Booz | Allen | Hamilton®

ALL-DOMAIN SOLUTIONS FOR THE PACIFIC DETERRENCE INITIATIVE

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

CONTENTS

INTRODUCTION

We are pleased to present this eBook, which compiles a series of articles by Booz Allen authors originally published in the U.S. Naval Institute's Proceedings magazine. The articles, by former Navy leaders and advanced technology experts at Booz Allen, address some of the key challenges the Department of Defense faces in the Indo-Pacific Region. We believe the articles present thought-provoking ways to begin to address some of those challenges.

The articles in this eBook offer new approaches to Pacific Deterrence Initiative (PDI) challenges in areas such as unmanned, cyber, predictive maintenance, sensor fusion and digital engineering. Each shows how the DoD can build on the rapid progress it is already making in those areas.

We are grateful for the insights offered by the authors of the articles. We are especially grateful for the review and perspective provided by retired Adm. James Stavridis. We welcome the opportunity to share our insights and expertise in these and other PDI critical priorities.

Respectfully,

Steve Soules
Executive Vice President
Booz Allen Hamilton

Brian Abbe
Executive Vice President
Booz Allen Hamilton

KEEPING FORCES OPERATIONALLY AVAILABLE WITH AI-ENABLED PREDICTIVE MAINTENANCE

By Captain Steve Soules, U.S. Navy (Retired), 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 the 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 STEVE SOULES
soules_stephen@bah.com,
a Booz Allen executive vice president who leads the firm's Joint Combatant Command account, retired from the U.S Navy after serving 27 years, including in six Western Pacific/Indian Ocean deployments.

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.

MAKING DIGITAL ENGINEERING FOR UNMANNED SYSTEMS MORE OPEN

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

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.

MIKE LAPIERRE
lapierre_michael@bah.com,
is a senior systems engineer at Booz Allen specializing in developmental engineering and platform HW/SW integration using MBSE and digital engineering-based analyses.

Booz | Allen | Hamilton®

KEEPING NAVY PORT SUPPLY OPERATIONS RESILIENT IN THE FACE OF CYBERATTACKS

By Jandria Alexander, Mike George, Gregory Buck and Captain Jeff Griffin, U.S. Navy (Retired)

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

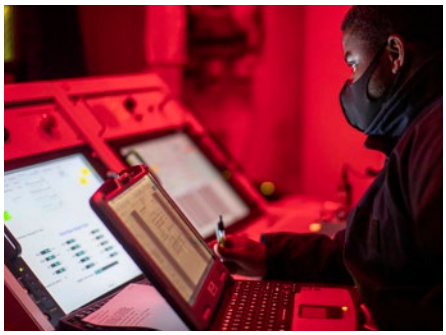
The next layer of defense is aimed at detecting malware that has been hidden on port systems, but not yet activated. Such malware is often very difficult to find—cybersecurity experts may not know where to look, or even what to look for. However, AI can hunt for second-order effects of an attack—subtle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

DR. MIKE GEORGE
george_stephen2@bah.com, leads Booz Allen's Federal Threat Hunt team and researches machine learning approaches for detecting sophisticated cyber adversaries.

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 Cyber-space Solarium Commission.

CAPTAIN JEFF GRIFFIN
griffin_jeffrey@bah.com, a retired Surface Warfare Officer and former Chief of Staff, U.S 7th Fleet, is Booz Allen's lead exercise planner for multi-domain operations, supporting headquarters, U.S. Army Pacific.

CAN TRAINING FOR THE NAVY'S UNMANNED SYSTEMS KEEP PACE WITH CHANGE? HOW AR/VR CAN HELP.

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.

HOW AI-ENABLED FUSION CAN HELP MAKE SENSE OF CONFLICTING SENSOR DATA

By Adam Weiner and Nathaniel J. Short

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 operatingenvironment. 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.

DR. NATHANIEL J. SHORT
short_nathaniel@bah.com is a Senior Lead Scientist at Booz Allen, where he conducts research and development in sensor exploitation, computer vision and data fusion for Department of Defense and other government clients.

Booz Allen is a new type of solutions provider for our defense clients—one that understands their missions and creatively brings them the best emerging technology to help them quickly and easily modernize, achieve interoperability, and win.

For more than 75 years, Booz Allen has been advancing the state of the art for the U.S. military and its allies. Our ability to blend mission understanding with cutting-edge technology creates transformative solutions. And our open architecture-based approach puts clients in control of their systems, enabling readiness, resilience, and upgradability.

We accelerate innovation to help defend the nation.


ANALYSIS PROCESSING NODE
Executor
SECTOR: 11
93
SECTOR: 06
02
SECTOR: 91
68
SECTOR: 73
90
DATA POINT 002-
DATA MODE A
DAT
ACCESS POINT 234-
ANALYSIS P
ACCESS POINT 557-
ANALYSIS P
SYS : 001 - SECTOR 98042
SYS : 002 - SECTOR 68317
SYS : 003 - SECTOR 17359
SYSTEM ANALYSIS_
SYSTEM ANALYSIS_
DATA - ANALYSIS
29.33
90.67
56.00
18.00
DATA - QTC 0026
EXTRACTION

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by its most sensitive agencies. We work shoulder-to-shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia, our firm employs nearly 27,700 people globally, and had revenue of $7.9 billion for the 12 months ended March 31, 2021. To learn more, visit BoozAllen.com. (NYSE: BAH)