelligence that can provide UVs with these and other advanced autonomous capabilities will soon be available. But there’s a problem. Such sophisticated AI requires computers that are too big, and require too much power, to fit on UVs.

What the AI needs is a way to lighten its workload, so that onboard computers can be smaller and use less power. And two new approaches are now able to do that, by making computers—and the AI itself—mimic how the brain operates.

One approach is an emerging new design for computers, allowing them to process and store information the same location—similar to the way the brain does—rather than in two different locations. With the second new



U.S. NAVY (ANITA CHEBAHTAH)

approach, the AI reaches conclusions with less data, through inference—comparable to how we can identify an object even if we have only a partial view of it, by filling in the blanks.

Currently, small, low-power computers on UVs can only support “narrow AI”—good for a few basic activities, such as surveillance and reconnaissance. But with the two “brain-inspired” approaches, even highly sophisticated AI can run on the smaller computers. This makes it technologically feasible for the joint forces to bring high-level autonomy to unmanned surface, undersea, and aerial vehicles in the Indo-Pacific and beyond.

## BEYOND NARROW AI

With narrow AI, unmanned vehicles are not intelligent enough to act autonomously in a number of

important ways. For example, they can’t independently determine whether something they’ve spotted is important enough to alert an operator—currently, UVs check in at scheduled times. They don’t always know how to use their fuel efficiently when tracking contacts, or how to conduct ISR without being detected. They typically can’t autonomously distinguish between combatants and non-combatants, and don’t know how to apply rules of engagement. They have only limited situational awareness.

UVs theoretically could tap into sophisticated AI by connecting to the cloud—but that’s not a workable option. UVs can’t count on satellite communications in a contested environment. And power and bandwidth constraints would limit back-and-forth with the cloud, even in peacetime. So, the AI has to be able to run onboard.

## MIMICKING THE BRAIN

The two brain-inspired approaches don't make the AI smarter—AI is already gaining the ability to provide many aspects of advanced autonomy. What the approaches do is simply make it possible for the AI to run on the small, low-power edge computers that UVs have to rely on.

One of the approaches actually changes how computers work. Today's computers have separate processing cores and memory cores. This means that for each computation, the processor reaches into memory, takes out the data it needs, and then brings it back to process it. That continuous back-and-forth makes for a heavy workload—particularly for AI that does billions of computations a second. While the back-and-forth may not be a problem on large, powerful computers—such as those on conventional ships—it can quickly overwhelm a UV's edge computer.

Our brains operate in a different way. We're able to hold much of our memory in the same place that we process information, which allows even our most complex thinking to be almost instantaneous—a definite evolutionary advantage. Mimicking the brain's design, AI researchers are developing computers that put processing and memory in the same place. This makes the workload of even sophisticated AI manageable on a UV computer.

## TRAINING AI TO USE INFERENCE

Another way to reduce the workload is to simply use less data. AI researchers are achieving this by mimicking how the brain uses inference to make sense of the world with limited information. For example, when we're driving, we can anticipate the actions of other drivers by subtle cues, such as a car speeding up before changing lanes, or a car edging to the left as it approaches an intersection, in advance of actually making a right turn. We've seen these scenarios so many times that we don't need any additional information to adjust our driving. Our ability to make



U.S. NAVY (TYLER BALDINO)

inferences and predictions from just a few cues is one reason why we can (usually) drive safely on auto-pilot, our thoughts elsewhere.

By training AI to infer from a few cues, researchers are greatly reducing the amount of data—and power—the AI needs. For example, the AI might be provided with the “pattern of life” of an adversary's vessels in a particular area. If the UV's sensors pick up an anomaly—such as a vessel that's in an unexpected location, or is behaving in an unusual way—those may be cues that will enable the AI to infer the vessel's intention. The AI doesn't have to piece together every detail about the vessel, or sort through every potential action it might take. By picking out only the relevant cues, the AI could reach its conclusions with just a small fraction of possible computations—making it workable on a small edge UV computer. And the AI would be just as accurate as AI running a large, powerful computer on a destroyer.

Training AI to use inference is both an art and a science. The ability to select the right cues, and fully understand their implications, requires extremely deep domain and mission knowledge. At the same time, AI experts need know how to apply that knowledge to achieve autonomy.

If unmanned vehicles in the Indo-Pacific and elsewhere are to gain the level of autonomy required by the joint forces, AI-enabled edge computing needs to be rethought. The human brain can provide the inspiration.

### AYODEJI COKER

coker\_ayodeji@bah.com, is a former senior leader at the Office of Naval Research who is now an executive advisor at Booz Allen, where he leads intelligent autonomous systems strategic initiatives for the Navy. His roles at ONR included portfolio manager for autonomy, and leader of the Navy's intelligent autonomous systems strategy.

### JANDRIA ALEXANDER

alexander\_jandria@bah.com, is a vice president at Booz Allen who leads the firm's business for NAVSEA and S&T, including unmanned systems, resilient platform and weapon systems, data science, and enterprise digital transformation strategy and solutions for Navy clients.



# PROTECTING CLASSIFIED ALGORITHMS IN UNMANNED SYSTEMS IN THE PACIFIC

By Jandria Alexander and Mike Morgan

In the coming years, the joint forces will increasingly use artificial intelligence in unmanned systems in the Pacific. Many of the algorithms will be mission-specific and classified, making them potential targets of adversaries who may try to steal or disrupt them.

Protecting classified algorithms in unmanned systems in the Pacific presents a unique set of challenges. Unmanned systems may operate closer to adversaries than manned systems. And with unmanned systems, humans may not be available to detect attacks on the AI and take corrective measures.

However, by adopting a series of rigorous protections across the entire lifecycle of the algorithms—through all stages of development and deployment—and by building in resiliency, the joint forces can help keep classified algorithms in unmanned systems secure.

## PROTECTING THE ALGORITHMS DURING DEVELOPMENT

Often, many of the essential elements of a machine learning algorithm will be built in an unclassified environment, to take advantage of the expertise and innovations of the wider organization. The algorithm is then moved into a classified environment, where mission-specific and other classified elements are added.

It's critical that algorithms be protected while still in the unclassified environment. If an algorithm is stolen, an



adversary may figure out its purpose and methods—even if it hasn't yet been configured for a specific mission—and potentially develop countermeasures.

The joint forces can help protect the algorithms for unmanned in their early, unclassified stages through government-run AI/ML factories. Instead of relying on the industrial sector—which may not apply cybersecurity consistently—these factories can impose rigorous security controls through all phases of algorithm development, including both unclassified and classified. Many defense organizations are already moving toward this level of security with other types of software factories, and they can achieve the same goals with factories that specifically develop AI and ML.

At the same time, the joint forces can require that vendors adopt a comprehensive set of cybersecurity techniques when developing algorithms. Such measures include real-time threat-sharing, so that companies can take advantage of their collective knowledge, and cyber-as-a-service, so that there is active monitoring of systems and networks rather than just snapshot audits.

## PROTECTING THE ALGORITHMS DURING TRANSFER AND TESTING

Extra protection is also needed when transferring algorithms from unclassified to classified environments, and when moving algorithms between the labs doing the development and testing. The longtime practice of moving electronic information from one system to another by people—known as the “sneakernet”—carries a risk that malware could be placed on the laptops, disks and other items used in the transfers. With advances in technology, there is now more security in an infrastructure that allows direct connections between systems with different security classifications, especially on research and engineering networks.

The joint forces can also take steps to protect classified algorithms for unmanned during the testing itself. When algorithms are being tested in real-world conditions, adversaries may be able to determine how they're being used, or even steal them. One solution is to use digital engineering to test the algorithms with modeling and simulation. This not only keeps the algorithms from being exposed to

adversaries during testing—it also makes it possible to simulate cyberattacks and model different defenses.

### **PROTECTING THE ALGORITHMS DURING DEPLOYMENT**

Classified algorithms require particularly rigorous protections once they're deployed in unmanned systems. If a cyberattack corrupts the data being analyzed by the algorithms—or compromises the AI/ML systems themselves—humans may not be immediately aware that something is wrong.

One way of reducing the risk is to develop automated responses to data drift or model drift. If the data coming in from sensors is significantly different from what might be expected—potentially indicating a cyberattack—the AI/ML system might automatically shut down, or switch to data from other types of sensors. There is both an art and a science to identifying patterns in the data that might suggest a cyberattack, and establishing the thresholds that will trigger the automated responses.

Another step is to make it more difficult for a cyberattack on one AI/ML system on an unmanned vehicle to spread to other components of the vehicle—for example, from algorithms analyzing radar data to ones analyzing video feeds or signals intelligence. Here, the solution is to create a separate security boundary for each AI/ML system on the unmanned platform. This makes it possible to more tightly control the flow of data from one system to another, and to cut the connections between systems, if necessary, to keep a cyberattack from spreading.

Additional steps can help protect classified algorithms in the event an unmanned vehicle is captured by an adversary. Along with anti-tamper measures—which can make it difficult for an adversary to access and possibly reverse engineer a captured AI/ML system—the joint forces can apply an approach known as disaggregation.

An AI/ML system—one that analyzes radar data, for example—typically has

a complex collection of mission algorithms. With disaggregation, no single UV in a mission has all the algorithms. Each does just a portion of the analysis and sends its piece of the puzzle to a central processing location. The goal is that even if adversaries can overcome the anti-tamper measures on a captured AI/ML system, they won't be able to glean enough information to unlock the secrets of the system and its algorithms.

### **PROTECTING THE ALGORITHMS WITH RESILIENCY**

If cyber protections do fail, the classified algorithms on an unmanned vehicle need to be replaced as quickly as possible with new and better algorithms to maintain the mission. However, with conventional approaches, algorithms can't easily be switched in and out—often the entire AI/ML system has to be rearchitected, which can take months. In addition, algorithms and other components in a system are often so interdependent that fixing one problem—such as switching out an algorithm—can create other, unexpected problems in the system, leading to rework and more delays.

Once again, the modular approach provides an advantage. Using open architectures and other open techniques, the joint forces can build AI/ML systems that make it possible to quickly plug-and-play new algorithms and other components. In addition to helping maintain the mission, this has other benefits. AI/ML developers can regularly tweak the classified algorithms and replace them proactively—before any cyberattack—to make it difficult for adversaries to build up information on them. Plug-and-play also makes repurposing classified algorithms from one mission to the next easier and more secure.

Protecting classified algorithms on unmanned systems in the Pacific presents its own set of challenges. But by constructing strong cyber defenses throughout the algorithms' entire lifecycle, and by emphasizing resiliency, the joint forces can take steps to meet those challenges.



**JANDRIA ALEXANDER**  
alexander\_jandria@bah.com  
is a nationally recognized cybersecurity expert and a vice president at Booz Allen who leads the firm's business for NAVSEA and S&T, including unmanned systems, resilient platform and weapon systems, data science, and enterprise digital transformation strategy and solutions for Navy clients.

**MIKE MORGAN**  
morgan\_mike@bah.com  
is a principal at Booz Allen who leads the firm's NAVAIR line of business. He has over 20 years of experience supporting NAVAIR programs with a focus on systems development and cybersecurity for unmanned systems and C4ISR solutions.



# MAKING DIGITAL ENGINEERING FOR UNMANNED SYSTEMS MORE OPEN

By Brian Abbe and Commander Eric Billies, U.S. Navy (Retired)

Unmanned maritime systems (UMS) are poised to become a leading-edge capability for the Navy in potentially contested environments in the Western Pacific. As this unfolds, China will likely respond by aggressively introducing new methods and solutions to blunt the UMS' effectiveness. The Navy will then need to introduce even more advanced sensors, analytics and other technologies – which the Chinese in turn will seek to counter as quickly as they can.

The result may be a supercharged, ongoing technology race between the Navy's unmanned capabilities and China's countermeasures. If the Navy is to win that race, it is crucial that new capabilities be developed and fielded with digital engineering—but not the way digital engineering for the Navy is commonly practiced today. A new approach is needed, one that takes digital engineering out of the mostly exclusive realm of original equipment manufacturers (OEMs), and makes it more open to the Navy, and to a wider range of industry and other partners.

## THE PROBLEM: LIMITED INSIGHT INTO DESIGN DATA

Currently, most digital engineering practiced for major Navy programs of record and other projects is conducted by OEMs in their own digital environments. Because these environments are largely closed, the Navy lacks real-time insight into the



design data. The OEMs typically do their design work in their own digital environments, and then extract limited data points and present them to the Navy in contractual artifacts like spreadsheets, PowerPoint presentations, and pdf files. These artifacts are usually delivered only at major milestone design reviews.

This makes it difficult for the Navy to flag problems or gain detailed insight before a design goes to testing. Not only does the Navy have to wait until the end of a design phase to obtain the artifacts, the artifacts themselves may not have all the data Navy engineers need to fully evaluate and influence the design. This often results in extensive rework and other delays. Much of the speed that digital engineering offers the Navy is simply lost.

Closed OEM digital environments also hamper the ability of the Navy to tap innovation within the wider technology development community. Other providers normally have limited access to the information

they might need—including design and configuration data, system architectures and key interfaces—to determine whether they might possess new solutions to offer the Navy. While some of this information may be contained in legacy documents, it could take weeks or months to sort out—and even then it might not be enough. Here again, the Navy loses out on the potential of digital engineering.

## SHARED DIGITAL ENGINEERING ENVIRONMENTS

If the Navy is to take full advantage of digital engineering for unmanned systems, the design work needs to be conducted in common, or shared digital environments. Shared digital environments can take several different forms, but in essence they provide multiple parties with common access to design data. They might be sponsored or managed by the Navy, by OEMs, or by other entities. The Navy is already moving toward shared

digital environments, and now has the opportunity to build on that progress.

In a shared digital environment, the Navy can see the same design data the OEM is working with, and so can spot potential problems in real time, without needing to refer to artifacts at a later date. For example, if an OEM is developing a new side-scan sonar for an unmanned underwater vehicle, the Navy can provide much faster review, analysis and feedback across the entire lifecycle of the design—all of which would help get the sonar integrated, tested and fielded more rapidly.

Opening up digital engineering environments also fosters competition and innovation, by bringing in the wider community of technology providers, including academia and non-traditional defense contractors. Shared digital environments give providers earlier and deeper insight into what the Navy needs. And the more providers that can look at the problem, the greater chance that one of them will say, “We know how to solve it.”

### **MORE OPEN ARCHITECTURES, LESS VENDOR-LOCK**

One of the keys to rapid technology insertion in unmanned systems is the ability to plug-and-play the best new technologies from across the provider community. This requires open architectures, so that any provider can build solutions that will seamlessly integrate with current systems. Shared digital engineering environments do much to encourage these open architectures. That’s because shared environments aren’t effective unless the architectures let everyone in. Shared digital engineering environments and open architectures go hand-in-hand; each promotes the other.

At the same time, this approach substantially reduces vendor-lock. When other providers have direct insight into design data—rather than just legacy documents—the Navy is less dependent on the OEMs for system updates and upgrades. And with open architectures, the Navy is no longer locked into an OEM’s proprietary

approaches. Naturally, all of this must occur under appropriate levels of cybersecurity to prevent intrusions, manipulations, and theft of cutting-edge technical data—even as we reap the benefits of open architectures.

### **FASTER ADOPTION OF DIGITAL ENGINEERING**

Shared digital environments are the key to digital engineering not only for emerging platforms such as unmanned systems, but also for the Navy’s transformational technologies for critical priorities, including Project Overmatch. Shared digital environments speed this wider adoption of digital engineering.

Currently, each OEM typically has its own set of digital engineering tools and techniques, which are often not compatible with others. Common digital environments encourage common approaches, making it easier for the Navy to take digital engineering out of isolated pockets, and scale it across any number of projects.

### **BUILDING ON THE NAVY’S PROGRESS**

The Navy is already moving toward shared digital environments. One example is the planned Rapid Autonomy Integration Laboratory (RAIL), which will test new autonomous capabilities for unmanned maritime vehicles. Another example is The Forge, where the Navy can rapidly develop, test and distribute software upgrades to the Aegis and the Ship Self-Defense System (SSDS) platforms.

Both RAIL and The Forge are Navy-sponsored shared digital environments. This model of government-industry collaboration gives the Navy full access to the digital environments, and taps the innovation of the wider community of technology providers.

By building on the successes of these and other shared digital environments, the Navy has the opportunity to unlock the full power of digital engineering for unmanned vehicles on the leading edge in the Pacific, and for initiatives across the Navy.



#### **BRIAN ABBE**

abbe\_brian@bah.com, is the client service officer for Booz Allen’s Navy/ Marine Corps business. He leads the development of solutions and technologies for the Navy and Marine Corps in areas such as unmanned systems; information warfare; biometrics; anti-tamper; air traffic control; position, navigation, and timing; augmented reality/virtual reality; and fabrication and prototyping.

#### **COMMANDER ERIC BILLIES**

billies\_eric@bah.com, a retired surface warfare officer, leads Booz Allen’s business in the Pacific Northwest helping Navy clients chart innovative approaches for USV/UUV employment, and driving immersive tech (VR/AR/XR) across Booz Allen’s Global Defense Group.



# KEEPING UNMANNED AGILE WITH AR/VR TRAINING

By Joe Reck and Steve Boatwright

In the not-too-distant future, large unmanned Navy vehicles—both surface and undersea—may be regularly patrolling the waters of the South China Sea, equipped with sophisticated sensors, formidable weapon systems, and advanced analytics. As with any emerging military technology—particularly those with new, untested missions—much about how this will play out can't be fully predicted.

How will potential adversaries like China respond to the large unmanned surface vehicles (USVs) and unmanned undersea vehicles (UUVs), and how will mission planning need to be altered as a result? Which tactics, techniques and procedures (TTP) will prove successful, and which will need a reboot? How will the onboard analytics and other complex software need to be improved?

Changes to the large unmanned vehicles (UVs) and their operations are likely to come fast, as the Navy learns what works and what doesn't, and makes often rapid, iterative adjustments. But there's a potential snag. With all this change, UV operators will continually be required to do things in new and different ways. Can the training keep up?

## THE RISKS OF FALLING BEHIND

Conventional Navy schoolhouse training can give operators basic hands-on experience with the large



UVs, but it will not be able to provide training updates as fast they'll be needed. Sailors may have to wait weeks and even months for the latest schoolhouse training. That's fine when new training is needed only infrequently. But that won't be the case with the incorporation of large USVs and UUVs into the Fleet. Critical updates in mission planning, TTP, software—and even hardware like sensors—will likely come far more often.

The Navy plans to train sailors on the large USVs and UUVs as they're rolled out and tested, and so ideally, when the vehicles are first put into action, the operators will be up to date. But that may be the only time they will be. As Navy quickly adapts the new USVs and UUVs to real-world conditions in the Pacific Rim, the sailors' training could fall further and further behind.

There are several risks to such a growing lag in training. The Navy

may not be able to take full advantage of increasingly sophisticated capabilities for the large USVs and UUVs—capabilities critically needed to keep ahead of our adversaries. The training may be several generations behind new mission plans, capabilities and payloads. We can't count on our adversaries having a similar training lag.

In addition, if sailors aren't properly trained on unfamiliar aspects of the UVs, there's a greater risk that something could go wrong. There may be more of a chance that the UVs could get lost—or even worse—fall into adversaries' hands. There may be more of a chance they might accidentally damage Navy or civilian ships, causing injuries or perhaps even loss of life.

Navy decision-makers—many of whom are already wary of these kinds of risks—may be reluctant to deploy the large USVs and UUVs if they feel

the training is inadequate. This could significantly slow the Navy's rollout and expansion of unmanned vehicles, at a time when the Navy has signaled it wants to move quickly as possible to counter emerging threats in the Pacific Rim.

#### **ADDING A NEW LAYER OF TRAINING: AR/VR**

The success of large USVs and UUVs in the Pacific Rim will depend largely on the ability of the training to keep pace with rapid operational and technological change. There is now an opportunity to achieve this by supplementing conventional training with training using augmented reality (AR) and virtual reality (VR).

With AR/VR, the training can be forward deployed—that is, on ships and submarines, and at remote military installations. Sailors won't have to wait for visits to ports that might have the appropriate simulators and other trainers when training updates are needed. Using highly portable AR/VR goggles and heads-up displays, they can train at their current location, whether in port or at sea, gaining the “reps and sets” they need to become proficient with new mission plans, capabilities, payloads and other changes.

Just as important, the AR/VR training can be kept fully up to date, incorporating changes to UVs as they become available. One of the drawbacks of schoolhouses is that the trainers often lag operations—they may get new software and hardware months or even years after they've been introduced into the Fleet. AR/VR software can be quickly updated, so that the training is kept current and relevant. Operators can even train on new UV software and hardware as its being developed, by tapping into the digital models being built by system engineers and architects. That way, the operators are ready to go the day the changes take effect.

#### **SPEED AND FLEXIBILITY**

Forward-deployed AR/VR also offers much more flexibility than schoolhouse trainers. For example, the Navy might deploy a number of large UUVs with various software and hardware configurations, based on their missions. It is difficult for a single physical trainer to accommodate all those different configurations, and so operators may learn how to operate only one of those UUV configurations. With AR/VR, the operators of each UUV could get customized training.

Combining that flexibility with onboard training could be crucial as the new USVs and UUV are deployed in unpredictable situations. For example, if China responds an unexpected way to the UVs, the Navy may need to revise the scenarios it is planning for. Training for those scenarios can't wait for the schoolhouse. With AR/VR, forward-deployed UV operators can quickly begin training for any new scenarios.

Because the large USVs and UUVs are essentially emerging technologies with emerging missions, there will be a sharp learning curve for operators. It will be essential that forward UV teams share their lessons learned with one another. AR/VR makes it possible to aggregate this knowledge, by incorporating feedback from users into updated training, which is then pushed out to the operators. Revisions to the AR/VR training are typically placed on disk drives, which can then be delivered to the next port of call of the UV operators.

AR/VR training for large UVs does not remove the need for conventional schoolhouse training. That's still important to give operators tactile experiences, and to help them develop muscle memory. But once the large USVs and UUVs are incorporated into the Navy's Pacific Rim operations, they will need to quickly and constantly adapt to change. Forward-deployed AR/VR training can help smooth the way.

**JOE RECK**  
reck\_joseph@bah.com and

**STEVE BOATWRIGHT**  
boatwright\_stephen@bah.com, are lead engineers at Booz Allen Hamilton, are retired U.S. Navy submariners and UUV operators who help design AR/VR products for Navy UUV systems. They are experienced in Navy curriculum and training, and in conducting research and development into real-world UUV operations and undersea systems across the globe.





# AFTERWORD

Booz Allen is helping defense organizations develop and deploy a wide range of solutions to stay ahead of the pacing threat. We understand the DOD's emerging missions and challenges in the Pacific, and we combine that understanding with our expertise in advanced technologies and our culture of innovation.

The DOD is well positioned to build on the rapid progress it is now making across the critical priorities. With transformative technologies such as generative AI, digital twins and edge processing, the DOD can accelerate that progress to stay ahead of potential adversaries now and into the future.

Articles developed by Scott Flander,  
Booz Allen Capabilities Strategist



## **About Booz Allen**

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: Empower People to Change the World®.

**[BoozAllen.com/Defense](https://BoozAllen.com/Defense)**