Booz | Allen | Hamilton®

MEETING CHALLENGES IN THE PACIFIC WITH INNOVATIVE SOLUTIONS

PROCEEDINGS MAGAZINE ARTICLES BY BOOZ ALLEN HAMILTON – **VOLUME 2**

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

CONTENTS

INTRODUCTION

We are pleased to present our second 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 difficult challenges facing the joint forces in the Indo-Pacific region.

Articles in this volume address critical areas such as JADC2, persistent targeting, counter-C5ISR, predictive maintenance and integration of allies and partners—all in contested environments.

We are grateful for the opportunity to share our insights and expertise in these and other topics of importance to the joint forces in the Indo-Pacific. In addition, we offer our continued thanks to retired Adm. James Stavridis, who has generously reviewed these articles and offered his perspective.

Respectfully,

Jennie Brooks
Senior Vice President
Booz Allen Hamilton

Rex Jordan
Senior Vice President
Booz Allen Hamilton

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

By Mike Morgan, Steven Tomita, and Cliff Warner

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-site 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 of 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.

CLIFF WARNER
warner_clifford@bah.com
is a chief engineer at Booz Allen. He led the research on the mesh rely network for the Office of Naval Research in the 1990s when he was with what is now Naval Information Warfare Center Pacific. He currently develops and analyzes system-of-system architectures for Navy clients.

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 paring, 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.

CREATING A DIGITAL OPLAN ENVIRONMENT TO INTEGRATE ALLIES AND PARTNERS IN THE INDO-PACIFIC

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

Comprehensive operation plans (OPLANs) 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 simula-tion 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 simula-tion 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 OPLAN 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.

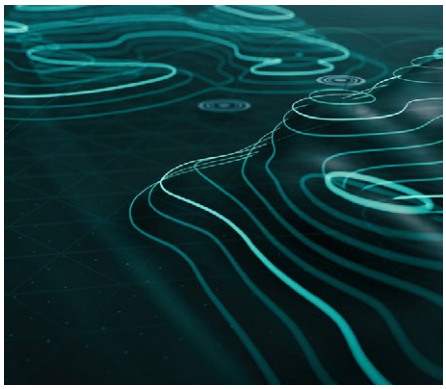
RAPIDLY UPDATING OPLANS

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

USING REINFORCEMENT LEARNING TO INTEGRATE ALLIES AND PARTNERS IN THE PACIFIC

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 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.

Booz | Allen | Hamilton®

ENHANCING COUNTER-C5ISR OPERATIONS WITH THE DATA LAKE AND AI

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

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 down-loaded 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 communcations-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 electro-magnetic 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.

JOHN JACKSON
jackson_john@bah.com
a retired Army spectrum manager who supported communications and EW/IW for 82nd Airborne and Special Operations, leads Booz Allen's C5ISR rapid prototyping team, addressing the challenges of unmanned systems, sensors, and 5G.

KEEPING AI-ENABLED PREDICTIVE MAINTENANCE ACCURATE 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.

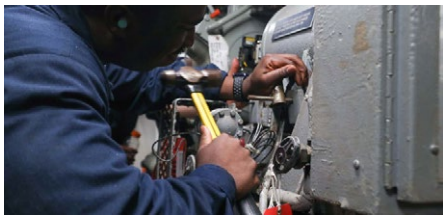
BRINGING IN AUTOMATION AND AI-READINESS

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_jarrod@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.

AFTERWORD

Booz Allen is helping the DoD develop and deploy a wide range of Joint All-Domain solutions in support of the Pacific Deterrence Initiative. We understand the DoD's emerging missions and challenges in the Indo-Pacific, and we bring to that understanding 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 approaches such as open architectures, and powerful technologies like AI and edge processing, the DoD can accelerate that progress to stay ahead of potential adversaries now and into the future.


SECTOR: 11
93
SECTOR: 06
02
SECTOR: 91
68
SECTOR: 73
90
ANALYSIS PROCESSING NODE
Executor
DATA POINT 002-
ACCESS POINT 234-
ACCESS POINT 557-
SYSTEM ANALYSIS_
SYSTEM ANALYSIS_
DATA - ANALYSIS
29.33
90.67
56.00
18.00
DATA - QTC 0028
EXTRACTION

About Booz Allen

Booz Allen is the premier digital integrator for the Department of Defense, blending decades of mission experience with state-of-the-art AI/ML, next-generation data solutions, networking, cyber, and advanced software development to help the department achieve information dominance. We bring our defense clients the best emerging technology to help them quickly and easily modernize, achieve interoperability, and win. We design open architectures to avoid vendor lock, lower lifecycle cost, and maintain a technological edge. Our technologists work hand-in-hand with our domain experts to build solutions that deliver the warfighter mission-critical information in today's digital battlespace. We're accelerating innovation to help defend the nation. To learn more, visit BoozAllen.com/Defense.