COALITION SECURITY SERIES

COALITION AIR AND MISSILE DEFENSE: INTEGRATION AND INTEROPERABILITY

ANDREA MCFEELY, RACHEL GIACHINTA, TYLER MILNER, ELIAHU NIEWOOD, ROBERT COONS, MEG ADAMS, MOIRA MCCARTHY, AND DAINIS BUTNERS

Table of Contents

INTRODUCTION

Recent events in the Middle East, in particular conflicts with the Houthis in the Red Sea and the defense of Israel against the Iranian attack on April 13, demonstrate the importance of effective coalition integrated air and missile defense (IAMD) against a range of threats.

The defense in both cases highlight a number of characteristics that are needed for effectiveness. In the battle with the Houthis, while the coalition has been largely successful in defeating constant attacks, it does so using exquisite and expensive defensive munitions against low-cost offensive munitions deployed at scale.[1] That is not a trade a coalition would want to make against a better resourced adversary such as China or Russia. The attack on Israel was defeated in part due to the layered defense system the Israelis have developed over years of preparation and intermittent conflict.[2]

The Israeli layered air defense program, which has been honed since facing Iraqi Scud missiles in the 1991 Gulf War, has an outer layer aimed at intercepting missiles in space, a middle layer aimed at short-range missiles or drones, and the famed Iron Dome focusing on smaller and slower targets.[3] The layered networks are linked by central command nodes allowing the layers to interact as needed.

Equally important to the success of the defense in the Middle East conflicts has been the broad, multi-national coalition that was brought to bear to mount the defense. In the case of the Iranian attack on Israel, the response demonstrated the efficacy of the longstanding IAMD integration efforts in the region,[4] including Jordan contributing to the defensive response, and Saudi Arabia and the United Arab Emirates sharing intelligence on Iran's attack prior to the offensive launch.[5] The U.S. military used ground, air, and sea assets to take down more than 80 Iranian drones and at least six ballistic missiles that were launched from Iran, Iraq, Syria, and Yemen.[6, 7] British, French, and Jordanian fighter planes reportedly shot down several drones, with British assets taking lead near their existing missions,[8, 9, 10] and Israeli assets shot down the majority of the almost 300 threats.[11]

The U.S. Air Force Central Commander at the time of the attack, Lieutenant General Alexus Grynkewich, remarked that allies and partners were successful against these threats because they share concerns over regional stability and have worked over the years to share information and threat warning within the coalition.[12] Another senior U.S. defense official noted to Reuters that no individual country could have successfully defended against "that very substantial, high-end barrage by Iran," with the defense instead relying on a high level of integration among several nations.[13] Because the drones and missiles were launched from several countries, it was critical for Arab nations to contribute to the defense of the region, including sharing information on Iranian plans and radar tracking information, opening up airspace for coalition planes, and supplying their own forces.[14]

U.S. Central Command (CENTCOM) managed the coalition forces coordination at the Combined Air Operations Center in Qatar and through operations centers in the continental United States. Although Lt. Gen. Grynkewich did not discuss specifics of the joint defense approach, he noted, "we take whatever assets we have that are in theater … under our tactical control or in a direct support role across the joint force and the coalition, and we stitch them together so that we can synchronize the fires and effects when we get into that air defense fight."[15]

International partnerships in air defense go back to World War I, with one example being the United Kingdom (U.K.) and France cooperating to defend French territory and regain territory during the Battle of the Somme.[16, 17] Today, however, nations face a myriad of diverse and modern threats that challenge previously held assumptions and beliefs on threat awareness and defeat capabilities. Unfortunately, many nations, including the United States, are not ready in many theaters to effectively operate in conjunction with their partners and allies to perform IAMD. Even in the CENTCOM Area of Responsibility (AOR), Lt. Gen. Grynkewich noted, "the ultimate goal is to get a much deeper and fuller integration."[18] If that is the case in an area where the United States has had decades of coalition operations to drive the building of networks that connect various partners and allies, to put in place data sharing agreements, and to build trust and cooperation, it highlights the challenge for other areas, such as the Indo-Pacific and Europe.

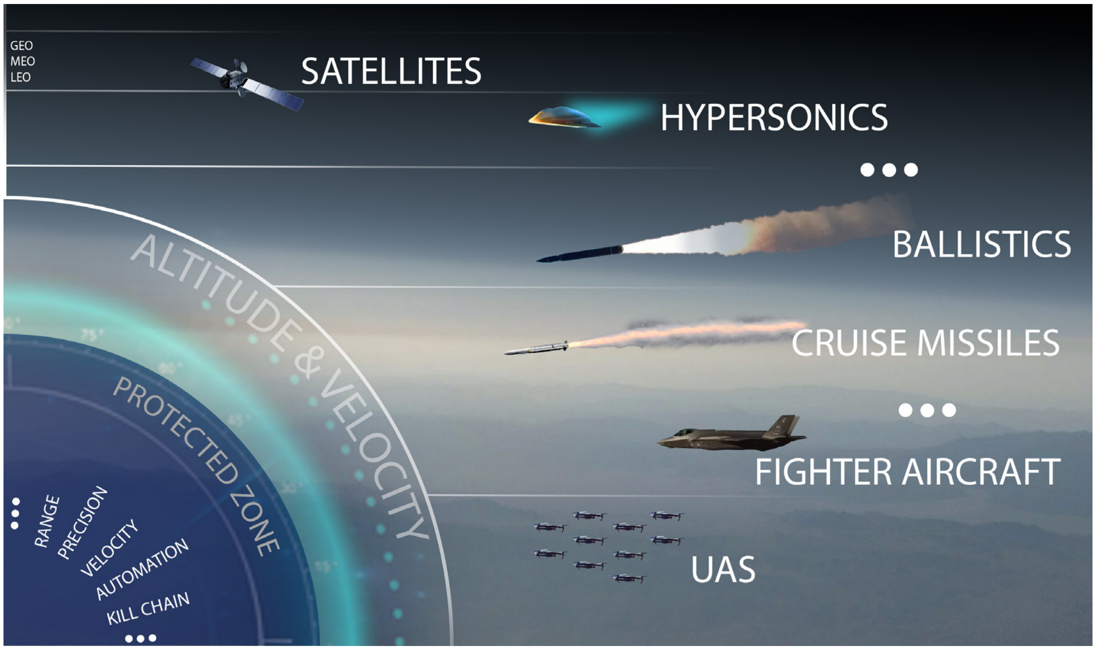

Figure 1. Weapons now span all domains, with missiles (including unmanned aircraft systems [UAS]) being launched from land, air, and sea, and non-kinetic weapons such as directed energy weapons being extensible across domains (e.g., attached to a fighter aircraft). This image is not an all-encompassing list of weapons, as depicted by the white dots; rather, it demonstrates the expanding threat environment and sets the stage for what must be considered to effectively protect an area.[19, 20, 21, 22, 23, 24, 25]

This paper describes some of the challenges of coalition-based IAMD and provides recommendations to address them. IAMD is a widely used term; however, its definition carries nuanced emphasis according to the context in which it is used. For example, while focus is traditionally placed on defense against air threats, the defensive systems used to counter those threats now span many domains (i.e., land, sea, space, cyber, and air) and include "left of launch" indicators. NATO defines IAMD as all measures to contribute to deter any air and missile threat or to nullify or reduce the effectiveness of hostile air action to protect populations, territory, and forces against the full spectrum of air and missile threats.

This paper does not aim to explain the full complexity of IAMD, particularly within a nation's internal capabilities. It focuses on three steps needed to implement a coalition-based approach to IAMD. The first step is integrating partner information from sensors and other data sources in secure federated networks that can create an integrated air picture using all available data and then distributing that picture, or tailored subsets thereof, to the coalition to ensure synchronized and consistent situational awareness of the IAMD battlespace. This step requires agreements among all participants to share the data in a manner that does not compromise sensitive sources and methods, as well as tailoring the distributed picture based on the information each partner is authorized to receive. The second step is using the integrated information to facilitate rapid decision making to layer and sequence the most efficient and effective defeat capabilities from across the coalition against the given array of threats. The third step is modeling and simulation (M&S) of the various threats and coalition capabilities for both air surveillance and threat defeat to help support understanding an integrated system performance, identifying gaps, and prioritizing future investments.

Creating and Sharing a Common Air Picture

In a theater like the Middle East or Europe, building an effective air picture to thwart IAMD threats requires bringing together a wide variety of national air and missile sensors including commercial air traffic control radars; dedicated military radars that span the maritime, ground, air, and space domains; signal intelligence sources deployed in a variety of locations; and even personal cell phones taking pictures of small UAS (sUAS) and estimating their locations.[26] Even in the Indo-Pacific, where national civil air surveillance may be more limited, there will still be challenges in bringing together various military systems with civil air surveillance around Japan and other nearby island nations. Timeliness is also critical for success in IAMD. Depending on the type and proximity of a threat, a target nation may have only seconds to issue an effective defeat response to protect its territory, so the latency associated with developing and sharing that common air picture must be faster than the threat. Within the context of this paper, the air picture is intended to capture a common data set, including air and missile tracks, as well as other surveillance data necessary to capture both pre- and post-launch activity associated with any threat that may traverse the air domain. The air picture is also not the same for all; the right information must be available at the right place to support the right decision at the right time.

The first step in addressing these challenges is to ensure that the individual nations are willing to share their data or to identify what data they are willing to share with whom, including identifying data sources and sensitivity levels of data. Solving this challenge is easiest if all the nations involved are willing to share all their data with all the other involved nations or to share across an alliance like NATO. However, countries are often reluctant to share data because of concerns over compromising sensitive or classified data, sources, or methods, particularly when there is a lack of trust between regional neighbors. Building an air surveillance picture will be considerably more challenging if Country A is willing to share with Country B but not Country C, while Country C is willing to share with Country B but not Country A. It is also more challenging if a nation is willing to share certain types of data but not others, for example its commercial data but not its military system data or willing to share radar data but not data derived from signals intelligence. It may also be that while individual countries are not willing to share their raw data with others, they might be willing to share the fused output of data with everyone in the form of tracks or a summary air picture. Ideally, nations would be willing to share raw radar plots, or the equivalent from other sources, that could then be fused to provide tracks built from multiple sensors. This would allow for reduced duplication between tracks. If not, fusion could still be performed at the track level if countries are only willing to share those tracks. Regardless of the specifics, defining what type of data will be shared between nations must be part of this first step.

In the end, it is likely that the information used to inform a coalition-wide tailorable air picture will need to form the basis of multiple tailored air pictures, each of which intend to provide appropriate operational and tactical awareness to partners and various command hierarchies. This awareness will form the basis upon which informed decision-making and battle damage assessment (BDA) can occur, coordinated across the coalition.

The next step in developing tailorable air pictures is to assemble the networks and compute environments needed to bring together the data from different nations and different types of systems. In most cases, this will also require cross-domain solutions (CDS) to provide connectivity between networks at different classification levels. Today, the networks available for doing that tend to be ad hoc collections of different national networks or bespoke networks custom built to allow connectivity between a specific set of nations for a specific application. Decisions will also need to be made to determine at which classification level to bring data together. Collecting data at the highest classification level of any sensor or system detecting air targets will make it difficult to share the tailorable air picture with all contributors. If data is collected at a lower classification level, it may not provide the best possible air picture, and individual nations may continue to develop their own air pictures at a higher classification level, potentially leading to confusion as battle management is executed. Latency and data throughput along the networks and through the CDS will be important for ensuring the tailorable air picture has the time accuracy needed for cueing weapon systems like airborne interceptor radars and surface-to-air missile system fire control radars.

Today, one approach for sharing data between organizations is centralizing and synchronizing data in a "data lake" or a "data warehouse." While that may work for a common air picture used to provide high-latency situational awareness, it likely will not be sufficient for the tighter timelines needed for IAMD. A federated data system where air and missile detections and tracks are deliberately pushed from sensors or collectors to correlation and fusion systems will be required. That federated system will need to ensure that only data approved for sharing within the coalition would be accessible using "data mesh" principles and through commonly deployed, well-defined application programming interfaces (APIs) at the individual data provider level, allowing nations to safeguard sensitive sources and methods. A federated data system approach allows data to be pushed and processed as needed and then integrated into downstream applications, without the need to centralize data in any single repository—which may not even be feasible with large-volume or dynamic data sources.

If successful, a federated system will enhance reliability and resiliency, because data is not stored in one single place and operations can continue even if one node fails. By embracing the diverse systems offered by each partner, tactical execution will not be subject to common vulnerabilities because hardware and software will be diverse, offering resiliency in contested operations. Highly redundant mesh interconnections further enhance system resilience by providing multiple pathways for data transmission. If one pathway fails, data can be rerouted through another, minimizing the impact of individual component failures on overall system operations.

A federated system also allows for improved performance, scalability, and flexibility. Development of the data and analytics can be processed in parallel, reducing development times for large or complex tasks. New nodes can be added to the system as needed, providing excellent scalability. Each node or system maintains its autonomy, allowing it to operate independently and make local decisions as needed. This provides a high degree of flexibility, as changes or updates can be made to individual nodes without disrupting the entire system. The federation of roles, and software implementation to fulfill them, provides flexibility regarding where roles are performed and allows the roles to relocate if necessary. This enhances enterprise reliability and resilience because if a node fails, the functions can be fulfilled elsewhere.

Once data is brought together, it may need to be converted into some form of standard format or translators may be needed to fuse data in different formats. While data interoperability has been a challenge in the past, new approaches that leverage APIs for each of the data sources and increasing availability of automated systems to "read" an API and understand how to work with data from the system behind that API provide new ways to accelerate integration of new data sources and types. Once ingested and understood, the data will need to be fused to provide a full air picture. That could be done at the plot or the track level, depending on the nature of the data available. Technology for achieving that fusion is fairly common, so this aspect of the process should not present significant difficulty. Finally, the air picture will need to be shared back with the nations that contributed to it. As described above, doing so will be relatively easy if all the input data is shareable with all the contributors or if the contributors all agree to share fused tracks irrespective of the shareability of the raw data. It will be more challenging if restrictions are placed on what track information can be shared with whom. Navigating that would require including the meta data around data sources to ensure data sources are shared appropriately. One example of this working is at U.S. Air Force Central Command's Expeditionary Air Control Squadron where coalition partners develop common air pictures from a fusion of various sensors.

Ukraine Lessons Learned on Information Sharing

The Russian invasion of Ukraine in February 2022 sparked a significant geopolitical and strategic shift in terms of coalition collaboration that few thought possible.[27] NATO, the United States, and Ukraine initiated information and intelligence sharing agreements that enabled a much deeper understanding of the threats posed by Russia as well as real-time threat reporting from the field. In Congressional testimony during the early months of Russia's full-scale invasion, General Scott Berrier, director of the U.S. Defense Intelligence Agency, described the intelligence sharing between the United States and Ukraine as "revolutionary in terms of what we can do" as the intelligence has been accurate, timely, and actionable. General James Hecker, U.S. Air Forces Europe & Africa Commander, stressed the importance and value of information sharing to shape threat awareness and capability development, noting "it's amazing what you can do if you share information amongst your allies—and how much better and capable you make each other really at zero cost. It's just a policy change, but an important one."[28]

Technically, interoperability has been significantly increased through the deployment of the Patriot missile system and the accompanying Link-16 system in Ukraine. These batteries enable Link-16 data (such as data on Russian sUAS and cruise missile attacks) to pass from the Ukrainians to other Link-16 networked military hardware, specifically within the NATO architecture. Further, tracks of Russian sorties acquired by U.S. and NATO systems can be passed to the Ukrainian Patriot batteries, which can then prosecute the linked tracks.[29]

What is clear from the ongoing Russia-Ukraine war is that intelligence related to and informing IAMD operations helps commanders understand the operational environment to understand, adapt to, and counter airborne threats. Information sharing is a "key strategic, operational, and tactical enabler"[30] that is becoming a prerequisite for effective IAMD operations in a coalition environment. For future conflict scenarios and contingencies, the ability to effectively share key data, information, and intelligence with allies and partners will play a crucial role in multi-domain, coalition operations.

Cross-Coalition Integrated Decision Making and Effects

The entire premise behind developing synchronized and timely coalition situational awareness is to enable coordinated responses which leverage the right defensive effects, at the right time and balances the efficacy and cost of the response—be it a reaction, pre-emptive action or BDA. Like the federation aspects associated with providing consistent situational awareness across the coalition, the set of nationally owned defeat capabilities must be leveraged holistically to prosecute both sophisticated threats such as hypersonic cruise missiles and hyperglide vehicles, and cheap, high-volume threats such as sUAS. The primary challenges with coordinating defeat options are (1) maintaining awareness of the available federated, nationally owned effects; (2) assessing, in real time, informed courses of action (COAs) from across the coalition to prosecute perceived IAMD threats; and (3) tasking and authorization (i.e., the command and control [C2]) for collaborative execution of IAMD across coalition partners.

Enabling distributed operations across the coalition to accomplish collaborative IAMD requires the situational awareness aspects described in the previous section, including the systems, networks, and infrastructure that support the nationally owned effects and C2. An effective coalition IAMD response will need to layer defensive infrastructure to balance response cost and efficacy based on the threat landscape perceived by the shared situational awareness. Further, a successful coalition will need to layer its air picture, tailoring the views presented to senior leaders, commanders, and operators to ensure they have precisely what is needed to inform their decisions. New and emerging categories of high-end air and missile assault weapons (e.g., hypersonic glide vehicles, scramjet cruise missiles, maneuvering re-entry vehicles, orbital bombardment systems)[31] require defeat capabilities to have greater precision and even more speed and maneuverability, all of which contribute to significant cost incurrence needed to develop these defeat technologies. These high-end technologies may be inaccessible to some coalition members due to the cost and complexity of acquisition, which can be overcome through a combination of joint acquisitions within the coalition and assessing holistic coalition effect capabilities and leveraging them to the benefit of all coalition members.

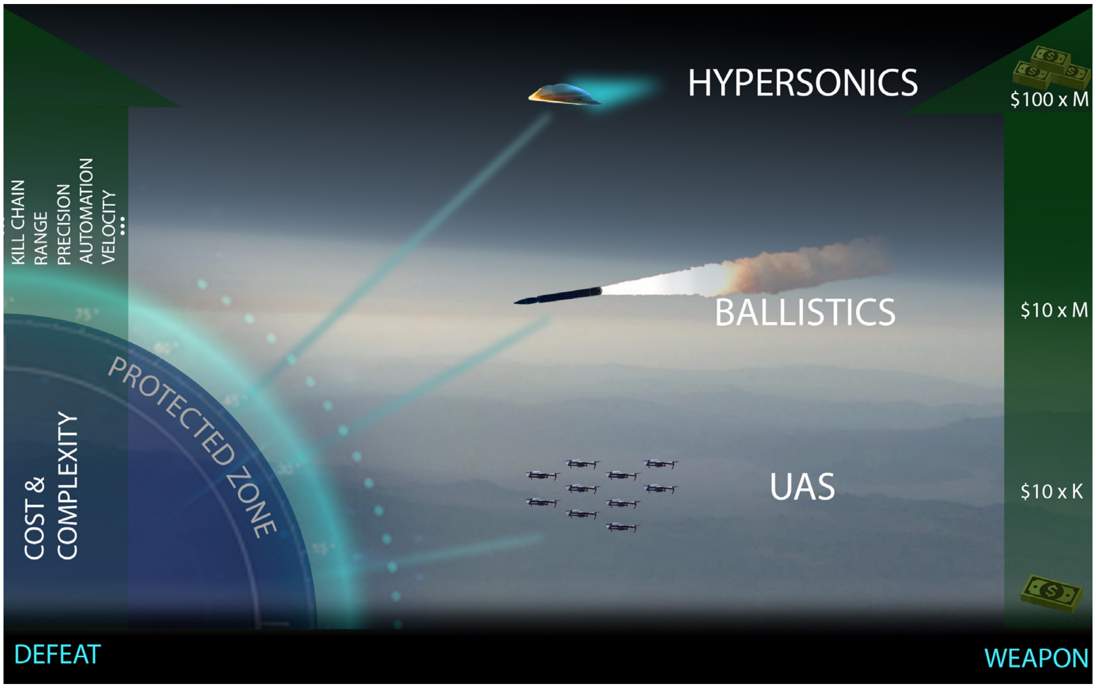

Figure 2. As the costs for weapon production and usage increase as weapons become more sophisticated, so do the costs and complexity associated with defeating those weapons. Average costs for each weapon vary, with averages given in the graphic above on the right. A subset of the factors that will increase cost and complexity for defeat of these weapons are listed to the left. Quantifying the cost of defeat will vary based on scenarios (e.g., the number of and type of weapons in an assault; the proximity of the assault; timeliness of detection, which also includes consideration of sensing and communication in the area).

Emerging technology options, such as those listed below, offer cost-effective alternatives to the defeat tactics traditionally associated with air defense.

Laser Systems— Lasers are a lower cost alternative to missile interception, but the current challenge is to develop the precision and power needed to reliably intercept the target. The U.K. is making progress with development of the new DragonFire capability, which is demonstrating highly accurate targeting.[32] Israel is testing the Iron Beam system, which boasts a close-to-zero cost to fire and unlimited magazine depth.[33]

Net Guns— Drone swarms have challenged ballistic, or even drone-on-drone, means of interception. However, innovators are leveraging and redesigning net guns, a traditional means of capturing birds, to defeat the threat without "debris falling from the sky, no explosion in the air," and introducing the opportunity reuse drones.[34]

Jammers— Electronic attacks are emerging as a key to air superiority, degrading aircraft radar and communication systems' operational effectiveness. The countermeasure to an electronic attack is the same means of deploying the attack, which has been simplified to "jamming the jammers," in the electromagnetic battlespace.[35]

sUAS to intercept sUAS— Several recent developments in the sUAS space include interceptor capabilities integrated into drones. Examples of this technology include using a racing drone to deploy a net to take down sUAS threats,[36] and an unmanned combat aerial vehicle equipped with air-to-air rockets that can intercept swarms of drones.[37]

To enable an operator or decision-maker to select the "right" COA for execution the real-time situational awareness data must be explored and measures, which quantify the cost-benefit of an option, evaluated. To accomplish this level of harmonization across the coalition, several aspects must be considered once data sharing considerations have been addressed. The measures of cost and efficacy of a response must be derived and provide context at the coalition level and consider impacts to individual partners. Like the shared operational picture construct, a coalition-level perspective must be developed to coordinate assignments across the coalition and then be distilled into subsets of relevant information each partner nation needs for its regional areas of responsibility and assigned threats. Perspectives to consider include financial, infrastructure, and population aspects, while efficacy may include intercept performance and timeliness of response. From these measures, various algorithms can be developed to identify, in real time, the optimum set of response options available to the coalition.

The Joint Fires Network (JFN) is a prototype that has demonstrated the ability to share a common understanding of the battle space to a geographically dispersed joint force.[38] With this shared understanding, commanders will have increased flexibility on how to deploy current and future sensors and weapon systems resulting in increased lethality. The JFN leverages and integrates best-of-breed approaches from the services and research labs to provide decision advantage to deliver effects at the speed and scale required for deterrence or combat success. For now, the JFN prototype is focused on a different mission and largely a U.S.-only system, there are important lessons that can be learned from JFN for coalition based IAMD. The federated integration of service and intelligence capabilities—sensors and effects—to support joint decision-making has resulted in a scalable approach that is applicable to many joint warfighting missions.

Finally, the tasking and authorization aspect has challenges on multiple fronts, including but not limited to establishing:

- Who is responsible for compiling the common data and then ensuring it and appropriate tailored air pictures are distributed to partners and throughout the command hierarchy (right view at the right place to inform the right decision).
- Who determines the appropriate metrics as a basis for machine-assisted COA development.
- Who develops the algorithms to infer COAs from this situational awareness.
- Who is responsible for selecting the appropriate COA the coalition should take and subsequently tasking each partner based on the details of the selected COA.

Coalition COAs cannot be developed if the coalition members are not willing to share some information with one another about the capabilities of their response options. That information does not have to include all the details of the defensive system, but it likely will need to include which types of IAMD threats the system is effective against, what data inputs the system needs to be effective, and what timeline the system operates on for response options. International defense organizations and those of pre-established alliances (like NATO) benefit from having defined acquisition mechanisms and responsibilities as well as strategic, operational, and tactical authorities delegated and deconflicted based on doctrine. Not all regions have formal defense alliances (e.g., Pacific), and not all alliances include all nations in the region that can contribute to and benefit from inclusion in the alliance (e.g., such as the case for Ukraine). The establishment of new alliances and the development of frameworks for establishing ad hoc alliances at the time of need should be explored. Interoperable C2 systems and C2 networks will be required, as will shared tasking mechanisms to communicate execution options to the partners. One approach that may help with interoperability, similar to what is being done with JFN, is to use a federated approach, where each national system is relied on for executing specific IAMD tasks, while a cross-coalition system is able to interoperate with the national systems in a loosely coupled way, providing tasking across the range of threats and keeping track of which tasks are being executed by each nation.

Integrated Coalition Modeling and Simulation

M&S, along with the operational analysis that M&S supports, is used in a variety of important ways for many national security applications, including IAMD. M&S may be used to help understand gaps in current IAMD performance; to help assess new weapons, sensors, and other systems that could be added to an IAMD architecture; to design concepts of operations; or to inform an operator about potential courses of action. M&S is used as a mechanism to explore and evaluate alternative technologies, processes, algorithms, platforms, force postures, and many other facets of a nation's or coalition's defensive capabilities and how these capabilities perform when under threat.

M&S is a scalable and inexpensive way to understand optimum placement of sensing capabilities and optimum combinations of defeat effects; to gain an understanding of features and environmental considerations that drive performance, cost, and schedule; and to identify deficiencies in performance of a system or system of systems within the contest of varied contested environments. These systems could include algorithms that assess the battlespace and current environment and present commanders with qualitative or quantitative metrics associated with COAs to overcome the current threat space, or specific technologies needed to detect objects, identify and track threats, and intercept threats through kinetic or non-kinetic means, for example.

Building and operating a coalition IAMD system would benefit from the ability to perform cross-coalition M&S. Unfortunately, cross-coalition M&S currently cannot be executed easily or in a scalable way. Not only are specific models of threat systems or of national IAMD systems not shareable with most partners, even the simulations themselves are often not releasable or shareable across a coalition. For example, the Advanced Framework for Simulation, Integration, and Modeling (AFSIM) is a U.S. government–provided tool for M&S used by a wide range of Department of Defense and industry organizations. However, AFSIM itself is subject to defense trade controls, and neither the model nor the results from it can be shared with most coalition or partner nations.

To support coalition analysis, organizations like The MITRE Corporation have developed dedicated M&S tools that are shareable or have adapted their own in-house tools for releasability. MITRE has used both its Enterprise Intelligence, Surveillance, and Reconnaissance Modeling and Simulation and Joint Operations and Visualization Environment tools with allies and partners. In the long term, however, developing releasable versions of U.S. government standard tools, at least for limited release, is critical. Having libraries of threat and coalition systems that could be released along with those models would also provide significant benefits. For further descriptions on some specific M&S tools, please see the appendix.

M&S provides insights to enable data-driven decisions and should continuously be used to adapt defense designs to reflect the evolving threat landscape. When a threat's capability or capacity changes, the M&S must account for these changes to recalibrate the response measures. This requires regular engagement of all key stakeholders. For example, when working on the development of the North American IAMD architecture, stakeholders across nations, along with academic partners, met on a weekly cadence to ensure the M&S scenarios were calibrated to adapt to changing environments and threats.[39]

CONCLUSION: THE NEED FOR COALITION ARCHITECTURES

The Russian war against Ukraine, battles with the Houthis in the Red Sea, and the defense of Israel against the Iranian air and missile barrage all highlight the need for coalition IAMD.

The United States and its partners need systems that share information and data in a direct and timely way. They need integration and interoperability of C2 systems as well as weapons for IAMD. They need shareable modeling and simulation tools to understand the threat, effectiveness of current IAMD, and utility of additional developments and partnerships.

A successful coalition architecture relies on building on and taking advantage of assets within each category in a federated manner rather than attempting to apply a one-solution-fits-all approach. Each nation has its own unique requirements for sovereign defense and deterrence missions that allies and partners seeking to align IAMD must embrace to be successful. While some past approaches have attempted to address IAMD by eliminating the diversity and creating a single system that captured all requirements from all nations, a more efficient system is to embrace the existing diversity and aim to federate and integrate across the variety of national systems to provide effective capabilities across the coalition.

Coalition IAMD Architecture in the Pacific

In the Indo-Pacific, the United States continues to build trust and strengthen its commitment to regional IAMD through engagement with allies and partners. For key regional partners such as Japan, the Republic of Korea, and Australia, IAMD investments will improve interoperability and integration with the United States.[40] Australia's burgeoning AIR6500 program is highlighted by U.S. Indo-Pacific Command (USINDOPACOM) as a regional champion of the IAMD vision. The joint air battle management systems will leverage fifth-generation system capabilities to provide high situational awareness and defense against air and missile threats, while being designed specifically to be interoperable with existing U.S. systems and coalition partners.[41] Combined exercises such as Valiant Shield 24 offer the opportunity for allies and partners to practice the "reps and sets" they need to respond to threats as a seamlessly integrated force.

The concept of an integrated and interoperable fire-control architecture and an advanced joint and combined IAMD battle management and engagement coordination system for the Indo-Pacific was first proposed in USINDOPACOM's IAMD *Vision 2028*.[42] *Vision 2028* challenges the combined joint force to move from coordinated operations where partners and allies work in parallel toward the same mission outcome to integrated operations using the same tactics, techniques, and procedures and working from the same common operating picture fed by AOR-wide "integrated, netted, and layered sensor coverage."

In Europe, the Pacific, and the Middle East—against a range of strategic competitors—no single nation can match or defend against adversary capabilities. Allies and partners understand the need to implement mechanisms that allow for integration and interoperability. However, there are gaps in technical alignment to face the threat and in policy agreements to ensure adequate sharing of data. Integrated threat awareness, coalition-level planning, and interoperable defeat capabilities are three essential pieces of a coalition IAMD architecture that offer technical ways forward. However, they rely on coalition commitment and action.

We offer the following recommendations to actualize a coalition IAMD architecture that will ensure secure sharing and communications, mission-based operational and acquisition requirements, agility and scalability, and inclusion of cost-effective emerging technologies. The recommendations are divided into four sections that focus on national defense considerations for each nation, creating and sharing a common air picture, cross-coalition decision making and effects, and shareable M&S.

Recommendations for Each Nation

1. **Ensure national cross-service integration** to enable cross-service sharing of systems, processes, and procedures among its organizations and missions engaged in IAMD. New policies should be issued to match updated senior level guidance to ensure implementation within the services.
2. **Design coalition interoperability** into new acquisition and policies that have the potential to participate in or influence coalition operations This may include using open-system standards, deploying common compute and storage hardware, and producing coalition-releasable versions of fusion and C2 software.
3. **Enhance efficiency and effectiveness of national defense sale programs** to ensure systems can be integrated into national and regional systems and maintain interoperability with coalition efforts. This may include interoperability clauses in those foreign sales to ensure systems level integration within coalition architectures and operations.

Recommendations for Creating and Sharing Common Data for Tailorable Air Pictures

4. **Operationalize tailored air pictures** to enable the right decision at the right time. While a common air picture is desirable to ensure everyone has access to the same information, it must be tailorable to ensure the prominent information available to senior leaders, commanders, and operators is precisely what is needed to inform their decisions.
5. **Formalize information sharing agreements among partners** to enable holistic and consistent threat awareness through establishing clear implementation plans, role and responsibilities assignments, and agreements on classification equivalents, mutually acceptable data and cybersecurity standards across partner systems.
6. **Establish a new approach to cross-domain solutions** that de-emphasize protection of an entire classification domain and refocus on protecting individual data to enable flexibility in information sharing across classification equivalents and dynamically between them (low to high or high to low).

Recommendations for Cross-Coalition Decision Making and Effects

7. **Establish a framework for distributed joint operations that enables the rapid stand-up of ad-hoc alliances.** This includes the necessary command structure, tasking and execution, areas of responsibility, data-management and distribution considerations for both awareness and effects synchronization, and other strategic and operational aspects that will reduce timelines associated with coordinated tactical responses to initial waves of threats.
8. **Accelerate acquisition of coalition defense industrial base (DIB) IAMD inputs.** Nations and coalitions should adopt an agile acquisition mindset, working together wherever possible, to opt for rapid prototyping and fielding purchase mechanisms that prioritize speed of delivery, cost-effectiveness, and simplicity. Coalition members should enable acquisition outside of their national defense industrial bases into the broader coalition defense industries to take advantage of the technology and capability developments of partners. From a policy perspective, this will require changes and/or agreements across governments that support the closer coordination and integration of coalition DIBs. From a cultural perspective, governments must shift towards close and continuous industry engagement to align coalition suppliers to mission needs. Innovative and flexible acquisition strategies, such as consortium models and challenge-based acquisition, can support the acceleration of rapid prototyping and fielding demands.
9. **Invest in lower cost defeat research and technologies** to achieve "balance[e] [in] the range, size, speed, survivability, and capacity. … [of] a mix of weapons that will maximize the cost-effectiveness of penetrating strike operations conducted at scale."[43] Rather than focus only on performance governments need to consider value as a driver to ensure defense investments have a corollary value proposition against cheaper threats.

Recommendations for Shareable Modeling and Simulation

10. **Develop releasable versions of government standard tools** to provide a mechanism for consistent modeling activities across the coalition and facilitate collaborative M&S activities for coalition IAMD planning.
11. **Establish releasable libraries of coalition systems and threats** to further ensure consistency and accuracy in the representations of national systems, threat systems and joint/coalition systems across M&S activities.

Appendix: M&S Tools

The type of analytical method, and modeling and simulation (M&S) tools used, should be tailored to answer a specific question, with consideration given to the scale and scope of the scenarios input data. No tool offers a silver bullet solution to ensuring coalition integrated air and missile defense (IAMD) success; rather, a suite of such tools should be leveraged to meet the breadth of modern IAMD threats. Three tools are highlighted below. However, they are exemplars and not an exhaustive list of the tools available. All the tools described have limited foreign releasable versions available. Enterprise Intelligence, Surveillance, and Reconnaissance Modeling and Simulation (EIMS) and Joint Operations and Visualization Environment (JOVE) are best for M&S of a discrete event, allowing events to occur at arbitrary points in simulation time, whereas Advanced Framework for Simulation, Integration and Modeling (AFSIM) provides a flexible cross-domain, multi-fidelity (e.g., multi-event) scenario environment.

EIMS

EIMS is a toolbox supporting a modeling and analysis framework designed to support the evaluation of numerous architectures as well as the visualization of cost and performance. EIMS has informed the acquisition of defense and defeat capabilities for coalition partners. It best supports engineering-level M&S, with discrete data specification delivering high-fidelity actions, via various models within its software components, including:

- Environmental models (earth mapping, atmospheric, maritime clutter, terrain obscuration)
- Target models (airborne and maritime, theater ballistic missile)
- Sensor models (monostatic radar, electronic surveillance measurements, passive coherent location)
- Analysis calculations (target location accuracy, tracker accuracy)
- Communications models (wired communications, wireless line-of-sight, atmospheric attenuation and satellite communicationsmodeling, communications jammers, code structure for moving objects)

JOVE

JOVE is a scenario simulation modeling tool originally used to simulate naval and air warfare. However, it has evolved to include operation planning and course of action development. It is designed to visualize and prioritize options by relying on two steps of input:

- Specification of entity types, sensors, and armaments
- Assignment of intended routes to entities

JOVE has been used successfully to model weapons performance, sensor performance, command and control, communication links jammer performance, and platform changes.

AFSIM

AFSIM is a modular object-oriented, multi-domain, multi-resolution M&S framework for military analysis, experimentation, and wargaming.[44] Compared with a tool like EIMS, it models larger scenarios with many red versus blue actors in a 24-hour scenario, accelerated in the simulation to minutes, and can simplify likely outcomes of a complex number of interactions. Key characteristics of its effectiveness within IAMD include its "plug and play" modules, which enable extensibility and user reuse of or modification to existing models without changing the core code. Its offerings span a broad spectrum of military simulations (i.e., engineering, engagement, mission, and "campaign-lite") to enable users to scale a scenario in either virtual (i.e., real operators controlling simulated systems) or constructive (i.e., simulated operators control simulated systems) environments.

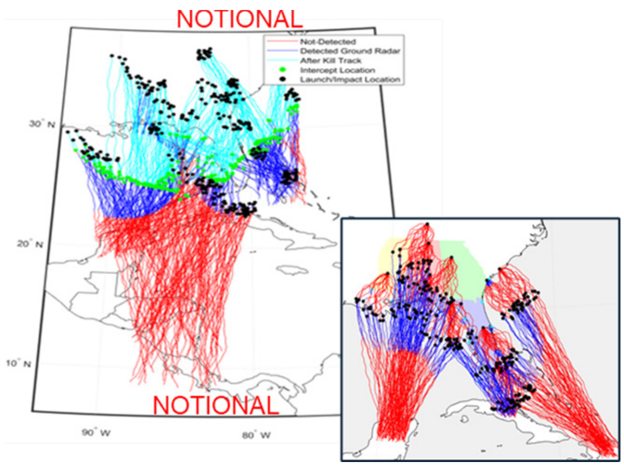

Figure 3. This depicts two fictional EIMS simulations of airborne threats (in red) being detected at different times after initial launch by ground radars (in blue) and intercepted by various options (in green). Where the red lines continue, the threat was not intercepted, and cyan shows the intended tracks of intercepted threats after kill. These M&S capabilities allow for cost-effective mechanisms of determining placement of sensors and sequencing and layering of intercept capabilities.

References

1. Martin, T. High price of Red Sea shootdowns speeds Navy's pursuit of 'cost-effective' solutions https://breakingdefense.com/2024/05/high-price-of-red-sea-shootdowns-speeds-navys-pursuit-of-cost-effective-solutions/
2. Vidal, E. CTECH. 99% interception success rate: Behind Israel's multi-layered air defense system that thwarted Iran. https://www.calcalistech.com/ctechnews/article/hkrztvfl0
3. Doyle, G., Zafra, M., Arranz, A., & Chowdhury, J. (2024, April 18). Israel's Iron Dome. Reuters. https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/IRAN-DEFENCE/mypmkljzopr/
4. Lendon, B. (2024, April 14). Analysis: How Israel and Allied defenses intercepted more than 300 Iranian missiles and drones. CNN. https://www.cnn.com/2024/04/14/middleeast/israel-air-missile-defense-iran-attack-intl-hnk-ml/index.html
5. Bradley, M. (2024, April 16). Arab states helped to defend Israel from Iran. Their resolve may be tested. NBC News. https://www.nbcnews.com/news/world/iran-attack-israel-hamas-war-saudi-arabia-jordan-uae-coalition-rcna147965
6. Doyle, G., Zafra, M., Arranz, A., & Chowdhury, J. (2024, April 18). Israel's Iron Dome. Reuters. https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/IRAN-DEFENCE/mypmkljzopr/
7. Thomas, C., Zanotti, J., & Sharp, J. M. (2024, April 22). Escalation of the Israel-Iran conflict—CRS reports. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN12347
8. Ministry of Defence. (2024, April 13). UK military activity in the Middle East. GOV.UK. https://www.gov.uk/government/news/uk-military-activity-in-the-middle-east
9. Cloud, D. S., Lieber, D., Kalin, S., & Said, S. (2024, April 15). How the U.S. forged a fragile Middle Eastern alliance to repel Iran's Israel attack. WSJ. https://www.wsj.com/world/middle-east/how-the-u-s-forged-a-fragile-middle-eastern-alliance-to-repel-irans-israel-attack-4a1fbc00
10. House of Commons. (2024, April 23). Israel-Iran April 2024: UK and international response. UK Parliament. https://commonslibrary.parliament.uk/research-briefings/cbp-10002
11. Gordon, C. (2024, April 15). USAF fighters shoot down Iranian drones in defense of Israel. Air & Space Forces Magazine. https://www.airandspaceforces.com/usaf-fighters-shoot-down-iranian-drones-in-defense-of-israel/
12. Ibid.
13. Stewart, P., & Ali, I. (2024, May 22). After Israel defense, US sees chance to entice Gulf allies on Missile Shield. Reuters. https://www.reuters.com/world/after-israel-defense-us-sees-chance-entice-gulf-allies-missile-shield-2024-05-22/

14. Cloud, D. S., Lieber, D., Kalin, S., & Said, S. (2024, April 15). How the U.S. forged a fragile Middle Eastern alliance to repel Iran's Israel attack. WSJ. https://www.wsj.com/world/middle-east/how-the-u-s-forged-a-fragile-middle-eastern-alliance-to-repel-irans-israel-attack-4a1fbc00

15. Gordon, C. (2024, April 15). USAF fighters shoot down Iranian drones in defense of Israel. Air & Space Forces Magazine. https://www.airandspaceforces.com/usaf-fighters-shoot-down-iranian-drones-in-defense-of-israel/

16. A&E Television Networks. (2023, July 13). Battle of the Somme: Casualties & who won. History.com. https://www.history.com/topics/world-war-i/battle-of-the-somme

17. Encyclopædia Britannica, Inc. (n.d.). Entente Cordiale. Encyclopædia Britannica. https://www.britannica.com/event/Entente-Cordiale

18. Gordon, C. (2024, April 18). Outgoing AFCENT boss on the future of the Middle East. Air & Space Forces Magazine. https://www.airandspaceforces.com/outgoing-afcent-boss-on-the-future-of-the-middle-east-grynkewich/

19. Amazon. (2019). Boost glide hypersonic. https://nextbigfuture.s3.amazonaws.com/uploads/2019/03/boostglidehypersonic.jpeg

20. The Hill. (2019). Ballistic missile. The Hill. https://thehill.com/wp-content/uploads/sites/2/2019/04/ballistic_missile_10142002.jpg?w=1280

21. Bing. (n.d.). Unmanned aerial system. https://th.bing.com/th/id/OIP.M2HBrtZFQzS9OcHsTtiYqAHaFj?w=256&h=191&c=7&r=0&o=5&dpr=2.5&pid=1.7

22. Adobe. (n.d.). Radar. Adobe Stock. https://as1.ftcdn.net/v2/jpg/05/06/14/14/1000_F_506141497_07pCzCM0P0w2cgd9LiXEyIFtZmOubY35.jpg

23. Crew Daily. (2019). F-35. Crew Daily. https://crewdaily.com/wp-content/uploads/2019/05/F-22-vs-F-35-758x426.jpg

24. imgix, Inc. (2020). Satellite. IMGIX. https://img.militaryaerospace.com/files/base/ebm/mae/image/2020/10/satellites_13_Oct_2020.5f84b31093440.png?auto=format&w=1000&h=562&fit=clip&dpr=2

25. glitch.news. (2017). Cruise missile. Glitch. https://glitch.news/wp-content/uploads/sites/19/2017/06/Missiles.jpg

26. The MITRE Corporation. (2023, June 27). Carpe Dronvm: Enabling everyone to be a counter unmanned aerial system sensor. MITRE. https://www.mitre.org/our-impact/intellectual-property/carpe-dronvm-enabling-everyone-be-counter-unmanned-aerial-system

27. USNI News. (2022, March 18.) Intel sharing between U.S. and Ukraine 'revolutionary' says DIA director. USNI News, pg. 1.

28. Garamone, J. (2023, August 18). Europe/Africa Air Force chief cites lessons from war in Ukraine. U.S. Department of Defense, DoD News. https://www.defense.gov/News/News-Stories/Article/Article/3498038/europeafrica-air-force-chief-cites-lessons-from-war-in-ukraine/

29. Mitchell, P. (2022, December 29). Patriot missiles, NATO, and Ukraine: Tactical weapons with strategic impacts. Modern War Institute. https://mwi.westpoint.edu/patriot-missiles-nato-and-ukraine-tactical-weapons-with-strategic-impacts/

30. Garamone, J. (2023, August 18). Europe/Africa Air Force chief cites lessons from war in Ukraine. U.S. Department of Defense, DoD News. https://www.defense.gov/News/News-Stories/Article/Article/3498038/europeafrica-air-force-chief-cites-lessons-from-war-in-ukraine/

31. Ibid.

32. Faulkner, D. (2024, January 19). DragonFire Laser: Mod tests weapon as low-cost alternative to missiles. BBC News. https://www.bbc.com/news/uk-68031257

33. Skovlund, J. (2023, October 31). Israel's Iron Beam: Everything you need to know. Task & Purpose. https://taskandpurpose.com/military-life/israel-iron-beam-air-defense/

34. Gruen, J. (2023, October 12). A better C-UAS option? Capture enemy drones in a net. Breaking Defense. https://breakingdefense.com/2023/10/a-better-c-uas-option-capture-enemy-drones-in-a-net/

35. RTX. (2023, September 27). Airborne electronic attack: Owning the invisible battlespace. Raytheon. https://www.rtx.com/raytheon/news/2023/09/27/airborne-electronic-attack-owning-the-invisible-battlespace#:~:text=It%20includes%3A%201%20Disabling%2C%20degrading%20and%20denying%20enemy,threats%20through%20jamming%20their%20radar%20and%20communications%20systems

36. Kamps, H.J. (2022, April 20). This kamikaze drone sacrifices its own rotors to take down other drones. https://techcrunch.com/2022/04/20/interceptor-drone/

37. Macey, J. (2024, January 25). Drone interceptor weapon system unveiled. Defense Advancement. https://www.defenseadvancement.com/news/drone-interceptor-weapon-system-unveiled/

38. Pomerleau, M. (2024, March 21). Indo-Pacific Command to test prototype of Joint Fires Network this year. DefenseScoop. https://defensescoop.com/2024/03/21/joint-fires-network-indo-pacific-command-test-prototype/

39. Giachinta, R., & Friedman, J. (2024, April 5). IAMD Interview. Personal.

40. Written Statement of Mr. John D. Hill Deputy Assistant Secretary of Defense for Space and Missile Defense Policy House Armed Services Committee Strategic Forces Subcommittee, "Fiscal Year (FY) 2025 Budget Request for Missile Defense and Missile Defeat Programs." (2024, April 12). https://armedservices.house.gov/hearings/str-hearing-fy25-budget-request-missile-defense-and-missile-defeat-programs

41. Savage, L. (2022, January 28). US INDOPACOM's integrated air and missile defense vision 2028: Integrated Deterrence toward a free and open Indo-Pacific. Air University. https://www.airuniversity.af.edu/JIPA/Display/Article/2915508/us-indopacoms-integrated-air-and-missile-defense-vision-2028-integrated-deterre/

42. Savage, L. (2022, January 28). US INDOPACOM's integrated air and missile defense vision 2028: Integrated Deterrence toward a free and open Indo-Pacific. Air University. https://www.airuniversity.af.edu/JIPA/Display/Article/2915508/us-indopacoms-integrated-air-and-missile-defense-vision-2028-integrated-deterre/

43. Gunzinger, M. A. (2021, November 29). Affordable mass: The need for a cost-effective PGM mix for Great Power Conflict. Mitchell Institute for Aerospace Studies. https://mitchellaerospacepower.org/affordable-mass-the-need-for-a-cost-effective-pgm-mix-for-great-power-conflict/

44. West, T. D., & Birkmire, B. (2020, January 9). AFSIM: The Air Force Research Laboratory's approach to making M&S ubiquitous in the weapon system concept development process. CSIAC. https://csiac.org/articles/afsim-the-air-force-research-laboratorys-approach-to-making-ms-ubiquitous-in-the-weapon-system-concept-development-process/

Authors

Andrea McFeely

Rachel Giachinta

Tyler Milner

Eliahu Niewood

Robert Coons

Meg Adams

Moira McCarthy

Dainis Butners

Contributors

Chris Franklin

Jerry Friedman

Jason Styslinger

Kyle Noth

Larry Herlacher

Jim Heigle

Rob Gleich

Dale Ormand

About the Coalition Security Series

This paper is part of a coalition security series published by MITRE's National Security Sector to examine options that can help the U.S. more effectively work with allies and partners in competition, deterrence, and conflict.

Portions of this technical data were produced for the U. S. Government under Contract No. FA8702-19-C-0001 and W56KGU-18-D-0004, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (FEB 2014)

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®