OWL Cyber Defense

WHITE PAPER

Overcoming the Challenges of Coalition Data Sharing

Executive Summary

> *"It is not enough to be joint, when conducting future operations. We must find the most effective methods for integrating and improving interoperability with allied and coalition partners. Although our Armed Forces will maintain decisive unilateral strength, we expect to work in concert with allied and coalition forces in nearly all of our future operations, and increasingly, our procedures, programs, and planning must recognize this reality."*
>
> –Chairman of the U.S. Joint Chiefs of Staff, Joint Vision 2010 (1996)

At its highest level, the alignment of strategic objectives, worldviews, and doctrines and the willingness of partner nations to work cooperatively to adopt and achieve them can make a coalition whole greater than the sum of its parts. Indeed, such that alliances and politically motivated military support exist in nearly every modern battlespace, there are few situations in which the combat theatre would not include other partner nations with political or other interests at stake. As such, while the United States and other coalition partners necessarily retain the capability to act unilaterally for their own interests, building, maintaining, and improving allied and coalition partnerships is now vital for effective mission operations in contested environments.

The purpose and focus of cooperation and interoperability within the coalition battlespace is to satisfy the strategic objectives within the given constraints and with the maximum possible efficiency and economy of force.[1]

The achieve this purpose, and to maintain an asymmetric advantage in the modern contested environment, partner nations and their network systems within the coalition battlespace must be able to communicate vital information in a secure and timely manner. From the top down, from logistics and C4/I communications to identification friend or foe (IFF) positions and sensor data, the more complete the common operating picture provided by data from every available element within the coalition battlespace, the more effective and efficient coalition operations and command become.

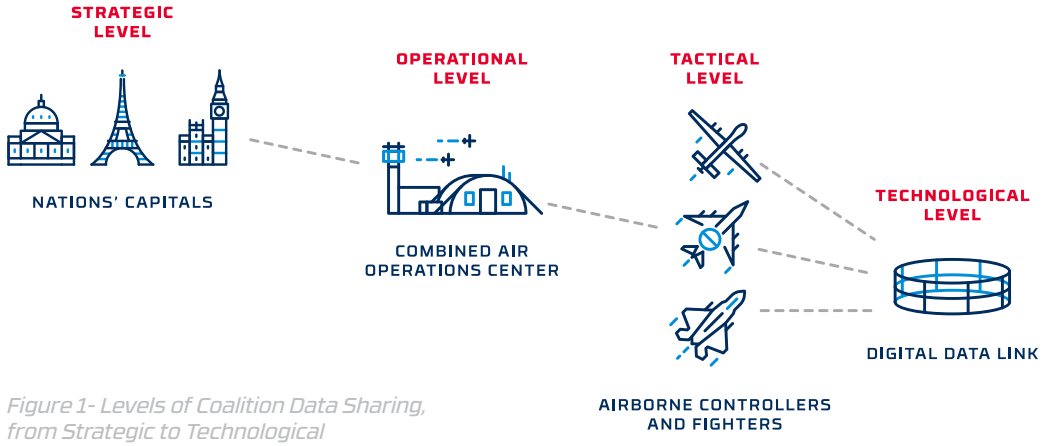


Figure 1- Levels of Coalition Data Sharing, from Strategic to Technological

[1] https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1235/MR1235.chap2.pdf

As such, the secure real-time transfer, collection, and integration of coalition partner data is the paramount challenge to such a common operating picture. However, as evidenced by the statement above from the Joint Chiefs of Staff in 1996, overcoming this challenge is critical, longstanding, and has only increased in complexity since then.

Internally, the U.S. now leads all coalition partners in digital capabilities. Massive amounts of data are transferred throughout the coalition battlespace, ballooning from mere megabytes in the 1990's to hundreds of gigabytes per day in the 2020's. However, there are massive technological disparities among the other nations. This disparity alone creates massive gaps in information capture, exchange, and actionable intelligence. In addition, the U.S. and other digitally advanced coalition partner nations have struggled to build and maintain the multitude of integrations and common platforms necessary to achieve a common operating picture.

Even beyond the inequalities in technological capabilities and the multitude of integrations required, there are fundamental issues of trust and national security which must be addressed. No matter how close an alliance, there will always be a necessary distance from full disclosure for national security, technological or informational superiority, and other political and defense interests. Therefore, in the sharing of information between even friendly nations, there must also be certain limitations and restrictions on the details shared. International Traffic in Arms Regulations (ITAR) restrictions in the United States are a classic case in the limitation of technological cooperation and availability. However, this limitation must be enforced not just as a policy but also as a matter of technological implementation.

As the most efficient data architecture includes both a centralized data reservoir for synthesis and dissemination and a distributed system of delivery mechanisms, secure coalition data sharing also requires a complex, intelligent network infrastructure. This infrastructure must include a data-centric network architecture that implements a sophisticated security policy in combination with a variety of technologies to implement multidimensional data classification, and limit both the transferred and access to data based on its classification and what a user is authorized to see. These security technologies typically take the form of cross domain solutions – complex, layered network security devices with advanced content filtering – augmented with other security software such as artificial intelligence/machine learning to achieve a highly secure, dynamic, and efficient data sharing solution.

The United States Department of Defense has developed a number of smaller iterations that could be used as models to create a common coalition data sharing platform. For example, the U.S. Army has developed a number of data sharing environments, such as Combined Enterprise Regional Information Exchange (CENTRIX) Network Extension Packages, or CX NEPs, which are tactical enclaves which enable the exchange of data between U.S. Joint and coalition force networks to support a Mission Partner Environment during military and stability operations, counter-insurgency missions, or disaster/humanitarian contingencies.

However, there are, in practice, several challenges to implementing such a solution at scale for a more cohesive coalition operating environment, especially outside of the Five Eyes nations. Each nation and each level of command has its own requirements and policies, and as such, a variety of solutions that meet a different set of these requirements are needed to adequately assure both that the data flow is not disrupted and that unauthorized data is never leaked or transferred.

[2] https://www.army.mil/article/218179/army_uses_rapid_acquisition_to_deliver_coalition_network_enclaves

From tactical field environments and vehicles to command posts to shared data centers, from sensor data to file transfers, there is no one-size-fits-all solution to meet each situational need. In addition, because the U.S. government forbids the use of accredited solutions currently in use in U.S. defense or intelligence implementations, non-ITAR-constrained solutions must be made available for non-Five Eyes coalition partners to employ a similar secure data-centric network architecture for secure operational data sharing.

Overcoming these challenges is paramount to the U.S. coalition mission, and therefore in the interest of all coalition partners, including the U.S. This document is intended as both an elucidation of the political, technical, and operational challenges to secure coalition data sharing, as well as an investigation into the available solutions and existing models upon which to build a secure shared data environment.

The opinions expressed herein are those of Owl Cyber Defense in no way intended as an endorsement by or statement on behalf of the U.S. government or Department of Defense.

Introduction

Effective military operations are defined by the satisfaction of strategic objectives with the greatest possible economy of force – i.e., achieving the mission without wasted effort or unnecessary risk. Coalition building between partner nations is a vital strategy for the United States to not only achieve maximum efficacy but maintain operational superiority in the face of peer or near-peer adversaries and adversarial coalitions.

To that end, the effective execution of military operations is fundamentally dependent on information and communication. Information superiority is the ability to gain situational awareness, exchange relevant information, and make decisions faster than the enemy. By extension, as most, if not all U.S. future military and defense operations will be conducted with allied and coalition partners, the expectation of communication and information sharing must naturally expand beyond detachments or branches of the U.S. military to those of partner defense organizations and nations as well.

Seamless coalition data sharing and interoperability holds the promise to move beyond "joint" operations to an effectively combined all-domain military organizational command and control infrastructure and combat force. Achieving effective communication across coalition partners must therefore be a principal goal not just at the strategic level, but every level down to the individual data links between vehicles, installations, equipment, and personnel.

Coalition partner nations may share some common objectives and interests, they remain disparate in terms of their capabilities and maturity. This disparity in capability not only inhibits effective combined operations, but inevitably leads to a degradation of trust. The United States is a dominant figure in technological advancements and implementation, but how might the coalition – and therefore the United States – stand to benefit if the U.S. and all its coalition partners were able to share information seamlessly without compromising security?

While not a simple undertaking by any means, the branches of the U.S. military forces have already made advances to improve communications and data sharing between each other to create a unified fighting force. How might these advances be used as a model to build and improve a truly combined coalition data sharing architecture? What might such a combined solution look like? How might it be achieved in the face of a host of political, logistical, and technological challenges? What current solutions are available to ensure effective data sharing between coalition partners without compromising national interests and security?

Through a thorough investigation of the purpose, requirements, and impediments of coalition data sharing, this paper aims to elucidate the potential policies, technologies, and best practices to overcome the challenges of achieving a seamless coalition data environment.

Purpose

The importance of creating a common operating picture within the coalition battlespace cannot be overstated. However, before discussing the challenges involved in the creation of such an environment, we must first discuss the purpose of data sharing in order to define the requirements of possible solutions.

Data

Data is a strategic asset – defense data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage. Orders, reports, images, video, logistics, sensors, terrain, fires, friendly and enemy positions – every bit is a piece of the operating picture puzzle. The key to creating a truly combined all-domain command and control rests in collecting and disseminating that data across a diverse and varied command structure among multiple coalition partners. The faster, more reliably, and secure this data sharing can be accomplished, the more cohesive and transparent the common operating picture becomes. Increased compatibility and shared usage, including common protocols, platforms, and data types, can also help to overcome language barriers among partner nations.

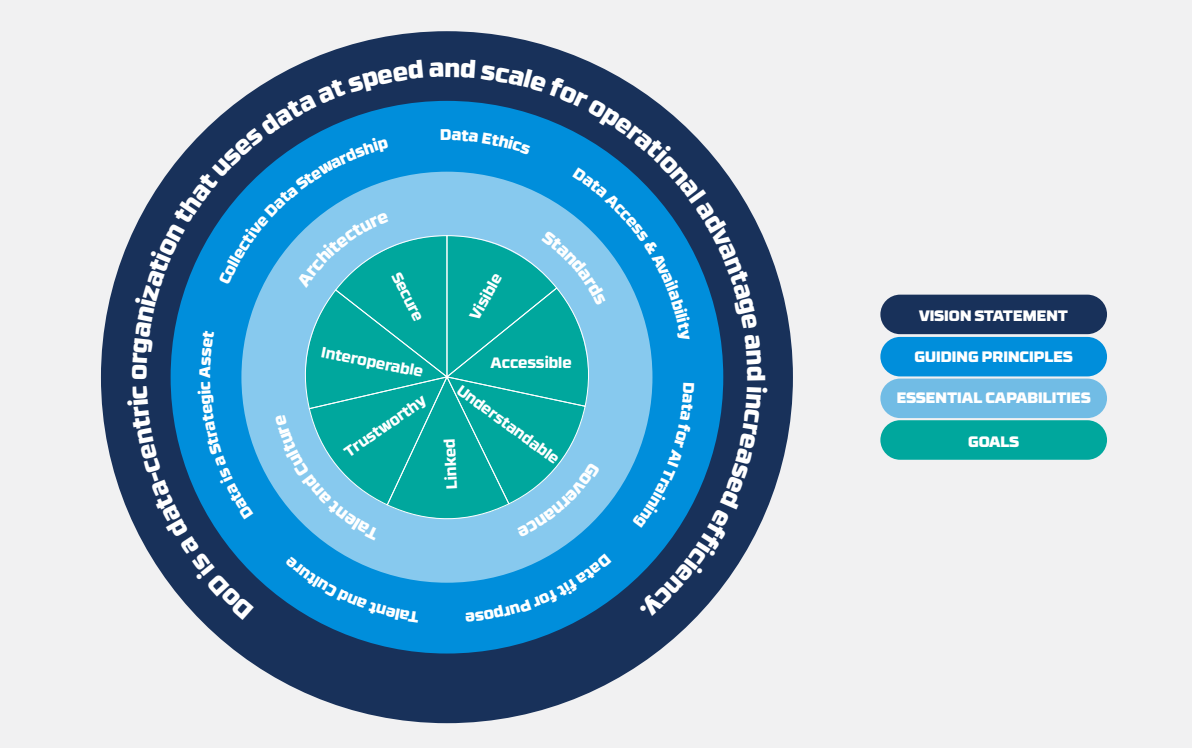


Figure 1 U.S. DoD Data Strategy[3]

[3] https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

Technological Parity

One of the primary impediments to coalition data sharing, and therefore also one of the greatest opportunities for increased interoperability, is the technological disparity between the United States and its coalition partners. Bridging this gap is a primary goal in the interest of coalition data sharing, in order to fill gaps in information exchange and achieve a greater unity of effort among partner nations. This can take the form of both common defense technologies and compatible secure communications technologies such as cross domain solutions (CDSs) to connect the technologies and forces across the coalition battlespace in real-time.

Common Operating Picture

The clear end goal of coalition data sharing, a common operating picture for joint, all-domain command and control must enable all partner nations to both communicate as well as receive and integrate vital information in real-time to increase combat effectiveness. From more accurate weapons targeting to improved surveillance confidence, as well as reduced redundancies, cross-coalition conflict, and blue on blue incidents – a unified command architecture is the key to the efficient utilization of resources and effectiveness of operations. The United States is well positioned to take the lead and set the standard for the technologies and strategies necessary to collect, share, and parse data in single common coalition environment within the C4I architecture.

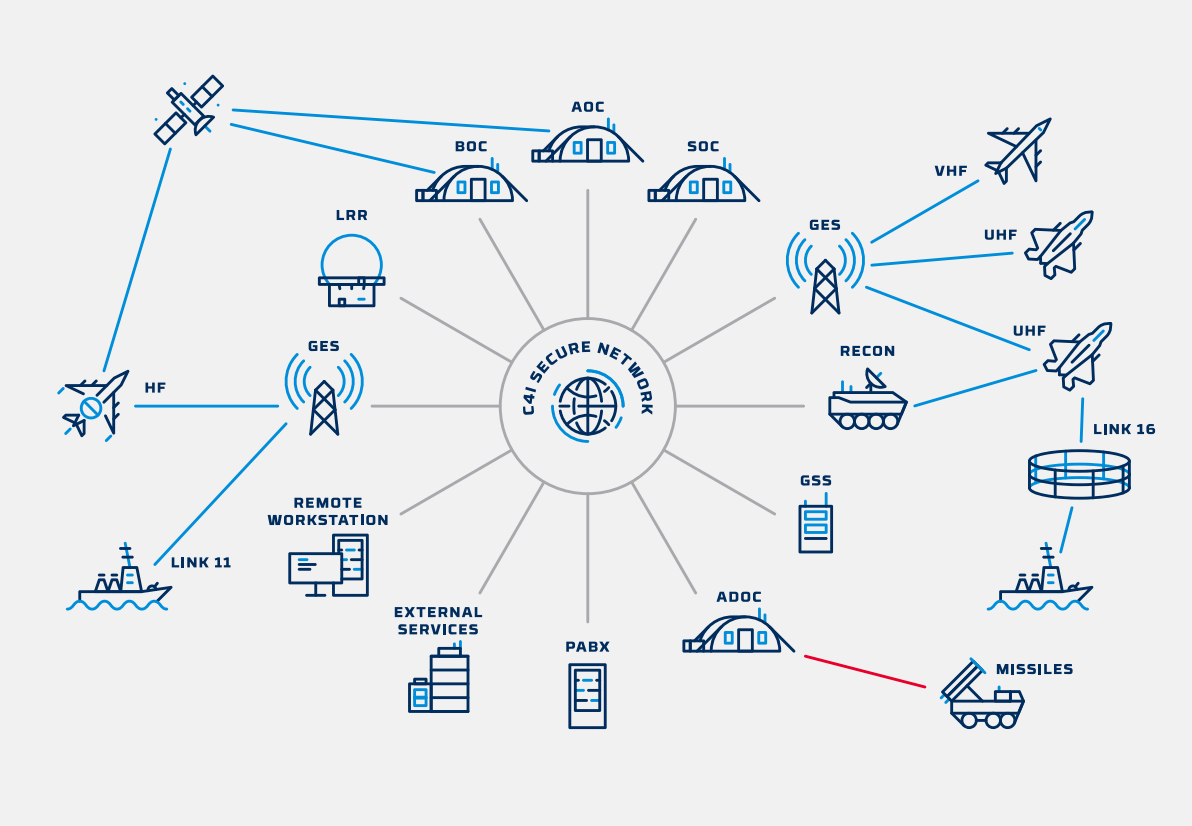


Figure 2 - Command, Control, Communications, Computer, and Intelligence (C4I) Architecture

Challenges

The sheer complexity of the coalition operating environment lends itself to myriad logistical, security, and technological challenges. Collecting, processing, storing, and disseminating massive amounts of data across the countless connected systems, vehicles, devices, assets, and personnel within the U.S. armed services is fraught enough before considering integrating a shared architecture across a number of partner nations. However, if these challenges are to be overcome, the requirements to do so must be clearly defined and understood.

Information Glut

The problem of being overwhelmed by data in the U.S. military is not an external challenge. Instead, the U.S. military is inflicting information overload on itself[4]. The U.S. military, and by extension, its joint coalition force, is generating more data than it is able process. The coalescence of human intelligence (HUMINT), geospatial intelligence (GEOINT), signals intelligence (SIGINT), and open source intelligence (OSINT) in information generation and collection has created a mountain of information far too massive and steep for any human to climb. There is simply too much information to sort, sift, and properly process for actionable decision-making.

+1,600%

Increase in data generated by defense surveillance technology over 10 years

14M

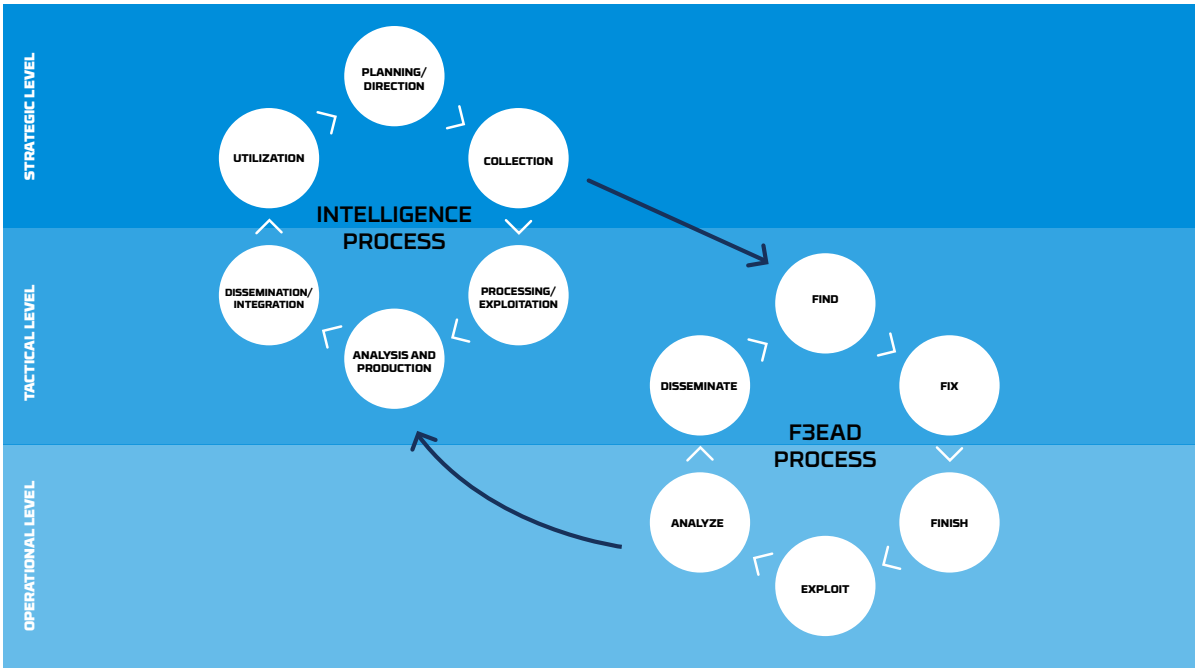
Approximate number of connected devices in the U.S. Armed Services

In addition, there are not only numerous data types, protocols, and media involved in the modern battlespace, but multiple languages, security methods, and geographically and logistically disparate sources. This complexity only compounds the information glut challenge and further constricts the ability of individuals from any particular partner nation to utilize data for timely action. Any potential coalition data sharing solution must include strategies and technologies to reduce information waste and enable increased automation in information processing.

[4] https://warontherocks.com/2020/02/the-input-output-problem-managing-the-militarys-big-data-in-the-age-of-ai/

Time to Action

The coalition data sharing problem is a problem of time. The speed with which information can be generated, transmitted, collected, filtered, aggregated, synthesized, analyzed, processed, and turned around for orders or other dissemination is primarily determined by the amount of data generated, but also by the limitations of humans themselves.



[5]

Figure 3 - Cyber Intelligence Process Integration

This speed (or lack thereof) can mean the difference between actionable intelligence and missing a window of opportunity. It is imperative that any shared coalition architecture implement solutions that streamline this information lifecycle and reduce the time to action as much as possible.

Unified Command

The cost of operating jointly manifests itself in the time and effort wasted dealing with structural inefficiencies in the flow of information. Despite its benefits (e.g., unity of effort, flexibility), unified command is a costly and often inefficient enterprise. Especially in combination with the type of tiered formal hierarchy present in the U.S. defense organization, unified command can slow data flows by forcing information to be redundantly processed at each tier of leadership. In order to leverage joint resources, requests must be sent and processed up the chain of command until the request arrives at the resource-controlling commander. Increasing the breadth across coalition partners operating separately – rather than as a unified force – only acts as a cost multiplier. Potential coalition data sharing solutions must at least acknowledge if not address these costly inefficiencies.

[5] https://www.first.org/global/sigs/cti/curriculum/methods-methodology

Interoperability

The diverse data and technologies within the coalition environment are somewhat inevitable. However, in order to be effective, coalition data sharing systems must be able to "talk" to each other by the most efficient means possible. At the strategic level, interoperability is an enabler for coalition building. It facilitates meaningful contributions by coalition partners and supports whatever allied "buy-in" may be necessary for the U.S. to use its forces effectively in regions of interest.[6]

However, interoperability at the national level can be difficult to achieve and may come at a cost. Political costs and military risks might result from specific interoperability initiatives, which may lead to decisions not to sell or transfer the most advanced systems and technologies to allies. As such, the U.S. has already barred the use of many of its own defense and security technologies from being shared outside of its closest partner nations.

While the diversity of systems and data can be detrimental to performance, potential coalition data sharing solutions must harness the ability of data to overcome language barriers and utilize common platforms and technologies to increase interoperability.

Equal Security Measures

As data will be shared across coalition partners, there is a critical need for equal information and network security measures. Without them, there is a risk of a "weak link" attack in the architecture, wherein an adversary can exploit a target with inferior security and gain access to information that would otherwise be more powerfully protected.

As with interoperability, as a matter of national security, there is also a need to control both the security technologies and the data which is shared with other nations – even friendly, partner nations. State secrets, proprietary technologies, and other sensitive information must be restricted from data transfers between coalition partners. There are also risks of proliferation of shared technologies and systems to third parties – the U.S. may find that they have been exploited by other/hostile states to produce effective countermeasures.

However, unless all partners in the coalition have equal protections for their sensitive information, including content filtering and confidentiality technologies and policies, they will be reticent to share any data at all. Any potential coalition data sharing solution will require high-speed cross domain content filtration capabilities as well as well-established and consistently enforced security policies.

[6] https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1235/MR1235.chap2.pdf

Domain Separation

In addition to the security measures which prevent unauthorized data sharing/leakage, there also remains a need to logically and/or physically separate domains. This segmentation enables a modular network architecture and ensures that data sharing will not enable lateral threat jumping, should a breach occur. This is typically enforced by a software guard or hardware-enforced domain separation with a one-way transfer (OWT) solution or data diode.

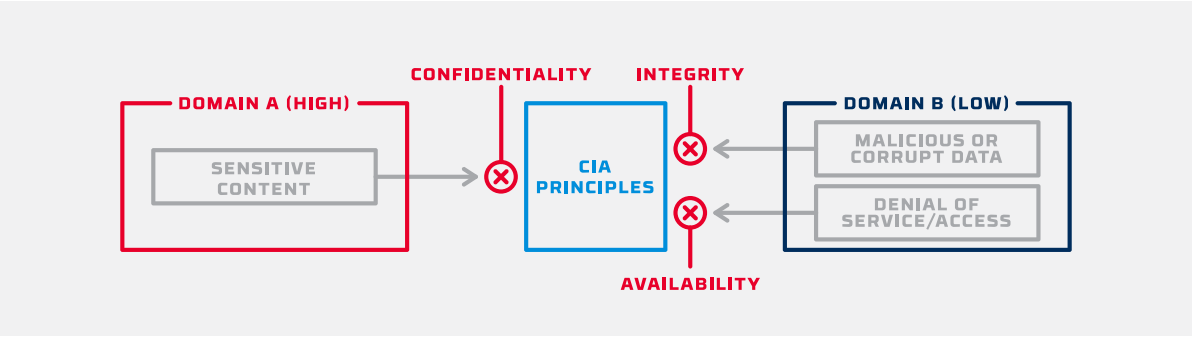


Figure 4 – Domain Separation Principles

Any U.S. information domains established by this separation must follow DoD policy and any partner nation restrictions, including any necessary risk assessments and determinations of authorized access. Potential coalition data sharing solutions will require implementation of domain separation at multiple points in the network architecture to segment and layer defenses.

Solutions

Designing a coalition network architecture which meets the demands of all of the aforementioned challenges is a daunting task. There is no one-size-fits-all solution – some situations will by their nature be simpler or more complex than others – but there are common elements that can provide answers to the challenges presented. The goal of creating a secure, real-time data sharing architecture will require a combination of innovative technologies and strategies from both the defense and private sector and established templates for data sharing within the U.S. DoD and intelligence community. While the actual solutions will require much more sophisticated analysis and design, the following offers an outline of some of the technologies and strategies that may be of the most use in any implementation.

Artificial Intelligence

Due to the glut of information and countless sources creating it, the coalition fighting force can become bogged down in weeding through this information and sending it up or down the command chain. There are only two options: either make decisions faster or buy more time. As time is a finite resource, artificial intelligence (AI) is a possible solution to accelerate decision making and reduce the reliance on human intervention for data processing at every level of command.

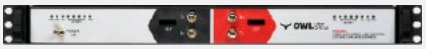
In order to be effective, AI typically requires a large amount of data to draw from and make decisions. In fact, the lack of sufficient available data often poses a significant barrier to entry for AI applications. However, by virtue of its reliance on large amounts of data and iterative design, the military operations process is rife with ideal data pools available for AI. AI integrates well with existing structured systems of planning and assessment, and it takes advantage of vast data streams that currently sit untapped. AI also lends itself to those tasks that occupy the most time, freeing people to think critically and creatively about how to win wars.

Functionally Equivalent Systems

To overcome the limitations of incompatible technologies and reduce the political and military risks of shared technology, functionally equivalent but developmentally distinct software and hardware systems should be created. These systems must be designed, procured, tested, upgraded, operated, and sustained specifically with data interoperability as a key requirement. This consistency enables reliable collecting, filtering, storing, manipulating, and transferring the variety of formats, protocols, and data types that are present in these environments, including a wide array of both proprietary defense protocols as well as commercial formats.

Cross Domain Solutions

Due to the domain separation and information security demands of coalition partner networks, there is a pressing need for a "universal" cross domain solution (CDS) for use among coalition partners outside the Five Eyes (FVEY). A form of controlled interface (a boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems) that provides the ability to manually and/or automatically access and/or transfer information between different security domains. CDSs are information domain separation devices capable of controlling and filtering data transfers between domains. While some partner nations may have developed home grown solutions, the U.S. remains the technological forerunner among them, and has already accredited solutions for immediate use within all partner nation networks – even those outside of the Five Eyes.



XD GUARDIAN

Functionally equivalent to the solutions used within U.S. defense and intelligence applications, **XD Guardian**[7] from Owl Cyber Defense can provide real-time cross domain transfer capabilities to partner nations without the need to develop or accredit their own solutions.

Tactical Data Links

There has long been a need for interoperable tactical digital information link (TADIL) communications for coalition aircraft. To this day, many of the U.S. and its allies' fighters still communicate using unsecure, voice-only analog radios. This severely limits the coalition partners' ability to reliably share a wide range of combat data. Communications systems that include TADIL capabilities offer a solution for exchanging digital information over a common network that is continuously and automatically updated.

The most recently developed is the JTIDS/TADIL J system, commonly referred to as "Link 16" in the United States. Link 16 is an encrypted, jam-resistant, nodeless tactical digital data link network established by JTIDS-compatible communication terminals that transmit and receive data messages in the TADIL J message catalog. Other systems in use today include USMTF (United States Message Text Format)/VMF (Variable message formats), created by the U.S. and coordinated with NATO for coalition interoperability, and ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange), a state-of-the-art surveillance data format developed in Europe and designed for use in air traffic communications.

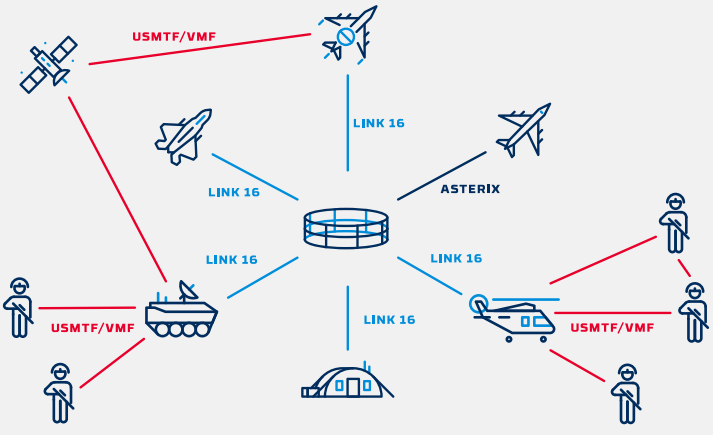


Figure 5 – Tactical Data Links in the Modern Battlespace

[7] https://owlcyberdefense.com/product/xd-guardian/
[8] https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1235/MR1235.chap9.pdf

These systems can provide a basis for coalition partners to communicate sophisticated combat data and situational intelligence far beyond the simple and severely limited FM radio communication.

Example Data Sharing Platforms/Implementations

The U.S. has already implemented a number of data sharing platforms and technologies for use among the branches of its DoD and intelligence community that can be used as examples or templates for further use in a comprehensive coalition data sharing context. These include:

- **Mission Partner Environment (MPE)**: MPE is a coalition network architecture that provides services such as chat, email with attachments, web, file-share, command and control (C2), weather, logistics, and planning to 45,000 users. It is designed to enable U.S. joint forces to plan, prepare, and execute C4ISR at the same releasability and classification level as mission partners. MPE provides the means to clearly communicate commander's intent for desired operational effects to all mission partners.[9]

- **U.S. Army Commercial Coalition Equipment (CCE)**: CCE provides expeditionary coalition or commercial network connectivity to enable mission command, network communications (voice, video, and data) and situational awareness between Army, Joint and coalition forces, in support of both military and civil operations. Each of the coalition countries has their own unique transport networks that enable them to connect into the combined coalition network. The U.S. Army uses CCE to connect to the coalition network over its tactical communications network.[10]

- **Combined Enterprise Regional Information Exchange (CENTRIX) Network Extension Packages – CX NEPs**: Fielded in response to an operational needs statement from theater, CX NEPs are expeditionary commercial-off-the-shelf coalition network enclaves designed to enable the exchange of data between U.S. Joint and coalition force networks to support a Mission Partner Environment during military and stability operations, counter-insurgency missions, or disaster/humanitarian contingencies. They allow U.S. and coalition nations and their forces to securely share operational/intelligence information in Communities of Interest (COI) Network.[11]

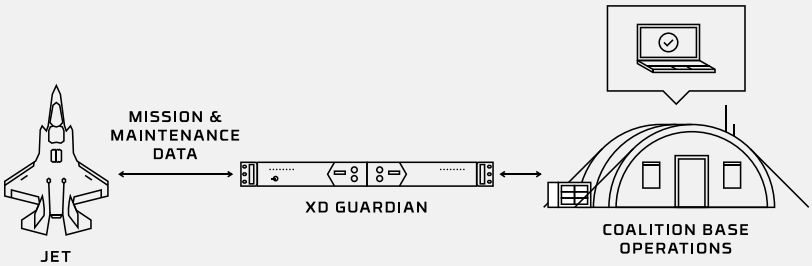
[9] https://dodcio.defense.gov/In-the-News/MPE/
[10] https://peoc3t.army.mil/tn/cce.php
[11] https://www.army.mil/article/218179/army_uses_rapid_acquisition_to_deliver_coalition_network_enclaves

Use Cases

There are many instances in which coalition data sharing technologies have already been implemented to increase interoperability and completeness of vision in a C4I joint, all-domain command and control. These implementations can serve as a basis for expanding a data sharing architecture across the coalition battlespace.

Secure Data Transfer for Coalition Aircraft

Allied forces utilizing U.S.-manufactured aircraft required secure data transfers for mission and maintenance data to and from the aircraft. The information exchange requirements for content inspection and filtering needed to meet the same standards as the U.S. configuration, necessitating the use of an accredited cross domain solution (CDS). However, export restrictions on accredited CDSs meant that no solution to meet these requirements was available for coalition partners outside of the Five Eyes (Australia, Canada, New Zealand, U.K., U.S.). In addition, because the aircraft utilized proprietary software, any new solution would also have to be configured and integrated with the software.

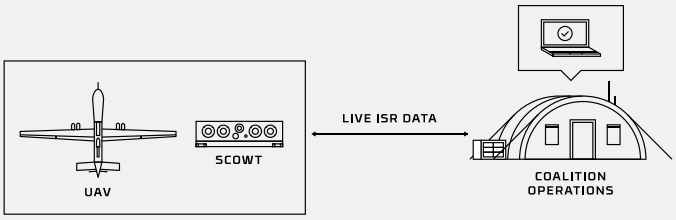


REQUIREMENTS

- Exportable CDS certified to handle classified data
- No shared code base with existing U.S. accredited CDSs
- Bidirectional transfer of multiple data types
- Customizable content filtering, policy, and configuration

Secure Live ISR Data Sharing

Due to challenges with integrating coalition partners within the Link16 defense communication network, intelligence, surveillance, and reconnaissance (ISR) data sharing was limited to a “walk-net” of physical hand-offs. To increase operational effectiveness without sacrificing security, U.S. forces required an alternative method for securely sharing live ISR data between allies, including those outside of the Five Eyes (Australia, Canada, New Zealand, U.K., U.S.).



REQUIREMENTS

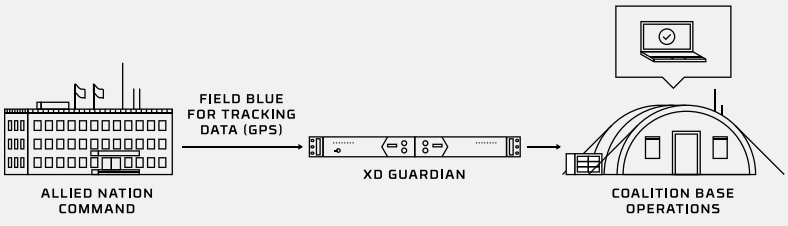
- Exportable CDS certified to handle classified data
- No shared code base with existing U.S. accredited CDSs
- High-speed filtering and direct transfer of live ISR data for targeting
- Tactical form factor for UAV deployment

Real-Time Blue Force Tracking

Due to challenges with securely integrating GPS data from non-Five Eyes coalition partners within the US Link16 defense communication network, there remains a gap in real-time identification of allied forces (Blue Forces) in the field. In order to share identification data with the coalition network, the coalition partners required a cross domain solution (CDS) both capable of meeting the standards of the US Intelligence Community (IC) and exportable outside of the Five Eyes nations (Australia, Canada, New Zealand, U.K., and U.S.).

REQUIREMENTS

- Exportable U.S. Government accredited CDS
- No shared code base with existing U.S. accredited CDSs
- Able to transfer live GPS data for blue force tracking
- High-speed content filtering of streaming data



Conclusion

While the challenges presented by the modern coalition data environment are varied and complex, today there are numerous technologies and strategies in place that can help to not just overcome them, but create a new, comprehensive, and secure data sharing architecture. Mitigating the various risks and information gaps will require a sophisticated implementation of a number of cutting-edge innovations and improving the digital capabilities of partner nations, but it is a vital task that must be undertaken to maintain the asymmetric advantage of the U.S. and its allies against near peer adversaries. From secure video conferencing to AI-enabled data analysis, new tools can enable commanders to collaborate, plan, and assess operations at a global scale and dominate the information battlefield.